CHAPTER

# 1 The Foundations: Logic and Proofs



The rules of logic specify the meaning of mathematical statements. For instance, these rules help us understand and reason with statements such as "There exists an integer that is not the sum of two squares" and "For every positive integer $n$, the sum of the positive integers not exceeding $n$ is $n(n + 1)/2$." Logic is the basis of all mathematical reasoning, and of all automated reasoning. It has practical applications to the design of computing machines, to the specification of systems, to artificial intelligence, to computer programming, to programming languages, and to other areas of computer science, as well as to many other fields of study.

To understand mathematics, we must understand what makes up a correct mathematical argument, that is, a proof. Once we prove a mathematical statement is true, we call it a theorem. A collection of theorems on a topic organize what we know about this topic. To learn a mathematical topic, a person needs to actively construct mathematical arguments on this topic, and not just read exposition. Moreover, knowing the proof of a theorem often makes it possible to modify the result to fit new situations.

Everyone knows that proofs are important throughout mathematics, but many people find it surprising how important proofs are in computer science. In fact, proofs are used to verify that computer programs produce the correct output for all possible input values, to show that algorithms always produce the correct result, to establish the security of a system, and to create artificial intelligence. Furthermore, automated reasoning systems have been created to allow computers to construct their own proofs.

In this chapter, we will explain what makes up a correct mathematical argument and introduce tools to construct these arguments. We will develop an arsenal of different proof methods that will enable us to prove many different types of results. After introducing many different methods of proof, we will introduce several strategies for constructing proofs. We will introduce the notion of a conjecture and explain the process of developing mathematics by studying conjectures.

## 1.1 Propositional Logic

### Introduction

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments. Because a major goal of this book is to teach the reader how to understand and how to construct correct mathematical arguments, we begin our study of discrete mathematics with an introduction to logic.

Besides the importance of logic in understanding mathematical reasoning, logic has numerous applications to computer science. These rules are used in the design of computer circuits, the construction of computer programs, the verification of the correctness of programs, and in many other ways. Furthermore, software systems have been developed for constructing some, but not all, types of proofs automatically. We will discuss these applications of logic in this and later chapters.

## Propositions

Our discussion begins with an introduction to the basic building blocks of logic—propositions. A **proposition** is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both.

**EXAMPLE 1** All the following declarative sentences are propositions.

Extra Examples

1. Washington, D.C., is the capital of the United States of America.
2. Toronto is the capital of Canada.
3. $1 + 1 = 2$.
4. $2 + 2 = 3$.

Propositions 1 and 3 are true, whereas 2 and 4 are false. ◀

Some sentences that are not propositions are given in Example 2.

**EXAMPLE 2** Consider the following sentences.

1. What time is it?
2. Read this carefully.
3. $x + 1 = 2$.
4. $x + y = z$.

Sentences 1 and 2 are not propositions because they are not declarative sentences. Sentences 3 and 4 are not propositions because they are neither true nor false. Note that each of sentences 3 and 4 can be turned into a proposition if we assign values to the variables. We will also discuss other ways to turn sentences such as these into propositions in Section 1.4. ◀

We use letters to denote **propositional variables** (or **statement variables**), that is, variables that represent propositions, just as letters are used to denote numerical variables. The

Links

ARISTOTLE (384 B.C.E.–322 B.C.E.) Aristotle was born in Stagirus (Stagira) in northern Greece. His father was the personal physician of the King of Macedonia. Because his father died when Aristotle was young, Aristotle could not follow the custom of following his father's profession. Aristotle became an orphan at a young age when his mother also died. His guardian who raised him taught him poetry, rhetoric, and Greek. At the age of 17, his guardian sent him to Athens to further his education. Aristotle joined Plato's Academy, where for 20 years he attended Plato's lectures, later presenting his own lectures on rhetoric. When Plato died in 347 B.C.E., Aristotle was not chosen to succeed him because his views differed too much from those of Plato. Instead, Aristotle joined the court of King Hermeas where he remained for three years, and married the niece of the King. When the Persians defeated Hermeas, Aristotle moved to Mytilene and, at the invitation of King Philip of Macedonia, he tutored Alexander, Philip's son, who later became Alexander the Great. Aristotle tutored Alexander for five years and after the death of King Philip, he returned to Athens and set up his own school, called the Lyceum.

Aristotle's followers were called the peripatetics, which means "to walk about," because Aristotle often walked around as he discussed philosophical questions. Aristotle taught at the Lyceum for 13 years where he lectured to his advanced students in the morning and gave popular lectures to a broad audience in the evening. When Alexander the Great died in 323 B.C.E., a backlash against anything related to Alexander led to trumped-up charges of impiety against Aristotle. Aristotle fled to Chalcis to avoid prosecution. He only lived one year in Chalcis, dying of a stomach ailment in 322 B.C.E.

Aristotle wrote three types of works: those written for a popular audience, compilations of scientific facts, and systematic treatises. The systematic treatises included works on logic, philosophy, psychology, physics, and natural history. Aristotle's writings were preserved by a student and were hidden in a vault where a wealthy book collector discovered them about 200 years later. They were taken to Rome, where they were studied by scholars and issued in new editions, preserving them for posterity.

conventional letters used for propositional variables are $p, q, r, s, \ldots$ . The **truth value** of a proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.

The area of logic that deals with propositions is called the **propositional calculus** or **propositional logic**. It was first developed systematically by the Greek philosopher Aristotle more than 2300 years ago.

Links

We now turn our attention to methods for producing new propositions from those that we already have. These methods were discussed by the English mathematician George Boole in 1854 in his book *The Laws of Thought.* Many mathematical statements are constructed by combining one or more propositions. New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

**DEFINITION 1**

Let $p$ be a proposition. The *negation of* $p$, denoted by $\neg p$ (also denoted by $\overline{p}$), is the statement

"It is not the case that $p$."

The proposition $\neg p$ is read "not $p$." The truth value of the negation of $p$, $\neg p$, is the opposite of the truth value of $p$.

**EXAMPLE 3** Find the negation of the proposition

"Michael's PC runs Linux"

Extra Examples

and express this in simple English.

*Solution:* The negation is

"It is not the case that Michael's PC runs Linux."

This negation can be more simply expressed as

"Michael's PC does not run Linux."

◀

**EXAMPLE 4** Find the negation of the proposition

"Vandana's smartphone has at least 32GB of memory"

and express this in simple English.

*Solution:* The negation is

"It is not the case that Vandana's smartphone has at least 32GB of memory."

This negation can also be expressed as

"Vandana's smartphone does not have at least 32GB of memory"

or even more simply as

"Vandana's smartphone has less than 32GB of memory."

◀

**TABLE 1 The Truth Table for the Negation of a Proposition.**

| $p$ | $\neg p$ |
|---|---|
| T | F |
| F | T |

Table 1 displays the **truth table** for the negation of a proposition $p$. This table has a row for each of the two possible truth values of a proposition $p$. Each row shows the truth value of $\neg p$ corresponding to the truth value of $p$ for this row.

The negation of a proposition can also be considered the result of the operation of the **negation operator** on a proposition. The negation operator constructs a new proposition from a single existing proposition. We will now introduce the logical operators that are used to form new propositions from two or more existing propositions. These logical operators are also called **connectives**.

**DEFINITION 2**

Let $p$ and $q$ be propositions. The *conjunction* of $p$ and $q$, denoted by $p \wedge q$, is the proposition "$p$ and $q$." The conjunction $p \wedge q$ is true when both $p$ and $q$ are true and is false otherwise.

Table 2 displays the truth table of $p \wedge q$. This table has a row for each of the four possible combinations of truth values of $p$ and $q$. The four rows correspond to the pairs of truth values TT, TF, FT, and FF, where the first truth value in the pair is the truth value of $p$ and the second truth value is the truth value of $q$.

Note that in logic the word "but" sometimes is used instead of "and" in a conjunction. For example, the statement "The sun is shining, but it is raining" is another way of saying "The sun is shining and it is raining." (In natural language, there is a subtle difference in meaning between "and" and "but"; we will not be concerned with this nuance here.)

**EXAMPLE 5** Find the conjunction of the propositions $p$ and $q$ where $p$ is the proposition "Rebecca's PC has more than 16 GB free hard disk space" and $q$ is the proposition "The processor in Rebecca's PC runs faster than 1 GHz."

*Solution:* The conjunction of these propositions, $p \wedge q$, is the proposition "Rebecca's PC has more than 16 GB free hard disk space, and the processor in Rebecca's PC runs faster than 1 GHz." This conjunction can be expressed more simply as "Rebecca's PC has more than 16 GB free hard disk space, and its processor runs faster than 1 GHz." For this conjunction to be true, both conditions given must be true. It is false, when one or both of these conditions are false. ◀

**DEFINITION 3**

Let $p$ and $q$ be propositions. The *disjunction* of $p$ and $q$, denoted by $p \vee q$, is the proposition "$p$ or $q$." The disjunction $p \vee q$ is false when both $p$ and $q$ are false and is true otherwise.

Table 3 displays the truth table for $p \vee q$.

**TABLE 2 The Truth Table for the Conjunction of Two Propositions.**

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

**TABLE 3 The Truth Table for the Disjunction of Two Propositions.**

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

The use of the connective *or* in a disjunction corresponds to one of the two ways the word *or* is used in English, namely, as an **inclusive or**. A disjunction is true when at least one of the two propositions is true. For instance, the inclusive or is being used in the statement

"Students who have taken calculus or computer science can take this class."

Here, we mean that students who have taken both calculus and computer science can take the class, as well as the students who have taken only one of the two subjects. On the other hand, we are using the **exclusive or** when we say

"Students who have taken calculus or computer science, but not both, can enroll in this class."

Here, we mean that students who have taken both calculus and a computer science course cannot take the class. Only those who have taken exactly one of the two courses can take the class.

Similarly, when a menu at a restaurant states, "Soup or salad comes with an entrée," the restaurant almost always means that customers can have either soup or salad, but not both. Hence, this is an exclusive, rather than an inclusive, or.

**EXAMPLE 6** What is the disjunction of the propositions $p$ and $q$ where $p$ and $q$ are the same propositions as in Example 5?

Extra Examples

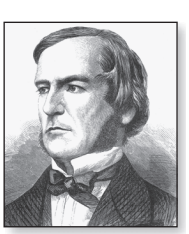
*Solution:* The disjunction of $p$ and $q$, $p \vee q$, is the proposition

"Rebecca's PC has at least 16 GB free hard disk space, or the processor in Rebecca's PC runs faster than 1 GHz."

This proposition is true when Rebecca's PC has at least 16 GB free hard disk space, when the PC's processor runs faster than 1 GHz, and when both conditions are true. It is false when both of these conditions are false, that is, when Rebecca's PC has less than 16 GB free hard disk space and the processor in her PC runs at 1 GHz or slower. ◀

As was previously remarked, the use of the connective *or* in a disjunction corresponds to one of the two ways the word *or* is used in English, namely, in an inclusive way. Thus, a disjunction is true when at least one of the two propositions in it is true. Sometimes, we use *or* in an exclusive sense. When the exclusive or is used to connect the propositions $p$ and $q$, the proposition "$p$ or $q$ (but not both)" is obtained. This proposition is true when $p$ is true and $q$ is false, and when $p$ is false and $q$ is true. It is false when both $p$ and $q$ are false and when both are true.

Links



GEORGE BOOLE (1815–1864) George Boole, the son of a cobbler, was born in Lincoln, England, in November 1815. Because of his family's difficult financial situation, Boole struggled to educate himself while supporting his family. Nevertheless, he became one of the most important mathematicians of the 1800s. Although he considered a career as a clergyman, he decided instead to go into teaching, and soon afterward opened a school of his own. In his preparation for teaching mathematics, Boole—unsatisfied with textbooks of his day—decided to read the works of the great mathematicians. While reading papers of the great French mathematician Lagrange, Boole made discoveries in the calculus of variations, the branch of analysis dealing with finding curves and surfaces by optimizing certain parameters.

In 1848 Boole published *The Mathematical Analysis of Logic*, the first of his contributions to symbolic logic. In 1849 he was appointed professor of mathematics at Queen's College in Cork, Ireland. In 1854 he published *The Laws of Thought*, his most famous work. In this book, Boole introduced what is now called *Boolean algebra* in his honor. Boole wrote textbooks on differential equations and on difference equations that were used in Great Britain until the end of the nineteenth century. Boole married in 1855; his wife was the niece of the professor of Greek at Queen's College. In 1864 Boole died from pneumonia, which he contracted as a result of keeping a lecture engagement even though he was soaking wet from a rainstorm.

**TABLE 4** The Truth Table for the Exclusive Or of Two Propositions.

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| T | T | F |
| T | F | T |
| F | T | T |
| F | F | F |

**TABLE 5** The Truth Table for the Conditional Statement $p \rightarrow q$.

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

**DEFINITION 4** Let $p$ and $q$ be propositions. The *exclusive or* of $p$ and $q$, denoted by $p \oplus q$, is the proposition that is true when exactly one of $p$ and $q$ is true and is false otherwise.

The truth table for the exclusive or of two propositions is displayed in Table 4.

## Conditional Statements

We will discuss several other important ways in which propositions can be combined.

**DEFINITION 5** Let $p$ and $q$ be propositions. The *conditional statement* $p \rightarrow q$ is the proposition "if $p$, then $q$." The conditional statement $p \rightarrow q$ is false when $p$ is true and $q$ is false, and true otherwise. In the conditional statement $p \rightarrow q$, $p$ is called the *hypothesis* (or *antecedent* or *premise*) and $q$ is called the *conclusion* (or *consequence*).

Assessment

The statement $p \rightarrow q$ is called a conditional statement because $p \rightarrow q$ asserts that $q$ is true on the condition that $p$ holds. A conditional statement is also called an **implication**.

The truth table for the conditional statement $p \rightarrow q$ is shown in Table 5. Note that the statement $p \rightarrow q$ is true when both $p$ and $q$ are true and when $p$ is false (no matter what truth value $q$ has).

Because conditional statements play such an essential role in mathematical reasoning, a variety of terminology is used to express $p \rightarrow q$. You will encounter most if not all of the following ways to express this conditional statement:

"if $p$, then $q$"
"if $p$, $q$"
"$p$ is sufficient for $q$"
"$q$ if $p$"
"$q$ when $p$"
"a necessary condition for $p$ is $q$"
"$q$ unless $\neg p$"
"$p$ implies $q$"
"$p$ only if $q$"
"a sufficient condition for $q$ is $p$"
"$q$ whenever $p$"
"$q$ is necessary for $p$"
"$q$ follows from $p$"

A useful way to understand the truth value of a conditional statement is to think of an obligation or a contract. For example, the pledge many politicians make when running for office is

"If I am elected, then I will lower taxes."

If the politician is elected, voters would expect this politician to lower taxes. Furthermore, if the politician is not elected, then voters will not have any expectation that this person will lower taxes, although the person may have sufficient influence to cause those in power to lower taxes. It is only when the politician is elected but does not lower taxes that voters can say that the politician has broken the campaign pledge. This last scenario corresponds to the case when $p$ is true but $q$ is false in $p \rightarrow q$.

Similarly, consider a statement that a professor might make:

"If you get 100% on the final, then you will get an A."

If you manage to get a 100% on the final, then you would expect to receive an A. If you do not get 100% you may or may not receive an A depending on other factors. However, if you do get 100%, but the professor does not give you an A, you will feel cheated.

Of the various ways to express the conditional statement $p \rightarrow q$, the two that seem to cause the most confusion are "$p$ only if $q$" and "$q$ unless $\neg p$." Consequently, we will provide some guidance for clearing up this confusion.

To remember that "$p$ only if $q$" expresses the same thing as "if $p$, then $q$," note that "$p$ only if $q$" says that $p$ cannot be true when $q$ is not true. That is, the statement is false if $p$ is true, but $q$ is false. When $p$ is false, $q$ may be either true or false, because the statement says nothing about the truth value of $q$. Be careful not to use "$q$ only if $p$" to express $p \rightarrow q$ because this is incorrect. To see this, note that the true values of "$q$ only if $p$" and $p \rightarrow q$ are different when $p$ and $q$ have different truth values.

You might have trouble understanding how "unless" is used in conditional statements unless you read this paragraph carefully.

To remember that "$q$ unless $\neg p$" expresses the same conditional statement as "if $p$, then $q$," note that "$q$ unless $\neg p$" means that if $\neg p$ is false, then $q$ must be true. That is, the statement "$q$ unless $\neg p$" is false when $p$ is true but $q$ is false, but it is true otherwise. Consequently, "$q$ unless $\neg p$" and $p \rightarrow q$ always have the same truth value.

We illustrate the translation between conditional statements and English statements in Example 7.

**EXAMPLE 7** Let $p$ be the statement "Maria learns discrete mathematics" and $q$ the statement "Maria will find a good job." Express the statement $p \rightarrow q$ as a statement in English.

Extra Examples

*Solution:* From the definition of conditional statements, we see that when $p$ is the statement "Maria learns discrete mathematics" and $q$ is the statement "Maria will find a good job," $p \rightarrow q$ represents the statement

"If Maria learns discrete mathematics, then she will find a good job."

There are many other ways to express this conditional statement in English. Among the most natural of these are:

"Maria will find a good job when she learns discrete mathematics."

"For Maria to get a good job, it is sufficient for her to learn discrete mathematics."

and

"Maria will find a good job unless she does not learn discrete mathematics." ◀

Note that the way we have defined conditional statements is more general than the meaning attached to such statements in the English language. For instance, the conditional statement in Example 7 and the statement

"If it is sunny, then we will go to the beach."

are statements used in normal language where there is a relationship between the hypothesis and the conclusion. Further, the first of these statements is true unless Maria learns discrete mathematics, but she does not get a good job, and the second is true unless it is indeed sunny, but we do not go to the beach. On the other hand, the statement

"If Juan has a smartphone, then $2 + 3 = 5$"

is true from the definition of a conditional statement, because its conclusion is true. (The truth value of the hypothesis does not matter then.) The conditional statement

"If Juan has a smartphone, then $2 + 3 = 6$"

is true if Juan does not have a smartphone, even though $2 + 3 = 6$ is false. We would not use these last two conditional statements in natural language (except perhaps in sarcasm), because there is no relationship between the hypothesis and the conclusion in either statement. In mathematical reasoning, we consider conditional statements of a more general sort than we use in English. The mathematical concept of a conditional statement is independent of a cause-and-effect relationship between hypothesis and conclusion. Our definition of a conditional statement specifies its truth values; it is not based on English usage. Propositional language is an artificial language; we only parallel English usage to make it easy to use and remember.

The if-then construction used in many programming languages is different from that used in logic. Most programming languages contain statements such as **if** $p$ **then** $S$, where $p$ is a proposition and $S$ is a program segment (one or more statements to be executed). When execution of a program encounters such a statement, $S$ is executed if $p$ is true, but $S$ is not executed if $p$ is false, as illustrated in Example 8.

**EXAMPLE 8** What is the value of the variable $x$ after the statement

**if** $2 + 2 = 4$ **then** $x := x + 1$

if $x = 0$ before this statement is encountered? (The symbol $:=$ stands for assignment. The statement $x := x + 1$ means the assignment of the value of $x + 1$ to $x$.)

*Solution:* Because $2 + 2 = 4$ is true, the assignment statement $x := x + 1$ is executed. Hence, $x$ has the value $0 + 1 = 1$ after this statement is encountered. ◀

CONVERSE, CONTRAPOSITIVE, AND INVERSE We can form some new conditional statements starting with a conditional statement $p \rightarrow q$. In particular, there are three related conditional statements that occur so often that they have special names. The proposition $q \rightarrow p$ is called the **converse** of $p \rightarrow q$. The **contrapositive** of $p \rightarrow q$ is the proposition $\neg q \rightarrow \neg p$. The proposition $\neg p \rightarrow \neg q$ is called the **inverse** of $p \rightarrow q$. We will see that of these three conditional statements formed from $p \rightarrow q$, only the contrapositive always has the same truth value as $p \rightarrow q$.

We first show that the contrapositive, $\neg q \rightarrow \neg p$, of a conditional statement $p \rightarrow q$ always has the same truth value as $p \rightarrow q$. To see this, note that the contrapositive is false only when $\neg p$ is false and $\neg q$ is true, that is, only when $p$ is true and $q$ is false. We now show that neither the converse, $q \rightarrow p$, nor the inverse, $\neg p \rightarrow \neg q$, has the same truth value as $p \rightarrow q$ for all possible truth values of $p$ and $q$. Note that when $p$ is true and $q$ is false, the original conditional statement is false, but the converse and the inverse are both true.

Remember that the contrapositive, but neither the converse or inverse, of a conditional statement is equivalent to it.

When two compound propositions always have the same truth value we call them **equivalent**, so that a conditional statement and its contrapositive are equivalent. The converse and the inverse of a conditional statement are also equivalent, as the reader can verify, but neither is equivalent to the original conditional statement. (We will study equivalent propositions in Section 1.3.) Take note that one of the most common logical errors is to assume that the converse or the inverse of a conditional statement is equivalent to this conditional statement.

We illustrate the use of conditional statements in Example 9.

**EXAMPLE 9** What are the contrapositive, the converse, and the inverse of the conditional statement

"The home team wins whenever it is raining?"

Extra Examples

*Solution:* Because "$q$ whenever $p$" is one of the ways to express the conditional statement $p \rightarrow q$, the original statement can be rewritten as

"If it is raining, then the home team wins."

Consequently, the contrapositive of this conditional statement is

"If the home team does not win, then it is not raining."

The converse is

"If the home team wins, then it is raining."

The inverse is

"If it is not raining, then the home team does not win."

Only the contrapositive is equivalent to the original statement. ◀

BICONDITIONALS We now introduce another way to combine propositions that expresses that two propositions have the same truth value.

**DEFINITION 6** Let $p$ and $q$ be propositions. The *biconditional statement* $p \leftrightarrow q$ is the proposition "$p$ if and only if $q$." The biconditional statement $p \leftrightarrow q$ is true when $p$ and $q$ have the same truth values, and is false otherwise. Biconditional statements are also called *bi-implications*.

The truth table for $p \leftrightarrow q$ is shown in Table 6. Note that the statement $p \leftrightarrow q$ is true when both the conditional statements $p \rightarrow q$ and $q \rightarrow p$ are true and is false otherwise. That is why we use the words "if and only if" to express this logical connective and why it is symbolically written by combining the symbols $\rightarrow$ and $\leftarrow$. There are some other common ways to express $p \leftrightarrow q$:

"$p$ is necessary and sufficient for $q$"
"if $p$ then $q$, and conversely"
"$p$ iff $q$."

The last way of expressing the biconditional statement $p \leftrightarrow q$ uses the abbreviation "iff" for "if and only if." Note that $p \leftrightarrow q$ has exactly the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$.

**TABLE 6 The Truth Table for the Biconditional $p \leftrightarrow q$.**

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

**EXAMPLE 10** Let $p$ be the statement "You can take the flight," and let $q$ be the statement "You buy a ticket." Then $p \leftrightarrow q$ is the statement

"You can take the flight if and only if you buy a ticket."

Extra Examples

This statement is true if $p$ and $q$ are either both true or both false, that is, if you buy a ticket and can take the flight or if you do not buy a ticket and you cannot take the flight. It is false when $p$ and $q$ have opposite truth values, that is, when you do not buy a ticket, but you can take the flight (such as when you get a free trip) and when you buy a ticket but you cannot take the flight (such as when the airline bumps you). ◀

IMPLICIT USE OF BICONDITIONALS You should be aware that biconditionals are not always explicit in natural language. In particular, the "if and only if" construction used in biconditionals is rarely used in common language. Instead, biconditionals are often expressed using an "if, then" or an "only if" construction. The other part of the "if and only if" is implicit. That is, the converse is implied, but not stated. For example, consider the statement in English "If you finish your meal, then you can have dessert." What is really meant is "You can have dessert if and only if you finish your meal." This last statement is logically equivalent to the two statements "If you finish your meal, then you can have dessert" and "You can have dessert only if you finish your meal." Because of this imprecision in natural language, we need to make an assumption whether a conditional statement in natural language implicitly includes its converse. Because precision is essential in mathematics and in logic, we will always distinguish between the conditional statement $p \rightarrow q$ and the biconditional statement $p \leftrightarrow q$.

## Truth Tables of Compound Propositions

Demo

We have now introduced four important logical connectives—conjunctions, disjunctions, conditional statements, and biconditional statements—as well as negations. We can use these connectives to build up complicated compound propositions involving any number of propositional variables. We can use truth tables to determine the truth values of these compound propositions, as Example 11 illustrates. We use a separate column to find the truth value of each compound expression that occurs in the compound proposition as it is built up. The truth values of the compound proposition for each combination of truth values of the propositional variables in it is found in the final column of the table.

**EXAMPLE 11** Construct the truth table of the compound proposition

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

*Solution:* Because this truth table involves two propositional variables $p$ and $q$, there are four rows in this truth table, one for each of the pairs of truth values TT, TF, FT, and FF. The first two columns are used for the truth values of $p$ and $q$, respectively. In the third column we find the truth value of $\neg q$, needed to find the truth value of $p \vee \neg q$, found in the fourth column. The fifth column gives the truth value of $p \wedge q$. Finally, the truth value of $(p \vee \neg q) \rightarrow (p \wedge q)$ is found in the last column. The resulting truth table is shown in Table 7. ◀

**TABLE 7 The Truth Table of $(p \vee \neg q) \rightarrow (p \wedge q)$.**

| $p$ | $q$ | $\neg q$ | $p \vee \neg q$ | $p \wedge q$ | $(p \vee \neg q) \rightarrow (p \wedge q)$ |
|---|---|---|---|---|---|
| T | T | F | T | T | T |
| T | F | T | T | F | F |
| F | T | F | F | F | T |
| F | F | T | T | F | F |

## Precedence of Logical Operators

**TABLE 8**
**Precedence of Logical Operators.**

| *Operator* | *Precedence* |
|---|---|
| $\neg$ | 1 |
| $\wedge$ | 2 |
| $\vee$ | 3 |
| $\rightarrow$ | 4 |
| $\leftrightarrow$ | 5 |

We can construct compound propositions using the negation operator and the logical operators defined so far. We will generally use parentheses to specify the order in which logical operators in a compound proposition are to be applied. For instance, $(p \vee q) \wedge (\neg r)$ is the conjunction of $p \vee q$ and $\neg r$. However, to reduce the number of parentheses, we specify that the negation operator is applied before all other logical operators. This means that $\neg p \wedge q$ is the conjunction of $\neg p$ and $q$, namely, $(\neg p) \wedge q$, not the negation of the conjunction of $p$ and $q$, namely $\neg(p \wedge q)$.

Another general rule of precedence is that the conjunction operator takes precedence over the disjunction operator, so that $p \wedge q \vee r$ means $(p \wedge q) \vee r$ rather than $p \wedge (q \vee r)$. Because this rule may be difficult to remember, we will continue to use parentheses so that the order of the disjunction and conjunction operators is clear.

Finally, it is an accepted rule that the conditional and biconditional operators $\rightarrow$ and $\leftrightarrow$ have lower precedence than the conjunction and disjunction operators, $\wedge$ and $\vee$. Consequently, $p \vee q \rightarrow r$ is the same as $(p \vee q) \rightarrow r$. We will use parentheses when the order of the conditional operator and biconditional operator is at issue, although the conditional operator has precedence over the biconditional operator. Table 8 displays the precedence levels of the logical operators, $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$.

## Logic and Bit Operations

| *Truth Value* | *Bit* |
|---|---|
| T | 1 |
| F | 0 |

Links

Computers represent information using bits. A **bit** is a symbol with two possible values, namely, 0 (zero) and 1 (one). This meaning of the word bit comes from *b*inary dig*it*, because zeros and ones are the digits used in binary representations of numbers. The well-known statistician John Tukey introduced this terminology in 1946. A bit can be used to represent a truth value, because there are two truth values, namely, *true* and *false*. As is customarily done, we will use a 1 bit to represent true and a 0 bit to represent false. That is, 1 represents T (true), 0 represents F (false). A variable is called a **Boolean variable** if its value is either true or false. Consequently, a Boolean variable can be represented using a bit.

Computer **bit operations** correspond to the logical connectives. By replacing true by a one and false by a zero in the truth tables for the operators $\wedge$, $\vee$, and $\oplus$, the tables shown in Table 9 for the corresponding bit operations are obtained. We will also use the notation *OR*, *AND*, and *XOR* for the operators $\vee$, $\wedge$, and $\oplus$, as is done in various programming languages.

Links

JOHN WILDER TUKEY (1915–2000) Tukey, born in New Bedford, Massachusetts, was an only child. His parents, both teachers, decided home schooling would best develop his potential. His formal education began at Brown University, where he studied mathematics and chemistry. He received a master's degree in chemistry from Brown and continued his studies at Princeton University, changing his field of study from chemistry to mathematics. He received his Ph.D. from Princeton in 1939 for work in topology, when he was appointed an instructor in mathematics at Princeton. With the start of World War II, he joined the Fire Control Research Office, where he began working in statistics. Tukey found statistical research to his liking and impressed several leading statisticians with his skills. In 1945, at the conclusion of the war, Tukey returned to the mathematics department at Princeton as a professor of statistics, and he also took a position at AT&T Bell Laboratories. Tukey founded the Statistics Department at Princeton in 1966 and was its first chairman. Tukey made significant contributions to many areas of statistics, including the analysis of variance, the estimation of spectra of time series, inferences about the values of a set of parameters from a single experiment, and the philosophy of statistics. However, he is best known for his invention, with J. W. Cooley, of the fast Fourier transform. In addition to his contributions to statistics, Tukey was noted as a skilled wordsmith; he is credited with coining the terms *bit* and *software*.

Tukey contributed his insight and expertise by serving on the President's Science Advisory Committee. He chaired several important committees dealing with the environment, education, and chemicals and health. He also served on committees working on nuclear disarmament. Tukey received many awards, including the National Medal of Science.

HISTORICAL NOTE There were several other suggested words for a binary digit, including *binit* and *bigit*, that never were widely accepted. The adoption of the word *bit* may be due to its meaning as a common English word. For an account of Tukey's coining of the word *bit*, see the April 1984 issue of *Annals of the History of Computing*.

**TABLE 9** **Table for the Bit Operators *OR*, *AND*, and *XOR*.**

| $x$ | $y$ | $x \vee y$ | $x \wedge y$ | $x \oplus y$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

Information is often represented using bit strings, which are lists of zeros and ones. When this is done, operations on the bit strings can be used to manipulate this information.

**DEFINITION 7**

A *bit string* is a sequence of zero or more bits. The *length* of this string is the number of bits in the string.

**EXAMPLE 12** 101010011 is a bit string of length nine. ◀

We can extend bit operations to bit strings. We define the **bitwise *OR***, **bitwise *AND***, and **bitwise *XOR*** of two strings of the same length to be the strings that have as their bits the *OR*, *AND*, and *XOR* of the corresponding bits in the two strings, respectively. We use the symbols $\vee$, $\wedge$, and $\oplus$ to represent the bitwise *OR*, bitwise *AND*, and bitwise *XOR* operations, respectively. We illustrate bitwise operations on bit strings with Example 13.

**EXAMPLE 13** Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of the bit strings 01 1011 0110 and 11 0001 1101. (Here, and throughout this book, bit strings will be split into blocks of four bits to make them easier to read.)

*Solution:* The bitwise *OR*, bitwise *AND*, and bitwise *XOR* of these strings are obtained by taking the *OR*, *AND*, and *XOR* of the corresponding bits, respectively. This gives us

$$\begin{array}{ll} 01\ 1011\ 0110 & \\ 11\ 0001\ 1101 & \\ \hline 11\ 1011\ 1111 & \text{bitwise } \textit{OR} \\ 01\ 0001\ 0100 & \text{bitwise } \textit{AND} \\ 10\ 1010\ 1011 & \text{bitwise } \textit{XOR} \end{array}$$

◀

## Exercises

**1.** Which of these sentences are propositions? What are the truth values of those that are propositions?
- **a)** Boston is the capital of Massachusetts.
- **b)** Miami is the capital of Florida.
- **c)** $2 + 3 = 5$.
- **d)** $5 + 7 = 10$.
- **e)** $x + 2 = 11$.
- **f)** Answer this question.

**2.** Which of these are propositions? What are the truth values of those that are propositions?
- **a)** Do not pass go.
- **b)** What time is it?
- **c)** There are no black flies in Maine.
- **d)** $4 + x = 5$.
- **e)** The moon is made of green cheese.
- **f)** $2^n \geq 100$.

**3.** What is the negation of each of these propositions?
- **a)** Mei has an MP3 player.
- **b)** There is no pollution in New Jersey.
- **c)** $2 + 1 = 3$.
- **d)** The summer in Maine is hot and sunny.

**4.** What is the negation of each of these propositions?
- **a)** Jennifer and Teja are friends.
- **b)** There are 13 items in a baker's dozen.
- **c)** Abby sent more than 100 text messages every day.
- **d)** 121 is a perfect square.

**5.** What is the negation of each of these propositions?
**a)** Steve has more than 100 GB free disk space on his laptop.
**b)** Zach blocks e-mails and texts from Jennifer.
**c)** $7 \cdot 11 \cdot 13 = 999$.
**d)** Diane rode her bicycle 100 miles on Sunday.

**6.** Suppose that Smartphone A has 256 MB RAM and 32 GB ROM, and the resolution of its camera is 8 MP; Smartphone B has 288 MB RAM and 64 GB ROM, and the resolution of its camera is 4 MP; and Smartphone C has 128 MB RAM and 32 GB ROM, and the resolution of its camera is 5 MP. Determine the truth value of each of these propositions.
**a)** Smartphone B has the most RAM of these three smartphones.
**b)** Smartphone C has more ROM or a higher resolution camera than Smartphone B.
**c)** Smartphone B has more RAM, more ROM, and a higher resolution camera than Smartphone A.
**d)** If Smartphone B has more RAM and more ROM than Smartphone C, then it also has a higher resolution camera.
**e)** Smartphone A has more RAM than Smartphone B if and only if Smartphone B has more RAM than Smartphone A.

**7.** Suppose that during the most recent fiscal year, the annual revenue of Acme Computer was 138 billion dollars and its net profit was 8 billion dollars, the annual revenue of Nadir Software was 87 billion dollars and its net profit was 5 billion dollars, and the annual revenue of Quixote Media was 111 billion dollars and its net profit was 13 billion dollars. Determine the truth value of each of these propositions for the most recent fiscal year.
**a)** Quixote Media had the largest annual revenue.
**b)** Nadir Software had the lowest net profit and Acme Computer had the largest annual revenue.
**c)** Acme Computer had the largest net profit or Quixote Media had the largest net profit.
**d)** If Quixote Media had the smallest net profit, then Acme Computer had the largest annual revenue.
**e)** Nadir Software had the smallest net profit if and only if Acme Computer had the largest annual revenue.

**8.** Let $p$ and $q$ be the propositions
$p$ : I bought a lottery ticket this week.
$q$ : I won the million dollar jackpot.
Express each of these propositions as an English sentence.
**a)** $\neg p$ **b)** $p \vee q$ **c)** $p \rightarrow q$
**d)** $p \wedge q$ **e)** $p \leftrightarrow q$ **f)** $\neg p \rightarrow \neg q$
**g)** $\neg p \wedge \neg q$ **h)** $\neg p \vee (p \wedge q)$

**9.** Let $p$ and $q$ be the propositions "Swimming at the New Jersey shore is allowed" and "Sharks have been spotted near the shore," respectively. Express each of these compound propositions as an English sentence.
**a)** $\neg q$ **b)** $p \wedge q$ **c)** $\neg p \vee q$
**d)** $p \rightarrow \neg q$ **e)** $\neg q \rightarrow p$ **f)** $\neg p \rightarrow \neg q$
**g)** $p \leftrightarrow \neg q$ **h)** $\neg p \wedge (p \vee \neg q)$

**10.** Let $p$ and $q$ be the propositions "The election is decided" and "The votes have been counted," respectively. Express each of these compound propositions as an English sentence.
**a)** $\neg p$ **b)** $p \vee q$
**c)** $\neg p \wedge q$ **d)** $q \rightarrow p$
**e)** $\neg q \rightarrow \neg p$ **f)** $\neg p \rightarrow \neg q$
**g)** $p \leftrightarrow q$ **h)** $\neg q \vee (\neg p \wedge q)$

**11.** Let $p$ and $q$ be the propositions
$p$ : It is below freezing.
$q$ : It is snowing.
Write these propositions using $p$ and $q$ and logical connectives (including negations).
**a)** It is below freezing and snowing.
**b)** It is below freezing but not snowing.
**c)** It is not below freezing and it is not snowing.
**d)** It is either snowing or below freezing (or both).
**e)** If it is below freezing, it is also snowing.
**f)** Either it is below freezing or it is snowing, but it is not snowing if it is below freezing.
**g)** That it is below freezing is necessary and sufficient for it to be snowing.

**12.** Let $p$, $q$, and $r$ be the propositions
$p$ : You have the flu.
$q$ : You miss the final examination.
$r$ : You pass the course.
Express each of these propositions as an English sentence.
**a)** $p \rightarrow q$ **b)** $\neg q \leftrightarrow r$
**c)** $q \rightarrow \neg r$ **d)** $p \vee q \vee r$
**e)** $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$
**f)** $(p \wedge q) \vee (\neg q \wedge r)$

**13.** Let $p$ and $q$ be the propositions
$p$ : You drive over 65 miles per hour.
$q$ : You get a speeding ticket.
Write these propositions using $p$ and $q$ and logical connectives (including negations).
**a)** You do not drive over 65 miles per hour.
**b)** You drive over 65 miles per hour, but you do not get a speeding ticket.
**c)** You will get a speeding ticket if you drive over 65 miles per hour.
**d)** If you do not drive over 65 miles per hour, then you will not get a speeding ticket.
**e)** Driving over 65 miles per hour is sufficient for getting a speeding ticket.
**f)** You get a speeding ticket, but you do not drive over 65 miles per hour.
**g)** Whenever you get a speeding ticket, you are driving over 65 miles per hour.

**14.** Let $p$, $q$, and $r$ be the propositions
$p$ : You get an A on the final exam.
$q$ : You do every exercise in this book.
$r$ : You get an A in this class.
Write these propositions using $p$, $q$, and $r$ and logical connectives (including negations).

**a)** You get an A in this class, but you do not do every exercise in this book.
**b)** You get an A on the final, you do every exercise in this book, and you get an A in this class.
**c)** To get an A in this class, it is necessary for you to get an A on the final.
**d)** You get an A on the final, but you don't do every exercise in this book; nevertheless, you get an A in this class.
**e)** Getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.
**f)** You will get an A in this class if and only if you either do every exercise in this book or you get an A on the final.

**15.** Let $p$, $q$, and $r$ be the propositions

$p$ : Grizzly bears have been seen in the area.
$q$ : Hiking is safe on the trail.
$r$ : Berries are ripe along the trail.

Write these propositions using $p$, $q$, and $r$ and logical connectives (including negations).

**a)** Berries are ripe along the trail, but grizzly bears have not been seen in the area.
**b)** Grizzly bears have not been seen in the area and hiking on the trail is safe, but berries are ripe along the trail.
**c)** If berries are ripe along the trail, hiking is safe if and only if grizzly bears have not been seen in the area.
**d)** It is not safe to hike on the trail, but grizzly bears have not been seen in the area and the berries along the trail are ripe.
**e)** For hiking on the trail to be safe, it is necessary but not sufficient that berries not be ripe along the trail and for grizzly bears not to have been seen in the area.
**f)** Hiking is not safe on the trail whenever grizzly bears have been seen in the area and berries are ripe along the trail.

**16.** Determine whether these biconditionals are true or false.

**a)** $2 + 2 = 4$ if and only if $1 + 1 = 2$.
**b)** $1 + 1 = 2$ if and only if $2 + 3 = 4$.
**c)** $1 + 1 = 3$ if and only if monkeys can fly.
**d)** $0 > 1$ if and only if $2 > 1$.

**17.** Determine whether each of these conditional statements is true or false.

**a)** If $1 + 1 = 2$, then $2 + 2 = 5$.
**b)** If $1 + 1 = 3$, then $2 + 2 = 4$.
**c)** If $1 + 1 = 3$, then $2 + 2 = 5$.
**d)** If monkeys can fly, then $1 + 1 = 3$.

**18.** Determine whether each of these conditional statements is true or false.

**a)** If $1 + 1 = 3$, then unicorns exist.
**b)** If $1 + 1 = 3$, then dogs can fly.
**c)** If $1 + 1 = 2$, then dogs can fly.
**d)** If $2 + 2 = 4$, then $1 + 2 = 3$.

**19.** For each of these sentences, determine whether an inclusive or, or an exclusive or, is intended. Explain your answer.

**a)** Coffee or tea comes with dinner.
**b)** A password must have at least three digits or be at least eight characters long.
**c)** The prerequisite for the course is a course in number theory or a course in cryptography.
**d)** You can pay using U.S. dollars or euros.

**20.** For each of these sentences, determine whether an inclusive or, or an exclusive or, is intended. Explain your answer.

**a)** Experience with C++ or Java is required.
**b)** Lunch includes soup or salad.
**c)** To enter the country you need a passport or a voter registration card.
**d)** Publish or perish.

**21.** For each of these sentences, state what the sentence means if the logical connective or is an inclusive or (that is, a disjunction) versus an exclusive or. Which of these meanings of or do you think is intended?

**a)** To take discrete mathematics, you must have taken calculus or a course in computer science.
**b)** When you buy a new car from Acme Motor Company, you get \$2000 back in cash or a 2% car loan.
**c)** Dinner for two includes two items from column A or three items from column B.
**d)** School is closed if more than 2 feet of snow falls or if the wind chill is below $-100$.

**22.** Write each of these statements in the form "if $p$, then $q$" in English. [*Hint:* Refer to the list of common ways to express conditional statements provided in this section.]

**a)** It is necessary to wash the boss's car to get promoted.
**b)** Winds from the south imply a spring thaw.
**c)** A sufficient condition for the warranty to be good is that you bought the computer less than a year ago.
**d)** Willy gets caught whenever he cheats.
**e)** You can access the website only if you pay a subscription fee.
**f)** Getting elected follows from knowing the right people.
**g)** Carol gets seasick whenever she is on a boat.

**23.** Write each of these statements in the form "if $p$, then $q$" in English. [*Hint:* Refer to the list of common ways to express conditional statements.]

**a)** It snows whenever the wind blows from the northeast.
**b)** The apple trees will bloom if it stays warm for a week.
**c)** That the Pistons win the championship implies that they beat the Lakers.
**d)** It is necessary to walk 8 miles to get to the top of Long's Peak.
**e)** To get tenure as a professor, it is sufficient to be world-famous.
**f)** If you drive more than 400 miles, you will need to buy gasoline.
**g)** Your guarantee is good only if you bought your CD player less than 90 days ago.
**h)** Jan will go swimming unless the water is too cold.

**24.** Write each of these statements in the form "if $p$, then $q$" in English. [*Hint:* Refer to the list of common ways to express conditional statements provided in this section.]

**a)** I will remember to send you the address only if you send me an e-mail message.
**b)** To be a citizen of this country, it is sufficient that you were born in the United States.
**c)** If you keep your textbook, it will be a useful reference in your future courses.
**d)** The Red Wings will win the Stanley Cup if their goalie plays well.
**e)** That you get the job implies that you had the best credentials.
**f)** The beach erodes whenever there is a storm.
**g)** It is necessary to have a valid password to log on to the server.
**h)** You will reach the summit unless you begin your climb too late.

**25.** Write each of these propositions in the form "$p$ if and only if $q$" in English.

**a)** If it is hot outside you buy an ice cream cone, and if you buy an ice cream cone it is hot outside.
**b)** For you to win the contest it is necessary and sufficient that you have the only winning ticket.
**c)** You get promoted only if you have connections, and you have connections only if you get promoted.
**d)** If you watch television your mind will decay, and conversely.
**e)** The trains run late on exactly those days when I take it.

**26.** Write each of these propositions in the form "$p$ if and only if $q$" in English.

**a)** For you to get an A in this course, it is necessary and sufficient that you learn how to solve discrete mathematics problems.
**b)** If you read the newspaper every day, you will be informed, and conversely.
**c)** It rains if it is a weekend day, and it is a weekend day if it rains.
**d)** You can see the wizard only if the wizard is not in, and the wizard is not in only if you can see him.

**27.** State the converse, contrapositive, and inverse of each of these conditional statements.

**a)** If it snows today, I will ski tomorrow.
**b)** I come to class whenever there is going to be a quiz.
**c)** A positive integer is a prime only if it has no divisors other than 1 and itself.

**28.** State the converse, contrapositive, and inverse of each of these conditional statements.

**a)** If it snows tonight, then I will stay at home.
**b)** I go to the beach whenever it is a sunny summer day.
**c)** When I stay up late, it is necessary that I sleep until noon.

**29.** How many rows appear in a truth table for each of these compound propositions?

**a)** $p \rightarrow \neg p$
**b)** $(p \vee \neg r) \wedge (q \vee \neg s)$
**c)** $q \vee p \vee \neg s \vee \neg r \vee \neg t \vee u$
**d)** $(p \wedge r \wedge t) \leftrightarrow (q \wedge t)$

**30.** How many rows appear in a truth table for each of these compound propositions?

**a)** $(q \rightarrow \neg p) \vee (\neg p \rightarrow \neg q)$
**b)** $(p \vee \neg t) \wedge (p \vee \neg s)$
**c)** $(p \rightarrow r) \vee (\neg s \rightarrow \neg t) \vee (\neg u \rightarrow v)$
**d)** $(p \wedge r \wedge s) \vee (q \wedge t) \vee (r \wedge \neg t)$

**31.** Construct a truth table for each of these compound propositions.

**a)** $p \wedge \neg p$ **b)** $p \vee \neg p$
**c)** $(p \vee \neg q) \rightarrow q$ **d)** $(p \vee q) \rightarrow (p \wedge q)$
**e)** $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
**f)** $(p \rightarrow q) \rightarrow (q \rightarrow p)$

**32.** Construct a truth table for each of these compound propositions.

**a)** $p \rightarrow \neg p$ **b)** $p \leftrightarrow \neg p$
**c)** $p \oplus (p \vee q)$ **d)** $(p \wedge q) \rightarrow (p \vee q)$
**e)** $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$
**f)** $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$

**33.** Construct a truth table for each of these compound propositions.

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

**34.** Construct a truth table for each of these compound propositions.

**a)** $p \oplus p$ **b)** $p \oplus \neg p$
**c)** $p \oplus \neg q$ **d)** $\neg p \oplus \neg q$
**e)** $(p \oplus q) \vee (p \oplus \neg q)$ **f)** $(p \oplus q) \wedge (p \oplus \neg q)$

**35.** Construct a truth table for each of these compound propositions.

**a)** $p \rightarrow \neg q$ **b)** $\neg p \leftrightarrow q$
**c)** $(p \rightarrow q) \vee (\neg p \rightarrow q)$ **d)** $(p \rightarrow q) \wedge (\neg p \rightarrow q)$
**e)** $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$
**f)** $(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$

**36.** Construct a truth table for each of these compound propositions.

**a)** $(p \vee q) \vee r$ **b)** $(p \vee q) \wedge r$
**c)** $(p \wedge q) \vee r$ **d)** $(p \wedge q) \wedge r$
**e)** $(p \vee q) \wedge \neg r$ **f)** $(p \wedge q) \vee \neg r$

**37.** Construct a truth table for each of these compound propositions.

**a)** $p \rightarrow (\neg q \vee r)$
**b)** $\neg p \rightarrow (q \rightarrow r)$
**c)** $(p \rightarrow q) \vee (\neg p \rightarrow r)$
**d)** $(p \rightarrow q) \wedge (\neg p \rightarrow r)$
**e)** $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$
**f)** $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$

**38.** Construct a truth table for $((p \rightarrow q) \rightarrow r) \rightarrow s$.

**39.** Construct a truth table for $(p \leftrightarrow q) \leftrightarrow (r \leftrightarrow s)$.

☞ **40.** Explain, without using a truth table, why $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true when $p$, $q$, and $r$ have the same truth value and it is false otherwise.

☞ **41.** Explain, without using a truth table, why $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is true when at least one of $p$, $q$, and $r$ is true and at least one is false, but is false when all three variables have the same truth value.

**42.** What is the value of $x$ after each of these statements is encountered in a computer program, if $x = 1$ before the statement is reached?

**a)** **if** $x + 2 = 3$ **then** $x := x + 1$
**b)** **if** $(x + 1 = 3)$ *OR* $(2x + 2 = 3)$ **then** $x := x + 1$
**c)** **if** $(2x + 3 = 5)$ *AND* $(3x + 4 = 7)$ **then** $x := x + 1$
**d)** **if** $(x + 1 = 2)$ *XOR* $(x + 2 = 3)$ **then** $x := x + 1$
**e)** **if** $x < 2$ **then** $x := x + 1$

**43.** Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of each of these pairs of bit strings.

**a)** 101 1110, 010 0001
**b)** 1111 0000, 1010 1010
**c)** 00 0111 0001, 10 0100 1000
**d)** 11 1111 1111, 00 0000 0000

**44.** Evaluate each of these expressions.

**a)** $1\ 1000 \wedge (0\ 1011 \vee 1\ 1011)$
**b)** $(0\ 1111 \wedge 1\ 0101) \vee 0\ 1000$
**c)** $(0\ 1010 \oplus 1\ 1011) \oplus 0\ 1000$
**d)** $(1\ 1011 \vee 0\ 1010) \wedge (1\ 0001 \vee 1\ 1011)$

**Fuzzy logic** is used in artificial intelligence. In fuzzy logic, a proposition has a truth value that is a number between 0 and 1, inclusive. A proposition with a truth value of 0 is false and one with a truth value of 1 is true. Truth values that are between 0 and 1 indicate varying degrees of truth. For instance, the truth value 0.8 can be assigned to the statement "Fred is happy," because Fred is happy most of the time, and the truth value 0.4 can be assigned to the statement "John is happy," because John is happy slightly less than half the time. Use these truth values to solve Exercises 45–47.

**45.** The truth value of the negation of a proposition in fuzzy logic is 1 minus the truth value of the proposition. What are the truth values of the statements "Fred is not happy" and "John is not happy?"

**46.** The truth value of the conjunction of two propositions in fuzzy logic is the minimum of the truth values of the two propositions. What are the truth values of the statements "Fred and John are happy" and "Neither Fred nor John is happy?"

**47.** The truth value of the disjunction of two propositions in fuzzy logic is the maximum of the truth values of the two propositions. What are the truth values of the statements "Fred is happy, or John is happy" and "Fred is not happy, or John is not happy?"

***48.** Is the assertion "This statement is false" a proposition?

***49.** The $n$th statement in a list of 100 statements is "Exactly $n$ of the statements in this list are false."

**a)** What conclusions can you draw from these statements?
**b)** Answer part (a) if the $n$th statement is "At least $n$ of the statements in this list are false."
**c)** Answer part (b) assuming that the list contains 99 statements.

**50.** An ancient Sicilian legend says that the barber in a remote town who can be reached only by traveling a dangerous mountain road shaves those people, and only those people, who do not shave themselves. Can there be such a barber?

# 1.2 Applications of Propositional Logic

## Introduction

Logic has many important applications to mathematics, computer science, and numerous other disciplines. Statements in mathematics and the sciences and in natural language often are imprecise or ambiguous. To make such statements precise, they can be translated into the language of logic. For example, logic is used in the specification of software and hardware, because these specifications need to be precise before development begins. Furthermore, propositional logic and its rules can be used to design computer circuits, to construct computer programs, to verify the correctness of programs, and to build expert systems. Logic can be used to analyze and solve many familiar puzzles. Software systems based on the rules of logic have been developed for constructing some, but not all, types of proofs automatically. We will discuss some of these applications of propositional logic in this section and in later chapters.

## Translating English Sentences

There are many reasons to translate English sentences into expressions involving propositional variables and logical connectives. In particular, English (and every other human language) is

often ambiguous. Translating sentences into compound statements (and other types of logical expressions, which we will introduce later in this chapter) removes the ambiguity. Note that this may involve making a set of reasonable assumptions based on the intended meaning of the sentence. Moreover, once we have translated sentences from English into logical expressions we can analyze these logical expressions to determine their truth values, we can manipulate them, and we can use rules of inference (which are discussed in Section 1.6) to reason about them.

To illustrate the process of translating an English sentence into a logical expression, consider Examples 1 and 2.

**EXAMPLE 1** How can this English sentence be translated into a logical expression?

"You can access the Internet from campus only if you are a computer science major or you are not a freshman."


*Solution:* There are many ways to translate this sentence into a logical expression. Although it is possible to represent the sentence by a single propositional variable, such as $p$, this would not be useful when analyzing its meaning or reasoning with it. Instead, we will use propositional variables to represent each sentence part and determine the appropriate logical connectives between them. In particular, we let $a$, $c$, and $f$ represent "You can access the Internet from campus," "You are a computer science major," and "You are a freshman," respectively. Noting that "only if" is one way a conditional statement can be expressed, this sentence can be represented as

$$a \rightarrow (c \vee \neg f).$$ ◀

**EXAMPLE 2** How can this English sentence be translated into a logical expression?

"You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old."

*Solution:* Let $q$, $r$, and $s$ represent "You can ride the roller coaster," "You are under 4 feet tall," and "You are older than 16 years old," respectively. Then the sentence can be translated to

$$(r \wedge \neg s) \rightarrow \neg q.$$

Of course, there are other ways to represent the original sentence as a logical expression, but the one we have used should meet our needs. ◀

## System Specifications

Translating sentences in natural language (such as English) into logical expressions is an essential part of specifying both hardware and software systems. System and software engineers take requirements in natural language and produce precise and unambiguous specifications that can be used as the basis for system development. Example 3 shows how compound propositions can be used in this process.

**EXAMPLE 3** Express the specification "The automated reply cannot be sent when the file system is full" using logical connectives.


*Solution:* One way to translate this is to let $p$ denote "The automated reply can be sent" and $q$ denote "The file system is full." Then $\neg p$ represents "It is not the case that the automated

reply can be sent," which can also be expressed as "The automated reply cannot be sent." Consequently, our specification can be represented by the conditional statement $q \rightarrow \neg p$. ◀

System specifications should be **consistent**, that is, they should not contain conflicting requirements that could be used to derive a contradiction. When specifications are not consistent, there would be no way to develop a system that satisfies all specifications.

**EXAMPLE 4** Determine whether these system specifications are consistent:

"The diagnostic message is stored in the buffer or it is retransmitted."
"The diagnostic message is not stored in the buffer."
"If the diagnostic message is stored in the buffer, then it is retransmitted."

*Solution:* To determine whether these specifications are consistent, we first express them using logical expressions. Let $p$ denote "The diagnostic message is stored in the buffer" and let $q$ denote "The diagnostic message is retransmitted." The specifications can then be written as $p \vee q$, $\neg p$, and $p \rightarrow q$. An assignment of truth values that makes all three specifications true must have $p$ false to make $\neg p$ true. Because we want $p \vee q$ to be true but $p$ must be false, $q$ must be true. Because $p \rightarrow q$ is true when $p$ is false and $q$ is true, we conclude that these specifications are consistent, because they are all true when $p$ is false and $q$ is true. We could come to the same conclusion by use of a truth table to examine the four possible assignments of truth values to $p$ and $q$. ◀

**EXAMPLE 5** Do the system specifications in Example 4 remain consistent if the specification "The diagnostic message is not retransmitted" is added?

*Solution:* By the reasoning in Example 4, the three specifications from that example are true only in the case when $p$ is false and $q$ is true. However, this new specification is $\neg q$, which is false when $q$ is true. Consequently, these four specifications are inconsistent. ◀

## Boolean Searches

Logical connectives are used extensively in searches of large collections of information, such as indexes of Web pages. Because these searches employ techniques from propositional logic, they are called **Boolean searches**.

Links

In Boolean searches, the connective *AND* is used to match records that contain both of two search terms, the connective *OR* is used to match one or both of two search terms, and the connective *NOT* (sometimes written as *AND NOT* ) is used to exclude a particular search term. Careful planning of how logical connectives are used is often required when Boolean searches are used to locate information of potential interest. Example 6 illustrates how Boolean searches are carried out.

**EXAMPLE 6** **Web Page Searching** Most Web search engines support Boolean searching techniques, which usually can help find Web pages about particular subjects. For instance, using Boolean searching to find Web pages about universities in New Mexico, we can look for pages matching NEW *AND* MEXICO *AND* UNIVERSITIES. The results of this search will include those pages that contain the three words NEW, MEXICO, and UNIVERSITIES. This will include all of the pages of interest, together with others such as a page about new universities in Mexico. (Note that in Google, and many other search engines, the word "AND" is not needed, although it is understood, because all search terms are included by default. These search engines also support the use of quotation marks to search for specific phrases. So, it may be more effective to search for pages matching "New Mexico" *AND* UNIVERSITIES.)

Extra Examples

Next, to find pages that deal with universities in New Mexico or Arizona, we can search for pages matching (NEW *AND* MEXICO *OR* ARIZONA) *AND* UNIVERSITIES. (*Note:* Here the *AND* operator takes precedence over the *OR* operator. Also, in Google, the terms used for this search would be NEW MEXICO *OR* ARIZONA.) The results of this search will include all pages that contain the word UNIVERSITIES and either both the words NEW and MEXICO or the word ARIZONA. Again, pages besides those of interest will be listed. Finally, to find Web pages that deal with universities in Mexico (and not New Mexico), we might first look for pages matching MEXICO *AND* UNIVERSITIES, but because the results of this search will include pages about universities in New Mexico, as well as universities in Mexico, it might be better to search for pages matching (MEXICO *AND* UNIVERSITIES) *NOT* NEW. The results of this search include pages that contain both the words MEXICO and UNIVERSITIES but do not contain the word NEW. (In Google, and many other search engines, the word "NOT" is replaced by the symbol "-". In Google, the terms used for this last search would be MEXICO UNIVERSITIES -NEW.) ◀

## Logic Puzzles

Links

Puzzles that can be solved using logical reasoning are known as **logic puzzles**. Solving logic puzzles is an excellent way to practice working with the rules of logic. Also, computer programs designed to carry out logical reasoning often use well-known logic puzzles to illustrate their capabilities. Many people enjoy solving logic puzzles, published in periodicals, books, and on the Web, as a recreational activity.

We will discuss two logic puzzles here. We begin with a puzzle originally posed by Raymond Smullyan, a master of logic puzzles, who has published more than a dozen books containing challenging puzzles that involve logical reasoning. In Section 1.3 we will also discuss the extremely popular logic puzzle Sudoku.

**EXAMPLE 7**

Extra Examples

In [Sm78] Smullyan posed many puzzles about an island that has two kinds of inhabitants, knights, who always tell the truth, and their opposites, knaves, who always lie. You encounter two people $A$ and $B$. What are $A$ and $B$ if $A$ says "$B$ is a knight" and $B$ says "The two of us are opposite types?"

*Solution:* Let $p$ and $q$ be the statements that $A$ is a knight and $B$ is a knight, respectively, so that $\neg p$ and $\neg q$ are the statements that $A$ is a knave and $B$ is a knave, respectively.

We first consider the possibility that $A$ is a knight; this is the statement that $p$ is true. If $A$ is a knight, then he is telling the truth when he says that $B$ is a knight, so that $q$ is true, and $A$ and $B$ are the same type. However, if $B$ is a knight, then $B$'s statement that $A$ and $B$ are of opposite types, the statement $(p \wedge \neg q) \vee (\neg p \wedge q)$, would have to be true, which it is not, because $A$ and $B$ are both knights. Consequently, we can conclude that $A$ is not a knight, that is, that $p$ is false.

If $A$ is a knave, then because everything a knave says is false, $A$'s statement that $B$ is a knight, that is, that $q$ is true, is a lie. This means that $q$ is false and $B$ is also a knave. Furthermore, if $B$ is a knave, then $B$'s statement that $A$ and $B$ are opposite types is a lie, which is consistent with both $A$ and $B$ being knaves. We can conclude that both $A$ and $B$ are knaves. ◀

We pose more of Smullyan's puzzles about knights and knaves in Exercises 19–23. In Exercises 24–31 we introduce related puzzles where we have three types of people, knights and knaves as in this puzzle together with spies who can lie.

Next, we pose a puzzle known as the **muddy children puzzle** for the case of two children.

**EXAMPLE 8** A father tells his two children, a boy and a girl, to play in their backyard without getting dirty. However, while playing, both children get mud on their foreheads. When the children stop playing, the father says "At least one of you has a muddy forehead," and then asks the children to answer "Yes" or "No" to the question: "Do you know whether you have a muddy forehead?" The father asks this question twice. What will the children answer each time this question is asked, assuming that a child can see whether his or her sibling has a muddy forehead, but cannot see his or her own forehead? Assume that both children are honest and that the children answer each question simultaneously.

*Solution:* Let $s$ be the statement that the son has a muddy forehead and let $d$ be the statement that the daughter has a muddy forehead. When the father says that at least one of the two children has a muddy forehead, he is stating that the disjunction $s \vee d$ is true. Both children will answer "No" the first time the question is asked because each sees mud on the other child's forehead. That is, the son knows that $d$ is true, but does not know whether $s$ is true, and the daughter knows that $s$ is true, but does not know whether $d$ is true.

After the son has answered "No" to the first question, the daughter can determine that $d$ must be true. This follows because when the first question is asked, the son knows that $s \vee d$ is true, but cannot determine whether $s$ is true. Using this information, the daughter can conclude that $d$ must be true, for if $d$ were false, the son could have reasoned that because $s \vee d$ is true, then $s$ must be true, and he would have answered "Yes" to the first question. The son can reason in a similar way to determine that $s$ must be true. It follows that both children answer "Yes" the second time the question is asked. ◀

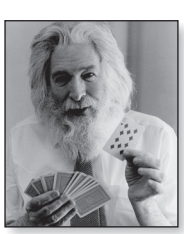
## Logic Circuits

Propositional logic can be applied to the design of computer hardware. This was first observed in 1938 by Claude Shannon in his MIT master's thesis. In Chapter 12 we will study this topic in depth. (See that chapter for a biography of Shannon.) We give a brief introduction to this application here.

A **logic circuit** (or **digital circuit**) receives input signals $p_1, p_2, \ldots, p_n$, each a bit [either 0 (off) or 1 (on)], and produces output signals $s_1, s_2, \ldots, s_n$, each a bit. In this section we will restrict our attention to logic circuits with a single output signal; in general, digital circuits may have multiple outputs.

In Chapter 12 we design some useful circuits.

Links



RAYMOND SMULLYAN (BORN 1919) Raymond Smullyan dropped out of high school. He wanted to study what he was really interested in and not standard high school material. After jumping from one university to the next, he earned an undergraduate degree in mathematics at the University of Chicago in 1955. He paid his college expenses by performing magic tricks at parties and clubs. He obtained a Ph.D. in logic in 1959 at Princeton, studying under Alonzo Church. After graduating from Princeton, he taught mathematics and logic at Dartmouth College, Princeton University, Yeshiva University, and the City University of New York. He joined the philosophy department at Indiana University in 1981 where he is now an emeritus professor.

Smullyan has written many books on recreational logic and mathematics, including *Satan, Cantor, and Infinity; What Is the Name of This Book?; The Lady or the Tiger?; Alice in Puzzleland; To Mock a Mockingbird; Forever Undecided;* and *The Riddle of Scheherazade: Amazing Logic Puzzles, Ancient and Modern*. Because his logic puzzles are challenging, entertaining, and thought-provoking, he is considered to be a modern-day Lewis Carroll. Smullyan has also written several books about the application of deductive logic to chess, three collections of philosophical essays and aphorisms, and several advanced books on mathematical logic and set theory. He is particularly interested in self-reference and has worked on extending some of Gödel's results that show that it is impossible to write a computer program that can solve all mathematical problems. He is also particularly interested in explaining ideas from mathematical logic to the public.

Smullyan is a talented musician and often plays piano with his wife, who is a concert-level pianist. Making telescopes is one of his hobbies. He is also interested in optics and stereo photography. He states "I've never had a conflict between teaching and research as some people do because when I'm teaching, I'm doing research." Smullyan is the subject of a documentary short film entitled *This Film Needs No Title*.

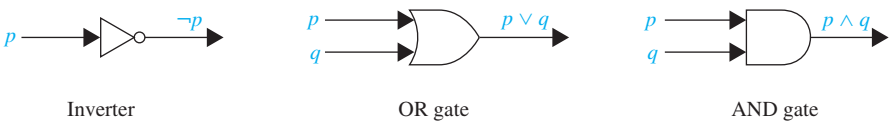



**FIGURE 1** **Basic logic gates.**

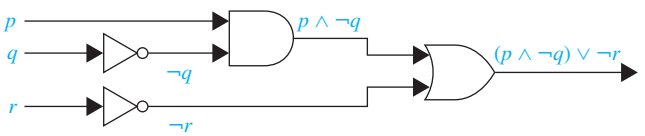



**FIGURE 2** **A combinatorial circuit.**

Complicated digital circuits can be constructed from three basic circuits, called **gates**, shown in Figure 1. The **inverter**, or **NOT gate**, takes an input bit $p$, and produces as output $\neg p$. The **OR gate** takes two input signals $p$ and $q$, each a bit, and produces as output the signal $p \vee q$. Finally, the **AND gate** takes two input signals $p$ and $q$, each a bit, and produces as output the signal $p \wedge q$. We use combinations of these three basic gates to build more complicated circuits, such as that shown in Figure 2.

Given a circuit built from the basic logic gates and the inputs to the circuit, we determine the output by tracing through the circuit, as Example 9 shows.

**EXAMPLE 9** Determine the output for the combinatorial circuit in Figure 2.

*Solution:* In Figure 2 we display the output of each logic gate in the circuit. We see that the AND gate takes input of $p$ and $\neg q$, the output of the inverter with input $q$, and produces $p \wedge \neg q$. Next, we note that the OR gate takes input $p \wedge \neg q$ and $\neg r$, the output of the inverter with input $r$, and produces the final output $(p \wedge \neg q) \vee \neg r$. ◀

Suppose that we have a formula for the output of a digital circuit in terms of negations, disjunctions, and conjunctions. Then, we can systematically build a digital circuit with the desired output, as illustrated in Example 10.

**EXAMPLE 10** Build a digital circuit that produces the output $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$ when given input bits $p$, $q$, and $r$.

*Solution:* To construct the desired circuit, we build separate circuits for $p \vee \neg r$ and for $\neg p \vee (q \vee \neg r)$ and combine them using an AND gate. To construct a circuit for $p \vee \neg r$, we use an inverter to produce $\neg r$ from the input $r$. Then, we use an OR gate to combine $p$ and $\neg r$. To build a circuit for $\neg p \vee (q \vee \neg r)$, we first use an inverter to obtain $\neg r$. Then we use an OR gate with inputs $q$ and $\neg r$ to obtain $q \vee \neg r$. Finally, we use another inverter and an OR gate to get $\neg p \vee (q \vee \neg r)$ from the inputs $p$ and $q \vee \neg r$.

To complete the construction, we employ a final AND gate, with inputs $p \vee \neg r$ and $\neg p \vee (q \vee \neg r)$. The resulting circuit is displayed in Figure 3. ◀

We will study logic circuits in great detail in Chapter 12 in the context of Boolean algebra, and with different notation.

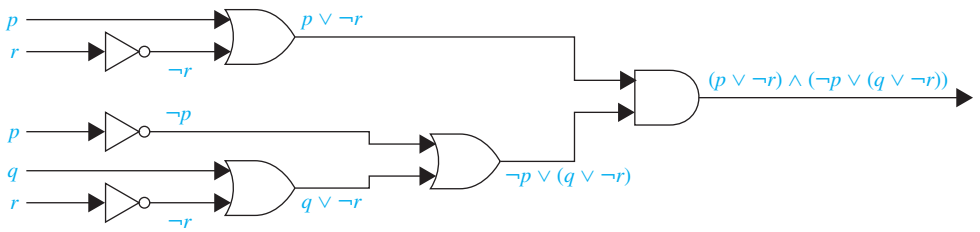



**FIGURE 3** **The circuit for $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$.**

## Exercises

In Exercises 1–6, translate the given statement into propositional logic using the propositions provided.

1. You cannot edit a protected Wikipedia entry unless you are an administrator. Express your answer in terms of $e$: "You can edit a protected Wikipedia entry" and $a$: "You are an administrator."
2. You can see the movie only if you are over 18 years old or you have the permission of a parent. Express your answer in terms of $m$: "You can see the movie," $e$: "You are over 18 years old," and $p$: "You have the permission of a parent."
3. You can graduate only if you have completed the requirements of your major and you do not owe money to the university and you do not have an overdue library book. Express your answer in terms of $g$: "You can graduate," $m$: "You owe money to the university," $r$: "You have completed the requirements of your major," and $b$: "You have an overdue library book."
4. To use the wireless network in the airport you must pay the daily fee unless you are a subscriber to the service. Express your answer in terms of $w$: "You can use the wireless network in the airport," $d$: "You pay the daily fee," and $s$: "You are a subscriber to the service."
5. You are eligible to be President of the U.S.A. only if you are at least 35 years old, were born in the U.S.A, or at the time of your birth both of your parents were citizens, and you have lived at least 14 years in the country. Express your answer in terms of $e$: "You are eligible to be President of the U.S.A.," $a$: "You are at least 35 years old," $b$: "You were born in the U.S.A," $p$: "At the time of your birth, both of your parents where citizens," and $r$: "You have lived at least 14 years in the U.S.A."
6. You can upgrade your operating system only if you have a 32-bit processor running at 1 GHz or faster, at least 1 GB RAM, and 16 GB free hard disk space, or a 64-bit processor running at 2 GHz or faster, at least 2 GB RAM, and at least 32 GB free hard disk space. Express you answer in terms of $u$: "You can upgrade your operating system," $b_{32}$: "You have a 32-bit processor," $b_{64}$: "You have a 64-bit processor," $g_1$: "Your processor runs at 1 GHz or faster," $g_2$: "Your processor runs at 2 GHz or faster," $r_1$: "Your processor has at least 1 GB RAM," $r_2$: "Your processor has at least 2 GB RAM," $h_{16}$: "You have at least 16 GB free hard disk space," and $h_{32}$: "You have at least 32 GB free hard disk space."
7. Express these system specifications using the propositions $p$ "The message is scanned for viruses" and $q$ "The message was sent from an unknown system" together with logical connectives (including negations).
   **a)** "The message is scanned for viruses whenever the message was sent from an unknown system."
   **b)** "The message was sent from an unknown system but it was not scanned for viruses."
   **c)** "It is necessary to scan the message for viruses whenever it was sent from an unknown system."
   **d)** "When a message is not sent from an unknown system it is not scanned for viruses."
8. Express these system specifications using the propositions $p$ "The user enters a valid password," $q$ "Access is granted," and $r$ "The user has paid the subscription fee" and logical connectives (including negations).
   **a)** "The user has paid the subscription fee, but does not enter a valid password."
   **b)** "Access is granted whenever the user has paid the subscription fee and enters a valid password."
   **c)** "Access is denied if the user has not paid the subscription fee."
   **d)** "If the user has not entered a valid password but has paid the subscription fee, then access is granted."
9. Are these system specifications consistent? "The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode."

**10.** Are these system specifications consistent? "Whenever the system software is being upgraded, users cannot access the file system. If users can access the file system, then they can save new files. If users cannot save new files, then the system software is not being upgraded."

**11.** Are these system specifications consistent? "The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed, The router does not support the new address space."

**12.** Are these system specifications consistent? "If the file system is not locked, then new messages will be queued. If the file system is not locked, then the system is functioning normally, and conversely. If new messages are not queued, then they will be sent to the message buffer. If the file system is not locked, then new messages will be sent to the message buffer. New messages will not be sent to the message buffer."

**13.** What Boolean search would you use to look for Web pages about beaches in New Jersey? What if you wanted to find Web pages about beaches on the isle of Jersey (in the English Channel)?

**14.** What Boolean search would you use to look for Web pages about hiking in West Virginia? What if you wanted to find Web pages about hiking in Virginia, but not in West Virginia?

***15.** Each inhabitant of a remote village always tells the truth or always lies. A villager will give only a "Yes" or a "No" response to a question a tourist asks. Suppose you are a tourist visiting this area and come to a fork in the road. One branch leads to the ruins you want to visit; the other branch leads deep into the jungle. A villager is standing at the fork in the road. What one question can you ask the villager to determine which branch to take?

**16.** An explorer is captured by a group of cannibals. There are two types of cannibals—those who always tell the truth and those who always lie. The cannibals will barbecue the explorer unless he can determine whether a particular cannibal always lies or always tells the truth. He is allowed to ask the cannibal exactly one question.

**a)** Explain why the question "Are you a liar?" does not work.

**b)** Find a question that the explorer can use to determine whether the cannibal always lies or always tells the truth.

**17.** When three professors are seated in a restaurant, the hostess asks them: "Does everyone want coffee?" The first professor says: "I do not know." The second professor then says: "I do not know." Finally, the third professor says: "No, not everyone wants coffee." The hostess comes back and gives coffee to the professors who want it. How did she figure out who wanted coffee?

**18.** When planning a party you want to know whom to invite. Among the people you would like to invite are three touchy friends. You know that if Jasmine attends, she will become unhappy if Samir is there, Samir will attend only if Kanti will be there, and Kanti will not attend unless Jasmine also does. Which combinations of these three friends can you invite so as not to make someone unhappy?

Exercises 19–23 relate to inhabitants of the island of knights and knaves created by Smullyan, where knights always tell the truth and knaves always lie. You encounter two people, $A$ and $B$. Determine, if possible, what $A$ and $B$ are if they address you in the ways described. If you cannot determine what these two people are, can you draw any conclusions?

**19.** $A$ says "At least one of us is a knave" and $B$ says nothing.

**20.** $A$ says "The two of us are both knights" and $B$ says "$A$ is a knave."

**21.** $A$ says "I am a knave or $B$ is a knight" and $B$ says nothing.

**22.** Both $A$ and $B$ say "I am a knight."

**23.** $A$ says "We are both knaves" and $B$ says nothing.

Exercises 24–31 relate to inhabitants of an island on which there are three kinds of people: knights who always tell the truth, knaves who always lie, and spies (called normals by Smullyan [Sm78]) who can either lie or tell the truth. You encounter three people, $A$, $B$, and $C$. You know one of these people is a knight, one is a knave, and one is a spy. Each of the three people knows the type of person each of other two is. For each of these situations, if possible, determine whether there is a unique solution and determine who the knave, knight, and spy are. When there is no unique solution, list all possible solutions or state that there are no solutions.

**24.** $A$ says "$C$ is the knave," $B$ says, "$A$ is the knight," and $C$ says "I am the spy."

**25.** $A$ says "I am the knight," $B$ says "I am the knave," and $C$ says "$B$ is the knight."

**26.** $A$ says "I am the knave," $B$ says "I am the knave," and $C$ says "I am the knave."

**27.** $A$ says "I am the knight," $B$ says "$A$ is telling the truth," and $C$ says "I am the spy."

**28.** $A$ says "I am the knight," $B$ says, "$A$ is not the knave," and $C$ says "$B$ is not the knave."

**29.** $A$ says "I am the knight," $B$ says "I am the knight," and $C$ says "I am the knight."

**30.** $A$ says "I am not the spy," $B$ says "I am not the spy," and $C$ says "$A$ is the spy."

**31.** $A$ says "I am not the spy," $B$ says "I am not the spy," and $C$ says "I am not the spy."

Exercises 32–38 are puzzles that can be solved by translating statements into logical expressions and reasoning from these expressions using truth tables.

**32.** The police have three suspects for the murder of Mr. Cooper: Mr. Smith, Mr. Jones, and Mr. Williams. Smith, Jones, and Williams each declare that they did not kill Cooper. Smith also states that Cooper was a friend of Jones and that Williams disliked him. Jones also states that he did not know Cooper and that he was out of town the day Cooper was killed. Williams also states that he

saw both Smith and Jones with Cooper the day of the killing and that either Smith or Jones must have killed him. Can you determine who the murderer was if

**a)** one of the three men is guilty, the two innocent men are telling the truth, but the statements of the guilty man may or may not be true?

**b)** innocent men do not lie?

**33.** Steve would like to determine the relative salaries of three coworkers using two facts. First, he knows that if Fred is not the highest paid of the three, then Janice is. Second, he knows that if Janice is not the lowest paid, then Maggie is paid the most. Is it possible to determine the relative salaries of Fred, Maggie, and Janice from what Steve knows? If so, who is paid the most and who the least? Explain your reasoning.

**34.** Five friends have access to a chat room. Is it possible to determine who is chatting if the following information is known? Either Kevin or Heather, or both, are chatting. Either Randy or Vijay, but not both, are chatting. If Abby is chatting, so is Randy. Vijay and Kevin are either both chatting or neither is. If Heather is chatting, then so are Abby and Kevin. Explain your reasoning.

**35.** A detective has interviewed four witnesses to a crime. From the stories of the witnesses the detective has concluded that if the butler is telling the truth then so is the cook; the cook and the gardener cannot both be telling the truth; the gardener and the handyman are not both lying; and if the handyman is telling the truth then the cook is lying. For each of the four witnesses, can the detective determine whether that person is telling the truth or lying? Explain your reasoning.

**36.** Four friends have been identified as suspects for an unauthorized access into a computer system. They have made statements to the investigating authorities. Alice said "Carlos did it." John said "I did not do it." Carlos said "Diana did it." Diana said "Carlos lied when he said that I did it."

**a)** If the authorities also know that exactly one of the four suspects is telling the truth, who did it? Explain your reasoning.

**b)** If the authorities also know that exactly one is lying, who did it? Explain your reasoning.

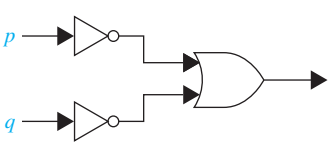
**37.** Suppose there are signs on the doors to two rooms. The sign on the first door reads "In this room there is a lady, and in the other one there is a tiger"; and the sign on the second door reads "In one of these rooms, there is a lady, and in one of them there is a tiger." Suppose that you know that one of these signs is true and the other is false. Behind which door is the lady?

***38.** Solve this famous logic puzzle, attributed to Albert Einstein, and known as the **zebra puzzle**. Five men with different nationalities and with different jobs live in consecutive houses on a street. These houses are painted different colors. The men have different pets and have different favorite drinks. Determine who owns a zebra and whose favorite drink is mineral water (which is one of the favorite drinks) given these clues: The Englishman lives in the red house. The Spaniard owns a dog. The Japanese man is a painter. The Italian drinks tea. The Norwegian lives in the first house on the left. The green house is immediately to the right of the white one. The photographer breeds snails. The diplomat lives in the yellow house. Milk is drunk in the middle house. The owner of the green house drinks coffee. The Norwegian's house is next to the blue one. The violinist drinks orange juice. The fox is in a house next to that of the physician. The horse is in a house next to that of the diplomat. [*Hint:* Make a table where the rows represent the men and columns represent the color of their houses, their jobs, their pets, and their favorite drinks and use logical reasoning to determine the correct entries in the table.]

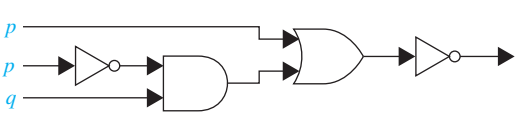
**39.** Freedonia has fifty senators. Each senator is either honest or corrupt. Suppose you know that at least one of the Freedonian senators is honest and that, given any two Freedonian senators, at least one is corrupt. Based on these facts, can you determine how many Freedonian senators are honest and how many are corrupt? If so, what is the answer?

**40.** Find the output of each of these combinatorial circuits.

a)

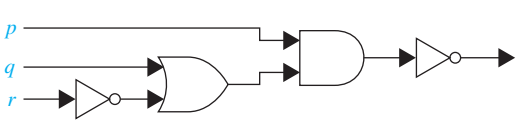



b)

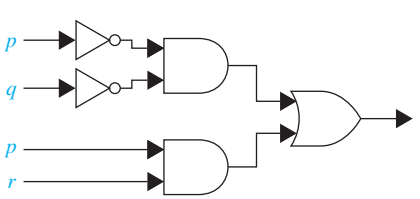



**41.** Find the output of each of these combinatorial circuits.

a)




b)




**42.** Construct a combinatorial circuit using inverters, OR gates, and AND gates that produces the output $(p \wedge \neg r) \vee (\neg q \wedge r)$ from input bits $p$, $q$, and $r$.

**43.** Construct a combinatorial circuit using inverters, OR gates, and AND gates that produces the output $((\neg p \vee \neg r) \wedge \neg q) \vee (\neg p \wedge (q \vee r))$ from input bits $p$, $q$, and $r$.

# 1.3 Propositional Equivalences

## Introduction

An important type of step used in a mathematical argument is the replacement of a statement with another statement with the same truth value. Because of this, methods that produce propositions with the same truth value as a given compound proposition are used extensively in the construction of mathematical arguments. Note that we will use the term "compound proposition" to refer to an expression formed from propositional variables using logical operators, such as $p \wedge q$.

We begin our discussion with a classification of compound propositions according to their possible truth values.

**DEFINITION 1**

A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a *tautology*. A compound proposition that is always false is called a *contradiction*. A compound proposition that is neither a tautology nor a contradiction is called a *contingency*.

Tautologies and contradictions are often important in mathematical reasoning. Example 1 illustrates these types of compound propositions.

**EXAMPLE 1** We can construct examples of tautologies and contradictions using just one propositional variable. Consider the truth tables of $p \vee \neg p$ and $p \wedge \neg p$, shown in Table 1. Because $p \vee \neg p$ is always true, it is a tautology. Because $p \wedge \neg p$ is always false, it is a contradiction. ◀

## Logical Equivalences

Demo

Compound propositions that have the same truth values in all possible cases are called **logically equivalent**. We can also define this notion as follows.

**DEFINITION 2**

The compound propositions $p$ and $q$ are called *logically equivalent* if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that $p$ and $q$ are logically equivalent.

***Remark:*** The symbol $\equiv$ is not a logical connective, and $p \equiv q$ is not a compound proposition but rather is the statement that $p \leftrightarrow q$ is a tautology. The symbol $\Leftrightarrow$ is sometimes used instead of $\equiv$ to denote logical equivalence.

One way to determine whether two compound propositions are equivalent is to use a truth table. In particular, the compound propositions $p$ and $q$ are equivalent if and only if the columns

**TABLE 1 Examples of a Tautology and a Contradiction.**

| $p$ | $\neg p$ | $p \vee \neg p$ | $p \wedge \neg p$ |
|---|---|---|---|
| T | F | T | F |
| F | T | T | F |

**TABLE 2 De Morgan's Laws.**

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

Extra Examples

giving their truth values agree. Example 2 illustrates this method to establish an extremely important and useful logical equivalence, namely, that of $\neg(p \vee q)$ with $\neg p \wedge \neg q$. This logical equivalence is one of the two **De Morgan laws**, shown in Table 2, named after the English mathematician Augustus De Morgan, of the mid-nineteenth century.

**EXAMPLE 2** Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

*Solution:* The truth tables for these compound propositions are displayed in Table 3. Because the truth values of the compound propositions $\neg(p \vee q)$ and $\neg p \wedge \neg q$ agree for all possible combinations of the truth values of $p$ and $q$, it follows that $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ is a tautology and that these compound propositions are logically equivalent. ◀

**TABLE 3 Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$.**

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

**EXAMPLE 3** Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

*Solution:* We construct the truth table for these compound propositions in Table 4. Because the truth values of $\neg p \vee q$ and $p \rightarrow q$ agree, they are logically equivalent. ◀

**TABLE 4 Truth Tables for $\neg p \vee q$ and $p \rightarrow q$.**

| $p$ | $q$ | $\neg p$ | $\neg p \vee q$ | $p \rightarrow q$ |
|---|---|---|---|---|
| T | T | F | T | T |
| T | F | F | F | F |
| F | T | T | T | T |
| F | F | T | T | T |

We will now establish a logical equivalence of two compound propositions involving three different propositional variables $p$, $q$, and $r$. To use a truth table to establish such a logical equivalence, we need eight rows, one for each possible combination of truth values of these three variables. We symbolically represent these combinations by listing the truth values of $p$, $q$, and $r$, respectively. These eight combinations of truth values are TTT, TTF, TFT, TFF, FTT, FTF, FFT, and FFF; we use this order when we display the rows of the truth table. Note that we need to double the number of rows in the truth tables we use to show that compound propositions are equivalent for each additional propositional variable, so that 16 rows are needed to establish the logical equivalence of two compound propositions involving four propositional variables, and so on. In general, $2^n$ rows are required if a compound proposition involves $n$ propositional variables.

**TABLE 5** **A Demonstration That $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ Are Logically Equivalent.**

| $p$ | $q$ | $r$ | $q \wedge r$ | $p \vee (q \wedge r)$ | $p \vee q$ | $p \vee r$ | $(p \vee q) \wedge (p \vee r)$ |
|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T |
| T | T | F | F | T | T | T | T |
| T | F | T | F | T | T | T | T |
| T | F | F | F | T | T | T | T |
| F | T | T | T | T | T | T | T |
| F | T | F | F | F | T | F | F |
| F | F | T | F | F | F | T | F |
| F | F | F | F | F | F | F | F |

**EXAMPLE 4** Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent. This is the *distributive law* of disjunction over conjunction.

*Solution:* We construct the truth table for these compound propositions in Table 5. Because the truth values of $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ agree, these compound propositions are logically equivalent. ◀

The identities in Table 6 are a special case of Boolean algebra identities found in Table 5 of Section 12.1. See Table 1 in Section 2.2 for analogous set identities.

Table 6 contains some important equivalences. In these equivalences, **T** denotes the compound proposition that is always true and **F** denotes the compound proposition that is always

**TABLE 6** **Logical Equivalences.**

| *Equivalence* | *Name* |
|---|---|
| $p \wedge \mathbf{T} \equiv p$<br>$p \vee \mathbf{F} \equiv p$ | Identity laws |
| $p \vee \mathbf{T} \equiv \mathbf{T}$<br>$p \wedge \mathbf{F} \equiv \mathbf{F}$ | Domination laws |
| $p \vee p \equiv p$<br>$p \wedge p \equiv p$ | Idempotent laws |
| $\neg(\neg p) \equiv p$ | Double negation law |
| $p \vee q \equiv q \vee p$<br>$p \wedge q \equiv q \wedge p$ | Commutative laws |
| $(p \vee q) \vee r \equiv p \vee (q \vee r)$<br>$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | Associative laws |
| $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$<br>$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | Distributive laws |
| $\neg(p \wedge q) \equiv \neg p \vee \neg q$<br>$\neg(p \vee q) \equiv \neg p \wedge \neg q$ | De Morgan's laws |
| $p \vee (p \wedge q) \equiv p$<br>$p \wedge (p \vee q) \equiv p$ | Absorption laws |
| $p \vee \neg p \equiv \mathbf{T}$<br>$p \wedge \neg p \equiv \mathbf{F}$ | Negation laws |

**TABLE 7 Logical Equivalences Involving Conditional Statements.**

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

**TABLE 8 Logical Equivalences Involving Biconditional Statements.**

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

false. We also display some useful equivalences for compound propositions involving conditional statements and biconditional statements in Tables 7 and 8, respectively. The reader is asked to verify the equivalences in Tables 6–8 in the exercises.

The associative law for disjunction shows that the expression $p \vee q \vee r$ is well defined, in the sense that it does not matter whether we first take the disjunction of $p$ with $q$ and then the disjunction of $p \vee q$ with $r$, or if we first take the disjunction of $q$ and $r$ and then take the disjunction of $p$ with $q \vee r$. Similarly, the expression $p \wedge q \wedge r$ is well defined. By extending this reasoning, it follows that $p_1 \vee p_2 \vee \cdots \vee p_n$ and $p_1 \wedge p_2 \wedge \cdots \wedge p_n$ are well defined whenever $p_1, p_2, \ldots, p_n$ are propositions.

Furthermore, note that De Morgan's laws extend to

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n)$$

and

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv (\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n).$$

We will sometimes use the notation $\bigvee_{j=1}^{n} p_j$ for $p_1 \vee p_2 \vee \cdots \vee p_n$ and $\bigwedge_{j=1}^{n} p_j$ for $p_1 \wedge p_2 \wedge \cdots \wedge p_n$. Using this notation, the extended version of De Morgan's laws can be written concisely as $\neg\left(\bigvee_{j=1}^{n} p_j\right) \equiv \bigwedge_{j=1}^{n} \neg p_j$ and $\neg\left(\bigwedge_{j=1}^{n} p_j\right) \equiv \bigvee_{j=1}^{n} \neg p_j$. (Methods for proving these identities will be given in Section 5.1.)

## Using De Morgan's Laws

When using De Morgan's laws, remember to change the logical connective after you negate.

The two logical equivalences known as De Morgan's laws are particularly important. They tell us how to negate conjunctions and how to negate disjunctions. In particular, the equivalence $\neg(p \vee q) \equiv \neg p \wedge \neg q$ tells us that the negation of a disjunction is formed by taking the conjunction of the negations of the component propositions. Similarly, the equivalence $\neg(p \wedge q) \equiv \neg p \vee \neg q$ tells us that the negation of a conjunction is formed by taking the disjunction of the negations of the component propositions. Example 5 illustrates the use of De Morgan's laws.

**EXAMPLE 5** Use De Morgan's laws to express the negations of "Miguel has a cellphone and he has a laptop computer" and "Heather will go to the concert or Steve will go to the concert."

Assessment

*Solution:* Let $p$ be "Miguel has a cellphone" and $q$ be "Miguel has a laptop computer." Then "Miguel has a cellphone and he has a laptop computer" can be represented by $p \wedge q$. By the first of De Morgan's laws, $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$. Consequently, we can express the negation of our original statement as "Miguel does not have a cellphone or he does not have a laptop computer."

Let $r$ be "Heather will go to the concert" and $s$ be "Steve will go to the concert." Then "Heather will go to the concert or Steve will go to the concert" can be represented by $r \vee s$. By the second of De Morgan's laws, $\neg(r \vee s)$ is equivalent to $\neg r \wedge \neg s$. Consequently, we can express the negation of our original statement as "Heather will not go to the concert and Steve will not go to the concert." ◀

## Constructing New Logical Equivalences

The logical equivalences in Table 6, as well as any others that have been established (such as those shown in Tables 7 and 8), can be used to construct additional logical equivalences. The reason for this is that a proposition in a compound proposition can be replaced by a compound proposition that is logically equivalent to it without changing the truth value of the original compound proposition. This technique is illustrated in Examples 6–8, where we also use the fact that if $p$ and $q$ are logically equivalent and $q$ and $r$ are logically equivalent, then $p$ and $r$ are logically equivalent (see Exercise 56).

**EXAMPLE 6** Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent.

Extra Examples

*Solution:* We could use a truth table to show that these compound propositions are equivalent (similar to what we did in Example 4). Indeed, it would not be hard to do so. However, we want to illustrate how to use logical identities that we already know to establish new logical identities, something that is of practical importance for establishing equivalences of compound propositions with a large number of variables. So, we will establish this equivalence by developing a series of

Links

AUGUSTUS DE MORGAN (1806–1871) Augustus De Morgan was born in India, where his father was a colonel in the Indian army. De Morgan's family moved to England when he was 7 months old. He attended private schools, where in his early teens he developed a strong interest in mathematics. De Morgan studied at Trinity College, Cambridge, graduating in 1827. Although he considered medicine or law, he decided on mathematics for his career. He won a position at University College, London, in 1828, but resigned after the college dismissed a fellow professor without giving reasons. However, he resumed this position in 1836 when his successor died, remaining until 1866.

De Morgan was a noted teacher who stressed principles over techniques. His students included many famous mathematicians, including Augusta Ada, Countess of Lovelace, who was Charles Babbage's collaborator in his work on computing machines (see page 31 for biographical notes on Augusta Ada). (De Morgan cautioned the countess against studying too much mathematics, because it might interfere with her childbearing abilities!)

De Morgan was an extremely prolific writer, publishing more than 1000 articles in more than 15 periodicals. De Morgan also wrote textbooks on many subjects, including logic, probability, calculus, and algebra. In 1838 he presented what was perhaps the first clear explanation of an important proof technique known as *mathematical induction* (discussed in Section 5.1 of this text), a term he coined. In the 1840s De Morgan made fundamental contributions to the development of symbolic logic. He invented notations that helped him prove propositional equivalences, such as the laws that are named after him. In 1842 De Morgan presented what is considered to be the first precise definition of a limit and developed new tests for convergence of infinite series. De Morgan was also interested in the history of mathematics and wrote biographies of Newton and Halley.

In 1837 De Morgan married Sophia Frend, who wrote his biography in 1882. De Morgan's research, writing, and teaching left little time for his family or social life. Nevertheless, he was noted for his kindness, humor, and wide range of knowledge.

logical equivalences, using one of the equivalences in Table 6 at a time, starting with $\neg(p \rightarrow q)$ and ending with $p \wedge \neg q$. We have the following equivalences.

$$\begin{aligned}
\neg(p \rightarrow q) &\equiv \neg(\neg p \vee q) && \text{by Example 3} \\
&\equiv \neg(\neg p) \wedge \neg q && \text{by the second De Morgan law} \\
&\equiv p \wedge \neg q && \text{by the double negation law}
\end{aligned}$$

◀

**EXAMPLE 7** Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.

*Solution:* We will use one of the equivalences in Table 6 at a time, starting with $\neg(p \vee (\neg p \wedge q))$ and ending with $\neg p \wedge \neg q$. (*Note:* we could also easily establish this equivalence using a truth table.) We have the following equivalences.

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
&\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] && \text{by the first De Morgan law} \\
&\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
&\equiv \mathbf{F} \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv \mathbf{F} \\
&\equiv (\neg p \wedge \neg q) \vee \mathbf{F} && \text{by the commutative law for disjunction} \\
&\equiv \neg p \wedge \neg q && \text{by the identity law for } \mathbf{F}
\end{aligned}$$

Consequently $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent. ◀

**EXAMPLE 8** Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

*Solution:* To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to $\mathbf{T}$. (*Note:* This could also be done using a truth table.)

$$\begin{aligned}
(p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) && \text{by Example 3} \\
&\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{by the first De Morgan law} \\
&\equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{by the associative and commutative laws for disjunction} \\
&\equiv \mathbf{T} \vee \mathbf{T} && \text{by Example 1 and the commutative law for disjunction} \\
&\equiv \mathbf{T} && \text{by the domination law}
\end{aligned}$$

◀

## Propositional Satisfiability

A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true. When no such assignments exists, that is, when the compound proposition is false for all assignments of truth values to its variables, the compound proposition is **unsatisfiable**. Note that a compound proposition is unsatisfiable if and only if its negation is true for all assignments of truth values to the variables, that is, if and only if its negation is a tautology.

When we find a particular assignment of truth values that makes a compound proposition true, we have shown that it is satisfiable; such an assignment is called a **solution** of this particular

satisfiability problem. However, to show that a compound proposition is unsatisfiable, we need to show that *every* assignment of truth values to its variables makes it false. Although we can always use a truth table to determine whether a compound proposition is satisfiable, it is often more efficient not to, as Example 9 demonstrates.

**EXAMPLE 9** Determine whether each of the compound propositions $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$, and $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable.

*Solution:* Instead of using truth table to solve this problem, we will reason about truth values. Note that $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ is true when the three variable $p$, $q$, and $r$ have the same truth value (see Exercise 40 of Section 1.1). Hence, it is satisfiable as there is at least one assignment of truth values for $p$, $q$, and $r$ that makes it true. Similarly, note that $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is true when at least one of $p$, $q$, and $r$ is true and at least one is false (see Exercise 41 of Section 1.1). Hence, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable, as there is at least one assignment of truth values for $p$, $q$, and $r$ that makes it true.

Finally, note that for $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ to be true, $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ and $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ must both be true. For the first to be true, the three variables must have the same truth values, and for the second to be true, at least one of three variables must be true and at least one must be false. However, these conditions are contradictory. From these observations we conclude that no assignment of truth values to $p$, $q$, and $r$ makes $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ true. Hence, it is unsatisfiable. ◀

**Links**

AUGUSTA ADA, COUNTESS OF LOVELACE (1815–1852) Augusta Ada was the only child from the marriage of the famous poet Lord Byron and Lady Byron, Annabella Millbanke, who separated when Ada was 1 month old, because of Lord Byron's scandalous affair with his half sister. The Lord Byron had quite a reputation, being described by one of his lovers as "mad, bad, and dangerous to know." Lady Byron was noted for her intellect and had a passion for mathematics; she was called by Lord Byron "The Princess of Parallelograms." Augusta was raised by her mother, who encouraged her intellectual talents especially in music and mathematics, to counter what Lady Byron considered dangerous poetic tendencies. At this time, women were not allowed to attend universities and could not join learned societies. Nevertheless, Augusta pursued her mathematical studies independently and with mathematicians, including William Frend. She was also encouraged by another female mathematician, Mary Somerville, and in 1834 at a dinner party hosted by Mary Somerville, she learned about Charles Babbage's ideas for a calculating machine, called the Analytic Engine. In 1838 Augusta Ada married Lord King, later elevated to Earl of Lovelace. Together they had three children.

Augusta Ada continued her mathematical studies after her marriage. Charles Babbage had continued work on his Analytic Engine and lectured on this in Europe. In 1842 Babbage asked Augusta Ada to translate an article in French describing Babbage's invention. When Babbage saw her translation, he suggested she add her own notes, and the resulting work was three times the length of the original. The most complete accounts of the Analytic Engine are found in Augusta Ada's notes. In her notes, she compared the working of the Analytic Engine to that of the Jacquard loom, with Babbage's punch cards analogous to the cards used to create patterns on the loom. Furthermore, she recognized the promise of the machine as a general purpose computer much better than Babbage did. She stated that the "engine is the material expression of any indefinite function of any degree of generality and complexity." Her notes on the Analytic Engine anticipate many future developments, including computer-generated music. Augusta Ada published her writings under her initials A.A.L. concealing her identity as a woman as did many women at a time when women were not considered to be the intellectual equals of men. After 1845 she and Babbage worked toward the development of a system to predict horse races. Unfortunately, their system did not work well, leaving Augusta Ada heavily in debt at the time of her death at an unfortunately young age from uterine cancer.

In 1953 Augusta Ada's notes on the Analytic Engine were republished more than 100 years after they were written, and after they had been long forgotten. In his work in the 1950s on the capacity of computers to think (and his famous Turing Test), Alan Turing responded to Augusta Ada's statement that "The Analytic Engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform." This "dialogue" between Turing and Augusta Ada is still the subject of controversy. Because of her fundamental contributions to computing, the programming language Ada is named in honor of the Countess of Lovelace.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 2 | 9 | | | | 4 | | |
| | | | 5 | | | 1 | | |
| | 4 | | | | | | | |
| | | | | 4 | 2 | | | |
| 6 | | | | | | | 7 | |
| 5 | | | | | | | | |
| 7 | | | 3 | | | | | 5 |
| | 1 | | | 9 | | | | |
| | | | | | | | 6 | |

**FIGURE 1** **A 9 × 9 Sudoku puzzle.**

## Applications of Satisfiability

Many problems, in diverse areas such as robotics, software testing, computer-aided design, machine vision, integrated circuit design, computer networking, and genetics, can be modeled in terms of propositional satisfiability. Although most of these applications are beyond the scope of this book, we will study one application here. In particular, we will show how to use propositional satisfiability to model Sudoku puzzles.

SUDOKU A **Sudoku puzzle** is represented by a $9 \times 9$ grid made up of nine $3 \times 3$ subgrids, known as **blocks**, as shown in Figure 1. For each puzzle, some of the 81 cells, called **givens**, are assigned one of the numbers $1, 2, \ldots, 9$, and the other cells are blank. The puzzle is solved by assigning a number to each blank cell so that every row, every column, and every one of the nine $3 \times 3$ blocks contains each of the nine possible numbers. Note that instead of using a $9 \times 9$ grid, Sudoku puzzles can be based on $n^2 \times n^2$ grids, for any positive integer $n$, with the $n^2 \times n^2$ grid made up of $n^2$ $n \times n$ subgrids.

Links

The popularity of Sudoku dates back to the 1980s when it was introduced in Japan. It took 20 years for Sudoku to spread to rest of the world, but by 2005, Sudoku puzzles were a worldwide craze. The name Sudoku is short for the Japanese *suuji wa dokushin ni kagiru*, which means "the digits must remain single." The modern game of Sudoku was apparently designed in the late 1970s by an American puzzle designer. The basic ideas of Sudoku date back even further; puzzles printed in French newspapers in the 1890s were quite similar, but not identical, to modern Sudoku.

Sudoku puzzles designed for entertainment have two additional important properties. First, they have exactly one solution. Second, they can be solved using reasoning alone, that is, without resorting to searching all possible assignments of numbers to the cells. As a Sudoku puzzle is solved, entries in blank cells are successively determined by already known values. For instance, in the grid in Figure 1, the number 4 must appear in exactly one cell in the second row. How can we determine which of the seven blank cells it must appear? First, we observe that 4 cannot appear in one of the first three cells or in one of the last three cells of this row, because it already appears in another cell in the block each of these cells is in. We can also see that 4 cannot appear in the fifth cell in this row, as it already appears in the fifth column in the fourth row. This means that 4 must appear in the sixth cell of the second row.

Many strategies based on logic and mathematics have been devised for solving Sudoku puzzles (see [Da10], for example). Here, we discuss one of the ways that have been developed for solving Sudoku puzzles with the aid of a computer, which depends on modeling the puzzle as a propositional satisfiability problem. Using the model we describe, particular Sudoku puzzles can be solved using software developed to solve satisfiability problems. Currently, Sudoku puzzles can be solved in less than 10 milliseconds this way. It should be noted that there are many other approaches for solving Sudoku puzzles via computers using other techniques.

To encode a Sudoku puzzle, let $p(i, j, n)$ denote the proposition that is true when the number $n$ is in the cell in the $i$th row and $j$th column. There are $9 \times 9 \times 9 = 729$ such propositions, as $i$, $j$, and $n$ all range from 1 to 9. For example, for the puzzle in Figure 1, the number 6 is given as the value in the fifth row and first column. Hence, we see that $p(5, 1, 6)$ is true, but $p(5, j, 6)$ is false for $j = 2, 3, \ldots, 9$.

Given a particular Sudoku puzzle, we begin by encoding each of the given values. Then, we construct compound propositions that assert that every row contains every number, every column contains every number, every $3 \times 3$ block contains every number, and each cell contains no more than one number. It follows, as the reader should verify, that the Sudoku puzzle is solved by finding an assignment of truth values to the 729 propositions $p(i, j, n)$ with $i$, $j$, and $n$ each ranging from 1 to 9 that makes the conjunction of all these compound propositions true. After listing these assertions, we will explain how to construct the assertion that every row contains every integer from 1 to 9. We will leave the construction of the other assertions that every column contains every number and each of the nine $3 \times 3$ blocks contains every number to the exercises.

- For each cell with a given value, we assert $p(i, j, n)$ when the cell in row $i$ and column $j$ has the given value $n$.
- We assert that every row contains every number:

$$\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$$

- We assert that every column contains every number:

$$\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$$

It is tricky setting up the two inner indices so that all nine cells in each square block are examined.

- We assert that each of the nine $3 \times 3$ blocks contains every number:

$$\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r + i, 3s + j, n)$$

- To assert that no cell contains more than one number, we take the conjunction over all values of $n, n', i$, and $j$ where each variable ranges from 1 to 9 and $n \neq n'$ of $p(i, j, n) \rightarrow \neg p(i, j, n')$.

We now explain how to construct the assertion that every row contains every number. First, to assert that row $i$ contains the number $n$, we form $\bigvee_{j=1}^{9} p(i, j, n)$. To assert that row $i$ contains all $n$ numbers, we form the conjunction of these disjunctions over all nine possible values of $n$, giving us $\bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$. Finally, to assert that every row contains every number, we take the conjunction of $\bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$ over all nine rows. This gives us $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$. (Exercises 65 and 66 ask for explanations of the assertions that every column contains every number and that each of the nine $3 \times 3$ blocks contains every number.)

Given a particular Sudoku puzzle, to solve this puzzle we can find a solution to the satisfiability problems that asks for a set of truth values for the 729 variables $p(i, j, n)$ that makes the conjunction of all the listed assertions true.

## Solving Satisfiability Problems

A truth table can be used to determine whether a compound proposition is satisfiable, or equivalently, whether its negation is a tautology (see Exercise 60). This can be done by hand for a compound proposition with a small number of variables, but when the number of variables grows, this becomes impractical. For instance, there are $2^{20} = 1{,}048{,}576$ rows in the truth table for a compound proposition with 20 variables. Clearly, you need a computer to help you determine, in this way, whether a compound proposition in 20 variables is satisfiable.

When many applications are modeled, questions concerning the satisfiability of compound propositions with hundreds, thousands, or millions of variables arise. Note, for example, that when there are 1000 variables, checking every one of the $2^{1000}$ (a number with more than 300 decimal digits) possible combinations of truth values of the variables in a compound proposition cannot be done by a computer in even trillions of years. No procedure is known that a computer can follow to determine in a reasonable amount of time whether an arbitrary compound proposition in such a large number of variables is satisfiable. However, progress has been made developing methods for solving the satisfiability problem for the particular types of compound propositions that arise in practical applications, such as for the solution of Sudoku puzzles. Many computer programs have been developed for solving satisfiability problems which have practical use. In our discussion of the subject of algorithms in Chapter 3, we will discuss this question further. In particular, we will explain the important role the propositional satisfiability problem plays in the study of the complexity of algorithms.

Links

## Exercises

**1.** Use truth tables to verify these equivalences.
- **a)** $p \wedge \mathbf{T} \equiv p$
- **b)** $p \vee \mathbf{F} \equiv p$
- **c)** $p \wedge \mathbf{F} \equiv \mathbf{F}$
- **d)** $p \vee \mathbf{T} \equiv \mathbf{T}$
- **e)** $p \vee p \equiv p$
- **f)** $p \wedge p \equiv p$

**2.** Show that $\neg(\neg p)$ and $p$ are logically equivalent.

**3.** Use truth tables to verify the commutative laws
- **a)** $p \vee q \equiv q \vee p$.
- **b)** $p \wedge q \equiv q \wedge p$.

**4.** Use truth tables to verify the associative laws
- **a)** $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
- **b)** $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

**5.** Use a truth table to verify the distributive law $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

**6.** Use a truth table to verify the first De Morgan law $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

**7.** Use De Morgan's laws to find the negation of each of the following statements.
- **a)** Jan is rich and happy.
- **b)** Carlos will bicycle or run tomorrow.

Links

HENRY MAURICE SHEFFER (1883–1964) Henry Maurice Sheffer, born to Jewish parents in the western Ukraine, emigrated to the United States in 1892 with his parents and six siblings. He studied at the Boston Latin School before entering Harvard, where he completed his undergraduate degree in 1905, his master's in 1907, and his Ph.D. in philosophy in 1908. After holding a postdoctoral position at Harvard, Henry traveled to Europe on a fellowship. Upon returning to the United States, he became an academic nomad, spending one year each at the University of Washington, Cornell, the University of Minnesota, the University of Missouri, and City College in New York. In 1916 he returned to Harvard as a faculty member in the philosophy department. He remained at Harvard until his retirement in 1952.

Sheffer introduced what is now known as the Sheffer stroke in 1913; it became well known only after its use in the 1925 edition of Whitehead and Russell's *Principia Mathematica*. In this same edition Russell wrote that Sheffer had invented a powerful method that could be used to simplify the *Principia*. Because of this comment, Sheffer was something of a mystery man to logicians, especially because Sheffer, who published little in his career, never published the details of this method, only describing it in mimeographed notes and in a brief published abstract.

Sheffer was a dedicated teacher of mathematical logic. He liked his classes to be small and did not like auditors. When strangers appeared in his classroom, Sheffer would order them to leave, even his colleagues or distinguished guests visiting Harvard. Sheffer was barely five feet tall; he was noted for his wit and vigor, as well as for his nervousness and irritability. Although widely liked, he was quite lonely. He is noted for a quip he spoke at his retirement: "Old professors never die, they just become emeriti." Sheffer is also credited with coining the term "Boolean algebra" (the subject of Chapter 12 of this text). Sheffer was briefly married and lived most of his later life in small rooms at a hotel packed with his logic books and vast files of slips of paper he used to jot down his ideas. Unfortunately, Sheffer suffered from severe depression during the last two decades of his life.

**c)** Mei walks or takes the bus to class.
**d)** Ibrahim is smart and hard working.

**8.** Use De Morgan's laws to find the negation of each of the following statements.
**a)** Kwame will take a job in industry or go to graduate school.
**b)** Yoshiko knows Java and calculus.
**c)** James is young and strong.
**d)** Rita will move to Oregon or Washington.

☞ **9.** Show that each of these conditional statements is a tautology by using truth tables.
**a)** $(p \wedge q) \rightarrow p$ **b)** $p \rightarrow (p \vee q)$
**c)** $\neg p \rightarrow (p \rightarrow q)$ **d)** $(p \wedge q) \rightarrow (p \rightarrow q)$
**e)** $\neg(p \rightarrow q) \rightarrow p$ **f)** $\neg(p \rightarrow q) \rightarrow \neg q$

☞ **10.** Show that each of these conditional statements is a tautology by using truth tables.
**a)** $[\neg p \wedge (p \vee q)] \rightarrow q$
**b)** $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
**c)** $[p \wedge (p \rightarrow q)] \rightarrow q$
**d)** $[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$

**11.** Show that each conditional statement in Exercise 9 is a tautology without using truth tables.

**12.** Show that each conditional statement in Exercise 10 is a tautology without using truth tables.

**13.** Use truth tables to verify the absorption laws.
**a)** $p \vee (p \wedge q) \equiv p$ **b)** $p \wedge (p \vee q) \equiv p$

**14.** Determine whether $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$ is a tautology.

☞ **15.** Determine whether $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is a tautology.

Each of Exercises 16–28 asks you to show that two compound propositions are logically equivalent. To do this, either show that both sides are true, or that both sides are false, for exactly the same combinations of truth values of the propositional variables in these expressions (whichever is easier).

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

**17.** Show that $\neg(p \leftrightarrow q)$ and $p \leftrightarrow \neg q$ are logically equivalent.

**18.** Show that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are logically equivalent.

**19.** Show that $\neg p \leftrightarrow q$ and $p \leftrightarrow \neg q$ are logically equivalent.

**20.** Show that $\neg(p \oplus q)$ and $p \leftrightarrow q$ are logically equivalent.

**21.** Show that $\neg(p \leftrightarrow q)$ and $\neg p \leftrightarrow q$ are logically equivalent.

**22.** Show that $(p \rightarrow q) \wedge (p \rightarrow r)$ and $p \rightarrow (q \wedge r)$ are logically equivalent.

**23.** Show that $(p \rightarrow r) \wedge (q \rightarrow r)$ and $(p \vee q) \rightarrow r$ are logically equivalent.

**24.** Show that $(p \rightarrow q) \vee (p \rightarrow r)$ and $p \rightarrow (q \vee r)$ are logically equivalent.

**25.** Show that $(p \rightarrow r) \vee (q \rightarrow r)$ and $(p \wedge q) \rightarrow r$ are logically equivalent.

**26.** Show that $\neg p \rightarrow (q \rightarrow r)$ and $q \rightarrow (p \vee r)$ are logically equivalent.

**27.** Show that $p \leftrightarrow q$ and $(p \rightarrow q) \wedge (q \rightarrow p)$ are logically equivalent.

**28.** Show that $p \leftrightarrow q$ and $\neg p \leftrightarrow \neg q$ are logically equivalent.

**29.** Show that $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is a tautology.

☞ **30.** Show that $(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$ is a tautology.

**31.** Show that $(p \rightarrow q) \rightarrow r$ and $p \rightarrow (q \rightarrow r)$ are not logically equivalent.

**32.** Show that $(p \wedge q) \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$ are not logically equivalent.

**33.** Show that $(p \rightarrow q) \rightarrow (r \rightarrow s)$ and $(p \rightarrow r) \rightarrow (q \rightarrow s)$ are not logically equivalent.

The **dual** of a compound proposition that contains only the logical operators $\vee$, $\wedge$, and $\neg$ is the compound proposition obtained by replacing each $\vee$ by $\wedge$, each $\wedge$ by $\vee$, each **T** by **F**, and each **F** by **T**. The dual of $s$ is denoted by $s^*$.

**34.** Find the dual of each of these compound propositions.
**a)** $p \vee \neg q$ **b)** $p \wedge (q \vee (r \wedge \mathbf{T}))$
**c)** $(p \wedge \neg q) \vee (q \wedge \mathbf{F})$

**35.** Find the dual of each of these compound propositions.
**a)** $p \wedge \neg q \wedge \neg r$ **b)** $(p \wedge q \wedge r) \vee s$
**c)** $(p \vee \mathbf{F}) \wedge (q \vee \mathbf{T})$

**36.** When does $s^* = s$, where $s$ is a compound proposition?

**37.** Show that $(s^*)^* = s$ when $s$ is a compound proposition.

**38.** Show that the logical equivalences in Table 6, except for the double negation law, come in pairs, where each pair contains compound propositions that are duals of each other.

****39.** Why are the duals of two equivalent compound propositions also equivalent, where these compound propositions contain only the operators $\wedge$, $\vee$, and $\neg$?

**40.** Find a compound proposition involving the propositional variables $p$, $q$, and $r$ that is true when $p$ and $q$ are true and $r$ is false, but is false otherwise. [*Hint:* Use a conjunction of each propositional variable or its negation.]

**41.** Find a compound proposition involving the propositional variables $p$, $q$, and $r$ that is true when exactly two of $p$, $q$, and $r$ are true and is false otherwise. [*Hint:* Form a disjunction of conjunctions. Include a conjunction for each combination of values for which the compound proposition is true. Each conjunction should include each of the three propositional variables or its negations.]

☞ **42.** Suppose that a truth table in $n$ propositional variables is specified. Show that a compound proposition with this truth table can be formed by taking the disjunction of conjunctions of the variables or their negations, with one conjunction included for each combination of values for which the compound proposition is true. The resulting compound proposition is said to be in **disjunctive normal form**.

A collection of logical operators is called **functionally complete** if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

**43.** Show that $\neg$, $\wedge$, and $\vee$ form a functionally complete collection of logical operators. [*Hint:* Use the fact that every compound proposition is logically equivalent to one in disjunctive normal form, as shown in Exercise 42.]

***44.** Show that $\neg$ and $\wedge$ form a functionally complete collection of logical operators. [*Hint:* First use a De Morgan law to show that $p \vee q$ is logically equivalent to $\neg(\neg p \wedge \neg q)$.]

***45.** Show that $\neg$ and $\vee$ form a functionally complete collection of logical operators.

The following exercises involve the logical operators *NAND* and *NOR*. The proposition $p$ *NAND* $q$ is true when either $p$ or $q$, or both, are false; and it is false when both $p$ and $q$ are true. The proposition $p$ *NOR* $q$ is true when both $p$ and $q$ are false, and it is false otherwise. The propositions $p$ *NAND* $q$ and $p$ *NOR* $q$ are denoted by $p \mid q$ and $p \downarrow q$, respectively. (The operators $\mid$ and $\downarrow$ are called the **Sheffer stroke** and the **Peirce arrow** after H. M. Sheffer and C. S. Peirce, respectively.)

**46.** Construct a truth table for the logical operator *NAND*.

**47.** Show that $p \mid q$ is logically equivalent to $\neg(p \wedge q)$.

**48.** Construct a truth table for the logical operator *NOR*.

**49.** Show that $p \downarrow q$ is logically equivalent to $\neg(p \vee q)$.

**50.** In this exercise we will show that $\{\downarrow\}$ is a functionally complete collection of logical operators.

**a)** Show that $p \downarrow p$ is logically equivalent to $\neg p$.

**b)** Show that $(p \downarrow q) \downarrow (p \downarrow q)$ is logically equivalent to $p \vee q$.

**c)** Conclude from parts (a) and (b), and Exercise 49, that $\{\downarrow\}$ is a functionally complete collection of logical operators.

***51.** Find a compound proposition logically equivalent to $p \rightarrow q$ using only the logical operator $\downarrow$.

**52.** Show that $\{\mid\}$ is a functionally complete collection of logical operators.

**53.** Show that $p \mid q$ and $q \mid p$ are equivalent.

**54.** Show that $p \mid (q \mid r)$ and $(p \mid q) \mid r$ are not equivalent, so that the logical operator $\mid$ is not associative.

***55.** How many different truth tables of compound propositions are there that involve the propositional variables $p$ and $q$?

**56.** Show that if $p$, $q$, and $r$ are compound propositions such that $p$ and $q$ are logically equivalent and $q$ and $r$ are logically equivalent, then $p$ and $r$ are logically equivalent.

**57.** The following sentence is taken from the specification of a telephone system: "If the directory database is opened, then the monitor is put in a closed state, if the system is not in its initial state." This specification is hard to understand because it involves two conditional statements. Find an equivalent, easier-to-understand specification that involves disjunctions and negations but not conditional statements.

**58.** How many of the disjunctions $p \vee \neg q$, $\neg p \vee q$, $q \vee r$, $q \vee \neg r$, and $\neg q \vee \neg r$ can be made simultaneously true by an assignment of truth values to $p$, $q$, and $r$?

**59.** How many of the disjunctions $p \vee \neg q \vee s$, $\neg p \vee \neg r \vee s$, $\neg p \vee \neg r \vee \neg s$, $\neg p \vee q \vee \neg s$, $q \vee r \vee \neg s$, $q \vee \neg r \vee \neg s$, $\neg p \vee \neg q \vee \neg s$, $p \vee r \vee s$, and $p \vee r \vee \neg s$ can be made simultaneously true by an assignment of truth values to $p$, $q$, $r$, and $s$?

**60.** Show that the negation of an unsatisfiable compound proposition is a tautology and the negation of a compound proposition that is a tautology is unsatisfiable.

**61.** Determine whether each of these compound propositions is satisfiable.

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

**b)** $(p \rightarrow q) \wedge (p \rightarrow \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$

**c)** $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow q)$

**62.** Determine whether each of these compound propositions is satisfiable.

**a)** $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$

**b)** $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$

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

**63.** Show how the solution of a given $4 \times 4$ Sudoku puzzle can be found by solving a satisfiability problem.

**64.** Construct a compound proposition that asserts that every cell of a $9 \times 9$ Sudoku puzzle contains at least one number.

**65.** Explain the steps in the construction of the compound proposition given in the text that asserts that every column of a $9 \times 9$ Sudoku puzzle contains every number.

***66.** Explain the steps in the construction of the compound proposition given in the text that asserts that each of the nine $3 \times 3$ blocks of a $9 \times 9$ Sudoku puzzle contains every number.

# 1.4 Predicates and Quantifiers

## Introduction

Propositional logic, studied in Sections 1.1–1.3, cannot adequately express the meaning of all statements in mathematics and in natural language. For example, suppose that we know that

"Every computer connected to the university network is functioning properly."

No rules of propositional logic allow us to conclude the truth of the statement

"MATH3 is functioning properly,"

where MATH3 is one of the computers connected to the university network. Likewise, we cannot use the rules of propositional logic to conclude from the statement

"CS2 is under attack by an intruder,"

where CS2 is a computer on the university network, to conclude the truth of

"There is a computer on the university network that is under attack by an intruder."

In this section we will introduce a more powerful type of logic called **predicate logic**. We will see how predicate logic can be used to express the meaning of a wide range of statements in mathematics and computer science in ways that permit us to reason and explore relationships between objects. To understand predicate logic, we first need to introduce the concept of a predicate. Afterward, we will introduce the notion of quantifiers, which enable us to reason with statements that assert that a certain property holds for all objects of a certain type and with statements that assert the existence of an object with a particular property.

## Predicates

Statements involving variables, such as

"$x > 3$," "$x = y + 3$," "$x + y = z$,"

and

"computer $x$ is under attack by an intruder,"

and

"computer $x$ is functioning properly,"

are often found in mathematical assertions, in computer programs, and in system specifications. These statements are neither true nor false when the values of the variables are not specified. In this section, we will discuss the ways that propositions can be produced from such statements.

The statement "$x$ is greater than 3" has two parts. The first part, the variable $x$, is the subject of the statement. The second part—the **predicate**, "is greater than 3"—refers to a property that the subject of the statement can have. We can denote the statement "$x$ is greater than 3" by $P(x)$, where $P$ denotes the predicate "is greater than 3" and $x$ is the variable. The statement $P(x)$ is also said to be the value of the **propositional function** $P$ at $x$. Once a value has been assigned to the variable $x$, the statement $P(x)$ becomes a proposition and has a truth value. Consider Examples 1 and 2.

**EXAMPLE 1** Let $P(x)$ denote the statement "$x > 3$." What are the truth values of $P(4)$ and $P(2)$?

*Solution:* We obtain the statement $P(4)$ by setting $x = 4$ in the statement "$x > 3$." Hence, $P(4)$, which is the statement "$4 > 3$," is true. However, $P(2)$, which is the statement "$2 > 3$," is false. ◀

**EXAMPLE 2** Let $A(x)$ denote the statement "Computer $x$ is under attack by an intruder." Suppose that of the computers on campus, only CS2 and MATH1 are currently under attack by intruders. What are truth values of $A(\text{CS1})$, $A(\text{CS2})$, and $A(\text{MATH1})$?

*Solution:* We obtain the statement $A(\text{CS1})$ by setting $x = \text{CS1}$ in the statement "Computer $x$ is under attack by an intruder." Because CS1 is not on the list of computers currently under attack, we conclude that $A(\text{CS1})$ is false. Similarly, because CS2 and MATH1 are on the list of computers under attack, we know that $A(\text{CS2})$ and $A(\text{MATH1})$ are true. ◀

We can also have statements that involve more than one variable. For instance, consider the statement "$x = y + 3$." We can denote this statement by $Q(x, y)$, where $x$ and $y$ are variables and $Q$ is the predicate. When values are assigned to the variables $x$ and $y$, the statement $Q(x, y)$ has a truth value.

**EXAMPLE 3** Let $Q(x, y)$ denote the statement "$x = y + 3$." What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Extra Examples

*Solution:* To obtain $Q(1, 2)$, set $x = 1$ and $y = 2$ in the statement $Q(x, y)$. Hence, $Q(1, 2)$ is the statement "$1 = 2 + 3$," which is false. The statement $Q(3, 0)$ is the proposition "$3 = 0 + 3$," which is true. ◀

Links

CHARLES SANDERS PEIRCE (1839–1914) Many consider Charles Peirce, born in Cambridge, Massachusetts, to be the most original and versatile American intellect. He made important contributions to an amazing number of disciplines, including mathematics, astronomy, chemistry, geodesy, metrology, engineering, psychology, philology, the history of science, and economics. Peirce was also an inventor, a lifelong student of medicine, a book reviewer, a dramatist and an actor, a short story writer, a phenomenologist, a logician, and a metaphysician. He is noted as the preeminent system-building philosopher competent and productive in logic, mathematics, and a wide range of sciences. He was encouraged by his father, Benjamin Peirce, a professor of mathematics and natural philosophy at Harvard, to pursue a career in science. Instead, he decided to study logic and scientific methodology. Peirce attended Harvard (1855–1859) and received a Harvard master of arts degree (1862) and an advanced degree in chemistry from the Lawrence Scientific School (1863).

In 1861, Peirce became an aide in the U.S. Coast Survey, with the goal of better understanding scientific methodology. His service for the Survey exempted him from military service during the Civil War. While working for the Survey, Peirce did astronomical and geodesic work. He made fundamental contributions to the design of pendulums and to map projections, applying new mathematical developments in the theory of elliptic functions. He was the first person to use the wavelength of light as a unit of measurement. Peirce rose to the position of Assistant for the Survey, a position he held until forced to resign in 1891 when he disagreed with the direction taken by the Survey's new administration.

While making his living from work in the physical sciences, Peirce developed a hierarchy of sciences, with mathematics at the top rung, in which the methods of one science could be adapted for use by those sciences under it in the hierarchy. During this time, he also founded the American philosophical theory of pragmatism.

The only academic position Peirce ever held was lecturer in logic at Johns Hopkins University in Baltimore (1879–1884). His mathematical work during this time included contributions to logic, set theory, abstract algebra, and the philosophy of mathematics. His work is still relevant today, with recent applications of this work on logic to artificial intelligence. Peirce believed that the study of mathematics could develop the mind's powers of imagination, abstraction, and generalization. His diverse activities after retiring from the Survey included writing for periodicals, contributing to scholarly dictionaries, translating scientific papers, guest lecturing, and textbook writing. Unfortunately, his income from these pursuits was insufficient to protect him and his second wife from abject poverty. He was supported in his later years by a fund created by his many admirers and administered by the philosopher William James, his lifelong friend. Although Peirce wrote and published voluminously in a vast range of subjects, he left more than 100,000 pages of unpublished manuscripts. Because of the difficulty of studying his unpublished writings, scholars have only recently started to understand some of his varied contributions. A group of people is devoted to making his work available over the Internet to bring a better appreciation of Peirce's accomplishments to the world.

**EXAMPLE 4** Let $A(c, n)$ denote the statement "Computer $c$ is connected to network $n$," where $c$ is a variable representing a computer and $n$ is a variable representing a network. Suppose that the computer MATH1 is connected to network CAMPUS2, but not to network CAMPUS1. What are the values of $A$(MATH1, CAMPUS1) and $A$(MATH1, CAMPUS2)?

*Solution:* Because MATH1 is not connected to the CAMPUS1 network, we see that $A$(MATH1, CAMPUS1) is false. However, because MATH1 is connected to the CAMPUS2 network, we see that $A$(MATH1, CAMPUS2) is true. ◀

Similarly, we can let $R(x, y, z)$ denote the statement "$x + y = z$." When values are assigned to the variables $x$, $y$, and $z$, this statement has a truth value.

**EXAMPLE 5** What are the truth values of the propositions $R(1, 2, 3)$ and $R(0, 0, 1)$?

*Solution:* The proposition $R(1, 2, 3)$ is obtained by setting $x = 1$, $y = 2$, and $z = 3$ in the statement $R(x, y, z)$. We see that $R(1, 2, 3)$ is the statement "$1 + 2 = 3$," which is true. Also note that $R(0, 0, 1)$, which is the statement "$0 + 0 = 1$," is false. ◀

In general, a statement involving the $n$ variables $x_1, x_2, \ldots, x_n$ can be denoted by

$$P(x_1, x_2, \ldots, x_n).$$

A statement of the form $P(x_1, x_2, \ldots, x_n)$ is the value of the **propositional function** $P$ at the $n$-tuple $(x_1, x_2, \ldots, x_n)$, and $P$ is also called an **$n$-place predicate** or a **$n$-ary predicate**.

Propositional functions occur in computer programs, as Example 6 demonstrates.

**EXAMPLE 6** Consider the statement

**if** $x > 0$ **then** $x := x + 1$.

When this statement is encountered in a program, the value of the variable $x$ at that point in the execution of the program is inserted into $P(x)$, which is "$x > 0$." If $P(x)$ is true for this value of $x$, the assignment statement $x := x + 1$ is executed, so the value of $x$ is increased by 1. If $P(x)$ is false for this value of $x$, the assignment statement is not executed, so the value of $x$ is not changed. ◀

PRECONDITIONS AND POSTCONDITIONS Predicates are also used to establish the correctness of computer programs, that is, to show that computer programs always produce the desired output when given valid input. (Note that unless the correctness of a computer program is established, no amount of testing can show that it produces the desired output for all input values, unless every input value is tested.) The statements that describe valid input are known as **preconditions** and the conditions that the output should satisfy when the program has run are known as **postconditions**. As Example 7 illustrates, we use predicates to describe both preconditions and postconditions. We will study this process in greater detail in Section 5.5.

**EXAMPLE 7** Consider the following program, designed to interchange the values of two variables $x$ and $y$.

```
temp := x
x := y
y := temp
```

Find predicates that we can use as the precondition and the postcondition to verify the correctness of this program. Then explain how to use them to verify that for all valid input the program does what is intended.

*Solution:* For the precondition, we need to express that $x$ and $y$ have particular values before we run the program. So, for this precondition we can use the predicate $P(x, y)$, where $P(x, y)$ is the statement "$x = a$ and $y = b$," where $a$ and $b$ are the values of $x$ and $y$ before we run the program. Because we want to verify that the program swaps the values of $x$ and $y$ for all input values, for the postcondition we can use $Q(x, y)$, where $Q(x, y)$ is the statement "$x = b$ and $y = a$."

To verify that the program always does what it is supposed to do, suppose that the precondition $P(x, y)$ holds. That is, we suppose that the statement "$x = a$ and $y = b$" is true. This means that $x = a$ and $y = b$. The first step of the program, $temp := x$, assigns the value of $x$ to the variable $temp$, so after this step we know that $x = a$, $temp = a$, and $y = b$. After the second step of the program, $x := y$, we know that $x = b$, $temp = a$, and $y = b$. Finally, after the third step, we know that $x = b$, $temp = a$, and $y = a$. Consequently, after this program is run, the postcondition $Q(x, y)$ holds, that is, the statement "$x = b$ and $y = a$" is true. ◀

## Quantifiers

When the variables in a propositional function are assigned values, the resulting statement becomes a proposition with a certain truth value. However, there is another important way, called **quantification**, to create a proposition from a propositional function. Quantification expresses the extent to which a predicate is true over a range of elements. In English, the words *all*, *some*, *many*, *none*, and *few* are used in quantifications. We will focus on two types of quantification here: universal quantification, which tells us that a predicate is true for every element under consideration, and existential quantification, which tells us that there is one or more element under consideration for which the predicate is true. The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

Assessment

### THE UNIVERSAL QUANTIFIER

Assessment

Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called the **domain of discourse** (or the **universe of discourse**), often just referred to as the **domain**. Such a statement is expressed using universal quantification. The universal quantification of $P(x)$ for a particular domain is the proposition that asserts that $P(x)$ is true for all values of $x$ in this domain. Note that the domain specifies the possible values of the variable $x$. The meaning of the universal quantification of $P(x)$ changes when we change the domain. The domain must always be specified when a universal quantifier is used; without it, the universal quantification of a statement is not defined.

**DEFINITION 1**

The *universal quantification* of $P(x)$ is the statement

"$P(x)$ for all values of $x$ in the domain."

The notation $\forall x\, P(x)$ denotes the universal quantification of $P(x)$. Here $\forall$ is called the **universal quantifier.** We read $\forall x\, P(x)$ as "for all $x\, P(x)$" or "for every $x\, P(x)$." An element for which $P(x)$ is false is called a **counterexample** of $\forall x\, P(x)$.

The meaning of the universal quantifier is summarized in the first row of Table 1. We illustrate the use of the universal quantifier in Examples 8–13.

| **TABLE 1** Quantifiers. | | |
|---|---|---|
| ***Statement*** | ***When True?*** | ***When False?*** |
| $\forall x\,P(x)$ | $P(x)$ is true for every $x$. | There is an $x$ for which $P(x)$ is false. |
| $\exists x\,P(x)$ | There is an $x$ for which $P(x)$ is true. | $P(x)$ is false for every $x$. |

**EXAMPLE 8** Let $P(x)$ be the statement "$x + 1 > x$." What is the truth value of the quantification $\forall x\,P(x)$, where the domain consists of all real numbers?

Extra Examples

*Solution:* Because $P(x)$ is true for all real numbers $x$, the quantification

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

is true. ◀

***Remark:*** Generally, an implicit assumption is made that all domains of discourse for quantifiers are nonempty. Note that if the domain is empty, then $\forall x\,P(x)$ is true for any propositional function $P(x)$ because there are no elements $x$ in the domain for which $P(x)$ is false.

Remember that the truth value of $\forall x\,P(x)$ depends on the domain!

Besides "for all" and "for every," universal quantification can be expressed in many other ways, including "all of," "for each," "given any," "for arbitrary," "for each," and "for any."

***Remark:*** It is best to avoid using "for any $x$" because it is often ambiguous as to whether "any" means "every" or "some." In some cases, "any" is unambiguous, such as when it is used in negatives, for example, "there is not any reason to avoid studying."

A statement $\forall x\,P(x)$ is false, where $P(x)$ is a propositional function, if and only if $P(x)$ is not always true when $x$ is in the domain. One way to show that $P(x)$ is not always true when $x$ is in the domain is to find a counterexample to the statement $\forall x\,P(x)$. Note that a single counterexample is all we need to establish that $\forall x\,P(x)$ is false. Example 9 illustrates how counterexamples are used.

**EXAMPLE 9** Let $Q(x)$ be the statement "$x < 2$." What is the truth value of the quantification $\forall x\,Q(x)$, where the domain consists of all real numbers?

*Solution:* $Q(x)$ is not true for every real number $x$, because, for instance, $Q(3)$ is false. That is, $x = 3$ is a counterexample for the statement $\forall x\,Q(x)$. Thus

$$\forall x\,Q(x)$$

is false. ◀

**EXAMPLE 10** Suppose that $P(x)$ is "$x^2 > 0$." To show that the statement $\forall x\,P(x)$ is false where the universe of discourse consists of all integers, we give a counterexample. We see that $x = 0$ is a counterexample because $x^2 = 0$ when $x = 0$, so that $x^2$ is not greater than 0 when $x = 0$. ◀

Looking for counterexamples to universally quantified statements is an important activity in the study of mathematics, as we will see in subsequent sections of this book.

When all the elements in the domain can be listed—say, $x_1, x_2, \ldots, x_n$—it follows that the universal quantification $\forall x\,P(x)$ is the same as the conjunction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n),$$

because this conjunction is true if and only if $P(x_1), P(x_2), \ldots, P(x_n)$ are all true.

**EXAMPLE 11** What is the truth value of $\forall x\, P(x)$, where $P(x)$ is the statement "$x^2 < 10$" and the domain consists of the positive integers not exceeding 4?

*Solution:* The statement $\forall x\, P(x)$ is the same as the conjunction

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4),$$

because the domain consists of the integers 1, 2, 3, and 4. Because $P(4)$, which is the statement "$4^2 < 10$," is false, it follows that $\forall x\, P(x)$ is false. ◀

**EXAMPLE 12** What does the statement $\forall x\, N(x)$ mean if $N(x)$ is "Computer $x$ is connected to the network" and the domain consists of all computers on campus?

*Solution:* The statement $\forall x\, N(x)$ means that for every computer $x$ on campus, that computer $x$ is connected to the network. This statement can be expressed in English as "Every computer on campus is connected to the network." ◀

As we have pointed out, specifying the domain is mandatory when quantifiers are used. The truth value of a quantified statement often depends on which elements are in this domain, as Example 13 shows.

**EXAMPLE 13** What is the truth value of $\forall x(x^2 \geq x)$ if the domain consists of all real numbers? What is the truth value of this statement if the domain consists of all integers?

*Solution:* The universal quantification $\forall x(x^2 \geq x)$, where the domain consists of all real numbers, is false. For example, $(\frac{1}{2})^2 \not\geq \frac{1}{2}$. Note that $x^2 \geq x$ if and only if $x^2 - x = x(x-1) \geq 0$. Consequently, $x^2 \geq x$ if and only if $x \leq 0$ or $x \geq 1$. It follows that $\forall x(x^2 \geq x)$ is false if the domain consists of all real numbers (because the inequality is false for all real numbers $x$ with $0 < x < 1$). However, if the domain consists of the integers, $\forall x(x^2 \geq x)$ is true, because there are no integers $x$ with $0 < x < 1$. ◀

**THE EXISTENTIAL QUANTIFIER** Many mathematical statements assert that there is an element with a certain property. Such statements are expressed using existential quantification. With existential quantification, we form a proposition that is true if and only if $P(x)$ is true for at least one value of $x$ in the domain.

**DEFINITION 2** The *existential quantification* of $P(x)$ is the proposition

"There exists an element $x$ in the domain such that $P(x)$."

We use the notation $\exists x\, P(x)$ for the existential quantification of $P(x)$. Here $\exists$ is called the *existential quantifier*.

A domain must always be specified when a statement $\exists x\, P(x)$ is used. Furthermore, the meaning of $\exists x\, P(x)$ changes when the domain changes. Without specifying the domain, the statement $\exists x\, P(x)$ has no meaning.

Besides the phrase "there exists," we can also express existential quantification in many other ways, such as by using the words "for some," "for at least one," or "there is." The existential quantification $\exists x\, P(x)$ is read as

"There is an $x$ such that $P(x)$,"
"There is at least one $x$ such that $P(x)$,"

or

"For some $x\, P(x)$."

The meaning of the existential quantifier is summarized in the second row of Table 1. We illustrate the use of the existential quantifier in Examples 14–16.

**EXAMPLE 14** Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the quantification $\exists x\, P(x)$, where the domain consists of all real numbers?

Extra Examples

*Solution:* Because "$x > 3$" is sometimes true—for instance, when $x = 4$—the existential quantification of $P(x)$, which is $\exists x\, P(x)$, is true. ◀

Observe that the statement $\exists x\, P(x)$ is false if and only if there is no element $x$ in the domain for which $P(x)$ is true. That is, $\exists x\, P(x)$ is false if and only if $P(x)$ is false for every element of the domain. We illustrate this observation in Example 15.

**EXAMPLE 15** Let $Q(x)$ denote the statement "$x = x + 1$." What is the truth value of the quantification $\exists x\, Q(x)$, where the domain consists of all real numbers?

*Solution:* Because $Q(x)$ is false for every real number $x$, the existential quantification of $Q(x)$, which is $\exists x\, Q(x)$, is false. ◀

Remember that the truth value of $\exists x\, P(x)$ depends on the domain!

***Remark:*** Generally, an implicit assumption is made that all domains of discourse for quantifiers are nonempty. If the domain is empty, then $\exists x\, Q(x)$ is false whenever $Q(x)$ is a propositional function because when the domain is empty, there can be no element $x$ in the domain for which $Q(x)$ is true.

When all elements in the domain can be listed—say, $x_1, x_2, \ldots, x_n$— the existential quantification $\exists x\, P(x)$ is the same as the disjunction

$$P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n),$$

because this disjunction is true if and only if at least one of $P(x_1), P(x_2), \ldots, P(x_n)$ is true.

**EXAMPLE 16** What is the truth value of $\exists x\, P(x)$, where $P(x)$ is the statement "$x^2 > 10$" and the universe of discourse consists of the positive integers not exceeding 4?

*Solution:* Because the domain is $\{1, 2, 3, 4\}$, the proposition $\exists x\, P(x)$ is the same as the disjunction

$$P(1) \vee P(2) \vee P(3) \vee P(4).$$

Because $P(4)$, which is the statement "$4^2 > 10$," is true, it follows that $\exists x\, P(x)$ is true. ◀

It is sometimes helpful to think in terms of looping and searching when determining the truth value of a quantification. Suppose that there are $n$ objects in the domain for the variable $x$. To determine whether $\forall x\, P(x)$ is true, we can loop through all $n$ values of $x$ to see whether $P(x)$ is always true. If we encounter a value $x$ for which $P(x)$ is false, then we have shown that $\forall x\, P(x)$ is false. Otherwise, $\forall x\, P(x)$ is true. To see whether $\exists x\, P(x)$ is true, we loop through the $n$ values of $x$ searching for a value for which $P(x)$ is true. If we find one, then $\exists x\, P(x)$ is true. If we never find such an $x$, then we have determined that $\exists x\, P(x)$ is false. (Note that this searching procedure does not apply if there are infinitely many values in the domain. However, it is still a useful way of thinking about the truth values of quantifications.)

THE UNIQUENESS QUANTIFIER We have now introduced universal and existential quantifiers. These are the most important quantifiers in mathematics and computer science. However, there is no limitation on the number of different quantifiers we can define, such as "there are exactly two," "there are no more than three," "there are at least 100," and so on. Of these other quantifiers, the one that is most often seen is the **uniqueness quantifier**, denoted by $\exists!$ or $\exists_1$. The notation $\exists! x\, P(x)$ [or $\exists_1 x\, P(x)$] states "There exists a unique $x$ such that $P(x)$ is true." (Other phrases for uniqueness quantification include "there is exactly one" and "there is one and only one.") For instance, $\exists! x(x - 1 = 0)$, where the domain is the set of real numbers, states that there is a unique real number $x$ such that $x - 1 = 0$. This is a true statement, as $x = 1$ is the unique real number such that $x - 1 = 0$. Observe that we can use quantifiers and propositional logic to express uniqueness (see Exercise 52 in Section 1.5), so the uniqueness quantifier can be avoided. Generally, it is best to stick with existential and universal quantifiers so that rules of inference for these quantifiers can be used.

## Quantifiers with Restricted Domains

An abbreviated notation is often used to restrict the domain of a quantifier. In this notation, a condition a variable must satisfy is included after the quantifier. This is illustrated in Example 17. We will also describe other forms of this notation involving set membership in Section 2.1.

**EXAMPLE 17** What do the statements $\forall x < 0\, (x^2 > 0)$, $\forall y \neq 0\, (y^3 \neq 0)$, and $\exists z > 0\, (z^2 = 2)$ mean, where the domain in each case consists of the real numbers?

*Solution:* The statement $\forall x < 0\ (x^2 > 0)$ states that for every real number $x$ with $x < 0$, $x^2 > 0$. That is, it states "The square of a negative real number is positive." This statement is the same as $\forall x(x < 0 \rightarrow x^2 > 0)$.

The statement $\forall y \neq 0\, (y^3 \neq 0)$ states that for every real number $y$ with $y \neq 0$, we have $y^3 \neq 0$. That is, it states "The cube of every nonzero real number is nonzero." Note that this statement is equivalent to $\forall y(y \neq 0 \rightarrow y^3 \neq 0)$.

Finally, the statement $\exists z > 0\, (z^2 = 2)$ states that there exists a real number $z$ with $z > 0$ such that $z^2 = 2$. That is, it states "There is a positive square root of 2." This statement is equivalent to $\exists z(z > 0 \wedge z^2 = 2)$. ◀

Note that the restriction of a universal quantification is the same as the universal quantification of a conditional statement. For instance, $\forall x < 0\ (x^2 > 0)$ is another way of expressing $\forall x(x < 0 \rightarrow x^2 > 0)$. On the other hand, the restriction of an existential quantification is the same as the existential quantification of a conjunction. For instance, $\exists z > 0\ (z^2 = 2)$ is another way of expressing $\exists z(z > 0 \wedge z^2 = 2)$.

## Precedence of Quantifiers

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus. For example, $\forall x\, P(x) \vee Q(x)$ is the disjunction of $\forall x\, P(x)$ and $Q(x)$. In other words, it means $(\forall x\, P(x)) \vee Q(x)$ rather than $\forall x(P(x) \vee Q(x))$.

## Binding Variables

When a quantifier is used on the variable $x$, we say that this occurrence of the variable is **bound**. An occurrence of a variable that is not bound by a quantifier or set equal to a particular value is said to be **free**. All the variables that occur in a propositional function must be bound or set equal to a particular value to turn it into a proposition. This can be done using a combination of universal quantifiers, existential quantifiers, and value assignments.

The part of a logical expression to which a quantifier is applied is called the **scope** of this quantifier. Consequently, a variable is free if it is outside the scope of all quantifiers in the formula that specify this variable.

**EXAMPLE 18** In the statement $\exists x(x + y = 1)$, the variable $x$ is bound by the existential quantification $\exists x$, but the variable $y$ is free because it is not bound by a quantifier and no value is assigned to this variable. This illustrates that in the statement $\exists x(x + y = 1)$, $x$ is bound, but $y$ is free.

In the statement $\exists x(P(x) \wedge Q(x)) \vee \forall x R(x)$, all variables are bound. The scope of the first quantifier, $\exists x$, is the expression $P(x) \wedge Q(x)$ because $\exists x$ is applied only to $P(x) \wedge Q(x)$, and not to the rest of the statement. Similarly, the scope of the second quantifier, $\forall x$, is the expression $R(x)$. That is, the existential quantifier binds the variable $x$ in $P(x) \wedge Q(x)$ and the universal quantifier $\forall x$ binds the variable $x$ in $R(x)$. Observe that we could have written our statement using two different variables $x$ and $y$, as $\exists x(P(x) \wedge Q(x)) \vee \forall y R(y)$, because the scopes of the two quantifiers do not overlap. The reader should be aware that in common usage, the same letter is often used to represent variables bound by different quantifiers with scopes that do not overlap. ◀

## Logical Equivalences Involving Quantifiers

In Section 1.3 we introduced the notion of logical equivalences of compound propositions. We can extend this notion to expressions involving predicates and quantifiers.

**DEFINITION 3** Statements involving predicates and quantifiers are *logically equivalent* if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions. We use the notation $S \equiv T$ to indicate that two statements $S$ and $T$ involving predicates and quantifiers are logically equivalent.

Example 19 illustrates how to show that two statements involving predicates and quantifiers are logically equivalent.

**EXAMPLE 19** Show that $\forall x(P(x) \wedge Q(x))$ and $\forall x P(x) \wedge \forall x Q(x)$ are logically equivalent (where the same domain is used throughout). This logical equivalence shows that we can distribute a universal quantifier over a conjunction. Furthermore, we can also distribute an existential quantifier over a disjunction. However, we cannot distribute a universal quantifier over a disjunction, nor can we distribute an existential quantifier over a conjunction. (See Exercises 50 and 51.)

*Solution:* To show that these statements are logically equivalent, we must show that they always take the same truth value, no matter what the predicates $P$ and $Q$ are, and no matter which domain of discourse is used. Suppose we have particular predicates $P$ and $Q$, with a common domain. We can show that $\forall x(P(x) \wedge Q(x))$ and $\forall x P(x) \wedge \forall x Q(x)$ are logically equivalent by doing two things. First, we show that if $\forall x(P(x) \wedge Q(x))$ is true, then $\forall x P(x) \wedge \forall x Q(x)$ is true. Second, we show that if $\forall x P(x) \wedge \forall x Q(x)$ is true, then $\forall x(P(x) \wedge Q(x))$ is true.

So, suppose that $\forall x(P(x) \wedge Q(x))$ is true. This means that if $a$ is in the domain, then $P(a) \wedge Q(a)$ is true. Hence, $P(a)$ is true and $Q(a)$ is true. Because $P(a)$ is true and $Q(a)$ is true for every element in the domain, we can conclude that $\forall x P(x)$ and $\forall x Q(x)$ are both true. This means that $\forall x P(x) \wedge \forall x Q(x)$ is true.

Next, suppose that $\forall x P(x) \wedge \forall x Q(x)$ is true. It follows that $\forall x P(x)$ is true and $\forall x Q(x)$ is true. Hence, if $a$ is in the domain, then $P(a)$ is true and $Q(a)$ is true [because $P(x)$ and $Q(x)$ are both true for all elements in the domain, there is no conflict using the same value of $a$ here].

It follows that for all $a$, $P(a) \wedge Q(a)$ is true. It follows that $\forall x(P(x) \wedge Q(x))$ is true. We can now conclude that

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x).$$ ◀

## Negating Quantified Expressions

We will often want to consider the negation of a quantified expression. For instance, consider the negation of the statement

"Every student in your class has taken a course in calculus."

This statement is a universal quantification, namely,

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


where $P(x)$ is the statement "$x$ has taken a course in calculus" and the domain consists of the students in your class. The negation of this statement is "It is not the case that every student in your class has taken a course in calculus." This is equivalent to "There is a student in your class who has not taken a course in calculus." And this is simply the existential quantification of the negation of the original propositional function, namely,

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

This example illustrates the following logical equivalence:

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

To show that $\neg \forall x P(x)$ and $\exists x P(x)$ are logically equivalent no matter what the propositional function $P(x)$ is and what the domain is, first note that $\neg \forall x P(x)$ is true if and only if $\forall x P(x)$ is false. Next, note that $\forall x P(x)$ is false if and only if there is an element $x$ in the domain for which $P(x)$ is false. This holds if and only if there is an element $x$ in the domain for which $\neg P(x)$ is true. Finally, note that there is an element $x$ in the domain for which $\neg P(x)$ is true if and only if $\exists x \neg P(x)$ is true. Putting these steps together, we can conclude that $\neg \forall x P(x)$ is true if and only if $\exists x \neg P(x)$ is true. It follows that $\neg \forall x P(x)$ and $\exists x \neg P(x)$ are logically equivalent.

Suppose we wish to negate an existential quantification. For instance, consider the proposition "There is a student in this class who has taken a course in calculus." This is the existential quantification

$$\exists x Q(x),$$

where $Q(x)$ is the statement "$x$ has taken a course in calculus." The negation of this statement is the proposition "It is not the case that there is a student in this class who has taken a course in calculus." This is equivalent to "Every student in this class has not taken calculus," which is just the universal quantification of the negation of the original propositional function, or, phrased in the language of quantifiers,

$$\forall x \neg Q(x).$$

This example illustrates the equivalence

$$\neg \exists x Q(x) \equiv \forall x \neg Q(x).$$

To show that $\neg \exists x Q(x)$ and $\forall x \neg Q(x)$ are logically equivalent no matter what $Q(x)$ is and what the domain is, first note that $\neg \exists x Q(x)$ is true if and only if $\exists x Q(x)$ is false. This is true if and

**TABLE 2 De Morgan's Laws for Quantifiers.**

| *Negation* | *Equivalent Statement* | *When Is Negation True?* | *When False?* |
|---|---|---|---|
| $\neg\exists x\, P(x)$ | $\forall x \neg P(x)$ | For every $x$, $P(x)$ is false. | There is an $x$ for which $P(x)$ is true. |
| $\neg\forall x\, P(x)$ | $\exists x \neg P(x)$ | There is an $x$ for which $P(x)$ is false. | $P(x)$ is true for every $x$. |

only if no $x$ exists in the domain for which $Q(x)$ is true. Next, note that no $x$ exists in the domain for which $Q(x)$ is true if and only if $Q(x)$ is false for every $x$ in the domain. Finally, note that $Q(x)$ is false for every $x$ in the domain if and only if $\neg Q(x)$ is true for all $x$ in the domain, which holds if and only if $\forall x \neg Q(x)$ is true. Putting these steps together, we see that $\neg\exists x\, Q(x)$ is true if and only if $\forall x \neg Q(x)$ is true. We conclude that $\neg\exists x\, Q(x)$ and $\forall x\, \neg Q(x)$ are logically equivalent.

The rules for negations for quantifiers are called **De Morgan's laws for quantifiers**. These rules are summarized in Table 2.

***Remark:*** When the domain of a predicate $P(x)$ consists of $n$ elements, where $n$ is a positive integer greater than one, the rules for negating quantified statements are exactly the same as De Morgan's laws discussed in Section 1.3. This is why these rules are called De Morgan's laws for quantifiers. When the domain has $n$ elements $x_1, x_2, \ldots, x_n$, it follows that $\neg\forall x\, P(x)$ is the same as $\neg(P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n))$, which is equivalent to $\neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n)$ by De Morgan's laws, and this is the same as $\exists x \neg P(x)$. Similarly, $\neg\exists x\, P(x)$ is the same as $\neg(P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n))$, which by De Morgan's laws is equivalent to $\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \wedge \neg P(x_n)$, and this is the same as $\forall x \neg P(x)$.

We illustrate the negation of quantified statements in Examples 20 and 21.

**EXAMPLE 20** What are the negations of the statements "There is an honest politician" and "All Americans eat cheeseburgers"?

*Solution:* Let $H(x)$ denote "$x$ is honest." Then the statement "There is an honest politician" is represented by $\exists x H(x)$, where the domain consists of all politicians. The negation of this statement is $\neg\exists x H(x)$, which is equivalent to $\forall x \neg H(x)$. This negation can be expressed as "Every politician is dishonest." (*Note:* In English, the statement "All politicians are not honest" is ambiguous. In common usage, this statement often means "Not all politicians are honest." Consequently, we do not use this statement to express this negation.)

Extra Examples

Let $C(x)$ denote "$x$ eats cheeseburgers." Then the statement "All Americans eat cheeseburgers" is represented by $\forall x C(x)$, where the domain consists of all Americans. The negation of this statement is $\neg\forall x C(x)$, which is equivalent to $\exists x \neg C(x)$. This negation can be expressed in several different ways, including "Some American does not eat cheeseburgers" and "There is an American who does not eat cheeseburgers." ◀

**EXAMPLE 21** What are the negations of the statements $\forall x(x^2 > x)$ and $\exists x(x^2 = 2)$?

*Solution:* The negation of $\forall x(x^2 > x)$ is the statement $\neg\forall x(x^2 > x)$, which is equivalent to $\exists x \neg(x^2 > x)$. This can be rewritten as $\exists x(x^2 \leq x)$. The negation of $\exists x(x^2 = 2)$ is the statement $\neg\exists x(x^2 = 2)$, which is equivalent to $\forall x \neg(x^2 = 2)$. This can be rewritten as $\forall x(x^2 \neq 2)$. The truth values of these statements depend on the domain. ◀

We use De Morgan's laws for quantifiers in Example 22.

**EXAMPLE 22** Show that $\neg\forall x(P(x) \rightarrow Q(x))$ and $\exists x(P(x) \wedge \neg Q(x))$ are logically equivalent.

*Solution:* By De Morgan's law for universal quantifiers, we know that $\neg\forall x(P(x) \rightarrow Q(x))$ and $\exists x(\neg(P(x) \rightarrow Q(x)))$ are logically equivalent. By the fifth logical equivalence in Table 7 in Section 1.3, we know that $\neg(P(x) \rightarrow Q(x))$ and $P(x) \wedge \neg Q(x)$ are logically equivalent for every $x$. Because we can substitute one logically equivalent expression for another in a logical equivalence, it follows that $\neg\forall x(P(x) \rightarrow Q(x))$ and $\exists x(P(x) \wedge \neg Q(x))$ are logically equivalent. ◀

## Translating from English into Logical Expressions

Translating sentences in English (or other natural languages) into logical expressions is a crucial task in mathematics, logic programming, artificial intelligence, software engineering, and many other disciplines. We began studying this topic in Section 1.1, where we used propositions to express sentences in logical expressions. In that discussion, we purposely avoided sentences whose translations required predicates and quantifiers. Translating from English to logical expressions becomes even more complex when quantifiers are needed. Furthermore, there can be many ways to translate a particular sentence. (As a consequence, there is no "cookbook" approach that can be followed step by step.) We will use some examples to illustrate how to translate sentences from English into logical expressions. The goal in this translation is to produce simple and useful logical expressions. In this section, we restrict ourselves to sentences that can be translated into logical expressions using a single quantifier; in the next section, we will look at more complicated sentences that require multiple quantifiers.

**EXAMPLE 23** Express the statement "Every student in this class has studied calculus" using predicates and quantifiers.

*Solution:* First, we rewrite the statement so that we can clearly identify the appropriate quantifiers to use. Doing so, we obtain:

"For every student in this class, that student has studied calculus."

Extra Examples

Next, we introduce a variable $x$ so that our statement becomes

"For every student $x$ in this class, $x$ has studied calculus."

Continuing, we introduce $C(x)$, which is the statement "$x$ has studied calculus." Consequently, if the domain for $x$ consists of the students in the class, we can translate our statement as $\forall x C(x)$.

However, there are other correct approaches; different domains of discourse and other predicates can be used. The approach we select depends on the subsequent reasoning we want to carry out. For example, we may be interested in a wider group of people than only those in this class. If we change the domain to consist of all people, we will need to express our statement as

"For every person $x$, if person $x$ is a student in this class then $x$ has studied calculus."

If $S(x)$ represents the statement that person $x$ is in this class, we see that our statement can be expressed as $\forall x(S(x) \rightarrow C(x))$. [*Caution!* Our statement *cannot* be expressed as $\forall x(S(x) \wedge C(x))$ because this statement says that all people are students in this class and have studied calculus!]

Finally, when we are interested in the background of people in subjects besides calculus, we may prefer to use the two-variable quantifier $Q(x, y)$ for the statement "student $x$ has studied subject $y$." Then we would replace $C(x)$ by $Q(x, \text{calculus})$ in both approaches to obtain $\forall x Q(x, \text{calculus})$ or $\forall x(S(x) \rightarrow Q(x, \text{calculus}))$. ◀

In Example 23 we displayed different approaches for expressing the same statement using predicates and quantifiers. However, we should always adopt the simplest approach that is adequate for use in subsequent reasoning.

**EXAMPLE 24** Express the statements "Some student in this class has visited Mexico" and "Every student in this class has visited either Canada or Mexico" using predicates and quantifiers.

*Solution:* The statement "Some student in this class has visited Mexico" means that

> "There is a student in this class with the property that the student has visited Mexico."

We can introduce a variable $x$, so that our statement becomes

> "There is a student $x$ in this class having the property that $x$ has visited Mexico."

We introduce $M(x)$, which is the statement "$x$ has visited Mexico." If the domain for $x$ consists of the students in this class, we can translate this first statement as $\exists x M(x)$.

However, if we are interested in people other than those in this class, we look at the statement a little differently. Our statement can be expressed as

> "There is a person $x$ having the properties that $x$ is a student in this class and $x$ has visited Mexico."

In this case, the domain for the variable $x$ consists of all people. We introduce $S(x)$ to represent "$x$ is a student in this class." Our solution becomes $\exists x(S(x) \wedge M(x))$ because the statement is that there is a person $x$ who is a student in this class and who has visited Mexico. [*Caution!* Our statement cannot be expressed as $\exists x(S(x) \rightarrow M(x))$, which is true when there is someone not in the class because, in that case, for such a person $x$, $S(x) \rightarrow M(x)$ becomes either $\mathbf{F} \rightarrow \mathbf{T}$ or $\mathbf{F} \rightarrow \mathbf{F}$, both of which are true.]

Similarly, the second statement can be expressed as

> "For every $x$ in this class, $x$ has the property that $x$ has visited Mexico or $x$ has visited Canada."

(Note that we are assuming the inclusive, rather than the exclusive, or here.) We let $C(x)$ be "$x$ has visited Canada." Following our earlier reasoning, we see that if the domain for $x$ consists of the students in this class, this second statement can be expressed as $\forall x(C(x) \vee M(x))$. However, if the domain for $x$ consists of all people, our statement can be expressed as

> "For every person $x$, if $x$ is a student in this class, then $x$ has visited Mexico or $x$ has visited Canada."

In this case, the statement can be expressed as $\forall x(S(x) \rightarrow (C(x) \vee M(x)))$.

Instead of using $M(x)$ and $C(x)$ to represent that $x$ has visited Mexico and $x$ has visited Canada, respectively, we could use a two-place predicate $V(x, y)$ to represent "$x$ has visited country $y$." In this case, $V(x,$ Mexico) and $V(x,$ Canada) would have the same meaning as $M(x)$ and $C(x)$ and could replace them in our answers. If we are working with many statements that involve people visiting different countries, we might prefer to use this two-variable approach. Otherwise, for simplicity, we would stick with the one-variable predicates $M(x)$ and $C(x)$. ◀

## Using Quantifiers in System Specifications

In Section 1.2 we used propositions to represent system specifications. However, many system specifications involve predicates and quantifications. This is illustrated in Example 25.

**EXAMPLE 25** Use predicates and quantifiers to express the system specifications "Every mail message larger than one megabyte will be compressed" and "If a user is active, at least one network link will be available."

Extra Examples

*Solution:* Let $S(m, y)$ be "Mail message $m$ is larger than $y$ megabytes," where the variable $x$ has the domain of all mail messages and the variable $y$ is a positive real number, and let $C(m)$ denote "Mail message $m$ will be compressed." Then the specification "Every mail message larger than one megabyte will be compressed" can be represented as $\forall m(S(m, 1) \rightarrow C(m))$.

Remember the rules of precedence for quantifiers and logical connectives!

Let $A(u)$ represent "User $u$ is active," where the variable $u$ has the domain of all users, let $S(n, x)$ denote "Network link $n$ is in state $x$," where $n$ has the domain of all network links and $x$ has the domain of all possible states for a network link. Then the specification "If a user is active, at least one network link will be available" can be represented by $\exists u\, A(u) \rightarrow \exists n S(n, \text{available})$. ◀

## Examples from Lewis Carroll

Lewis Carroll (really C. L. Dodgson writing under a pseudonym), the author of *Alice in Wonderland*, is also the author of several works on symbolic logic. His books contain many examples of reasoning using quantifiers. Examples 26 and 27 come from his book *Symbolic Logic;* other examples from that book are given in the exercises at the end of this section. These examples illustrate how quantifiers are used to express various types of statements.

**EXAMPLE 26** Consider these statements. The first two are called *premises* and the third is called the *conclusion*. The entire set is called an *argument*.

"All lions are fierce."
"Some lions do not drink coffee."
"Some fierce creatures do not drink coffee."

(In Section 1.6 we will discuss the issue of determining whether the conclusion is a valid consequence of the premises. In this example, it is.) Let $P(x)$, $Q(x)$, and $R(x)$ be the statements "$x$ is a lion," "$x$ is fierce," and "$x$ drinks coffee," respectively. Assuming that the domain consists of all creatures, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, and $R(x)$.

Links

CHARLES LUTWIDGE DODGSON (1832–1898) We know Charles Dodgson as Lewis Carroll—the pseudonym he used in his literary works. Dodgson, the son of a clergyman, was the third of 11 children, all of whom stuttered. He was uncomfortable in the company of adults and is said to have spoken without stuttering only to young girls, many of whom he entertained, corresponded with, and photographed (sometimes in poses that today would be considered inappropriate). Although attracted to young girls, he was extremely puritanical and religious. His friendship with the three young daughters of Dean Liddell led to his writing *Alice in Wonderland*, which brought him money and fame.

Dodgson graduated from Oxford in 1854 and obtained his master of arts degree in 1857. He was appointed lecturer in mathematics at Christ Church College, Oxford, in 1855. He was ordained in the Church of England in 1861 but never practiced his ministry. His writings published under this real name include articles and books on geometry, determinants, and the mathematics of tournaments and elections. (He also used the pseudonym Lewis Carroll for his many works on recreational logic.)

*Solution:* We can express these statements as:

$$\forall x(P(x) \rightarrow Q(x)).$$
$$\exists x(P(x) \wedge \neg R(x)).$$
$$\exists x(Q(x) \wedge \neg R(x)).$$

Notice that the second statement cannot be written as $\exists x(P(x) \rightarrow \neg R(x))$. The reason is that $P(x) \rightarrow \neg R(x)$ is true whenever $x$ is not a lion, so that $\exists x(P(x) \rightarrow \neg R(x))$ is true as long as there is at least one creature that is not a lion, even if every lion drinks coffee. Similarly, the third statement cannot be written as

$$\exists x(Q(x) \rightarrow \neg R(x)).$$ ◀

**EXAMPLE 27** Consider these statements, of which the first three are premises and the fourth is a valid conclusion.

"All hummingbirds are richly colored."
"No large birds live on honey."
"Birds that do not live on honey are dull in color."
"Hummingbirds are small."

Let $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ be the statements "$x$ is a hummingbird," "$x$ is large," "$x$ lives on honey," and "$x$ is richly colored," respectively. Assuming that the domain consists of all birds, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, $R(x)$, and $S(x)$.

*Solution:* We can express the statements in the argument as

$$\forall x(P(x) \rightarrow S(x)).$$
$$\neg\exists x(Q(x) \wedge R(x)).$$
$$\forall x(\neg R(x) \rightarrow \neg S(x)).$$
$$\forall x(P(x) \rightarrow \neg Q(x)).$$

(Note we have assumed that "small" is the same as "not large" and that "dull in color" is the same as "not richly colored." To show that the fourth statement is a valid conclusion of the first three, we need to use rules of inference that will be discussed in Section 1.6.) ◀

## Logic Programming

Links

An important type of programming language is designed to reason using the rules of predicate logic. Prolog (from *Pro*gramming in *Log*ic), developed in the 1970s by computer scientists working in the area of artificial intelligence, is an example of such a language. Prolog programs include a set of declarations consisting of two types of statements, **Prolog facts** and **Prolog rules**. Prolog facts define predicates by specifying the elements that satisfy these predicates. Prolog rules are used to define new predicates using those already defined by Prolog facts. Example 28 illustrates these notions.

**EXAMPLE 28** Consider a Prolog program given facts telling it the instructor of each class and in which classes students are enrolled. The program uses these facts to answer queries concerning the professors who teach particular students. Such a program could use the predicates $instructor(p, c)$ and

*enrolled*$(s, c)$ to represent that professor $p$ is the instructor of course $c$ and that student $s$ is enrolled in course $c$, respectively. For example, the Prolog facts in such a program might include:

```
instructor(chan,math273)
instructor(patel,ee222)
instructor(grossman,cs301)
enrolled(kevin,math273)
enrolled(juana,ee222)
enrolled(juana,cs301)
enrolled(kiko,math273)
enrolled(kiko,cs301)
```

(Lowercase letters have been used for entries because Prolog considers names beginning with an uppercase letter to be variables.)

A new predicate *teaches*$(p, s)$, representing that professor $p$ teaches student $s$, can be defined using the Prolog rule

```
teaches(P,S) :- instructor(P,C), enrolled(S,C)
```

which means that *teaches*$(p, s)$ is true if there exists a class $c$ such that professor $p$ is the instructor of class $c$ and student $s$ is enrolled in class $c$. (Note that a comma is used to represent a conjunction of predicates in Prolog. Similarly, a semicolon is used to represent a disjunction of predicates.)

Prolog answers queries using the facts and rules it is given. For example, using the facts and rules listed, the query

```
?enrolled(kevin,math273)
```

produces the response

```
yes
```

because the fact *enrolled*(kevin, math273) was provided as input. The query

```
?enrolled(X,math273)
```

produces the response

```
kevin
kiko
```

To produce this response, Prolog determines all possible values of $X$ for which *enrolled*$(X,$ math273) has been included as a Prolog fact. Similarly, to find all the professors who are instructors in classes being taken by Juana, we use the query

```
?teaches(X,juana)
```

This query returns

```
patel
grossman
```

## Exercises

**1.** Let $P(x)$ denote the statement "$x \leq 4$." What are these truth values?
**a)** $P(0)$ **b)** $P(4)$ **c)** $P(6)$

**2.** Let $P(x)$ be the statement "the word $x$ contains the letter $a$." What are these truth values?
**a)** $P(\text{orange})$ **b)** $P(\text{lemon})$
**c)** $P(\text{true})$ **d)** $P(\text{false})$

**3.** Let $Q(x, y)$ denote the statement "$x$ is the capital of $y$." What are these truth values?
**a)** $Q(\text{Denver, Colorado})$
**b)** $Q(\text{Detroit, Michigan})$
**c)** $Q(\text{Massachusetts, Boston})$
**d)** $Q(\text{New York, New York})$

**4.** State the value of $x$ after the statement **if** $P(x)$ **then** $x := 1$ is executed, where $P(x)$ is the statement "$x > 1$," if the value of $x$ when this statement is reached is
**a)** $x = 0$. **b)** $x = 1$.
**c)** $x = 2$.

**5.** Let $P(x)$ be the statement "$x$ spends more than five hours every weekday in class," where the domain for $x$ consists of all students. Express each of these quantifications in English.
**a)** $\exists x P(x)$ **b)** $\forall x P(x)$
**c)** $\exists x \neg P(x)$ **d)** $\forall x \neg P(x)$

**6.** Let $N(x)$ be the statement "$x$ has visited North Dakota," where the domain consists of the students in your school. Express each of these quantifications in English.
**a)** $\exists x N(x)$ **b)** $\forall x N(x)$ **c)** $\neg\exists x N(x)$
**d)** $\exists x \neg N(x)$ **e)** $\neg\forall x N(x)$ **f)** $\forall x \neg N(x)$

**7.** Translate these statements into English, where $C(x)$ is "$x$ is a comedian" and $F(x)$ is "$x$ is funny" and the domain consists of all people.
**a)** $\forall x(C(x) \rightarrow F(x))$ **b)** $\forall x(C(x) \wedge F(x))$
**c)** $\exists x(C(x) \rightarrow F(x))$ **d)** $\exists x(C(x) \wedge F(x))$

**8.** Translate these statements into English, where $R(x)$ is "$x$ is a rabbit" and $H(x)$ is "$x$ hops" and the domain consists of all animals.
**a)** $\forall x(R(x) \rightarrow H(x))$ **b)** $\forall x(R(x) \wedge H(x))$
**c)** $\exists x(R(x) \rightarrow H(x))$ **d)** $\exists x(R(x) \wedge H(x))$

**9.** Let $P(x)$ be the statement "$x$ can speak Russian" and let $Q(x)$ be the statement "$x$ knows the computer language C++." Express each of these sentences in terms of $P(x)$, $Q(x)$, quantifiers, and logical connectives. The domain for quantifiers consists of all students at your school.
**a)** There is a student at your school who can speak Russian and who knows C++.
**b)** There is a student at your school who can speak Russian but who doesn't know C++.
**c)** Every student at your school either can speak Russian or knows C++.
**d)** No student at your school can speak Russian or knows C++.

**10.** Let $C(x)$ be the statement "$x$ has a cat," let $D(x)$ be the statement "$x$ has a dog," and let $F(x)$ be the statement "$x$ has a ferret." Express each of these statements in terms of $C(x)$, $D(x)$, $F(x)$, quantifiers, and logical connectives. Let the domain consist of all students in your class.
**a)** A student in your class has a cat, a dog, and a ferret.
**b)** All students in your class have a cat, a dog, or a ferret.
**c)** Some student in your class has a cat and a ferret, but not a dog.
**d)** No student in your class has a cat, a dog, and a ferret.
**e)** For each of the three animals, cats, dogs, and ferrets, there is a student in your class who has this animal as a pet.

**11.** Let $P(x)$ be the statement "$x = x^2$." If the domain consists of the integers, what are these truth values?
**a)** $P(0)$ **b)** $P(1)$ **c)** $P(2)$
**d)** $P(-1)$ **e)** $\exists x P(x)$ **f)** $\forall x P(x)$

**12.** Let $Q(x)$ be the statement "$x + 1 > 2x$." If the domain consists of all integers, what are these truth values?
**a)** $Q(0)$ **b)** $Q(-1)$ **c)** $Q(1)$
**d)** $\exists x Q(x)$ **e)** $\forall x Q(x)$ **f)** $\exists x \neg Q(x)$
**g)** $\forall x \neg Q(x)$

**13.** Determine the truth value of each of these statements if the domain consists of all integers.
**a)** $\forall n(n + 1 > n)$ **b)** $\exists n(2n = 3n)$
**c)** $\exists n(n = -n)$ **d)** $\forall n(3n \leq 4n)$

**14.** Determine the truth value of each of these statements if the domain consists of all real numbers.
**a)** $\exists x(x^3 = -1)$ **b)** $\exists x(x^4 < x^2)$
**c)** $\forall x((-x)^2 = x^2)$ **d)** $\forall x(2x > x)$

**15.** Determine the truth value of each of these statements if the domain for all variables consists of all integers.
**a)** $\forall n(n^2 \geq 0)$ **b)** $\exists n(n^2 = 2)$
**c)** $\forall n(n^2 \geq n)$ **d)** $\exists n(n^2 < 0)$

**16.** Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.
**a)** $\exists x(x^2 = 2)$ **b)** $\exists x(x^2 = -1)$
**c)** $\forall x(x^2 + 2 \geq 1)$ **d)** $\forall x(x^2 \neq x)$

**17.** Suppose that the domain of the propositional function $P(x)$ consists of the integers 0, 1, 2, 3, and 4. Write out each of these propositions using disjunctions, conjunctions, and negations.
**a)** $\exists x P(x)$ **b)** $\forall x P(x)$ **c)** $\exists x \neg P(x)$
**d)** $\forall x \neg P(x)$ **e)** $\neg\exists x P(x)$ **f)** $\neg\forall x P(x)$

**18.** Suppose that the domain of the propositional function $P(x)$ consists of the integers $-2$, $-1$, 0, 1, and 2. Write out each of these propositions using disjunctions, conjunctions, and negations.
**a)** $\exists x P(x)$ **b)** $\forall x P(x)$ **c)** $\exists x \neg P(x)$
**d)** $\forall x \neg P(x)$ **e)** $\neg\exists x P(x)$ **f)** $\neg\forall x P(x)$

**19.** Suppose that the domain of the propositional function $P(x)$ consists of the integers 1, 2, 3, 4, and 5. Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.

**a)** $\exists x P(x)$ **b)** $\forall x P(x)$
**c)** $\neg\exists x P(x)$ **d)** $\neg\forall x P(x)$
**e)** $\forall x((x \neq 3) \rightarrow P(x)) \vee \exists x \neg P(x)$

**20.** Suppose that the domain of the propositional function $P(x)$ consists of $-5$, $-3$, $-1$, 1, 3, and 5. Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.

**a)** $\exists x P(x)$ **b)** $\forall x P(x)$
**c)** $\forall x((x \neq 1) \rightarrow P(x))$
**d)** $\exists x((x \geq 0) \wedge P(x))$
**e)** $\exists x(\neg P(x)) \wedge \forall x((x < 0) \rightarrow P(x))$

**21.** For each of these statements find a domain for which the statement is true and a domain for which the statement is false.

**a)** Everyone is studying discrete mathematics.
**b)** Everyone is older than 21 years.
**c)** Every two people have the same mother.
**d)** No two different people have the same grandmother.

**22.** For each of these statements find a domain for which the statement is true and a domain for which the statement is false.

**a)** Everyone speaks Hindi.
**b)** There is someone older than 21 years.
**c)** Every two people have the same first name.
**d)** Someone knows more than two other people.

**23.** Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.

**a)** Someone in your class can speak Hindi.
**b)** Everyone in your class is friendly.
**c)** There is a person in your class who was not born in California.
**d)** A student in your class has been in a movie.
**e)** No student in your class has taken a course in logic programming.

**24.** Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.

**a)** Everyone in your class has a cellular phone.
**b)** Somebody in your class has seen a foreign movie.
**c)** There is a person in your class who cannot swim.
**d)** All students in your class can solve quadratic equations.
**e)** Some student in your class does not want to be rich.

**25.** Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.

**a)** No one is perfect.
**b)** Not everyone is perfect.
**c)** All your friends are perfect.
**d)** At least one of your friends is perfect.
**e)** Everyone is your friend and is perfect.
**f)** Not everybody is your friend or someone is not perfect.

**26.** Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.

**a)** Someone in your school has visited Uzbekistan.
**b)** Everyone in your class has studied calculus and C++.
**c)** No one in your school owns both a bicycle and a motorcycle.
**d)** There is a person in your school who is not happy.
**e)** Everyone in your school was born in the twentieth century.

**27.** Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.

**a)** A student in your school has lived in Vietnam.
**b)** There is a student in your school who cannot speak Hindi.
**c)** A student in your school knows Java, Prolog, and C++.
**d)** Everyone in your class enjoys Thai food.
**e)** Someone in your class does not play hockey.

**28.** Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.

**a)** Something is not in the correct place.
**b)** All tools are in the correct place and are in excellent condition.
**c)** Everything is in the correct place and in excellent condition.
**d)** Nothing is in the correct place and is in excellent condition.
**e)** One of your tools is not in the correct place, but it is in excellent condition.

**29.** Express each of these statements using logical operators, predicates, and quantifiers.

**a)** Some propositions are tautologies.
**b)** The negation of a contradiction is a tautology.
**c)** The disjunction of two contingencies can be a tautology.
**d)** The conjunction of two tautologies is a tautology.

**30.** Suppose the domain of the propositional function $P(x, y)$ consists of pairs $x$ and $y$, where $x$ is 1, 2, or 3 and $y$ is 1, 2, or 3. Write out these propositions using disjunctions and conjunctions.

**a)** $\exists x\, P(x, 3)$ **b)** $\forall y\, P(1, y)$
**c)** $\exists y \neg P(2, y)$ **d)** $\forall x \neg P(x, 2)$

**31.** Suppose that the domain of $Q(x, y, z)$ consists of triples $x, y, z$, where $x = 0$, 1, or 2, $y = 0$ or 1, and $z = 0$ or 1. Write out these propositions using disjunctions and conjunctions.

**a)** $\forall y Q(0, y, 0)$ **b)** $\exists x Q(x, 1, 1)$
**c)** $\exists z \neg Q(0, 0, z)$ **d)** $\exists x \neg Q(x, 0, 1)$

**32.** Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase "It is not the case that.")

**a)** All dogs have fleas.

**b)** There is a horse that can add.

**c)** Every koala can climb.

**d)** No monkey can speak French.

**e)** There exists a pig that can swim and catch fish.

**33.** Express each of these statements using quantifiers. Then form the negation of the statement, so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase "It is not the case that.")

**a)** Some old dogs can learn new tricks.

**b)** No rabbit knows calculus.

**c)** Every bird can fly.

**d)** There is no dog that can talk.

**e)** There is no one in this class who knows French and Russian.

**34.** Express the negation of these propositions using quantifiers, and then express the negation in English.

**a)** Some drivers do not obey the speed limit.

**b)** All Swedish movies are serious.

**c)** No one can keep a secret.

**d)** There is someone in this class who does not have a good attitude.

**35.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

**a)** $\forall x(x^2 \geq x)$

**b)** $\forall x(x > 0 \vee x < 0)$

**c)** $\forall x(x = 1)$

**36.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all real numbers.

**a)** $\forall x(x^2 \neq x)$ **b)** $\forall x(x^2 \neq 2)$

**c)** $\forall x(|x| > 0)$

**37.** Express each of these statements using predicates and quantifiers.

**a)** A passenger on an airline qualifies as an elite flyer if the passenger flies more than 25,000 miles in a year or takes more than 25 flights during that year.

**b)** A man qualifies for the marathon if his best previous time is less than 3 hours and a woman qualifies for the marathon if her best previous time is less than 3.5 hours.

**c)** A student must take at least 60 course hours, or at least 45 course hours and write a master's thesis, and receive a grade no lower than a B in all required courses, to receive a master's degree.

**d)** There is a student who has taken more than 21 credit hours in a semester and received all A's.

Exercises 38–42 deal with the translation between system specification and logical expressions involving quantifiers.

**38.** Translate these system specifications into English where the predicate $S(x, y)$ is "$x$ is in state $y$" and where the domain for $x$ and $y$ consists of all systems and all possible states, respectively.

**a)** $\exists x S(x, \text{open})$

**b)** $\forall x(S(x, \text{malfunctioning}) \vee S(x, \text{diagnostic}))$

**c)** $\exists x S(x, \text{open}) \vee \exists x S(x, \text{diagnostic})$

**d)** $\exists x \neg S(x, \text{available})$

**e)** $\forall x \neg S(x, \text{working})$

**39.** Translate these specifications into English where $F(p)$ is "Printer $p$ is out of service," $B(p)$ is "Printer $p$ is busy," $L(j)$ is "Print job $j$ is lost," and $Q(j)$ is "Print job $j$ is queued."

**a)** $\exists p(F(p) \wedge B(p)) \rightarrow \exists j L(j)$

**b)** $\forall p B(p) \rightarrow \exists j Q(j)$

**c)** $\exists j(Q(j) \wedge L(j)) \rightarrow \exists p F(p)$

**d)** $(\forall p B(p) \wedge \forall j Q(j)) \rightarrow \exists j L(j)$

**40.** Express each of these system specifications using predicates, quantifiers, and logical connectives.

**a)** When there is less than 30 megabytes free on the hard disk, a warning message is sent to all users.

**b)** No directories in the file system can be opened and no files can be closed when system errors have been detected.

**c)** The file system cannot be backed up if there is a user currently logged on.

**d)** Video on demand can be delivered when there are at least 8 megabytes of memory available and the connection speed is at least 56 kilobits per second.

**41.** Express each of these system specifications using predicates, quantifiers, and logical connectives.

**a)** At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.

**b)** Whenever there is an active alert, all queued messages are transmitted.

**c)** The diagnostic monitor tracks the status of all systems except the main console.

**d)** Each participant on the conference call whom the host of the call did not put on a special list was billed.

**42.** Express each of these system specifications using predicates, quantifiers, and logical connectives.

**a)** Every user has access to an electronic mailbox.

**b)** The system mailbox can be accessed by everyone in the group if the file system is locked.

**c)** The firewall is in a diagnostic state only if the proxy server is in a diagnostic state.

**d)** At least one router is functioning normally if the throughput is between 100 kbps and 500 kbps and the proxy server is not in diagnostic mode.

**43.** Determine whether $\forall x(P(x) \rightarrow Q(x))$ and $\forall x P(x) \rightarrow \forall x Q(x)$ are logically equivalent. Justify your answer.

**44.** Determine whether $\forall x(P(x) \leftrightarrow Q(x))$ and $\forall x\ P(x) \leftrightarrow \forall x Q(x)$ are logically equivalent. Justify your answer.

**45.** Show that $\exists x(P(x) \vee Q(x))$ and $\exists x P(x) \vee \exists x Q(x)$ are logically equivalent.

Exercises 46–49 establish rules for **null quantification** that we can use when a quantified variable does not appear in part of a statement.

**46.** Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.

**a)** $(\forall x P(x)) \vee A \equiv \forall x(P(x) \vee A)$

**b)** $(\exists x P(x)) \vee A \equiv \exists x(P(x) \vee A)$

**47.** Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.

**a)** $(\forall x P(x)) \wedge A \equiv \forall x(P(x) \wedge A)$

**b)** $(\exists x P(x)) \wedge A \equiv \exists x(P(x) \wedge A)$

**48.** Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.

**a)** $\forall x(A \rightarrow P(x)) \equiv A \rightarrow \forall x P(x)$

**b)** $\exists x(A \rightarrow P(x)) \equiv A \rightarrow \exists x P(x)$

**49.** Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.

**a)** $\forall x(P(x) \rightarrow A) \equiv \exists x P(x) \rightarrow A$

**b)** $\exists x(P(x) \rightarrow A) \equiv \forall x P(x) \rightarrow A$

**50.** Show that $\forall x P(x) \vee \forall x Q(x)$ and $\forall x(P(x) \vee Q(x))$ are not logically equivalent.

**51.** Show that $\exists x P(x) \wedge \exists x Q(x)$ and $\exists x(P(x) \wedge Q(x))$ are not logically equivalent.

**52.** As mentioned in the text, the notation $\exists! x P(x)$ denotes

"There exists a unique $x$ such that $P(x)$ is true."

If the domain consists of all integers, what are the truth values of these statements?

**a)** $\exists! x(x > 1)$ **b)** $\exists! x(x^2 = 1)$

**c)** $\exists! x(x + 3 = 2x)$ **d)** $\exists! x(x = x + 1)$

**53.** What are the truth values of these statements?

**a)** $\exists! x P(x) \rightarrow \exists x P(x)$

**b)** $\forall x P(x) \rightarrow \exists! x P(x)$

**c)** $\exists! x \neg P(x) \rightarrow \neg \forall x P(x)$

**54.** Write out $\exists! x P(x)$, where the domain consists of the integers 1, 2, and 3, in terms of negations, conjunctions, and disjunctions.

**55.** Given the Prolog facts in Example 28, what would Prolog return given these queries?

**a)** `?instructor(chan,math273)`

**b)** `?instructor(patel,cs301)`

**c)** `?enrolled(X,cs301)`

**d)** `?enrolled(kiko,Y)`

**e)** `?teaches(grossman,Y)`

**56.** Given the Prolog facts in Example 28, what would Prolog return when given these queries?

**a)** `?enrolled(kevin,ee222)`

**b)** `?enrolled(kiko,math273)`

**c)** `?instructor(grossman,X)`

**d)** `?instructor(X,cs301)`

**e)** `?teaches(X,kevin)`

**57.** Suppose that Prolog facts are used to define the predicates *mother*$(M, Y)$ and *father*$(F, X)$, which represent that $M$ is the mother of $Y$ and $F$ is the father of $X$, respectively. Give a Prolog rule to define the predicate *sibling*$(X, Y)$, which represents that $X$ and $Y$ are siblings (that is, have the same mother and the same father).

**58.** Suppose that Prolog facts are used to define the predicates *mother*$(M, Y)$ and *father*$(F, X)$, which represent that $M$ is the mother of $Y$ and $F$ is the father of $X$, respectively. Give a Prolog rule to define the predicate *grandfather*$(X, Y)$, which represents that $X$ is the grandfather of $Y$. [*Hint:* You can write a disjunction in Prolog either by using a semicolon to separate predicates or by putting these predicates on separate lines.]

Exercises 59–62 are based on questions found in the book *Symbolic Logic* by Lewis Carroll.

**59.** Let $P(x)$, $Q(x)$, and $R(x)$ be the statements "$x$ is a professor," "$x$ is ignorant," and "$x$ is vain," respectively. Express each of these statements using quantifiers; logical connectives; and $P(x)$, $Q(x)$, and $R(x)$, where the domain consists of all people.

**a)** No professors are ignorant.

**b)** All ignorant people are vain.

**c)** No professors are vain.

**d)** Does (c) follow from (a) and (b)?

**60.** Let $P(x)$, $Q(x)$, and $R(x)$ be the statements "$x$ is a clear explanation," "$x$ is satisfactory," and "$x$ is an excuse," respectively. Suppose that the domain for $x$ consists of all English text. Express each of these statements using quantifiers, logical connectives, and $P(x)$, $Q(x)$, and $R(x)$.

**a)** All clear explanations are satisfactory.

**b)** Some excuses are unsatisfactory.

**c)** Some excuses are not clear explanations.

***d)** Does (c) follow from (a) and (b)?

**61.** Let $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ be the statements "$x$ is a baby," "$x$ is logical," "$x$ is able to manage a crocodile," and "$x$ is despised," respectively. Suppose that the domain consists of all people. Express each of these statements using quantifiers; logical connectives; and $P(x)$, $Q(x)$, $R(x)$, and $S(x)$.

**a)** Babies are illogical.

**b)** Nobody is despised who can manage a crocodile.

**c)** Illogical persons are despised.

**d)** Babies cannot manage crocodiles.

***e)** Does (d) follow from (a), (b), and (c)? If not, is there a correct conclusion?

**62.** Let $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ be the statements "$x$ is a duck," "$x$ is one of my poultry," "$x$ is an officer," and "$x$ is willing to waltz," respectively. Express each of these statements using quantifiers; logical connectives; and $P(x)$, $Q(x)$, $R(x)$, and $S(x)$.

**a)** No ducks are willing to waltz.

**b)** No officers ever decline to waltz.

**c)** All my poultry are ducks.

**d)** My poultry are not officers.

***e)** Does (d) follow from (a), (b), and (c)? If not, is there a correct conclusion?

# 1.5 Nested Quantifiers

## Introduction

In Section 1.4 we defined the existential and universal quantifiers and showed how they can be used to represent mathematical statements. We also explained how they can be used to translate English sentences into logical expressions. However, in Section 1.4 we avoided **nested quantifiers**, where one quantifier is within the scope of another, such as

$$\forall x \exists y (x + y = 0).$$

Note that everything within the scope of a quantifier can be thought of as a propositional function. For example,

$$\forall x \exists y (x + y = 0)$$

is the same thing as $\forall x\, Q(x)$, where $Q(x)$ is $\exists y\, P(x, y)$, where $P(x, y)$ is $x + y = 0$.

Nested quantifiers commonly occur in mathematics and computer science. Although nested quantifiers can sometimes be difficult to understand, the rules we have already studied in Section 1.4 can help us use them. In this section we will gain experience working with nested quantifiers. We will see how to use nested quantifiers to express mathematical statements such as "The sum of two positive integers is always positive." We will show how nested quantifiers can be used to translate English sentences such as "Everyone has exactly one best friend" into logical statements. Moreover, we will gain experience working with the negations of statements involving nested quantifiers.

## Understanding Statements Involving Nested Quantifiers

To understand statements involving nested quantifiers, we need to unravel what the quantifiers and predicates that appear mean. This is illustrated in Examples 1 and 2.

**EXAMPLE 1** Assume that the domain for the variables $x$ and $y$ consists of all real numbers. The statement

$$\forall x \forall y (x + y = y + x)$$

Extra Examples says that $x + y = y + x$ for all real numbers $x$ and $y$. This is the commutative law for addition of real numbers. Likewise, the statement

$$\forall x \exists y (x + y = 0)$$

says that for every real number $x$ there is a real number $y$ such that $x + y = 0$. This states that every real number has an additive inverse. Similarly, the statement

$$\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$$

is the associative law for addition of real numbers. ◀

**EXAMPLE 2** Translate into English the statement

$$\forall x \forall y((x > 0) \wedge (y < 0) \rightarrow (xy < 0)),$$

where the domain for both variables consists of all real numbers.

*Solution:* This statement says that for every real number $x$ and for every real number $y$, if $x > 0$ and $y < 0$, then $xy < 0$. That is, this statement says that for real numbers $x$ and $y$, if $x$ is positive and $y$ is negative, then $xy$ is negative. This can be stated more succinctly as "The product of a positive real number and a negative real number is always a negative real number." ◀

THINKING OF QUANTIFICATION AS LOOPS In working with quantifications of more than one variable, it is sometimes helpful to think in terms of nested loops. (Of course, if there are infinitely many elements in the domain of some variable, we cannot actually loop through all values. Nevertheless, this way of thinking is helpful in understanding nested quantifiers.) For example, to see whether $\forall x \forall y P(x, y)$ is true, we loop through the values for $x$, and for each $x$ we loop through the values for $y$. If we find that $P(x, y)$ is true for all values for $x$ and $y$, we have determined that $\forall x \forall y P(x, y)$ is true. If we ever hit a value $x$ for which we hit a value $y$ for which $P(x, y)$ is false, we have shown that $\forall x \forall y P(x, y)$ is false.

Similarly, to determine whether $\forall x \exists y P(x, y)$ is true, we loop through the values for $x$. For each $x$ we loop through the values for $y$ until we find a $y$ for which $P(x, y)$ is true. If for every $x$ we hit such a $y$, then $\forall x \exists y P(x, y)$ is true; if for some $x$ we never hit such a $y$, then $\forall x \exists y P(x, y)$ is false.

To see whether $\exists x \forall y P(x, y)$ is true, we loop through the values for $x$ until we find an $x$ for which $P(x, y)$ is always true when we loop through all values for $y$. Once we find such an $x$, we know that $\exists x \forall y P(x, y)$ is true. If we never hit such an $x$, then we know that $\exists x \forall y P(x, y)$ is false.

Finally, to see whether $\exists x \exists y P(x, y)$ is true, we loop through the values for $x$, where for each $x$ we loop through the values for $y$ until we hit an $x$ for which we hit a $y$ for which $P(x, y)$ is true. The statement $\exists x \exists y P(x, y)$ is false only if we never hit an $x$ for which we hit a $y$ such that $P(x, y)$ is true.

## The Order of Quantifiers

Many mathematical statements involve multiple quantifications of propositional functions involving more than one variable. It is important to note that the order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

These remarks are illustrated by Examples 3–5.

**EXAMPLE 3** Let $P(x, y)$ be the statement "$x + y = y + x$." What are the truth values of the quantifications $\forall x \forall y P(x, y)$ and $\forall y \forall x P(x, y)$ where the domain for all variables consists of all real numbers?

*Solution:* The quantification

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

Extra Examples

denotes the proposition

"For all real numbers $x$, for all real numbers $y$, $x + y = y + x$."

Because $P(x, y)$ is true for all real numbers $x$ and $y$ (it is the commutative law for addition, which is an axiom for the real numbers—see Appendix 1), the proposition $\forall x \forall y P(x, y)$ is true. Note that the statement $\forall y \forall x P(x, y)$ says "For all real numbers $y$, for all real numbers $x$, $x + y = y + x$." This has the same meaning as the statement "For all real numbers $x$, for all real numbers $y$, $x + y = y + x$." That is, $\forall x \forall y P(x, y)$ and $\forall y \forall x P(x, y)$ have the same meaning,

and both are true. This illustrates the principle that the order of nested universal quantifiers in a statement without other quantifiers can be changed without changing the meaning of the quantified statement. ◀

**EXAMPLE 4** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?

*Solution:* The quantification

$$\exists y \forall x Q(x, y)$$

denotes the proposition

"There is a real number $y$ such that for every real number $x$, $Q(x, y)$."

No matter what value of $y$ is chosen, there is only one value of $x$ for which $x + y = 0$. Because there is no real number $y$ such that $x + y = 0$ for all real numbers $x$, the statement $\exists y \forall x Q(x, y)$ is false.

The quantification

$$\forall x \exists y Q(x, y)$$

denotes the proposition

"For every real number $x$ there is a real number $y$ such that $Q(x, y)$."

Given a real number $x$, there is a real number $y$ such that $x + y = 0$; namely, $y = -x$. Hence, the statement $\forall x \exists y Q(x, y)$ is true. ◀

Be careful with the order of existential and universal quantifiers!

Example 4 illustrates that the order in which quantifiers appear makes a difference. The statements $\exists y \forall x P(x, y)$ and $\forall x \exists y P(x, y)$ are not logically equivalent. The statement $\exists y \forall x P(x, y)$ is true if and only if there is a $y$ that makes $P(x, y)$ true for every $x$. So, for this statement to be true, there must be a particular value of $y$ for which $P(x, y)$ is true regardless of the choice of $x$. On the other hand, $\forall x \exists y P(x, y)$ is true if and only if for every value of $x$ there is a value of $y$ for which $P(x, y)$ is true. So, for this statement to be true, no matter which $x$ you choose, there must be a value of $y$ (possibly depending on the $x$ you choose) for which $P(x, y)$ is true. In other words, in the second case, $y$ can depend on $x$, whereas in the first case, $y$ is a constant independent of $x$.

From these observations, it follows that if $\exists y \forall x P(x, y)$ is true, then $\forall x \exists y P(x, y)$ must also be true. However, if $\forall x \exists y P(x, y)$ is true, it is not necessary for $\exists y \forall x P(x, y)$ to be true. (See Supplementary Exercises 30 and 31.)

Table 1 summarizes the meanings of the different possible quantifications involving two variables.

Quantifications of more than two variables are also common, as Example 5 illustrates.

**EXAMPLE 5** Let $Q(x, y, z)$ be the statement "$x + y = z$." What are the truth values of the statements $\forall x \forall y \exists z Q(x, y, z)$ and $\exists z \forall x \forall y Q(x, y, z)$, where the domain of all variables consists of all real numbers?

*Solution:* Suppose that $x$ and $y$ are assigned values. Then, there exists a real number $z$ such that $x + y = z$. Consequently, the quantification

$$\forall x \forall y \exists z Q(x, y, z),$$

which is the statement

"For all real numbers $x$ and for all real numbers $y$ there is a real number $z$ such that $x + y = z$,"

**TABLE 1 Quantifications of Two Variables.**

| *Statement* | *When True?* | *When False?* |
|---|---|---|
| $\forall x \forall y P(x, y)$<br>$\forall y \forall x P(x, y)$ | $P(x, y)$ is true for every pair $x, y$. | There is a pair $x, y$ for which $P(x, y)$ is false. |
| $\forall x \exists y P(x, y)$ | For every $x$ there is a $y$ for which $P(x, y)$ is true. | There is an $x$ such that $P(x, y)$ is false for every $y$. |
| $\exists x \forall y P(x, y)$ | There is an $x$ for which $P(x, y)$ is true for every $y$. | For every $x$ there is a $y$ for which $P(x, y)$ is false. |
| $\exists x \exists y P(x, y)$<br>$\exists y \exists x P(x, y)$ | There is a pair $x, y$ for which $P(x, y)$ is true. | $P(x, y)$ is false for every pair $x, y$. |

is true. The order of the quantification here is important, because the quantification

$$\exists z \forall x \forall y Q(x, y, z),$$

which is the statement

> "There is a real number $z$ such that for all real numbers $x$ and for all real numbers $y$ it is true that $x + y = z$,"

is false, because there is no value of $z$ that satisfies the equation $x + y = z$ for all values of $x$ and $y$. ◀

## Translating Mathematical Statements into Statements Involving Nested Quantifiers

Mathematical statements expressed in English can be translated into logical expressions, as Examples 6–8 show.

**EXAMPLE 6** Translate the statement "The sum of two positive integers is always positive" into a logical expression.

*Solution:* To translate this statement into a logical expression, we first rewrite it so that the implied quantifiers and a domain are shown: "For every two integers, if these integers are both positive, then the sum of these integers is positive." Next, we introduce the variables $x$ and $y$ to obtain "For all positive integers $x$ and $y$, $x + y$ is positive." Consequently, we can express this statement as

Extra Examples

$$\forall x \forall y((x > 0) \wedge (y > 0) \rightarrow (x + y > 0)),$$

where the domain for both variables consists of all integers. Note that we could also translate this using the positive integers as the domain. Then the statement "The sum of two positive integers is always positive" becomes "For every two positive integers, the sum of these integers is positive. We can express this as

$$\forall x \forall y(x + y > 0),$$

where the domain for both variables consists of all positive integers. ◀

**EXAMPLE 7** Translate the statement "Every real number except zero has a multiplicative inverse." (A **multiplicative inverse** of a real number $x$ is a real number $y$ such that $xy = 1$.)

*Solution:* We first rewrite this as "For every real number $x$ except zero, $x$ has a multiplicative inverse." We can rewrite this as "For every real number $x$, if $x \neq 0$, then there exists a real number $y$ such that $xy = 1$." This can be rewritten as

$$\forall x((x \neq 0) \rightarrow \exists y(xy = 1)).$$ ◀

One example that you may be familiar with is the concept of limit, which is important in calculus.

**EXAMPLE 8** (***Requires calculus***) Use quantifiers to express the definition of the limit of a real-valued function $f(x)$ of a real variable $x$ at a point $a$ in its domain.

*Solution:* Recall that the definition of the statement

$$\lim_{x \to a} f(x) = L$$

is: For every real number $\epsilon > 0$ there exists a real number $\delta > 0$ such that $|f(x) - L| < \epsilon$ whenever $0 < |x - a| < \delta$. This definition of a limit can be phrased in terms of quantifiers by

$$\forall \epsilon \exists \delta \forall x(0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon),$$

where the domain for the variables $\delta$ and $\epsilon$ consists of all positive real numbers and for $x$ consists of all real numbers.

This definition can also be expressed as

$$\forall \epsilon > 0\ \exists \delta > 0\ \forall x(0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)$$

when the domain for the variables $\epsilon$ and $\delta$ consists of all real numbers, rather than just the positive real numbers. [Here, restricted quantifiers have been used. Recall that $\forall x > 0\ P(x)$ means that for all $x$ with $x > 0$, $P(x)$ is true.] ◀

## Translating from Nested Quantifiers into English

Expressions with nested quantifiers expressing statements in English can be quite complicated. The first step in translating such an expression is to write out what the quantifiers and predicates in the expression mean. The next step is to express this meaning in a simpler sentence. This process is illustrated in Examples 9 and 10.

**EXAMPLE 9** Translate the statement

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x, y)))$$

into English, where $C(x)$ is "$x$ has a computer," $F(x, y)$ is "$x$ and $y$ are friends," and the domain for both $x$ and $y$ consists of all students in your school.

*Solution:* The statement says that for every student $x$ in your school, $x$ has a computer or there is a student $y$ such that $y$ has a computer and $x$ and $y$ are friends. In other words, every student in your school has a computer or has a friend who has a computer. ◀

**EXAMPLE 10** Translate the statement

$$\exists x \forall y \forall z((F(x, y) \wedge F(x, z) \wedge (y \neq z)) \rightarrow \neg F(y, z))$$

into English, where $F(a,b)$ means $a$ and $b$ are friends and the domain for $x$, $y$, and $z$ consists of all students in your school.

*Solution:* We first examine the expression $(F(x, y) \wedge F(x, z) \wedge (y \neq z)) \rightarrow \neg F(y, z)$. This expression says that if students $x$ and $y$ are friends, and students $x$ and $z$ are friends, and furthermore, if $y$ and $z$ are not the same student, then $y$ and $z$ are not friends. It follows that the original statement, which is triply quantified, says that there is a student $x$ such that for all students $y$ and all students $z$ other than $y$, if $x$ and $y$ are friends and $x$ and $z$ are friends, then $y$ and $z$ are not friends. In other words, there is a student none of whose friends are also friends with each other. ◀

## Translating English Sentences into Logical Expressions

In Section 1.4 we showed how quantifiers can be used to translate sentences into logical expressions. However, we avoided sentences whose translation into logical expressions required the use of nested quantifiers. We now address the translation of such sentences.

**EXAMPLE 11** Express the statement "If a person is female and is a parent, then this person is someone's mother" as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives.

*Solution:* The statement "If a person is female and is a parent, then this person is someone's mother" can be expressed as "For every person $x$, if person $x$ is female and person $x$ is a parent, then there exists a person $y$ such that person $x$ is the mother of person $y$." We introduce the propositional functions $F(x)$ to represent "$x$ is female," $P(x)$ to represent "$x$ is a parent," and $M(x, y)$ to represent "$x$ is the mother of $y$." The original statement can be represented as

$$\forall x((F(x) \wedge P(x)) \rightarrow \exists y M(x, y)).$$

Using the null quantification rule in part (b) of Exercise 47 in Section 1.4, we can move $\exists y$ to the left so that it appears just after $\forall x$, because $y$ does not appear in $F(x) \wedge P(x)$. We obtain the logically equivalent expression

$$\forall x \exists y((F(x) \wedge P(x)) \rightarrow M(x, y)).$$ ◀

**EXAMPLE 12** Express the statement "Everyone has exactly one best friend" as a logical expression involving predicates, quantifiers with a domain consisting of all people, and logical connectives.

*Solution:* The statement "Everyone has exactly one best friend" can be expressed as "For every person $x$, person $x$ has exactly one best friend." Introducing the universal quantifier, we see that this statement is the same as "$\forall x$(person $x$ has exactly one best friend)," where the domain consists of all people.

To say that $x$ has exactly one best friend means that there is a person $y$ who is the best friend of $x$, and furthermore, that for every person $z$, if person $z$ is not person $y$, then $z$ is not the best friend of $x$. When we introduce the predicate $B(x, y)$ to be the statement "$y$ is the best friend of $x$," the statement that $x$ has exactly one best friend can be represented as

$$\exists y(B(x, y) \wedge \forall z((z \neq y) \rightarrow \neg B(x, z))).$$

Consequently, our original statement can be expressed as

$$\forall x \exists y(B(x, y) \wedge \forall z((z \neq y) \rightarrow \neg B(x, z))).$$

[Note that we can write this statement as $\forall x \exists! y B(x, y)$, where $\exists!$ is the "uniqueness quantifier" defined in Section 1.4.] ◀

**EXAMPLE 13** Use quantifiers to express the statement "There is a woman who has taken a flight on every airline in the world."

*Solution:* Let $P(w, f)$ be "$w$ has taken $f$" and $Q(f, a)$ be "$f$ is a flight on $a$." We can express the statement as

$$\exists w \forall a \exists f (P(w, f) \wedge Q(f, a)),$$

where the domains of discourse for $w$, $f$, and $a$ consist of all the women in the world, all airplane flights, and all airlines, respectively.

The statement could also be expressed as

$$\exists w \forall a \exists f R(w, f, a),$$

where $R(w, f, a)$ is "$w$ has taken $f$ on $a$." Although this is more compact, it somewhat obscures the relationships among the variables. Consequently, the first solution is usually preferable. ◀

## Negating Nested Quantifiers

Assessment

Statements involving nested quantifiers can be negated by successively applying the rules for negating statements involving a single quantifier. This is illustrated in Examples 14–16.

**EXAMPLE 14** Express the negation of the statement $\forall x \exists y (xy = 1)$ so that no negation precedes a quantifier.

Extra Examples

*Solution:* By successively applying De Morgan's laws for quantifiers in Table 2 of Section 1.4, we can move the negation in $\neg \forall x \exists y (xy = 1)$ inside all the quantifiers. We find that $\neg \forall x \exists y (xy = 1)$ is equivalent to $\exists x \neg \exists y (xy = 1)$, which is equivalent to $\exists x \forall y \neg (xy = 1)$. Because $\neg (xy = 1)$ can be expressed more simply as $xy \neq 1$, we conclude that our negated statement can be expressed as $\exists x \forall y (xy \neq 1)$. ◀

**EXAMPLE 15** Use quantifiers to express the statement that "There does not exist a woman who has taken a flight on every airline in the world."

*Solution:* This statement is the negation of the statement "There is a woman who has taken a flight on every airline in the world" from Example 13. By Example 13, our statement can be expressed as $\neg \exists w \forall a \exists f (P(w, f) \wedge Q(f, a))$, where $P(w, f)$ is "$w$ has taken $f$" and $Q(f, a)$ is "$f$ is a flight on $a$." By successively applying De Morgan's laws for quantifiers in Table 2 of Section 1.4 to move the negation inside successive quantifiers and by applying De Morgan's law for negating a conjunction in the last step, we find that our statement is equivalent to each of this sequence of statements:

$$\begin{aligned} \forall w \neg \forall a \exists f (P(w, f) \wedge Q(f, a)) &\equiv \forall w \exists a \neg \exists f (P(w, f) \wedge Q(f, a)) \\ &\equiv \forall w \exists a \forall f \neg (P(w, f) \wedge Q(f, a)) \\ &\equiv \forall w \exists a \forall f (\neg P(w, f) \vee \neg Q(f, a)). \end{aligned}$$

This last statement states "For every woman there is an airline such that for all flights, this woman has not taken that flight or that flight is not on this airline." ◀

**EXAMPLE 16** (*Requires calculus*) Use quantifiers and predicates to express the fact that $\lim_{x \to a} f(x)$ does not exist where $f(x)$ is a real-valued function of a real variable $x$ and $a$ belongs to the domain of $f$.

*Solution:* To say that $\lim_{x \to a} f(x)$ does not exist means that for all real numbers $L$, $\lim_{x \to a} f(x) \neq L$. By using Example 8, the statement $\lim_{x \to a} f(x) \neq L$ can be expressed as

$$\neg \forall \epsilon > 0 \, \exists \delta > 0 \, \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon).$$

Successively applying the rules for negating quantified expressions, we construct this sequence of equivalent statements

$$\begin{aligned}
&\neg \forall \epsilon > 0 \, \exists \delta > 0 \, \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\
&\quad \equiv \exists \epsilon > 0 \, \neg \exists \delta > 0 \, \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\
&\quad \equiv \exists \epsilon > 0 \, \forall \delta > 0 \, \neg \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\
&\quad \equiv \exists \epsilon > 0 \, \forall \delta > 0 \, \exists x \, \neg (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon) \\
&\quad \equiv \exists \epsilon > 0 \, \forall \delta > 0 \, \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon).
\end{aligned}$$

In the last step we used the equivalence $\neg(p \rightarrow q) \equiv p \wedge \neg q$, which follows from the fifth equivalence in Table 7 of Section 1.3.

Because the statement "$\lim_{x \to a} f(x)$ does not exist" means for all real numbers $L$, $\lim_{x \to a} f(x) \neq L$, this can be expressed as

$$\forall L \exists \epsilon > 0 \, \forall \delta > 0 \, \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon).$$

This last statement says that for every real number $L$ there is a real number $\epsilon > 0$ such that for every real number $\delta > 0$, there exists a real number $x$ such that $0 < |x - a| < \delta$ and $|f(x) - L| \geq \epsilon$. ◀

## Exercises

1. Translate these statements into English, where the domain for each variable consists of all real numbers.
   **a)** $\forall x \exists y (x < y)$
   **b)** $\forall x \forall y (((x \geq 0) \wedge (y \geq 0)) \rightarrow (xy \geq 0))$
   **c)** $\forall x \forall y \exists z (xy = z)$
2. Translate these statements into English, where the domain for each variable consists of all real numbers.
   **a)** $\exists x \forall y (xy = y)$
   **b)** $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$
   **c)** $\forall x \forall y \exists z (x = y + z)$
3. Let $Q(x, y)$ be the statement "$x$ has sent an e-mail message to $y$," where the domain for both $x$ and $y$ consists of all students in your class. Express each of these quantifications in English.
   **a)** $\exists x \exists y Q(x, y)$ **b)** $\exists x \forall y Q(x, y)$
   **c)** $\forall x \exists y Q(x, y)$ **d)** $\exists y \forall x Q(x, y)$
   **e)** $\forall y \exists x Q(x, y)$ **f)** $\forall x \forall y Q(x, y)$
4. Let $P(x, y)$ be the statement "Student $x$ has taken class $y$," where the domain for $x$ consists of all students in your class and for $y$ consists of all computer science courses at your school. Express each of these quantifications in English.
   **a)** $\exists x \exists y P(x, y)$ **b)** $\exists x \forall y P(x, y)$
   **c)** $\forall x \exists y P(x, y)$ **d)** $\exists y \forall x P(x, y)$
   **e)** $\forall y \exists x P(x, y)$ **f)** $\forall x \forall y P(x, y)$
5. Let $W(x, y)$ mean that student $x$ has visited website $y$, where the domain for $x$ consists of all students in your school and the domain for $y$ consists of all websites. Express each of these statements by a simple English sentence.
   **a)** $W$(Sarah Smith, www.att.com)
   **b)** $\exists x W(x,$ www.imdb.org)
   **c)** $\exists y W($José Orez, $y)$
   **d)** $\exists y (W($Ashok Puri, $y) \wedge W($Cindy Yoon, $y))$
   **e)** $\exists y \forall z (y \neq$ (David Belcher) $\wedge$ ($W$(David Belcher, $z$) $\rightarrow W(y,z)$))
   **f)** $\exists x \exists y \forall z ((x \neq y) \wedge (W(x, z) \leftrightarrow W(y, z)))$
6. Let $C(x, y)$ mean that student $x$ is enrolled in class $y$, where the domain for $x$ consists of all students in your school and the domain for $y$ consists of all classes being

given at your school. Express each of these statements by a simple English sentence.

**a)** $C$(Randy Goldberg, CS 252)
**b)** $\exists x C(x,$ Math 695)
**c)** $\exists y C($Carol Sitea, $y)$
**d)** $\exists x(C(x,$ Math 222) $\wedge C(x,$ CS 252))
**e)** $\exists x \exists y \forall z((x \neq y) \wedge (C(x, z) \rightarrow C(y, z)))$
**f)** $\exists x \exists y \forall z((x \neq y) \wedge (C(x, z) \leftrightarrow C(y, z)))$

**7.** Let $T(x, y)$ mean that student $x$ likes cuisine $y$, where the domain for $x$ consists of all students at your school and the domain for $y$ consists of all cuisines. Express each of these statements by a simple English sentence.

**a)** $\neg T($Abdallah Hussein, Japanese)
**b)** $\exists x T(x,$ Korean) $\wedge \forall x T(x,$ Mexican)
**c)** $\exists y(T($Monique Arsenault, $y) \vee$ $T($Jay Johnson, $y))$
**d)** $\forall x \forall z \exists y((x \neq z) \rightarrow \neg(T(x, y) \wedge T(z, y)))$
**e)** $\exists x \exists z \forall y(T(x, y) \leftrightarrow T(z, y))$
**f)** $\forall x \forall z \exists y(T(x, y) \leftrightarrow T(z, y))$

**8.** Let $Q(x, y)$ be the statement "student $x$ has been a contestant on quiz show $y$." Express each of these sentences in terms of $Q(x, y)$, quantifiers, and logical connectives, where the domain for $x$ consists of all students at your school and for $y$ consists of all quiz shows on television.

**a)** There is a student at your school who has been a contestant on a television quiz show.
**b)** No student at your school has ever been a contestant on a television quiz show.
**c)** There is a student at your school who has been a contestant on *Jeopardy* and on *Wheel of Fortune*.
**d)** Every television quiz show has had a student from your school as a contestant.
**e)** At least two students from your school have been contestants on *Jeopardy*.

**9.** Let $L(x, y)$ be the statement "$x$ loves $y$," where the domain for both $x$ and $y$ consists of all people in the world. Use quantifiers to express each of these statements.

**a)** Everybody loves Jerry.
**b)** Everybody loves somebody.
**c)** There is somebody whom everybody loves.
**d)** Nobody loves everybody.
**e)** There is somebody whom Lydia does not love.
**f)** There is somebody whom no one loves.
**g)** There is exactly one person whom everybody loves.
**h)** There are exactly two people whom Lynn loves.
**i)** Everyone loves himself or herself.
**j)** There is someone who loves no one besides himself or herself.

**10.** Let $F(x, y)$ be the statement "$x$ can fool $y$," where the domain consists of all people in the world. Use quantifiers to express each of these statements.

**a)** Everybody can fool Fred.
**b)** Evelyn can fool everybody.
**c)** Everybody can fool somebody.
**d)** There is no one who can fool everybody.
**e)** Everyone can be fooled by somebody.
**f)** No one can fool both Fred and Jerry.
**g)** Nancy can fool exactly two people.
**h)** There is exactly one person whom everybody can fool.
**i)** No one can fool himself or herself.
**j)** There is someone who can fool exactly one person besides himself or herself.

**11.** Let $S(x)$ be the predicate "$x$ is a student," $F(x)$ the predicate "$x$ is a faculty member," and $A(x, y)$ the predicate "$x$ has asked $y$ a question," where the domain consists of all people associated with your school. Use quantifiers to express each of these statements.

**a)** Lois has asked Professor Michaels a question.
**b)** Every student has asked Professor Gross a question.
**c)** Every faculty member has either asked Professor Miller a question or been asked a question by Professor Miller.
**d)** Some student has not asked any faculty member a question.
**e)** There is a faculty member who has never been asked a question by a student.
**f)** Some student has asked every faculty member a question.
**g)** There is a faculty member who has asked every other faculty member a question.
**h)** Some student has never been asked a question by a faculty member.

**12.** Let $I(x)$ be the statement "$x$ has an Internet connection" and $C(x, y)$ be the statement "$x$ and $y$ have chatted over the Internet," where the domain for the variables $x$ and $y$ consists of all students in your class. Use quantifiers to express each of these statements.

**a)** Jerry does not have an Internet connection.
**b)** Rachel has not chatted over the Internet with Chelsea.
**c)** Jan and Sharon have never chatted over the Internet.
**d)** No one in the class has chatted with Bob.
**e)** Sanjay has chatted with everyone except Joseph.
**f)** Someone in your class does not have an Internet connection.
**g)** Not everyone in your class has an Internet connection.
**h)** Exactly one student in your class has an Internet connection.
**i)** Everyone except one student in your class has an Internet connection.
**j)** Everyone in your class with an Internet connection has chatted over the Internet with at least one other student in your class.
**k)** Someone in your class has an Internet connection but has not chatted with anyone else in your class.
**l)** There are two students in your class who have not chatted with each other over the Internet.
**m)** There is a student in your class who has chatted with everyone in your class over the Internet.
**n)** There are at least two students in your class who have not chatted with the same person in your class.
**o)** There are two students in the class who between them have chatted with everyone else in the class.

**13.** Let $M(x, y)$ be "$x$ has sent $y$ an e-mail message" and $T(x, y)$ be "$x$ has telephoned $y$," where the domain consists of all students in your class. Use quantifiers to express each of these statements. (Assume that all e-mail messages that were sent are received, which is not the way things often work.)

**a)** Chou has never sent an e-mail message to Koko.
**b)** Arlene has never sent an e-mail message to or telephoned Sarah.
**c)** José has never received an e-mail message from Deborah.
**d)** Every student in your class has sent an e-mail message to Ken.
**e)** No one in your class has telephoned Nina.
**f)** Everyone in your class has either telephoned Avi or sent him an e-mail message.
**g)** There is a student in your class who has sent everyone else in your class an e-mail message.
**h)** There is someone in your class who has either sent an e-mail message or telephoned everyone else in your class.
**i)** There are two different students in your class who have sent each other e-mail messages.
**j)** There is a student who has sent himself or herself an e-mail message.
**k)** There is a student in your class who has not received an e-mail message from anyone else in the class and who has not been called by any other student in the class.
**l)** Every student in the class has either received an e-mail message or received a telephone call from another student in the class.
**m)** There are at least two students in your class such that one student has sent the other e-mail and the second student has telephoned the first student.
**n)** There are two different students in your class who between them have sent an e-mail message to or telephoned everyone else in the class.

**14.** Use quantifiers and predicates with more than one variable to express these statements.

**a)** There is a student in this class who can speak Hindi.
**b)** Every student in this class plays some sport.
**c)** Some student in this class has visited Alaska but has not visited Hawaii.
**d)** All students in this class have learned at least one programming language.
**e)** There is a student in this class who has taken every course offered by one of the departments in this school.
**f)** Some student in this class grew up in the same town as exactly one other student in this class.
**g)** Every student in this class has chatted with at least one other student in at least one chat group.

**15.** Use quantifiers and predicates with more than one variable to express these statements.

**a)** Every computer science student needs a course in discrete mathematics.
**b)** There is a student in this class who owns a personal computer.
**c)** Every student in this class has taken at least one computer science course.
**d)** There is a student in this class who has taken at least one course in computer science.
**e)** Every student in this class has been in every building on campus.
**f)** There is a student in this class who has been in every room of at least one building on campus.
**g)** Every student in this class has been in at least one room of every building on campus.

**16.** A discrete mathematics class contains 1 mathematics major who is a freshman, 12 mathematics majors who are sophomores, 15 computer science majors who are sophomores, 2 mathematics majors who are juniors, 2 computer science majors who are juniors, and 1 computer science major who is a senior. Express each of these statements in terms of quantifiers and then determine its truth value.

**a)** There is a student in the class who is a junior.
**b)** Every student in the class is a computer science major.
**c)** There is a student in the class who is neither a mathematics major nor a junior.
**d)** Every student in the class is either a sophomore or a computer science major.
**e)** There is a major such that there is a student in the class in every year of study with that major.

**17.** Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.

**a)** Every user has access to exactly one mailbox.
**b)** There is a process that continues to run during all error conditions only if the kernel is working correctly.
**c)** All users on the campus network can access all websites whose url has a .edu extension.
***d)** There are exactly two systems that monitor every remote server.

**18.** Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.

**a)** At least one console must be accessible during every fault condition.
**b)** The e-mail address of every user can be retrieved whenever the archive contains at least one message sent by every user on the system.
**c)** For every security breach there is at least one mechanism that can detect that breach if and only if there is a process that has not been compromised.
**d)** There are at least two paths connecting every two distinct endpoints on the network.
**e)** No one knows the password of every user on the system except for the system administrator, who knows all passwords.[

**19.** Express each of these statements using mathematical and logical operators, predicates, and quantifiers, where the domain consists of all integers.

**a)** The sum of two negative integers is negative.
**b)** The difference of two positive integers is not necessarily positive.

**c)** The sum of the squares of two integers is greater than or equal to the square of their sum.
**d)** The absolute value of the product of two integers is the product of their absolute values.

**20.** Express each of these statements using predicates, quantifiers, logical connectives, and mathematical operators where the domain consists of all integers.
**a)** The product of two negative integers is positive.
**b)** The average of two positive integers is positive.
**c)** The difference of two negative integers is not necessarily negative.
**d)** The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers.

**21.** Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that every positive integer is the sum of the squares of four integers.

**22.** Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that there is a positive integer that is not the sum of three squares.

**23.** Express each of these mathematical statements using predicates, quantifiers, logical connectives, and mathematical operators.
**a)** The product of two negative real numbers is positive.
**b)** The difference of a real number and itself is zero.
**c)** Every positive real number has exactly two square roots.
**d)** A negative real number does not have a square root that is a real number.

**24.** Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.
**a)** $\exists x \forall y(x + y = y)$
**b)** $\forall x \forall y(((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$
**c)** $\exists x \exists y(((x \leq 0) \wedge (y \leq 0)) \wedge (x - y > 0))$
**d)** $\forall x \forall y((x \neq 0) \wedge (y \neq 0) \leftrightarrow (xy \neq 0))$

**25.** Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.
**a)** $\exists x \forall y(xy = y)$
**b)** $\forall x \forall y(((x < 0) \wedge (y < 0)) \rightarrow (xy > 0))$
**c)** $\exists x \exists y((x^2 > y) \wedge (x < y))$
**d)** $\forall x \forall y \exists z(x + y = z)$

**26.** Let $Q(x, y)$ be the statement "$x + y = x - y$." If the domain for both variables consists of all integers, what are the truth values?
**a)** $Q(1, 1)$ **b)** $Q(2, 0)$
**c)** $\forall y Q(1, y)$ **d)** $\exists x Q(x, 2)$
**e)** $\exists x \exists y Q(x, y)$ **f)** $\forall x \exists y Q(x, y)$
**g)** $\exists y \forall x Q(x, y)$ **h)** $\forall y \exists x Q(x, y)$
**i)** $\forall x \forall y Q(x, y)$

**27.** Determine the truth value of each of these statements if the domain for all variables consists of all integers.
**a)** $\forall n \exists m(n^2 < m)$ **b)** $\exists n \forall m(n < m^2)$
**c)** $\forall n \exists m(n + m = 0)$ **d)** $\exists n \forall m(nm = m)$
**e)** $\exists n \exists m(n^2 + m^2 = 5)$ **f)** $\exists n \exists m(n^2 + m^2 = 6)$
**g)** $\exists n \exists m(n + m = 4 \wedge n - m = 1)$
**h)** $\exists n \exists m(n + m = 4 \wedge n - m = 2)$
**i)** $\forall n \forall m \exists p(p = (m + n)/2)$

**28.** Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.
**a)** $\forall x \exists y(x^2 = y)$ **b)** $\forall x \exists y(x = y^2)$
**c)** $\exists x \forall y(xy = 0)$ **d)** $\exists x \exists y(x + y \neq y + x)$
**e)** $\forall x(x \neq 0 \rightarrow \exists y(xy = 1))$
**f)** $\exists x \forall y(y \neq 0 \rightarrow xy = 1)$
**g)** $\forall x \exists y(x + y = 1)$
**h)** $\exists x \exists y(x + 2y = 2 \wedge 2x + 4y = 5)$
**i)** $\forall x \exists y(x + y = 2 \wedge 2x - y = 1)$
**j)** $\forall x \forall y \exists z(z = (x + y)/2)$

**29.** Suppose the domain of the propositional function $P(x, y)$ consists of pairs $x$ and $y$, where $x$ is 1, 2, or 3 and $y$ is 1, 2, or 3. Write out these propositions using disjunctions and conjunctions.
**a)** $\forall x \forall y P(x, y)$ **b)** $\exists x \exists y P(x, y)$
**c)** $\exists x \forall y P(x, y)$ **d)** $\forall y \exists x P(x, y)$

**30.** Rewrite each of these statements so that negations appear only within predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).
**a)** $\neg \exists y \exists x P(x, y)$ **b)** $\neg \forall x \exists y P(x, y)$
**c)** $\neg \exists y(Q(y) \wedge \forall x \neg R(x, y))$
**d)** $\neg \exists y(\exists x R(x, y) \vee \forall x S(x, y))$
**e)** $\neg \exists y(\forall x \exists z T(x, y, z) \vee \exists x \forall z U(x, y, z))$

**31.** Express the negations of each of these statements so that all negation symbols immediately precede predicates.
**a)** $\forall x \exists y \forall z T(x, y, z)$
**b)** $\forall x \exists y P(x, y) \vee \forall x \exists y Q(x, y)$
**c)** $\forall x \exists y(P(x, y) \wedge \exists z R(x, y, z))$
**d)** $\forall x \exists y(P(x, y) \rightarrow Q(x, y))$

**32.** Express the negations of each of these statements so that all negation symbols immediately precede predicates.
**a)** $\exists z \forall y \forall x T(x, y, z)$
**b)** $\exists x \exists y P(x, y) \wedge \forall x \forall y Q(x, y)$
**c)** $\exists x \exists y(Q(x, y) \leftrightarrow Q(y, x))$
**d)** $\forall y \exists x \exists z(T(x, y, z) \vee Q(x, y))$

**33.** Rewrite each of these statements so that negations appear only within predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).
**a)** $\neg \forall x \forall y P(x, y)$ **b)** $\neg \forall y \exists x P(x, y)$
**c)** $\neg \forall y \forall x(P(x, y) \vee Q(x, y))$
**d)** $\neg(\exists x \exists y \neg P(x, y) \wedge \forall x \forall y Q(x, y))$
**e)** $\neg \forall x(\exists y \forall z P(x, y, z) \wedge \exists z \forall y P(x, y, z))$

**34.** Find a common domain for the variables $x$, $y$, and $z$ for which the statement $\forall x \forall y((x \neq y) \rightarrow \forall z((z = x) \vee (z = y)))$ is true and another domain for which it is false.

**35.** Find a common domain for the variables $x, y, z$, and $w$ for which the statement $\forall x \forall y \forall z \exists w((w \neq x) \wedge (w \neq y) \wedge (w \neq z))$ is true and another common domain for these variables for which it is false.

**36.** Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase "It is not the case that.")

**a)** No one has lost more than one thousand dollars playing the lottery.
**b)** There is a student in this class who has chatted with exactly one other student.
**c)** No student in this class has sent e-mail to exactly two other students in this class.
**d)** Some student has solved every exercise in this book.
**e)** No student has solved at least one exercise in every section of this book.

**37.** Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the phrase "It is not the case that.")

**a)** Every student in this class has taken exactly two mathematics classes at this school.
**b)** Someone has visited every country in the world except Libya.
**c)** No one has climbed every mountain in the Himalayas.
**d)** Every movie actor has either been in a movie with Kevin Bacon or has been in a movie with someone who has been in a movie with Kevin Bacon.

**38.** Express the negations of these propositions using quantifiers, and in English.

**a)** Every student in this class likes mathematics.
**b)** There is a student in this class who has never seen a computer.
**c)** There is a student in this class who has taken every mathematics course offered at this school.
**d)** There is a student in this class who has been in at least one room of every building on campus.

**39.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

**a)** $\forall x \forall y(x^2 = y^2 \rightarrow x = y)$
**b)** $\forall x \exists y(y^2 = x)$
**c)** $\forall x \forall y(xy \geq x)$

**40.** Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

**a)** $\forall x \exists y(x = 1/y)$
**b)** $\forall x \exists y(y^2 - x < 100)$
**c)** $\forall x \forall y(x^2 \neq y^3)$

**41.** Use quantifiers to express the associative law for multiplication of real numbers.

**42.** Use quantifiers to express the distributive laws of multiplication over addition for real numbers.

**43.** Use quantifiers and logical connectives to express the fact that every linear polynomial (that is, polynomial of degree 1) with real coefficients and where the coefficient of $x$ is nonzero, has exactly one real root.

**44.** Use quantifiers and logical connectives to express the fact that a quadratic polynomial with real number coefficients has at most two real roots.

**45.** Determine the truth value of the statement $\forall x \exists y(xy = 1)$ if the domain for the variables consists of

**a)** the nonzero real numbers.
**b)** the nonzero integers.
**c)** the positive real numbers.

**46.** Determine the truth value of the statement $\exists x \forall y(x \leq y^2)$ if the domain for the variables consists of

**a)** the positive real numbers.
**b)** the integers.
**c)** the nonzero real numbers.

**47.** Show that the two statements $\neg \exists x \forall y P(x, y)$ and $\forall x \exists y \neg P(x, y)$, where both quantifiers over the first variable in $P(x, y)$ have the same domain, and both quantifiers over the second variable in $P(x, y)$ have the same domain, are logically equivalent.

***48.** Show that $\forall x P(x) \vee \forall x Q(x)$ and $\forall x \forall y(P(x) \vee Q(y))$, where all quantifiers have the same nonempty domain, are logically equivalent. (The new variable $y$ is used to combine the quantifications correctly.)

***49. a)** Show that $\forall x P(x) \wedge \exists x Q(x)$ is logically equivalent to $\forall x \exists y\ (P(x) \wedge Q(y))$, where all quantifiers have the same nonempty domain.
**b)** Show that $\forall x P(x) \vee \exists x Q(x)$ is equivalent to $\forall x \exists y\ (P(x) \vee Q(y))$, where all quantifiers have the same nonempty domain.

A statement is in **prenex normal form (PNF)** if and only if it is of the form

$$Q_1 x_1 Q_2 x_2 \cdots Q_k x_k P(x_1, x_2, \ldots, x_k),$$

where each $Q_i, i = 1, 2, \ldots, k$, is either the existential quantifier or the universal quantifier, and $P(x_1, \ldots, x_k)$ is a predicate involving no quantifiers. For example, $\exists x \forall y(P(x, y) \wedge Q(y))$ is in prenex normal form, whereas $\exists x P(x) \vee \forall x Q(x)$ is not (because the quantifiers do not all occur first).

Every statement formed from propositional variables, predicates, **T**, and **F** using logical connectives and quantifiers is equivalent to a statement in prenex normal form. Exercise 51 asks for a proof of this fact.

***50.** Put these statements in prenex normal form. [*Hint:* Use logical equivalence from Tables 6 and 7 in Section 1.3, Table 2 in Section 1.4, Example 19 in Section 1.4, Exercises 45 and 46 in Section 1.4, and Exercises 48 and 49.]

**a)** $\exists x P(x) \vee \exists x Q(x) \vee A$, where $A$ is a proposition not involving any quantifiers.
**b)** $\neg(\forall x P(x) \vee \forall x Q(x))$
**c)** $\exists x P(x) \rightarrow \exists x Q(x)$

****51.** Show how to transform an arbitrary statement to a statement in prenex normal form that is equivalent to the given statement. (Note: A formal solution of this exercise requires use of structural induction, covered in Section 5.3.)

***52.** Express the quantification $\exists! x P(x)$, introduced in Section 1.4, using universal quantifications, existential quantifications, and logical operators.

# 1.6 Rules of Inference

## Introduction

Later in this chapter we will study proofs. Proofs in mathematics are valid arguments that establish the truth of mathematical statements. By an **argument**, we mean a sequence of statements that end with a conclusion. By **valid**, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or **premises**, of the argument. That is, an argument is valid if and only if it is impossible for all the premises to be true and the conclusion to be false. To deduce new statements from statements we already have, we use rules of inference which are templates for constructing valid arguments. Rules of inference are our basic tools for establishing the truth of statements.

Before we study mathematical proofs, we will look at arguments that involve only compound propositions. We will define what it means for an argument involving compound propositions to be valid. Then we will introduce a collection of rules of inference in propositional logic. These rules of inference are among the most important ingredients in producing valid arguments. After we illustrate how rules of inference are used to produce valid arguments, we will describe some common forms of incorrect reasoning, called **fallacies**, which lead to invalid arguments.

After studying rules of inference in propositional logic, we will introduce rules of inference for quantified statements. We will describe how these rules of inference can be used to produce valid arguments. These rules of inference for statements involving existential and universal quantifiers play an important role in proofs in computer science and mathematics, although they are often used without being explicitly mentioned.

Finally, we will show how rules of inference for propositions and for quantified statements can be combined. These combinations of rule of inference are often used together in complicated arguments.

## Valid Arguments in Propositional Logic

Consider the following argument involving propositions (which, by definition, is a sequence of propositions):

"If you have a current password, then you can log onto the network."

"You have a current password."

Therefore,

"You can log onto the network."

We would like to determine whether this is a valid argument. That is, we would like to determine whether the conclusion "You can log onto the network" must be true when the premises "If you have a current password, then you can log onto the network" and "You have a current password" are both true.

Before we discuss the validity of this particular argument, we will look at its form. Use $p$ to represent "You have a current password" and $q$ to represent "You can log onto the network." Then, the argument has the form

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

where $\therefore$ is the symbol that denotes "therefore."

We know that when $p$ and $q$ are propositional variables, the statement $((p \rightarrow q) \wedge p) \rightarrow q$ is a tautology (see Exercise 10(c) in Section 1.3). In particular, when both $p \rightarrow q$ and $p$ are true, we know that $q$ must also be true. We say this form of argument is **valid** because whenever all its premises (all statements in the argument other than the final one, the conclusion) are true, the conclusion must also be true. Now suppose that both "If you have a current password, then you can log onto the network" and "You have a current password" are true statements. When we replace $p$ by "You have a current password" and $q$ by "You can log onto the network," it necessarily follows that the conclusion "You can log onto the network" is true. This argument is **valid** because its form is valid. Note that whenever we replace $p$ and $q$ by propositions where $p \rightarrow q$ and $p$ are both true, then $q$ must also be true.

What happens when we replace $p$ and $q$ in this argument form by propositions where not both $p$ and $p \rightarrow q$ are true? For example, suppose that $p$ represents "You have access to the network" and $q$ represents "You can change your grade" and that $p$ is true, but $p \rightarrow q$ is false. The argument we obtain by substituting these values of $p$ and $q$ into the argument form is

"If you have access to the network, then you can change your grade."
"You have access to the network."

$\therefore$ "You can change your grade."

The argument we obtained is a valid argument, but because one of the premises, namely the first premise, is false, we cannot conclude that the conclusion is true. (Most likely, this conclusion is false.)

In our discussion, to analyze an argument, we replaced propositions by propositional variables. This changed an argument to an **argument form**. We saw that the validity of an argument follows from the validity of the form of the argument. We summarize the terminology used to discuss the validity of arguments with our definition of the key notions.

**DEFINITION 1**

An *argument* in propositional logic is a sequence of propositions. All but the final proposition in the argument are called *premises* and the final proposition is called the *conclusion*. An argument is *valid* if the truth of all its premises implies that the conclusion is true.

An *argument form* in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is *valid* no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

From the definition of a valid argument form we see that the argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion $q$ is valid, when $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$ is a tautology.

The key to showing that an argument in propositional logic is valid is to show that its argument form is valid. Consequently, we would like techniques to show that argument forms are valid. We will now develop methods for accomplishing this task.

## Rules of Inference for Propositional Logic

We can always use a truth table to show that an argument form is valid. We do this by showing that whenever the premises are true, the conclusion must also be true. However, this can be a tedious approach. For example, when an argument form involves 10 different propositional variables, to use a truth table to show this argument form is valid requires $2^{10} = 1024$ different rows. Fortunately, we do not have to resort to truth tables. Instead, we can first establish the validity of some relatively simple argument forms, called **rules of inference**. These rules of inference can be used as building blocks to construct more complicated valid argument forms. We will now introduce the most important rules of inference in propositional logic.

The tautology $(p \wedge (p \rightarrow q)) \rightarrow q$ is the basis of the rule of inference called **modus ponens**, or the **law of detachment**. (Modus ponens is Latin for *mode that affirms*.) This tautology leads to the following valid argument form, which we have already seen in our initial discussion about arguments (where, as before, the symbol $\therefore$ denotes "therefore"):

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore\ q \end{array}$$

Using this notation, the hypotheses are written in a column, followed by a horizontal bar, followed by a line that begins with the therefore symbol and ends with the conclusion. In particular, modus ponens tells us that if a conditional statement and the hypothesis of this conditional statement are both true, then the conclusion must also be true. Example 1 illustrates the use of modus ponens.

**EXAMPLE 1** Suppose that the conditional statement "If it snows today, then we will go skiing" and its hypothesis, "It is snowing today," are true. Then, by modus ponens, it follows that the conclusion of the conditional statement, "We will go skiing," is true. ◀

As we mentioned earlier, a valid argument can lead to an incorrect conclusion if one or more of its premises is false. We illustrate this again in Example 2.

**EXAMPLE 2** Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument.

"If $\sqrt{2} > \frac{3}{2}$, then $\left(\sqrt{2}\right)^2 > \left(\frac{3}{2}\right)^2$. We know that $\sqrt{2} > \frac{3}{2}$. Consequently, $\left(\sqrt{2}\right)^2 = 2 > \left(\frac{3}{2}\right)^2 = \frac{9}{4}$."

*Solution:* Let $p$ be the proposition "$\sqrt{2} > \frac{3}{2}$" and $q$ the proposition "$2 > (\frac{3}{2})^2$." The premises of the argument are $p \rightarrow q$ and $p$, and $q$ is its conclusion. This argument is valid because it is constructed by using modus ponens, a valid argument form. However, one of its premises, $\sqrt{2} > \frac{3}{2}$, is false. Consequently, we cannot conclude that the conclusion is true. Furthermore, note that the conclusion of this argument is false, because $2 < \frac{9}{4}$. ◀

There are many useful rules of inference for propositional logic. Perhaps the most widely used of these are listed in Table 1. Exercises 9, 10, 15, and 30 in Section 1.3 ask for the verifications that these rules of inference are valid argument forms. We now give examples of arguments that use these rules of inference. In each argument, we first use propositional variables to express the propositions in the argument. We then show that the resulting argument form is a rule of inference from Table 1.

**TABLE 1 Rules of Inference.**

| *Rule of Inference* | *Tautology* | *Name* |
|---|---|---|
| $p$<br>$p \rightarrow q$<br>$\therefore q$ | $(p \wedge (p \rightarrow q)) \rightarrow q$ | Modus ponens |
| $\neg q$<br>$p \rightarrow q$<br>$\therefore \neg p$ | $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ | Modus tollens |
| $p \rightarrow q$<br>$q \rightarrow r$<br>$\therefore p \rightarrow r$ | $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ | Hypothetical syllogism |
| $p \vee q$<br>$\neg p$<br>$\therefore q$ | $((p \vee q) \wedge \neg p) \rightarrow q$ | Disjunctive syllogism |
| $p$<br>$\therefore p \vee q$ | $p \rightarrow (p \vee q)$ | Addition |
| $p \wedge q$<br>$\therefore p$ | $(p \wedge q) \rightarrow p$ | Simplification |
| $p$<br>$q$<br>$\therefore p \wedge q$ | $((p) \wedge (q)) \rightarrow (p \wedge q)$ | Conjunction |
| $p \vee q$<br>$\neg p \vee r$<br>$\therefore q \vee r$ | $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$ | Resolution |

**EXAMPLE 3** State which rule of inference is the basis of the following argument: "It is below freezing now. Therefore, it is either below freezing or raining now."

*Solution:* Let $p$ be the proposition "It is below freezing now" and $q$ the proposition "It is raining now." Then this argument is of the form

$$\begin{array}{l} p \\ \hline \therefore\ p \vee q \end{array}$$

This is an argument that uses the addition rule. ◀

**EXAMPLE 4** State which rule of inference is the basis of the following argument: "It is below freezing and raining now. Therefore, it is below freezing now."

*Solution:* Let $p$ be the proposition "It is below freezing now," and let $q$ be the proposition "It is raining now." This argument is of the form

$$\begin{array}{l} p \wedge q \\ \hline \therefore\ p \end{array}$$

This argument uses the simplification rule. ◀

**EXAMPLE 5** State which rule of inference is used in the argument:

> If it rains today, then we will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

*Solution:* Let $p$ be the proposition "It is raining today," let $q$ be the proposition "We will not have a barbecue today," and let $r$ be the proposition "We will have a barbecue tomorrow." Then this argument is of the form

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore\ p \rightarrow r \end{array}$$

Hence, this argument is a hypothetical syllogism. ◀

## Using Rules of Inference to Build Arguments

When there are many premises, several rules of inference are often needed to show that an argument is valid. This is illustrated by Examples 6 and 7, where the steps of arguments are displayed on separate lines, with the reason for each step explicitly stated. These examples also show how arguments in English can be analyzed using rules of inference.

**EXAMPLE 6** Show that the premises "It is not sunny this afternoon and it is colder than yesterday," "We will go swimming only if it is sunny," "If we do not go swimming, then we will take a canoe trip," and "If we take a canoe trip, then we will be home by sunset" lead to the conclusion "We will be home by sunset."

Extra Examples

*Solution:* Let $p$ be the proposition "It is sunny this afternoon," $q$ the proposition "It is colder than yesterday," $r$ the proposition "We will go swimming," $s$ the proposition "We will take a canoe trip," and $t$ the proposition "We will be home by sunset." Then the premises become $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$. The conclusion is simply $t$. We need to give a valid argument with premises $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, and $s \rightarrow t$ and conclusion $t$.

We construct an argument to show that our premises lead to the desired conclusion as follows.

| Step | Reason |
|---|---|
| 1. $\neg p \wedge q$ | Premise |
| 2. $\neg p$ | Simplification using (1) |
| 3. $r \rightarrow p$ | Premise |
| 4. $\neg r$ | Modus tollens using (2) and (3) |
| 5. $\neg r \rightarrow s$ | Premise |
| 6. $s$ | Modus ponens using (4) and (5) |
| 7. $s \rightarrow t$ | Premise |
| 8. $t$ | Modus ponens using (6) and (7) |

Note that we could have used a truth table to show that whenever each of the four hypotheses is true, the conclusion is also true. However, because we are working with five propositional variables, $p$, $q$, $r$, $s$, and $t$, such a truth table would have 32 rows. ◀

**EXAMPLE 7** Show that the premises "If you send me an e-mail message, then I will finish writing the program," "If you do not send me an e-mail message, then I will go to sleep early," and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed."

*Solution:* Let $p$ be the proposition "You send me an e-mail message," $q$ the proposition "I will finish writing the program," $r$ the proposition "I will go to sleep early," and $s$ the proposition "I will wake up feeling refreshed." Then the premises are $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$. The desired conclusion is $\neg q \rightarrow s$. We need to give a valid argument with premises $p \rightarrow q$, $\neg p \rightarrow r$, and $r \rightarrow s$ and conclusion $\neg q \rightarrow s$.

This argument form shows that the premises lead to the desired conclusion.

| Step | Reason |
|---|---|
| 1. $p \rightarrow q$ | Premise |
| 2. $\neg q \rightarrow \neg p$ | Contrapositive of (1) |
| 3. $\neg p \rightarrow r$ | Premise |
| 4. $\neg q \rightarrow r$ | Hypothetical syllogism using (2) and (3) |
| 5. $r \rightarrow s$ | Premise |
| 6. $\neg q \rightarrow s$ | Hypothetical syllogism using (4) and (5) |

◀

## Resolution

Links

Computer programs have been developed to automate the task of reasoning and proving theorems. Many of these programs make use of a rule of inference known as **resolution**. This rule of inference is based on the tautology

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r).$$

(Exercise 30 in Section 1.3 asks for the verification that this is a tautology.) The final disjunction in the resolution rule, $q \vee r$, is called the **resolvent**. When we let $q = r$ in this tautology, we obtain $(p \vee q) \wedge (\neg p \vee q) \rightarrow q$. Furthermore, when we let $r = \mathbf{F}$, we obtain $(p \vee q) \wedge (\neg p) \rightarrow q$ (because $q \vee \mathbf{F} \equiv q$), which is the tautology on which the rule of disjunctive syllogism is based.

**EXAMPLE 8** Use resolution to show that the hypotheses "Jasmine is skiing or it is not snowing" and "It is snowing or Bart is playing hockey" imply that "Jasmine is skiing or Bart is playing hockey."

Extra Examples

*Solution:* Let $p$ be the proposition "It is snowing," $q$ the proposition "Jasmine is skiing," and $r$ the proposition "Bart is playing hockey." We can represent the hypotheses as $\neg p \vee q$ and $p \vee r$, respectively. Using resolution, the proposition $q \vee r$, "Jasmine is skiing or Bart is playing hockey," follows. ◀

Resolution plays an important role in programming languages based on the rules of logic, such as Prolog (where resolution rules for quantified statements are applied). Furthermore, it can be used to build automatic theorem proving systems. To construct proofs in propositional logic using resolution as the only rule of inference, the hypotheses and the conclusion must be expressed as **clauses**, where a clause is a disjunction of variables or negations of these variables. We can replace a statement in propositional logic that is not a clause by one or more equivalent statements that are clauses. For example, suppose we have a statement of the form $p \vee (q \wedge r)$. Because $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, we can replace the single statement $p \vee (q \wedge r)$ by two statements $p \vee q$ and $p \vee r$, each of which is a clause. We can replace a statement of the form $\neg(p \vee q)$ by the two statements $\neg p$ and $\neg q$ because De Morgan's law tells us that $\neg(p \vee q) \equiv \neg p \wedge \neg q$. We can also replace a conditional statement $p \rightarrow q$ with the equivalent disjunction $\neg p \vee q$.

**EXAMPLE 9** Show that the premises $(p \wedge q) \vee r$ and $r \rightarrow s$ imply the conclusion $p \vee s$.

*Solution:* We can rewrite the premises $(p \wedge q) \vee r$ as two clauses, $p \vee r$ and $q \vee r$. We can also replace $r \rightarrow s$ by the equivalent clause $\neg r \vee s$. Using the two clauses $p \vee r$ and $\neg r \vee s$, we can use resolution to conclude $p \vee s$. ◀

## Fallacies

Several common fallacies arise in incorrect arguments. These fallacies resemble rules of inference, but are based on contingencies rather than tautologies. These are discussed here to show the distinction between correct and incorrect reasoning.

The proposition $((p \rightarrow q) \wedge q) \rightarrow p$ is not a tautology, because it is false when $p$ is false and $q$ is true. However, there are many incorrect arguments that treat this as a tautology. In other words, they treat the argument with premises $p \rightarrow q$ and $q$ and conclusion $p$ as a valid argument form, which it is not. This type of incorrect reasoning is called the **fallacy of affirming the conclusion**.

**EXAMPLE 10** Is the following argument valid?

> If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics.
>
> Therefore, you did every problem in this book.

*Solution:* Let $p$ be the proposition "You did every problem in this book." Let $q$ be the proposition "You learned discrete mathematics." Then this argument is of the form: if $p \rightarrow q$ and $q$, then $p$. This is an example of an incorrect argument using the fallacy of affirming the conclusion. Indeed, it is possible for you to learn discrete mathematics in some way other than by doing every problem in this book. (You may learn discrete mathematics by reading, listening to lectures, doing some, but not all, the problems in this book, and so on.) ◀

The proposition $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$ is not a tautology, because it is false when $p$ is false and $q$ is true. Many incorrect arguments use this incorrectly as a rule of inference. This type of incorrect reasoning is called the **fallacy of denying the hypothesis**.

**EXAMPLE 11** Let $p$ and $q$ be as in Example 10. If the conditional statement $p \rightarrow q$ is true, and $\neg p$ is true, is it correct to conclude that $\neg q$ is true? In other words, is it correct to assume that you did not learn discrete mathematics if you did not do every problem in the book, assuming that if you do every problem in this book, then you will learn discrete mathematics?

*Solution:* It is possible that you learned discrete mathematics even if you did not do every problem in this book. This incorrect argument is of the form $p \rightarrow q$ and $\neg p$ imply $\neg q$, which is an example of the fallacy of denying the hypothesis. ◀

## Rules of Inference for Quantified Statements

We have discussed rules of inference for propositions. We will now describe some important rules of inference for statements involving quantifiers. These rules of inference are used extensively in mathematical arguments, often without being explicitly mentioned.

**Universal instantiation** is the rule of inference used to conclude that $P(c)$ is true, where $c$ is a particular member of the domain, given the premise $\forall x\, P(x)$. Universal instantiation is used when we conclude from the statement "All women are wise" that "Lisa is wise," where Lisa is a member of the domain of all women.

**TABLE 2 Rules of Inference for Quantified Statements.**

| *Rule of Inference* | *Name* |
|---|---|
| $\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$ | Universal instantiation |
| $\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, P(x)}$ | Universal generalization |
| $\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c}$ | Existential instantiation |
| $\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$ | Existential generalization |

**Universal generalization** is the rule of inference that states that $\forall x\, P(x)$ is true, given the premise that $P(c)$ is true for all elements $c$ in the domain. Universal generalization is used when we show that $\forall x\, P(x)$ is true by taking an arbitrary element $c$ from the domain and showing that $P(c)$ is true. The element $c$ that we select must be an arbitrary, and not a specific, element of the domain. That is, when we assert from $\forall x\, P(x)$ the existence of an element $c$ in the domain, we have no control over $c$ and cannot make any other assumptions about $c$ other than it comes from the domain. Universal generalization is used implicitly in many proofs in mathematics and is seldom mentioned explicitly. However, the error of adding unwarranted assumptions about the arbitrary element $c$ when universal generalization is used is all too common in incorrect reasoning.

**Existential instantiation** is the rule that allows us to conclude that there is an element $c$ in the domain for which $P(c)$ is true if we know that $\exists x\, P(x)$ is true. We cannot select an arbitrary value of $c$ here, but rather it must be a $c$ for which $P(c)$ is true. Usually we have no knowledge of what $c$ is, only that it exists. Because it exists, we may give it a name ($c$) and continue our argument.

**Existential generalization** is the rule of inference that is used to conclude that $\exists x\, P(x)$ is true when a particular element $c$ with $P(c)$ true is known. That is, if we know one element $c$ in the domain for which $P(c)$ is true, then we know that $\exists x\, P(x)$ is true.

We summarize these rules of inference in Table 2. We will illustrate how some of these rules of inference for quantified statements are used in Examples 12 and 13.

**EXAMPLE 12** Show that the premises "Everyone in this discrete mathematics class has taken a course in computer science" and "Marla is a student in this class" imply the conclusion "Marla has taken a course in computer science."

*Solution:* Let $D(x)$ denote "$x$ is in this discrete mathematics class," and let $C(x)$ denote "$x$ has taken a course in computer science." Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Marla})$. The conclusion is $C(\text{Marla})$.

Extra Examples

The following steps can be used to establish the conclusion from the premises.

| Step | Reason |
|---|---|
| 1. $\forall x(D(x) \rightarrow C(x))$ | Premise |
| 2. $D(\text{Marla}) \rightarrow C(\text{Marla})$ | Universal instantiation from (1) |
| 3. $D(\text{Marla})$ | Premise |
| 4. $C(\text{Marla})$ | Modus ponens from (2) and (3) |

◀

**EXAMPLE 13** Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

*Solution:* Let $C(x)$ be "$x$ is in this class," $B(x)$ be "$x$ has read the book," and $P(x)$ be "$x$ passed the first exam." The premises are $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. These steps can be used to establish the conclusion from the premises.

| Step | Reason |
|---|---|
| 1. $\exists x(C(x) \wedge \neg B(x))$ | Premise |
| 2. $C(a) \wedge \neg B(a)$ | Existential instantiation from (1) |
| 3. $C(a)$ | Simplification from (2) |
| 4. $\forall x(C(x) \rightarrow P(x))$ | Premise |
| 5. $C(a) \rightarrow P(a)$ | Universal instantiation from (4) |
| 6. $P(a)$ | Modus ponens from (3) and (5) |
| 7. $\neg B(a)$ | Simplification from (2) |
| 8. $P(a) \wedge \neg B(a)$ | Conjunction from (6) and (7) |
| 9. $\exists x(P(x) \wedge \neg B(x))$ | Existential generalization from (8) |

◀

## Combining Rules of Inference for Propositions and Quantified Statements

We have developed rules of inference both for propositions and for quantified statements. Note that in our arguments in Examples 12 and 13 we used both universal instantiation, a rule of inference for quantified statements, and modus ponens, a rule of inference for propositional logic. We will often need to use this combination of rules of inference. Because universal instantiation and modus ponens are used so often together, this combination of rules is sometimes called **universal modus ponens**. This rule tells us that if $\forall x(P(x) \rightarrow Q(x))$ is true, and if $P(a)$ is true for a particular element $a$ in the domain of the universal quantifier, then $Q(a)$ must also be true. To see this, note that by universal instantiation, $P(a) \rightarrow Q(a)$ is true. Then, by modus ponens, $Q(a)$ must also be true. We can describe universal modus ponens as follows:

$$\begin{array}{l} \forall x(P(x) \rightarrow Q(x)) \\ P(a), \text{ where } a \text{ is a particular element in the domain} \\ \hline \therefore Q(a) \end{array}$$

Universal modus ponens is commonly used in mathematical arguments. This is illustrated in Example 14.

**EXAMPLE 14** Assume that "For all positive integers $n$, if $n$ is greater than 4, then $n^2$ is less than $2^n$" is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

*Solution:* Let $P(n)$ denote "$n > 4$" and $Q(n)$ denote "$n^2 < 2^n$." The statement "For all positive integers $n$, if $n$ is greater than 4, then $n^2$ is less than $2^n$" can be represented by $\forall n(P(n) \rightarrow Q(n))$, where the domain consists of all positive integers. We are assuming that $\forall n(P(n) \rightarrow Q(n))$ is true. Note that $P(100)$ is true because $100 > 4$. It follows by universal modus ponens that $Q(100)$ is true, namely that $100^2 < 2^{100}$. ◀

Another useful combination of a rule of inference from propositional logic and a rule of inference for quantified statements is **universal modus tollens**. Universal modus tollens

combines universal instantiation and modus tollens and can be expressed in the following way:

$\forall x(P(x) \rightarrow Q(x))$
$\neg Q(a)$, where $a$ is a particular element in the domain
$\therefore \neg P(a)$

The verification of universal modus tollens is left as Exercise 25. Exercises 26–29 develop additional combinations of rules of inference in propositional logic and quantified statements.

## Exercises

**1.** Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?

If Socrates is human, then Socrates is mortal.
Socrates is human.
$\therefore$ Socrates is mortal.

**2.** Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?

If George does not have eight legs, then he is not a spider.
George is a spider.
$\therefore$ George has eight legs.

**3.** What rule of inference is used in each of these arguments?
- **a)** Alice is a mathematics major. Therefore, Alice is either a mathematics major or a computer science major.
- **b)** Jerry is a mathematics major and a computer science major. Therefore, Jerry is a mathematics major.
- **c)** If it is rainy, then the pool will be closed. It is rainy. Therefore, the pool is closed.
- **d)** If it snows today, the university will close. The university is not closed today. Therefore, it did not snow today.
- **e)** If I go swimming, then I will stay in the sun too long. If I stay in the sun too long, then I will sunburn. Therefore, if I go swimming, then I will sunburn.

**4.** What rule of inference is used in each of these arguments?
- **a)** Kangaroos live in Australia and are marsupials. Therefore, kangaroos are marsupials.
- **b)** It is either hotter than 100 degrees today or the pollution is dangerous. It is less than 100 degrees outside today. Therefore, the pollution is dangerous.
- **c)** Linda is an excellent swimmer. If Linda is an excellent swimmer, then she can work as a lifeguard. Therefore, Linda can work as a lifeguard.
- **d)** Steve will work at a computer company this summer. Therefore, this summer Steve will work at a computer company or he will be a beach bum.
- **e)** If I work all night on this homework, then I can answer all the exercises. If I answer all the exercises, I will understand the material. Therefore, if I work all night on this homework, then I will understand the material.

**5.** Use rules of inference to show that the hypotheses "Randy works hard," "If Randy works hard, then he is a dull boy," and "If Randy is a dull boy, then he will not get the job" imply the conclusion "Randy will not get the job."

**6.** Use rules of inference to show that the hypotheses "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on," "If the sailing race is held, then the trophy will be awarded," and "The trophy was not awarded" imply the conclusion "It rained."

**7.** What rules of inference are used in this famous argument? "All men are mortal. Socrates is a man. Therefore, Socrates is mortal."

**8.** What rules of inference are used in this argument? "No man is an island. Manhattan is an island. Therefore, Manhattan is not a man."

**9.** For each of these collections of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.
- **a)** "If I take the day off, it either rains or snows." "I took Tuesday off or I took Thursday off." "It was sunny on Tuesday." "It did not snow on Thursday."
- **b)** "If I eat spicy foods, then I have strange dreams." "I have strange dreams if there is thunder while I sleep." "I did not have strange dreams."
- **c)** "I am either clever or lucky." "I am not lucky." "If I am lucky, then I will win the lottery."
- **d)** "Every computer science major has a personal computer." "Ralph does not have a personal computer." "Ann has a personal computer."
- **e)** "What is good for corporations is good for the United States." "What is good for the United States is good for you." "What is good for corporations is for you to buy lots of stuff."
- **f)** "All rodents gnaw their food." "Mice are rodents." "Rabbits do not gnaw their food." "Bats are not rodents."

**10.** For each of these sets of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.

**a)** "If I play hockey, then I am sore the next day." "I use the whirlpool if I am sore." "I did not use the whirlpool."

**b)** "If I work, it is either sunny or partly sunny." "I worked last Monday or I worked last Friday." "It was not sunny on Tuesday." "It was not partly sunny on Friday."

**c)** "All insects have six legs." "Dragonflies are insects." "Spiders do not have six legs." "Spiders eat dragonflies."

**d)** "Every student has an Internet account." "Homer does not have an Internet account." "Maggie has an Internet account."

**e)** "All foods that are healthy to eat do not taste good." "Tofu is healthy to eat." "You only eat what tastes good." "You do not eat tofu." "Cheeseburgers are not healthy to eat."

**f)** "I am either dreaming or hallucinating." "I am not dreaming." "If I am hallucinating, I see elephants running down the road."

**11.** Show that the argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion $q \rightarrow r$ is valid if the argument form with premises $p_1, p_2, \ldots, p_n, q$, and conclusion $r$ is valid.

**12.** Show that the argument form with premises $(p \wedge t) \rightarrow (r \vee s)$, $q \rightarrow (u \wedge t)$, $u \rightarrow p$, and $\neg s$ and conclusion $q \rightarrow r$ is valid by first using Exercise 11 and then using rules of inference from Table 1.

**13.** For each of these arguments, explain which rules of inference are used for each step.

**a)** "Doug, a student in this class, knows how to write programs in JAVA. Everyone who knows how to write programs in JAVA can get a high-paying job. Therefore, someone in this class can get a high-paying job."

**b)** "Somebody in this class enjoys whale watching. Every person who enjoys whale watching cares about ocean pollution. Therefore, there is a person in this class who cares about ocean pollution."

**c)** "Each of the 93 students in this class owns a personal computer. Everyone who owns a personal computer can use a word processing program. Therefore, Zeke, a student in this class, can use a word processing program."

**d)** "Everyone in New Jersey lives within 50 miles of the ocean. Someone in New Jersey has never seen the ocean. Therefore, someone who lives within 50 miles of the ocean has never seen the ocean."

**14.** For each of these arguments, explain which rules of inference are used for each step.

**a)** "Linda, a student in this class, owns a red convertible. Everyone who owns a red convertible has gotten at least one speeding ticket. Therefore, someone in this class has gotten a speeding ticket."

**b)** "Each of five roommates, Melissa, Aaron, Ralph, Veneesha, and Keeshawn, has taken a course in discrete mathematics. Every student who has taken a course in discrete mathematics can take a course in algorithms. Therefore, all five roommates can take a course in algorithms next year."

**c)** "All movies produced by John Sayles are wonderful. John Sayles produced a movie about coal miners. Therefore, there is a wonderful movie about coal miners."

**d)** "There is someone in this class who has been to France. Everyone who goes to France visits the Louvre. Therefore, someone in this class has visited the Louvre."

**15.** For each of these arguments determine whether the argument is correct or incorrect and explain why.

**a)** All students in this class understand logic. Xavier is a student in this class. Therefore, Xavier understands logic.

**b)** Every computer science major takes discrete mathematics. Natasha is taking discrete mathematics. Therefore, Natasha is a computer science major.

**c)** All parrots like fruit. My pet bird is not a parrot. Therefore, my pet bird does not like fruit.

**d)** Everyone who eats granola every day is healthy. Linda is not healthy. Therefore, Linda does not eat granola every day.

**16.** For each of these arguments determine whether the argument is correct or incorrect and explain why.

**a)** Everyone enrolled in the university has lived in a dormitory. Mia has never lived in a dormitory. Therefore, Mia is not enrolled in the university.

**b)** A convertible car is fun to drive. Isaac's car is not a convertible. Therefore, Isaac's car is not fun to drive.

**c)** Quincy likes all action movies. Quincy likes the movie *Eight Men Out*. Therefore, *Eight Men Out* is an action movie.

**d)** All lobstermen set at least a dozen traps. Hamilton is a lobsterman. Therefore, Hamilton sets at least a dozen traps.

**17.** What is wrong with this argument? Let $H(x)$ be "$x$ is happy." Given the premise $\exists x\, H(x)$, we conclude that $H(\text{Lola})$. Therefore, Lola is happy.

**18.** What is wrong with this argument? Let $S(x, y)$ be "$x$ is shorter than $y$." Given the premise $\exists s\, S(s, \text{Max})$, it follows that $S(\text{Max}, \text{Max})$. Then by existential generalization it follows that $\exists x\, S(x, x)$, so that someone is shorter than himself.

**19.** Determine whether each of these arguments is valid. If an argument is correct, what rule of inference is being used? If it is not, what logical error occurs?

**a)** If $n$ is a real number such that $n > 1$, then $n^2 > 1$. Suppose that $n^2 > 1$. Then $n > 1$.

**b)** If $n$ is a real number with $n > 3$, then $n^2 > 9$. Suppose that $n^2 \leq 9$. Then $n \leq 3$.

**c)** If $n$ is a real number with $n > 2$, then $n^2 > 4$. Suppose that $n \leq 2$. Then $n^2 \leq 4$.

**20.** Determine whether these are valid arguments.

**a)** If $x$ is a positive real number, then $x^2$ is a positive real number. Therefore, if $a^2$ is positive, where $a$ is a real number, then $a$ is a positive real number.

**b)** If $x^2 \neq 0$, where $x$ is a real number, then $x \neq 0$. Let $a$ be a real number with $a^2 \neq 0$; then $a \neq 0$.

**21.** Which rules of inference are used to establish the conclusion of Lewis Carroll's argument described in Example 26 of Section 1.4?

**22.** Which rules of inference are used to establish the conclusion of Lewis Carroll's argument described in Example 27 of Section 1.4?

**23.** Identify the error or errors in this argument that supposedly shows that if $\exists x P(x) \wedge \exists x Q(x)$ is true then $\exists x(P(x) \wedge Q(x))$ is true.

| | |
|---|---|
| 1. $\exists x P(x) \vee \exists x Q(x)$ | Premise |
| 2. $\exists x P(x)$ | Simplification from (1) |
| 3. $P(c)$ | Existential instantiation from (2) |
| 4. $\exists x Q(x)$ | Simplification from (1) |
| 5. $Q(c)$ | Existential instantiation from (4) |
| 6. $P(c) \wedge Q(c)$ | Conjunction from (3) and (5) |
| 7. $\exists x(P(x) \wedge Q(x))$ | Existential generalization |

**24.** Identify the error or errors in this argument that supposedly shows that if $\forall x(P(x) \vee Q(x))$ is true then $\forall x P(x) \vee \forall x Q(x)$ is true.

| | |
|---|---|
| 1. $\forall x(P(x) \vee Q(x))$ | Premise |
| 2. $P(c) \vee Q(c)$ | Universal instantiation from (1) |
| 3. $P(c)$ | Simplification from (2) |
| 4. $\forall x P(x)$ | Universal generalization from (3) |
| 5. $Q(c)$ | Simplification from (2) |
| 6. $\forall x Q(x)$ | Universal generalization from (5) |
| 7. $\forall x(P(x) \vee \forall x Q(x))$ | Conjunction from (4) and (6) |

**25.** Justify the rule of universal modus tollens by showing that the premises $\forall x(P(x) \rightarrow Q(x))$ and $\neg Q(a)$ for a particular element $a$ in the domain, imply $\neg P(a)$.

**26.** Justify the rule of **universal transitivity**, which states that if $\forall x(P(x) \rightarrow Q(x))$ and $\forall x(Q(x) \rightarrow R(x))$ are true, then $\forall x(P(x) \rightarrow R(x))$ is true, where the domains of all quantifiers are the same.

**27.** Use rules of inference to show that if $\forall x(P(x) \rightarrow (Q(x) \wedge S(x)))$ and $\forall x(P(x) \wedge R(x))$ are true, then $\forall x(R(x) \wedge S(x))$ is true.

**28.** Use rules of inference to show that if $\forall x(P(x) \vee Q(x))$ and $\forall x((\neg P(x) \wedge Q(x)) \rightarrow R(x))$ are true, then $\forall x(\neg R(x) \rightarrow P(x))$ is also true, where the domains of all quantifiers are the same.

**29.** Use rules of inference to show that if $\forall x(P(x) \vee Q(x))$, $\forall x(\neg Q(x) \vee S(x))$, $\forall x(R(x) \rightarrow \neg S(x))$, and $\exists x \neg P(x)$ are true, then $\exists x \neg R(x)$ is true.

**30.** Use resolution to show the hypotheses "Allen is a bad boy or Hillary is a good girl" and "Allen is a good boy or David is happy" imply the conclusion "Hillary is a good girl or David is happy."

**31.** Use resolution to show that the hypotheses "It is not raining or Yvette has her umbrella," "Yvette does not have her umbrella or she does not get wet," and "It is raining or Yvette does not get wet" imply that "Yvette does not get wet."

**32.** Show that the equivalence $p \wedge \neg p \equiv \mathbf{F}$ can be derived using resolution together with the fact that a conditional statement with a false hypothesis is true. [*Hint:* Let $q = r = \mathbf{F}$ in resolution.]

**33.** Use resolution to show that the compound proposition $(p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$ is not satisfiable.

***34.** The Logic Problem, taken from *WFF'N PROOF, The Game of Logic*, has these two assumptions:

*1*. "Logic is difficult or not many students like logic."

*2*. "If mathematics is easy, then logic is not difficult."

By translating these assumptions into statements involving propositional variables and logical connectives, determine whether each of the following are valid conclusions of these assumptions:

**a)** That mathematics is not easy, if many students like logic.

**b)** That not many students like logic, if mathematics is not easy.

**c)** That mathematics is not easy or logic is difficult.

**d)** That logic is not difficult or mathematics is not easy.

**e)** That if not many students like logic, then either mathematics is not easy or logic is not difficult.

***35.** Determine whether this argument, taken from Kalish and Montague [KaMo64], is valid.

> If Superman were able and willing to prevent evil, he would do so. If Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent. Superman does not prevent evil. If Superman exists, he is neither impotent nor malevolent. Therefore, Superman does not exist.

# 1.7 Introduction to Proofs

## Introduction

In this section we introduce the notion of a proof and describe methods for constructing proofs. A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven

theorems. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

In our discussion we move from formal proofs of theorems toward more informal proofs. The arguments we introduced in Section 1.6 to show that statements involving propositions and quantified statements are true were formal proofs, where all steps were supplied, and the rules for each step in the argument were given. However, formal proofs of useful theorems can be extremely long and hard to follow. In practice, the proofs of theorems designed for human consumption are almost always **informal proofs**, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated. Informal proofs can often explain to humans why theorems are true, while computers are perfectly happy producing formal proofs using automated reasoning systems.

The methods of proof discussed in this chapter are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science. These applications include verifying that computer programs are correct, establishing that operating systems are secure, making inferences in artificial intelligence, showing that system specifications are consistent, and so on. Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

## Some Terminology

Formally, a **theorem** is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important. Less important theorems sometimes are called **propositions**. (Theorems can also be referred to as **facts** or **results**.) A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion. However, it may be some other type of logical statement, as the examples later in this chapter will show. We demonstrate that a theorem is true with a **proof**. A proof is a valid argument that establishes the truth of a theorem. The statements used in a proof can include **axioms** (or **postulates**), which are statements we assume to be true (for example, the axioms for the real numbers, given in Appendix 1, and the axioms of plane geometry), the premises, if any, of the theorem, and previously proven theorems. Axioms may be stated using primitive terms that do not require definition, but all other terms used in theorems and their proofs must be defined. Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem. However, for clarity, we will often recap the statement of the theorem as the final step of a proof.


A less important theorem that is helpful in the proof of other results is called a **lemma** (plural *lemmas* or *lemmata*). Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually. A **corollary** is a theorem that can be established directly from a theorem that has been proved. A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert. When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

## Understanding How Theorems Are Stated


Before we introduce methods for proving theorems, we need to understand how many mathematical theorems are stated. Many theorems assert that a property holds for all elements in a domain, such as the integers or the real numbers. Although the precise statement of such

theorems needs to include a universal quantifier, the standard convention in mathematics is to omit it. For example, the statement

"If $x > y$, where $x$ and $y$ are positive real numbers, then $x^2 > y^2$."

really means

"For all positive real numbers $x$ and $y$, if $x > y$, then $x^2 > y^2$."

Furthermore, when theorems of this type are proved, the first step of the proof usually involves selecting a general element of the domain. Subsequent steps show that this element has the property in question. Finally, universal generalization implies that the theorem holds for all members of the domain.

## Methods of Proving Theorems


Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful battery of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs. One we have chosen a proof method, we use axioms, definitions of terms, previously proved results, and rules of inference to complete the proof. Note that in this book we will always assume the axioms for real numbers found in Appendix 1. We will also assume the usual axioms whenever we prove a result about geometry. When you construct your own proofs, be careful not to use anything but these axioms, definitions, and previously proved results as facts!

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, our goal is to show that $P(c) \rightarrow Q(c)$ is true, where $c$ is an arbitrary element of the domain, and then apply universal generalization. In this proof, we need to show that a conditional statement is true. Because of this, we now focus on methods that show that conditional statements are true. Recall that $p \rightarrow q$ is true unless $p$ is true but $q$ is false. Note that to prove the statement $p \rightarrow q$, we need only show that $q$ is true if $p$ is true. The following discussion will give the most common techniques for proving conditional statements. Later we will discuss methods for proving other types of statements. In this section, and in Section 1.8, we will develop a large arsenal of proof techniques that can be used to prove a wide variety of theorems.

When you read proofs, you will often find the words "obviously" or "clearly." These words indicate that steps have been omitted that the author expects the reader to be able to fill in. Unfortunately, this assumption is often not warranted and readers are not at all sure how to fill in the gaps. We will assiduously try to avoid using these words and try not to omit too many steps. However, if we included all steps in proofs, our proofs would often be excruciatingly long.

## Direct Proofs

A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that $p$ is true; subsequent steps are constructed using rules of inference, with the final step showing that $q$ must also be true. A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that if $p$ is true, then $q$ must also be true, so that the combination $p$ true and $q$ false never occurs. In a direct proof, we assume that $p$ is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that $q$ must also be true. You will find that direct proofs of many results are quite straightforward, with a fairly obvious sequence of steps leading from the hypothesis to the conclusion. However, direct proofs sometimes require particular insights and can be quite tricky. The first direct proofs we present here are quite straightforward; later in the text you will see some that are less obvious.

We will provide examples of several different direct proofs. Before we give the first example, we need to define some terminology.

**DEFINITION 1** The integer $n$ is *even* if there exists an integer $k$ such that $n = 2k$, and $n$ is *odd* if there exists an integer $k$ such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

**EXAMPLE 1** Give a direct proof of the theorem "If $n$ is an odd integer, then $n^2$ is odd."

*Solution:* Note that this theorem states $\forall n\, P((n) \rightarrow Q(n))$, where $P(n)$ is "$n$ is an odd integer" and $Q(n)$ is "$n^2$ is odd." As we have said, we will follow the usual convention in mathematical proofs by showing that $P(n)$ implies $Q(n)$, and not explicitly using universal instantiation. To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that $n$ is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where $k$ is some integer. We want to show that $n^2$ is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses $n^2$. When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. By the definition of an odd integer, we can conclude that $n^2$ is an odd integer (it is one more than twice an integer). Consequently, we have proved that if $n$ is an odd integer, then $n^2$ is an odd integer. ◀

Extra Examples

**EXAMPLE 2** Give a direct proof that if $m$ and $n$ are both perfect squares, then $nm$ is also a perfect square. (An integer $a$ is a **perfect square** if there is an integer $b$ such that $a = b^2$.)

*Solution:* To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that $m$ and $n$ are both perfect squares. By the definition of a perfect square, it follows that there are integers $s$ and $t$ such that $m = s^2$ and $n = t^2$. The goal of the proof is to show that $mn$ must also be a perfect square when $m$ and $n$ are; looking ahead we see how we can show this by substituting $s^2$ for $m$ and $t^2$ for $n$ into $mn$. This tells us that $mn = s^2t^2$. Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication. By the definition of perfect square, it follows that $mn$ is also a perfect square, because it is the square of $st$, which is an integer. We have proved that if $m$ and $n$ are both perfect squares, then $mn$ is also a perfect square. ◀

## Proof by Contraposition

Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion. However, we will see that attempts at direct proofs often reach dead ends. We need other methods of proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$. Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called **indirect proofs**.

An extremely useful type of indirect proof is known as **proof by contraposition**. Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$. This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true. In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow. We will illustrate proof by contraposition with two examples. These examples show that proof by contraposition can succeed when we cannot easily find a direct proof.

**EXAMPLE 3** Prove that if $n$ is an integer and $3n + 2$ is odd, then $n$ is odd.

*Solution:* We first attempt a direct proof. To construct a direct proof, we first assume that $3n + 2$ is an odd integer. This means that $3n + 2 = 2k + 1$ for some integer $k$. Can we use this fact

Extra Examples

to show that $n$ is odd? We see that $3n + 1 = 2k$, but there does not seem to be any direct way to conclude that $n$ is odd. Because our attempt at a direct proof failed, we next try a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $3n + 2$ is odd, then $n$ is odd" is false; namely, assume that $n$ is even. Then, by the definition of an even integer, $n = 2k$ for some integer $k$. Substituting $2k$ for $n$, we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even (because it is a multiple of 2), and therefore not odd. This is the negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If $3n + 2$ is odd, then $n$ is odd." ◀

**EXAMPLE 4** Prove that if $n = ab$, where $a$ and $b$ are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

*Solution:* Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where $a$ and $b$ are positive integers, we attempt a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $n = ab$, where $a$ and $b$ are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" is false. That is, we assume that the statement $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ is false. Using the meaning of disjunction together with De Morgan's law, we see that this implies that both $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false. This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$. We can multiply these inequalities together (using the fact that if $0 < s < t$ and $0 < u < v$, then $su < tv$) to obtain $ab > \sqrt{n} \cdot \sqrt{n} = n$. This shows that $ab \neq n$, which contradicts the statement $n = ab$.

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if $n = ab$, where $a$ and $b$ are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. ◀

VACUOUS AND TRIVIAL PROOFS We can quickly prove that a conditional statement $p \rightarrow q$ is true when we know that $p$ is false, because $p \rightarrow q$ must be true when $p$ is false. Consequently, if we can show that $p$ is false, then we have a proof, called a **vacuous proof**, of the conditional statement $p \rightarrow q$. Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers [i.e., a theorem of the kind $\forall n P(n)$, where $P(n)$ is a propositional function]. Proof techniques for theorems of this kind will be discussed in Section 5.1.

**EXAMPLE 5** Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

*Solution:* Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true. ◀

***Remark:*** The fact that the conclusion of this conditional statement, $0^2 > 0$, is false is irrelevant to the truth value of the conditional statement, because a conditional statement with a false hypothesis is guaranteed to be true.

We can also quickly prove a conditional statement $p \rightarrow q$ if we know that the conclusion $q$ is true. By showing that $q$ is true, it follows that $p \rightarrow q$ must also be true. A proof of $p \rightarrow q$ that uses the fact that $q$ is true is called a **trivial proof**. Trivial proofs are often important when special cases of theorems are proved (see the discussion of proof by cases in Section 1.8) and in mathematical induction, which is a proof technique discussed in Section 5.1.

**EXAMPLE 6** Let $P(n)$ be "If $a$ and $b$ are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

*Solution:* The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof. ◀

A LITTLE PROOF STRATEGY We have described two important approaches for proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$: direct proof and proof by contraposition. We have also given examples that show how each is used. However, when you are presented with a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, which method should you use to attempt to prove it? We will provide a few rules of thumb here; in Section 1.8 we will discuss proof strategy at greater length. When you want to prove a statement of the form $\forall x(P(x) \rightarrow Q(x))$, first evaluate whether a direct proof looks promising. Begin by expanding the definitions in the hypotheses. Start to reason using these hypotheses, together with axioms and available theorems. If a direct proof does not seem to go anywhere, try the same thing with a proof by contraposition. Recall that in a proof by contraposition you assume that the conclusion of the conditional statement is false and use a direct proof to show this implies that the hypothesis must be false. We illustrate this strategy in Examples 7 and 8. Before we present our next example, we need a definition.

**DEFINITION 2** The real number $r$ is *rational* if there exist integers $p$ and $q$ with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*.

**EXAMPLE 7** Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number $r$ and every real number $s$, if $r$ and $s$ are rational numbers, then $r + s$ is rational.)

Extra Examples

*Solution:* We first attempt a direct proof. To begin, suppose that $r$ and $s$ are rational numbers. From the definition of a rational number, it follows that there are integers $p$ and $q$, with $q \neq 0$, such that $r = p/q$, and integers $t$ and $u$, with $u \neq 0$, such that $s = t/u$. Can we use this information to show that $r + s$ is rational? The obvious next step is to add $r = p/q$ and $s = t/u$, to obtain

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}.$$

Because $q \neq 0$ and $u \neq 0$, it follows that $qu \neq 0$. Consequently, we have expressed $r + s$ as the ratio of two integers, $pu + qt$ and $qu$, where $qu \neq 0$. This means that $r + s$ is rational. We have proved that the sum of two rational numbers is rational; our attempt to find a direct proof succeeded. ◀

**EXAMPLE 8** Prove that if $n$ is an integer and $n^2$ is odd, then $n$ is odd.

*Solution:* We first attempt a direct proof. Suppose that $n$ is an integer and $n^2$ is odd. Then, there exists an integer $k$ such that $n^2 = 2k + 1$. Can we use this information to show that $n$ is odd? There seems to be no obvious approach to show that $n$ is odd because solving for $n$ produces the equation $n = \pm\sqrt{2k + 1}$, which is not terribly useful.

Because this attempt to use a direct proof did not bear fruit, we next attempt a proof by contraposition. We take as our hypothesis the statement that $n$ is not odd. Because every integer is odd or even, this means that $n$ is even. This implies that there exists an integer $k$ such that $n = 2k$. To prove the theorem, we need to show that this hypothesis implies the conclusion that $n^2$ is not odd, that is, that $n^2$ is even. Can we use the equation $n = 2k$ to achieve this? By

squaring both sides of this equation, we obtain $n^2 = 4k^2 = 2(2k^2)$, which implies that $n^2$ is also even because $n^2 = 2t$, where $t = 2k^2$. We have proved that if $n$ is an integer and $n^2$ is odd, then $n$ is odd. Our attempt to find a proof by contraposition succeeded. ◀

## Proofs by Contradiction

Suppose we want to prove that a statement $p$ is true. Furthermore, suppose that we can find a contradiction $q$ such that $\neg p \rightarrow q$ is true. Because $q$ is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that $p$ is true. How can we find a contradiction $q$ that might help us prove that $p$ is true in this way?

Because the statement $r \wedge \neg r$ is a contradiction whenever $r$ is a proposition, we can prove that $p$ is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition $r$. Proofs of this type are called **proofs by contradiction**. Because a proof by contradiction does not prove a result directly, it is another type of indirect proof. We provide three examples of proof by contradiction. The first is an example of an application of the pigeonhole principle, a combinatorial technique that we will cover in depth in Section 6.2.

**EXAMPLE 9** Show that at least four of any 22 days must fall on the same day of the week.

Extra Examples

*Solution:* Let $p$ be the proposition "At least four of 22 chosen days fall on the same day of the week." Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day. This contradicts the premise that we have 22 days under consideration. That is, if $r$ is the statement that 22 days are chosen, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that $p$ is true. We have proved that at least four of 22 chosen days fall on the same day of the week. ◀

**EXAMPLE 10** Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

*Solution:* Let $p$ be the proposition "$\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$ is true. Note that $\neg p$ is the statement "It is not the case that $\sqrt{2}$ is irrational," which says that $\sqrt{2}$ is rational. We will show that assuming that $\neg p$ is true leads to a contradiction.

If $\sqrt{2}$ is rational, there exist integers $a$ and $b$ with $\sqrt{2} = a/b$, where $b \neq 0$ and $a$ and $b$ have no common factors (so that the fraction $a/b$ is in lowest terms.) (Here, we are using the fact that every rational number can be written in lowest terms.) Because $\sqrt{2} = a/b$, when both sides of this equation are squared, it follows that

$$2 = \frac{a^2}{b^2}.$$

Hence,

$$2b^2 = a^2.$$

By the definition of an even integer it follows that $a^2$ is even. We next use the fact that if $a^2$ is even, $a$ must also be even, which follows by Exercise 16. Furthermore, because $a$ is even, by the definition of an even integer, $a = 2c$ for some integer $c$. Thus,

$$2b^2 = 4c^2.$$

Dividing both sides of this equation by 2 gives

$$b^2 = 2c^2.$$

By the definition of even, this means that $b^2$ is even. Again using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that $b$ must be even as well.

We have now shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = a/b$, where $a$ and $b$ have no common factors, but both $a$ and $b$ are even, that is, 2 divides both $a$ and $b$. Note that the statement that $\sqrt{2} = a/b$, where $a$ and $b$ have no common factors, means, in particular, that 2 does not divide both $a$ and $b$. Because our assumption of $\neg p$ leads to the contradiction that 2 divides both $a$ and $b$ and 2 does not divide both $a$ and $b$, $\neg p$ must be false. That is, the statement $p$, "$\sqrt{2}$ is irrational," is true. We have proved that $\sqrt{2}$ is irrational. ◀

Proof by contradiction can be used to prove conditional statements. In such proofs, we first assume the negation of the conclusion. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction. (The reason that such proofs are valid rests on the logical equivalence of $p \rightarrow q$ and $(p \wedge \neg q) \rightarrow \mathbf{F}$. To see that these statements are equivalent, simply note that each is false in exactly one case, namely when $p$ is true and $q$ is false.)

Note that we can rewrite a proof by contraposition of a conditional statement as a proof by contradiction. In a proof of $p \rightarrow q$ by contraposition, we assume that $\neg q$ is true. We then show that $\neg p$ must also be true. To rewrite a proof by contraposition of $p \rightarrow q$ as a proof by contradiction, we suppose that both $p$ and $\neg q$ are true. Then, we use the steps from the proof of $\neg q \rightarrow \neg p$ to show that $\neg p$ is true. This leads to the contradiction $p \wedge \neg p$, completing the proof. Example 11 illustrates how a proof by contraposition of a conditional statement can be rewritten as a proof by contradiction.

**EXAMPLE 11** Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then $n$ is odd."

*Solution:* Let $p$ be "$3n + 2$ is odd" and $q$ be "$n$ is odd." To construct a proof by contradiction, assume that both $p$ and $\neg q$ are true. That is, assume that $3n + 2$ is odd and that $n$ is not odd. Because $n$ is not odd, we know that it is even. Because $n$ is even, there is an integer $k$ such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Because $3n + 2$ is $2t$, where $t = 3k + 1$, $3n + 2$ is even. Note that the statement "$3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd. Because both $p$ and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that if $3n + 2$ is odd, then $n$ is odd. ◀

Note that we can also prove by contradiction that $p \rightarrow q$ is true by assuming that $p$ and $\neg q$ are true, and showing that $q$ must be also be true. This implies that $\neg q$ and $q$ are both true, a contradiction. This observation tells us that we can turn a direct proof into a proof by contradiction.

PROOFS OF EQUIVALENCE To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$$

**EXAMPLE 12** Prove the theorem "If $n$ is an integer, then $n$ is odd if and only if $n^2$ is odd."

*Solution:* This theorem has the form "$p$ if and only if $q$," where $p$ is "$n$ is odd" and $q$ is "$n^2$ is odd." (As usual, we do not explicitly deal with the universal quantification.) To prove this theorem, we need to show that $p \rightarrow q$ and $q \rightarrow p$ are true.

Extra Examples

We have already shown (in Example 1) that $p \rightarrow q$ is true and (in Example 8) that $q \rightarrow p$ is true.

Because we have shown that both $p \rightarrow q$ and $q \rightarrow p$ are true, we have shown that the theorem is true. ◀

Sometimes a theorem states that several propositions are equivalent. Such a theorem states that propositions $p_1, p_2, p_3, \ldots, p_n$ are equivalent. This can be written as

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n,$$

which states that all $n$ propositions have the same truth values, and consequently, that for all $i$ and $j$ with $1 \leq i \leq n$ and $1 \leq j \leq n$, $p_i$ and $p_j$ are equivalent. One way to prove these mutually equivalent is to use the tautology

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \leftrightarrow (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1).$$

This shows that if the $n$ conditional statements $p_1 \rightarrow p_2, p_2 \rightarrow p_3, \ldots, p_n \rightarrow p_1$ can be shown to be true, then the propositions $p_1, p_2, \ldots, p_n$ are all equivalent.

This is much more efficient than proving that $p_i \rightarrow p_j$ for all $i \neq j$ with $1 \leq i \leq n$ and $1 \leq j \leq n$. (Note that there are $n^2 - n$ such conditional statements.)

When we prove that a group of statements are equivalent, we can establish any chain of conditional statements we choose as long as it is possible to work through the chain to go from any one of these statements to any other statement. For example, we can show that $p_1$, $p_2$, and $p_3$ are equivalent by showing that $p_1 \rightarrow p_3$, $p_3 \rightarrow p_2$, and $p_2 \rightarrow p_1$.

**EXAMPLE 13** Show that these statements about the integer $n$ are equivalent:

$p_1$: $n$ is even.
$p_2$: $n - 1$ is odd.
$p_3$: $n^2$ is even.

*Solution:* We will show that these three statements are equivalent by showing that the conditional statements $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, and $p_3 \rightarrow p_1$ are true.

We use a direct proof to show that $p_1 \rightarrow p_2$. Suppose that $n$ is even. Then $n = 2k$ for some integer $k$. Consequently, $n - 1 = 2k - 1 = 2(k - 1) + 1$. This means that $n - 1$ is odd because it is of the form $2m + 1$, where $m$ is the integer $k - 1$.

We also use a direct proof to show that $p_2 \rightarrow p_3$. Now suppose $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some integer $k$. Hence, $n = 2k + 2$ so that $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$. This means that $n^2$ is twice the integer $2k^2 + 4k + 2$, and hence is even.

To prove $p_3 \rightarrow p_1$, we use a proof by contraposition. That is, we prove that if $n$ is not even, then $n^2$ is not even. This is the same as proving that if $n$ is odd, then $n^2$ is odd, which we have already done in Example 1. This completes the proof. ◀

**COUNTEREXAMPLES** In Section 1.4 we stated that to show that a statement of the form $\forall x\, P(x)$ is false, we need only find a **counterexample**, that is, an example $x$ for which $P(x)$ is false. When presented with a statement of the form $\forall x\, P(x)$, which we believe to be false or which has resisted all proof attempts, we look for a counterexample. We illustrate the use of counterexamples in Example 14.

**EXAMPLE 14** Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Extra Examples

*Solution:* To show that this statement is false, we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers. It does not take long to find a counterexample, because 3 cannot be written as the sum of the squares of two integers. To show this is the case, note that the only perfect squares not exceeding 3 are $0^2 = 0$ and $1^2 = 1$. Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1. Consequently, we have shown that "Every positive integer is the sum of the squares of two integers" is false. ◀

## Mistakes in Proofs

There are many common errors made in constructing mathematical proofs. We will briefly describe some of these here. Among the most common errors are mistakes in arithmetic and basic algebra. Even professional mathematicians make such errors, especially when working with complicated formulae. Whenever you use such computations you should check them as carefully as possible. (You should also review any troublesome aspects of basic algebra, especially before you study Section 5.1.)


Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it. This is illustrated in Examples 15–17.

**EXAMPLE 15** What is wrong with this famous supposed "proof" that $1 = 2$?

*"Proof:"* We use these steps, where $a$ and $b$ are two equal positive integers.

| Step | Reason |
|---|---|
| 1. $a = b$ | Given |
| 2. $a^2 = ab$ | Multiply both sides of (1) by $a$ |
| 3. $a^2 - b^2 = ab - b^2$ | Subtract $b^2$ from both sides of (2) |
| 4. $(a - b)(a + b) = b(a - b)$ | Factor both sides of (3) |
| 5. $a + b = b$ | Divide both sides of (4) by $a - b$ |
| 6. $2b = b$ | Replace $a$ by $b$ in (5) because $a = b$ and simplify |
| 7. $2 = 1$ | Divide both sides of (6) by $b$ |

*Solution:* Every step is valid except for one, step 5 where we divided both sides by $a - b$. The error is that $a - b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero. ◀

**EXAMPLE 16** What is wrong with this "proof?"

"Theorem:" If $n^2$ is positive, then $n$ is positive.

*"Proof:"* Suppose that $n^2$ is positive. Because the conditional statement "If $n$ is positive, then $n^2$ is positive" is true, we can conclude that $n$ is positive.

*Solution:* Let $P(n)$ be "$n$ is positive" and $Q(n)$ be "$n^2$ is positive." Then our hypothesis is $Q(n)$. The statement "If $n$ is positive, then $n^2$ is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$. From the hypothesis $Q(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $P(n)$, because we are not using a valid rule of inference. Instead, this is an example of the fallacy of affirming the conclusion. A counterexample is supplied by $n = -1$ for which $n^2 = 1$ is positive, but $n$ is negative. ◀

**EXAMPLE 17** What is wrong with this "proof?"

"Theorem:" If $n$ is not positive, then $n^2$ is not positive. (This is the contrapositive of the "theorem" in Example 16.)

*"Proof:"* Suppose that $n$ is not positive. Because the conditional statement "If $n$ is positive, then $n^2$ is positive" is true, we can conclude that $n^2$ is not positive.

*Solution:* Let $P(n)$ and $Q(n)$ be as in the solution of Example 16. Then our hypothesis is $\neg P(n)$ and the statement "If $n$ is positive, then $n^2$ is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$. From the hypothesis $\neg P(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $\neg Q(n)$, because we are not using a valid rule of inference. Instead, this is an example of the fallacy of denying the hypothesis. A counterexample is supplied by $n = -1$, as in Example 16. ◀

Finally, we briefly discuss a particularly nasty type of error. Many incorrect arguments are based on a fallacy called **begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved. In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning**.

**EXAMPLE 18** Is the following argument correct? It supposedly shows that $n$ is an even integer whenever $n^2$ is an even integer.

Suppose that $n^2$ is even. Then $n^2 = 2k$ for some integer $k$. Let $n = 2l$ for some integer $l$. This shows that $n$ is even.

*Solution:* This argument is incorrect. The statement "let $n = 2l$ for some integer $l$" occurs in the proof. No argument has been given to show that $n$ can be written as $2l$ for some integer $l$. This is circular reasoning because this statement is equivalent to the statement being proved, namely, "$n$ is even." Of course, the result itself is correct; only the method of proof is wrong. ◀

Making mistakes in proofs is part of the learning process. When you make a mistake that someone else finds, you should carefully analyze where you went wrong and make sure that you do not make the same mistake again. Even professional mathematicians make mistakes in proofs. More than a few incorrect proofs of important results have fooled people for many years before subtle errors in them were found.

## Just a Beginning

We have now developed a basic arsenal of proof methods. In the next section we will introduce other important proof methods. We will also introduce several important proof techniques in Chapter 5, including mathematical induction, which can be used to prove results that hold for all positive integers. In Chapter 6 we will introduce the notion of combinatorial proofs.

In this section we introduced several methods for proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$, including direct proofs and proofs by contraposition. There are many theorems of this type whose proofs are easy to construct by directly working through the hypotheses and definitions of the terms of the theorem. However, it is often difficult to prove a theorem without resorting to a clever use of a proof by contraposition or a proof by contradiction, or some other proof technique. In Section 1.8 we will address proof strategy. We will describe various approaches that can be used to find proofs when straightforward approaches do not work. Constructing proofs is an art that can be learned only through experience, including writing proofs, having your proofs critiqued, and reading and analyzing other proofs.

## Exercises

**1.** Use a direct proof to show that the sum of two odd integers is even.

**2.** Use a direct proof to show that the sum of two even integers is even.

**3.** Show that the square of an even number is an even number using a direct proof.

**4.** Show that the additive inverse, or negative, of an even number is an even number using a direct proof.

**5.** Prove that if $m + n$ and $n + p$ are even integers, where $m, n$, and $p$ are integers, then $m + p$ is even. What kind of proof did you use?

**6.** Use a direct proof to show that the product of two odd numbers is odd.

**7.** Use a direct proof to show that every odd integer is the difference of two squares.

**8.** Prove that if $n$ is a perfect square, then $n + 2$ is not a perfect square.

**9.** Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.

**10.** Use a direct proof to show that the product of two rational numbers is rational.

**11.** Prove or disprove that the product of two irrational numbers is irrational.

**12.** Prove or disprove that the product of a nonzero rational number and an irrational number is irrational.

**13.** Prove that if $x$ is irrational, then $1/x$ is irrational.

**14.** Prove that if $x$ is rational and $x \neq 0$, then $1/x$ is rational.

**15.** Use a proof by contraposition to show that if $x + y \geq 2$, where $x$ and $y$ are real numbers, then $x \geq 1$ or $y \geq 1$.

☞ **16.** Prove that if $m$ and $n$ are integers and $mn$ is even, then $m$ is even or $n$ is even.

**17.** Show that if $n$ is an integer and $n^3 + 5$ is odd, then $n$ is even using

**a)** a proof by contraposition.
**b)** a proof by contradiction.

**18.** Prove that if $n$ is an integer and $3n + 2$ is even, then $n$ is even using

**a)** a proof by contraposition.
**b)** a proof by contradiction.

**19.** Prove the proposition $P(0)$, where $P(n)$ is the proposition "If $n$ is a positive integer greater than 1, then $n^2 > n$." What kind of proof did you use?

**20.** Prove the proposition $P(1)$, where $P(n)$ is the proposition "If $n$ is a positive integer, then $n^2 \geq n$." What kind of proof did you use?

**21.** Let $P(n)$ be the proposition "If $a$ and $b$ are positive real numbers, then $(a + b)^n \geq a^n + b^n$." Prove that $P(1)$ is true. What kind of proof did you use?

**22.** Show that if you pick three socks from a drawer containing just blue socks and black socks, you must get either a pair of blue socks or a pair of black socks.

**23.** Show that at least ten of any 64 days chosen must fall on the same day of the week.

**24.** Show that at least three of any 25 days chosen must fall in the same month of the year.

**25.** Use a proof by contradiction to show that there is no rational number $r$ for which $r^3 + r + 1 = 0$. [*Hint:* Assume that $r = a/b$ is a root, where $a$ and $b$ are integers and $a/b$ is in lowest terms. Obtain an equation involving integers by multiplying by $b^3$. Then look at whether $a$ and $b$ are each odd or even.]

**26.** Prove that if $n$ is a positive integer, then $n$ is even if and only if $7n + 4$ is even.

**27.** Prove that if $n$ is a positive integer, then $n$ is odd if and only if $5n + 6$ is odd.

**28.** Prove that $m^2 = n^2$ if and only if $m = n$ or $m = -n$.

**29.** Prove or disprove that if $m$ and $n$ are integers such that $mn = 1$, then either $m = 1$ and $n = 1$, or else $m = -1$ and $n = -1$.

**30.** Show that these three statements are equivalent, where $a$ and $b$ are real numbers: (*i*) $a$ is less than $b$, (*ii*) the average of $a$ and $b$ is greater than $a$, and (*iii*) the average of $a$ and $b$ is less than $b$.

**31.** Show that these statements about the integer $x$ are equivalent: (*i*) $3x + 2$ is even, (*ii*) $x + 5$ is odd, (*iii*) $x^2$ is even.

**32.** Show that these statements about the real number $x$ are equivalent: (*i*) $x$ is rational, (*ii*) $x/2$ is rational, (*iii*) $3x - 1$ is rational.

**33.** Show that these statements about the real number $x$ are equivalent: (*i*) $x$ is irrational, (*ii*) $3x + 2$ is irrational, (*iii*) $x/2$ is irrational.

**34.** Is this reasoning for finding the solutions of the equation $\sqrt{2x^2 - 1} = x$ correct? (*1*) $\sqrt{2x^2 - 1} = x$ is given; (*2*) $2x^2 - 1 = x^2$, obtained by squaring both sides of (1); (*3*) $x^2 - 1 = 0$, obtained by subtracting $x^2$ from both sides of (2); (*4*) $(x - 1)(x + 1) = 0$, obtained by factoring the left-hand side of $x^2 - 1$; (*5*) $x = 1$ or $x = -1$, which follows because $ab = 0$ implies that $a = 0$ or $b = 0$.

**35.** Are these steps for finding the solutions of $\sqrt{x + 3} = 3 - x$ correct? (*1*) $\sqrt{x + 3} = 3 - x$ is given; (*2*) $x + 3 = x^2 - 6x + 9$, obtained by squaring both sides of (1); (*3*) $0 = x^2 - 7x + 6$, obtained by subtracting $x + 3$ from both sides of (2); (*4*) $0 = (x - 1)(x - 6)$, obtained by factoring the right-hand side of (3); (*5*) $x = 1$ or $x = 6$, which follows from (4) because $ab = 0$ implies that $a = 0$ or $b = 0$.

**36.** Show that the propositions $p_1$, $p_2$, $p_3$, and $p_4$ can be shown to be equivalent by showing that $p_1 \leftrightarrow p_4$, $p_2 \leftrightarrow p_3$, and $p_1 \leftrightarrow p_3$.

**37.** Show that the propositions $p_1$, $p_2$, $p_3$, $p_4$, and $p_5$ can be shown to be equivalent by proving that the conditional statements $p_1 \rightarrow p_4$, $p_3 \rightarrow p_1$, $p_4 \rightarrow p_2$, $p_2 \rightarrow p_5$, and $p_5 \rightarrow p_3$ are true.

**38.** Find a counterexample to the statement that every positive integer can be written as the sum of the squares of three integers.

**39.** Prove that at least one of the real numbers $a_1, a_2, \ldots, a_n$ is greater than or equal to the average of these numbers. What kind of proof did you use?

**40.** Use Exercise 39 to show that if the first 10 positive integers are placed around a circle, in any order, there exist three integers in consecutive locations around the circle that have a sum greater than or equal to 17.

**41.** Prove that if $n$ is an integer, these four statements are equivalent: (*i*) $n$ is even, (*ii*) $n + 1$ is odd, (*iii*) $3n + 1$ is odd, (*iv*) $3n$ is even.

**42.** Prove that these four statements about the integer $n$ are equivalent: (*i*) $n^2$ is odd, (*ii*) $1 - n$ is even, (*iii*) $n^3$ is odd, (*iv*) $n^2 + 1$ is even.

# 1.8 Proof Methods and Strategy

## Introduction


In Section 1.7 we introduced many methods of proof and illustrated how each method can be used. In this section we continue this effort. We will introduce several other commonly used proof methods, including the method of proving a theorem by considering different cases separately. We will also discuss proofs where we prove the existence of objects with desired properties.

In Section 1.7 we briefly discussed the strategy behind constructing proofs. This strategy includes selecting a proof method and then successfully constructing an argument step by step, based on this method. In this section, after we have developed a versatile arsenal of proof methods, we will study some aspects of the art and science of proofs. We will provide advice on how to find a proof of a theorem. We will describe some tricks of the trade, including how proofs can be found by working backward and by adapting existing proofs.

When mathematicians work, they formulate conjectures and attempt to prove or disprove them. We will briefly describe this process here by proving results about tiling checkerboards with dominoes and other types of pieces. Looking at tilings of this kind, we will be able to quickly formulate conjectures and prove theorems without first developing a theory.

We will conclude the section by discussing the role of open questions. In particular, we will discuss some interesting problems either that have been solved after remaining open for hundreds of years or that still remain open.

## Exhaustive Proof and Proof by Cases

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases. We now introduce a method that can be used to prove a theorem, by considering different cases separately. This method is based on a rule of inference that we will now introduce. To prove a conditional statement of the form

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$$

the tautology

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

can be used as a rule of inference. This shows that the original conditional statement with a hypothesis made up of a disjunction of the propositions $p_1, p_2, \ldots, p_n$ can be proved by proving each of the $n$ conditional statements $p_i \rightarrow q$, $i = 1, 2, \ldots, n$, individually. Such an argument is called a **proof by cases**. Sometimes to prove that a conditional statement $p \rightarrow q$ is true, it is convenient to use a disjunction $p_1 \vee p_2 \vee \cdots \vee p_n$ instead of $p$ as the hypothesis of the conditional statement, where $p$ and $p_1 \vee p_2 \vee \cdots \vee p_n$ are equivalent.

EXHAUSTIVE PROOF Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion** because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each case involves checking a single example. We now provide some illustrations of exhaustive proofs.

**EXAMPLE 1** Prove that $(n + 1)^3 \geq 3^n$ if $n$ is a positive integer with $n \leq 4$.

*Solution:* We use a proof by exhaustion. We only need verify the inequality $(n + 1)^3 \geq 3^n$ when $n = 1, 2, 3$, and 4. For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$; for $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$; for $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$; and for $n = 4$, we have $(n + 1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$. In each of these four cases, we see that $(n + 1)^3 \geq 3^n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3^n$ if $n$ is a positive integer with $n \leq 4$. ◀

Extra Examples

**EXAMPLE 2** Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer is a **perfect power** if it equals $n^a$, where $a$ is an integer greater than 1.)

*Solution:* We use a proof by exhaustion. In particular, we can prove this fact by examining positive integers $n$ not exceeding 100, first checking whether $n$ is a perfect power, and if it is, checking whether $n + 1$ is also a perfect power. A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81. The fifth powers of positive integers not exceeding 100 are 1 and 32. The sixth powers of positive integers not exceeding 100 are 1 and 64. There are no powers of positive integers higher than the sixth power not exceeding 100, other than 1. Looking at this list of perfect powers not exceeding 100, we see that $n = 8$ is the only perfect power $n$ for which $n + 1$ is also a perfect power. That is, $2^3 = 8$ and $3^2 = 9$ are the only two consecutive perfect powers not exceeding 100. ◀

Proofs by exhaustion can tire out people and computers when the number of cases challenges the available processing power!

People can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement. Computers do not complain when they are asked to check a much larger number of instances of a statement, but they still have limitations. Note that not even a computer can check all instances when it is impossible to list all instances to check.

PROOF BY CASES A proof by cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

**EXAMPLE 3** Prove that if $n$ is an integer, then $n^2 \geq n$.

*Solution:* We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

*Case (i):* When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.

Extra Examples

*Case (ii):* When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer $n$, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

*Case (iii):* In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if $n$ is an integer, then $n^2 \geq n$. ◀

**EXAMPLE 4** Use a proof by cases to show that $|xy| = |x||y|$, where $x$ and $y$ are real numbers. (Recall that $|a|$, the absolute value of $a$, equals $a$ when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

*Solution:* In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a < 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: *(i)* $x$ and $y$ both nonnegative, *(ii)* $x$ nonnegative and $y$ is negative, *(iii)* $x$ negative and $y$ nonnegative, and *(iv)* $x$ negative and $y$ negative. We denote by $p_1$, $p_2$, $p_3$, and $p_4$, the proposition stating the assumption for each of these four cases, respectively.

(Note that we can remove the absolute value signs by making the appropriate choice of signs within each case.)

*Case (i):* We see that $p_1 \rightarrow q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$, so that $|xy| = xy = |x||y|$.

*Case (ii):* To see that $p_2 \rightarrow q$, note that if $x \geq 0$ and $y < 0$, then $xy \leq 0$, so that $|xy| = -xy = x(-y) = |x||y|$. (Here, because $y < 0$, we have $|y| = -y$.)

*Case (iii):* To see that $p_3 \rightarrow q$, we follow the same reasoning as the previous case with the roles of $x$ and $y$ reversed.

*Case (iv):* To see that $p_4 \rightarrow q$, note that when $x < 0$ and $y < 0$, it follows that $xy > 0$. Hence, $|xy| = xy = (-x)(-y) = |x||y|$.

Because $|xy| = |x||y|$ holds in each of the four cases and these cases exhaust all possibilities, we can conclude that $|xy| = |x||y|$, whenever $x$ and $y$ are real numbers. ◀

LEVERAGING PROOF BY CASES The examples we have presented illustrating proof by cases provide some insight into when to use this method of proof. In particular, when it is not possible to consider all cases of a proof at the same time, a proof by cases should be considered. When should you use such a proof? Generally, look for a proof by cases when there is no obvious way to begin a proof, but when extra information in each case helps move the proof forward. Example 5 illustrates how the method of proof by cases can be used effectively.

**EXAMPLE 5** Formulate a conjecture about the final decimal digit of the square of an integer and prove your result.

*Solution:* The smallest perfect squares are $1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225$, and so on. We notice that the digits that occur as the final digit of a square are $0, 1, 4, 5, 6$, and $9$, with $2, 3, 7$, and $8$ never appearing as the final digit of a square. We conjecture this theorem: The final decimal digit of a perfect square is $0, 1, 4, 5, 6$ or $9$. How can we prove this theorem?

We first note that we can express an integer $n$ as $10a + b$, where $a$ and $b$ are positive integers and $b$ is $0, 1, 2, 3, 4, 5, 6, 7, 8$, or $9$. Here $a$ is the integer obtained by subtracting the final decimal digit of $n$ from $n$ and dividing by 10. Next, note that $(10a + b)^2 = 100a^2 + 20ab + b^2 = 10(10a^2 + 2b) + b^2$, so that the final decimal digit of $n^2$ is the same as the final decimal digit of $b^2$. Furthermore, note that the final decimal digit of $b^2$ is the same as the final decimal digit of $(10 - b)^2 = 100 - 20b + b^2$. Consequently, we can reduce our proof to the consideration of six cases.

*Case (i):* The final digit of $n$ is 1 or 9. Then the final decimal digit of $n^2$ is the final decimal digit of $1^2 = 1$ or $9^2 = 81$, namely 1.

*Case (ii):* The final digit of $n$ is 2 or 8. Then the final decimal digit of $n^2$ is the final decimal digit of $2^2 = 4$ or $8^2 = 64$, namely 4.

*Case (iii):* The final digit of $n$ is 3 or 7. Then the final decimal digit of $n^2$ is the final decimal digit of $3^2 = 9$ or $7^2 = 49$, namely 9.

*Case (iv):* The final digit of $n$ is 4 or 6. Then the final decimal digit of $n^2$ is the final decimal digit of $4^2 = 16$ or $6^2 = 36$, namely 6.

*Case (v):* The final decimal digit of $n$ is 5. Then the final decimal digit of $n^2$ is the final decimal digit of $5^2 = 25$, namely 5.

*Case (vi):* The final decimal digit of $n$ is 0. Then the final decimal digit of $n^2$ is the final decimal digit of $0^2 = 0$, namely 0.

Because we have considered all six cases, we can conclude that the final decimal digit of $n^2$, where $n$ is an integer is either 0, 1, 2, 4, 5, 6, or 9. ◀

Sometimes we can eliminate all but a few examples in a proof by cases, as Example 6 illustrates.

**EXAMPLE 6** Show that there are no solutions in integers $x$ and $y$ of $x^2 + 3y^2 = 8$.

*Solution:* We can quickly reduce a proof to checking just a few simple cases because $x^2 > 8$ when $|x| \geq 3$ and $3y^2 > 8$ when $|y| \geq 2$. This leaves the cases when $x$ equals $-2, -1, 0, 1,$ or 2 and $y$ equals $-1, 0,$ or 1. We can finish using an exhaustive proof. To dispense with the remaining cases, we note that possible values for $x^2$ are 0, 1, and 4, and possible values for $3y^2$ are 0 and 3, and the largest sum of possible values for $x^2$ and $3y^2$ is 7. Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when $x$ and $y$ are integers. ◀

WITHOUT LOSS OF GENERALITY In the proof in Example 4, we dismissed case (*iii*), where $x < 0$ and $y \geq 0$, because it is the same as case (*ii*), where $x \geq 0$ and $y < 0$, with the roles of $x$ and $y$ reversed. To shorten the proof, we could have proved cases (*ii*) and (*iii*) together by assuming, **without loss of generality**, that $x \geq 0$ and $y < 0$. Implicit in this statement is that we can complete the case with $x < 0$ and $y \geq 0$ using the same argument as we used for the case with $x \geq 0$ and $y < 0$, but with the obvious changes.

In general, when the phrase "without loss of generality" is used in a proof (often abbreviated as WLOG), we assert that by proving one case of a theorem, no additional argument is required to prove other specified cases. That is, other cases follow by making straightforward changes to the argument, or by filling in some straightforward initial step. Proofs by cases can often be made much more efficient when the notion of without loss of generality is employed. Of course, incorrect use of this principle can lead to unfortunate errors. Sometimes assumptions are made that lead to a loss in generality. Such assumptions can be made that do not take into account that one case may be substantially different from others. This can lead to an incomplete, and possibly unsalvageable, proof. In fact, many incorrect proofs of famous theorems turned out to rely on arguments that used the idea of "without loss of generality" to establish cases that could not be quickly proved from simpler cases.

In a proof by cases be sure not to omit any cases and check that you have proved all cases correctly!

We now illustrate a proof where without loss of generality is used effectively together with other proof techniques.

**EXAMPLE 7** Show that if $x$ and $y$ are integers and both $xy$ and $x + y$ are even, then both $x$ and $y$ are even.

*Solution:* We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that $x$ and $y$ are not both even. That is, assume that $x$ is odd or that $y$ is odd (or both). Without loss of generality, we assume that $x$ is odd, so that $x = 2m + 1$ for some integer $k$.

To complete the proof, we need to show that $xy$ is odd or $x + y$ is odd. Consider two cases: (i) $y$ even, and (ii) $y$ odd. In (i), $y = 2n$ for some integer $n$, so that $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd. In (ii), $y = 2n + 1$ for some integer $n$, so that $xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd. This completes the proof by contraposition. (Note that our use of without loss of generality within the proof is justified because the proof when $y$ is odd can be obtained by simply interchanging the roles of $x$ and $y$ in the proof we have given.) ◀

COMMON ERRORS WITH EXHAUSTIVE PROOF AND PROOF BY CASES A common error of reasoning is to draw incorrect conclusions from examples. No matter how many separate examples are considered, a theorem is not proved by considering examples unless every possible

case is covered. The problem of proving a theorem is analogous to showing that a computer program always produces the output desired. No matter how many input values are tested, unless all input values are tested, we cannot conclude that the program always produces the correct output.

**EXAMPLE 8** Is it true that every positive integer is the sum of 18 fourth powers of integers?

*Solution:* To determine whether a positive integer $n$ can be written as the sum of 18 fourth powers of integers, we might begin by examining whether $n$ is the sum of 18 fourth powers of integers for the smallest positive integers. Because the fourth powers of integers are $0, 1, 16, 81, \ldots,$ if we can select 18 terms from these numbers that add up to $n$, then $n$ is the sum of 18 fourth powers. We can show that all positive integers up to 78 can be written as the sum of 18 fourth powers. (The details are left to the reader.) However, if we decided this was enough checking, we would come to the wrong conclusion. It is not true that every positive integer is the sum of 18 fourth powers because 79 is not the sum of 18 fourth powers (as the reader can verify). ◀

Another common error involves making unwarranted assumptions that lead to incorrect proofs by cases where not all cases are considered. This is illustrated in Example 9.

**EXAMPLE 9** What is wrong with this "proof?"

"Theorem:" If $x$ is a real number, then $x^2$ is a positive real number.

*"Proof:"* Let $p_1$ be "$x$ is positive," let $p_2$ be "$x$ is negative," and let $q$ be "$x^2$ is positive." To show that $p_1 \rightarrow q$ is true, note that when $x$ is positive, $x^2$ is positive because it is the product of two positive numbers, $x$ and $x$. To show that $p_2 \rightarrow q$, note that when $x$ is negative, $x^2$ is positive because it is the product of two negative numbers, $x$ and $x$. This completes the proof.

*Solution:* The problem with this "proof" is that we missed the case of $x = 0$. When $x = 0$, $x^2 = 0$ is not positive, so the supposed theorem is false. If $p$ is "$x$ is a real number," then we can prove results where $p$ is the hypothesis with three cases, $p_1$, $p_2$, and $p_3$, where $p_1$ is "$x$ is positive," $p_2$ is "$x$ is negative," and $p_3$ is "$x = 0$" because of the equivalence $p \leftrightarrow p_1 \vee p_2 \vee p_3$. ◀

## Existence Proofs

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x\, P(x)$, where $P$ is a predicate. A proof of a proposition of the form $\exists x\, P(x)$ is called an **existence proof**. There are several ways to prove a theorem of this type. Sometimes an existence proof of $\exists x\, P(x)$ can be given by finding an element $a$, called a **witness**, such that $P(a)$ is true. This type of existence proof is called **constructive**. It is also possible to give an existence proof that is **nonconstructive**; that is, we do not find an element $a$ such that $P(a)$ is true, but rather prove that $\exists x\, P(x)$ is true in some other way. One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction. The concept of a constructive existence proof is illustrated by Example 10 and the concept of a nonconstructive existence proof is illustrated by Example 11.

**EXAMPLE 10** **A Constructive Existence Proof** Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Extra Examples

*Solution:* After considerable computation (such as a computer search) we find that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

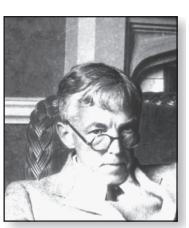
There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied "No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways." ◀

**EXAMPLE 11** **A Nonconstructive Existence Proof** Show that there exist irrational numbers $x$ and $y$ such that $x^y$ is rational.

*Solution:* By Example 10 in Section 1.7 we know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers $x$ and $y$ with $x^y$ rational, namely, $x = \sqrt{2}$ and $y = \sqrt{2}$. On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$.

This proof is an example of a nonconstructive existence proof because we have not found irrational numbers $x$ and $y$ such that $x^y$ is rational. Rather, we have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these two pairs works! ◀

Links



GODFREY HAROLD HARDY (1877–1947) Hardy, born in Cranleigh, Surrey, England, was the older of two children of Isaac Hardy and Sophia Hall Hardy. His father was the geography and drawing master at the Cranleigh School and also gave singing lessons and played soccer. His mother gave piano lessons and helped run a boardinghouse for young students. Hardy's parents were devoted to their children's education. Hardy demonstrated his numerical ability at the early age of two when he began writing down numbers into the millions. He had a private mathematics tutor rather than attending regular classes at the Cranleigh School. He moved to Winchester College, a private high school, when he was 13 and was awarded a scholarship. He excelled in his studies and demonstrated a strong interest in mathematics. He entered Trinity College, Cambridge, in 1896 on a scholarship and won several prizes during his time there, graduating in 1899.

Hardy held the position of lecturer in mathematics at Trinity College at Cambridge University from 1906 to 1919, when he was appointed to the Sullivan chair of geometry at Oxford. He had become unhappy with Cambridge over the dismissal of the famous philosopher and mathematician Bertrand Russell from Trinity for antiwar activities and did not like a heavy load of administrative duties. In 1931 he returned to Cambridge as the Sadleirian professor of pure mathematics, where he remained until his retirement in 1942. He was a pure mathematician and held an elitist view of mathematics, hoping that his research could never be applied. Ironically, he is perhaps best known as one of the developers of the Hardy–Weinberg law, which predicts patterns of inheritance. His work in this area appeared as a letter to the journal *Science* in which he used simple algebraic ideas to demonstrate errors in an article on genetics. Hardy worked primarily in number theory and function theory, exploring such topics as the Riemann zeta function, Fourier series, and the distribution of primes. He made many important contributions to many important problems, such as Waring's problem about representing positive integers as sums of $k$th powers and the problem of representing odd integers as sums of three primes. Hardy is also remembered for his collaborations with John E. Littlewood, a colleague at Cambridge, with whom he wrote more than 100 papers, and the famous Indian mathematical prodigy Srinivasa Ramanujan. His collaboration with Littlewood led to the joke that there were only three important English mathematicians at that time, Hardy, Littlewood, and Hardy–Littlewood, although some people thought that Hardy had invented a fictitious person, Littlewood, because Littlewood was seldom seen outside Cambridge. Hardy had the wisdom of recognizing Ramanujan's genius from unconventional but extremely creative writings Ramanujan sent him, while other mathematicians failed to see the genius. Hardy brought Ramanujan to Cambridge and collaborated on important joint papers, establishing new results on the number of partitions of an integer. Hardy was interested in mathematics education, and his book *A Course of Pure Mathematics* had a profound effect on undergraduate instruction in mathematics in the first half of the twentieth century. Hardy also wrote *A Mathematician's Apology*, in which he gives his answer to the question of whether it is worthwhile to devote one's life to the study of mathematics. It presents Hardy's view of what mathematics is and what a mathematician does.

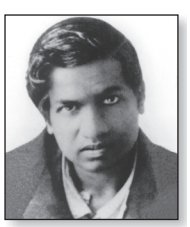
Hardy had a strong interest in sports. He was an avid cricket fan and followed scores closely. One peculiar trait he had was that he did not like his picture taken (only five snapshots are known) and disliked mirrors, covering them with towels immediately upon entering a hotel room.

Nonconstructive existence proofs often are quite subtle, as Example 12 illustrates.

**EXAMPLE 12** **Chomp** is a game played by two players. In this game, cookies are laid out on a rectangular grid. The cookie in the top left position is poisoned, as shown in Figure 1(a). The two players take turns making moves; at each move, a player is required to eat a remaining cookie, together with all cookies to the right and/or below it (see Figure 1(b), for example). The loser is the player who has no choice but to eat the poisoned cookie. We ask whether one of the two players has a winning strategy. That is, can one of the players always make moves that are guaranteed to lead to a win?

*Solution:* We will give a nonconstructive existence proof of a winning strategy for the first player. That is, we will show that the first player always has a winning strategy without explicitly describing the moves this player must follow.

First, note that the game ends and cannot finish in a draw because with each move at least one cookie is eaten, so after no more than $m \times n$ moves the game ends, where the initial grid is $m \times n$. Now, suppose that the first player begins the game by eating just the cookie in the bottom right corner. There are two possibilities, this is the first move of a winning strategy for the first player, or the second player can make a move that is the first move of a winning strategy for the second player. In this second case, instead of eating just the cookie in the bottom right corner, the first player could have made the same move that the second player made as the first



SRINIVASA RAMANUJAN (1887–1920) The famous mathematical prodigy Ramanujan was born and raised in southern India near the city of Madras (now called Chennai). His father was a clerk in a cloth shop. His mother contributed to the family income by singing at a local temple. Ramanujan studied at the local English language school, displaying his talent and interest for mathematics. At the age of 13 he mastered a textbook used by college students. When he was 15, a university student lent him a copy of *Synopsis of Pure Mathematics*. Ramanujan decided to work out the over 6000 results in this book, stated without proof or explanation, writing on sheets later collected to form notebooks. He graduated from high school in 1904, winning a scholarship to the University of Madras. Enrolling in a fine arts curriculum, he neglected his subjects other than mathematics and lost his scholarship. He failed to pass examinations at the university four times from 1904 to 1907, doing well only in mathematics. During this time he filled his notebooks with original writings, sometimes rediscovering already published work and at other times making new discoveries.

Without a university degree, it was difficult for Ramanujan to find a decent job. To survive, he had to depend on the goodwill of his friends. He tutored students in mathematics, but his unconventional ways of thinking and failure to stick to the syllabus caused problems. He was married in 1909 in an arranged marriage to a young woman nine years his junior. Needing to support himself and his wife, he moved to Madras and sought a job. He showed his notebooks of mathematical writings to his potential employers, but the books bewildered them. However, a professor at the Presidency College recognized his genius and supported him, and in 1912 he found work as an accounts clerk, earning a small salary.

Ramanujan continued his mathematical work during this time and published his first paper in 1910 in an Indian journal. He realized that his work was beyond that of Indian mathematicians and decided to write to leading English mathematicians. The first mathematicians he wrote to turned down his request for help. But in January 1913 he wrote to G. H. Hardy, who was inclined to turn Ramanujan down, but the mathematical statements in the letter, although stated without proof, puzzled Hardy. He decided to examine them closely with the help of his colleague and collaborator J. E. Littlewood. They decided, after careful study, that Ramanujan was probably a genius, because his statements "could only be written down by a mathematician of the highest class; they must be true, because if they were not true, no one would have the imagination to invent them."

Hardy arranged a scholarship for Ramanujan, bringing him to England in 1914. Hardy personally tutored him in mathematical analysis, and they collaborated for five years, proving significant theorems about the number of partitions of integers. During this time, Ramanujan made important contributions to number theory and also worked on continued fractions, infinite series, and elliptic functions. Ramanujan had amazing insight involving certain types of functions and series, but his purported theorems on prime numbers were often wrong, illustrating his vague idea of what constitutes a correct proof. He was one of the youngest members ever appointed a Fellow of the Royal Society. Unfortunately, in 1917 Ramanujan became extremely ill. At the time, it was thought that he had trouble with the English climate and had contracted tuberculosis. It is now thought that he suffered from a vitamin deficiency, brought on by Ramanujan's strict vegetarianism and shortages in wartime England. He returned to India in 1919, continuing to do mathematics even when confined to his bed. He was religious and thought his mathematical talent came from his family deity, Namagiri. He considered mathematics and religion to be linked. He said that "an equation for me has no meaning unless it expresses a thought of God." His short life came to an end in April 1920, when he was 32 years old. Ramanujan left several notebooks of unpublished results. The writings in these notebooks illustrate Ramanujan's insights but are quite sketchy. Several mathematicians have devoted many years of study to explaining and justifying the results in these notebooks.

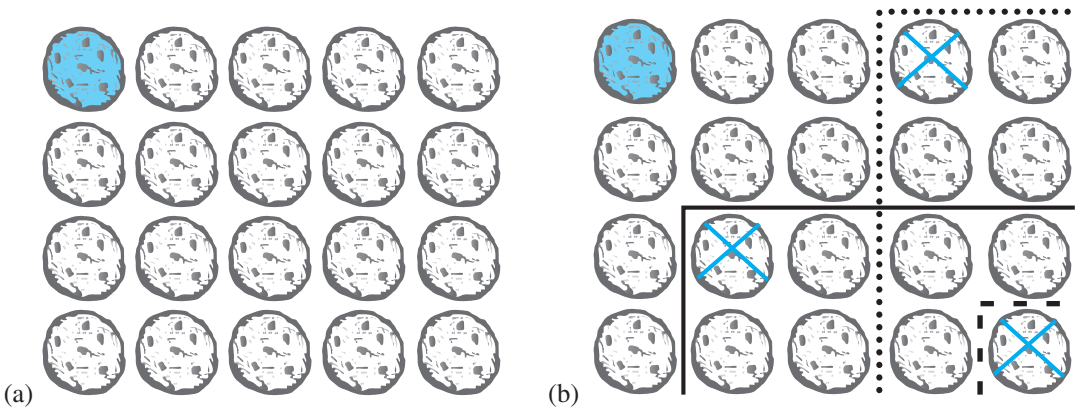


**FIGURE 1** **(a) Chomp (Top Left Cookie Poisoned). (b) Three Possible Moves.**

move of a winning strategy (and then continued to follow that winning strategy). This would guarantee a win for the first player.

Note that we showed that a winning strategy exists, but we did not specify an actual winning strategy. Consequently, the proof is a nonconstructive existence proof. In fact, no one has been able to describe a winning strategy for that Chomp that applies for all rectangular grids by describing the moves that the first player should follow. However, winning strategies can be described for certain special cases, such as when the grid is square and when the grid only has two rows of cookies (see Exercises 15 and 16 in Section 5.2). ◀

## Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a **uniqueness proof** are:

*Existence:* We show that an element $x$ with the desired property exists.
*Uniqueness:* We show that if $y \neq x$, then $y$ does not have the desired property.

Equivalently, we can show that if $x$ and $y$ both have the desired property, then $x = y$.

***Remark:*** Showing that there is a unique element $x$ such that $P(x)$ is the same as proving the statement $\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$.

We illustrate the elements of a uniqueness proof in Example 13.

**EXAMPLE 13** Show that if $a$ and $b$ are real numbers and $a \neq 0$, then there is a unique real number $r$ such that $ar + b = 0$.

*Solution:* First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$. Consequently, a real number $r$ exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that $s$ is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting $b$ from both sides, we find that $ar = as$. Dividing both sides of this last equation by $a$, which is nonzero, we see that $r = s$. This means that if $s \neq r$, then $as + b \neq 0$. This establishes the uniqueness part of the proof. ◀

Extra Examples

## Proof Strategies

Finding proofs can be a challenging business. When you are confronted with a statement to prove, you should first replace terms by their definitions and then carefully analyze what the hypotheses and the conclusion mean. After doing so, you can attempt to prove the result using one of the available methods of proof. Generally, if the statement is a conditional statement, you should first try a direct proof; if this fails, you can try an indirect proof. If neither of these approaches works, you might try a proof by contradiction.

FORWARD AND BACKWARD REASONING Whichever method you choose, you need a starting point for your proof. To begin a direct proof of a conditional statement, you start with the premises. Using these premises, together with axioms and known theorems, you can construct a proof using a sequence of steps that leads to the conclusion. This type of reasoning, called *forward reasoning*, is the most common type of reasoning used to prove relatively simple results. Similarly, with indirect reasoning you can start with the negation of the conclusion and, using a sequence of steps, obtain the negation of the premises.

Unfortunately, forward reasoning is often difficult to use to prove more complicated results, because the reasoning needed to reach the desired conclusion may be far from obvious. In such cases it may be helpful to use *backward reasoning*. To reason backward to prove a statement $q$, we find a statement $p$ that we can prove with the property that $p \rightarrow q$. (Note that it is not helpful to find a statement $r$ that you can prove such that $q \rightarrow r$, because it is the fallacy of begging the question to conclude from $q \rightarrow r$ and $r$ that $q$ is true.) Backward reasoning is illustrated in Examples 14 and 15.

**EXAMPLE 14** Given two positive real numbers $x$ and $y$, their **arithmetic mean** is $(x + y)/2$ and their **geometric mean** is $\sqrt{xy}$. When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. [For example, when $x = 4$ and $y = 6$, we have $5 = (4 + 6)/2 > \sqrt{4 \cdot 6} = \sqrt{24}$.] Can we prove that this inequality is always true?

*Solution:* To prove that $(x + y)/2 > \sqrt{xy}$ when $x$ and $y$ are distinct positive real numbers, we can work backward. We construct a sequence of equivalent inequalities. The equivalent inequalities are

$$
\begin{aligned}
(x + y)/2 &> \sqrt{xy}, \\
(x + y)^2/4 &> xy, \\
(x + y)^2 &> 4xy, \\
x^2 + 2xy + y^2 &> 4xy, \\
x^2 - 2xy + y^2 &> 0, \\
(x - y)^2 &> 0.
\end{aligned}
$$

Extra Examples

Because $(x - y)^2 > 0$ when $x \neq y$, it follows that the final inequality is true. Because all these inequalities are equivalent, it follows that $(x + y)/2 > \sqrt{xy}$ when $x \neq y$. Once we have carried out this backward reasoning, we can easily reverse the steps to construct a proof using forward reasoning. We now give this proof.

Suppose that $x$ and $y$ are distinct positive real numbers. Then $(x - y)^2 > 0$ because the square of a nonzero real number is positive (see Appendix 1). Because $(x - y)^2 = x^2 - 2xy + y^2$, this implies that $x^2 - 2xy + y^2 > 0$. Adding $4xy$ to both sides, we obtain $x^2 + 2xy + y^2 > 4xy$. Because $x^2 + 2xy + y^2 = (x + y)^2$, this means that $(x + y)^2 \geq 4xy$. Dividing both sides of this equation by 4, we see that $(x + y)^2/4 > xy$. Finally, taking square roots of both sides (which preserves the inequality because both sides are positive) yields

$(x + y)/2 > \sqrt{xy}$. We conclude that if $x$ and $y$ are distinct positive real numbers, then their arithmetic mean $(x + y)/2$ is greater than their geometric mean $\sqrt{xy}$. ◀

**EXAMPLE 15** Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

*Solution:* To prove that the first player can always win the game, we work backward. At the last step, the first player can win if this player is left with a pile containing one, two, or three stones. The second player will be forced to leave one, two, or three stones if this player has to remove stones from a pile containing four stones. Consequently, one way for the first person to win is to leave four stones for the second player on the next-to-last move. The first person can leave four stones when there are five, six, or seven stones left at the beginning of this player's move, which happens when the second player has to remove stones from a pile with eight stones. Consequently, to force the second player to leave five, six, or seven stones, the first player should leave eight stones for the second player at the second-to-last move for the first player. This means that there are nine, ten, or eleven stones when the first player makes this move. Similarly, the first player should leave twelve stones when this player makes the first move. We can reverse this argument to show that the first player can always make moves so that this player wins the game no matter what the second player does. These moves successively leave twelve, eight, and four stones for the second player. ◀

ADAPTING EXISTING PROOFS An excellent way to look for possible approaches that can be used to prove a statement is to take advantage of existing proofs of similar results. Often an existing proof can be adapted to prove other facts. Even when this is not the case, some of the ideas used in existing proofs may be helpful. Because existing proofs provide clues for new proofs, you should read and understand the proofs you encounter in your studies. This process is illustrated in Example 16.

**EXAMPLE 16** In Example 10 of Section 1.7 we proved that $\sqrt{2}$ is irrational. We now conjecture that $\sqrt{3}$ is irrational. Can we adapt the proof in Example 10 in Section 1.7 to show that $\sqrt{3}$ is irrational?

Extra Examples

*Solution:* To adapt the proof in Example 10 in Section 1.7, we begin by mimicking the steps in that proof, but with $\sqrt{2}$ replaced with $\sqrt{3}$. First, we suppose that $\sqrt{3} = d/c$ where the fraction $c/d$ is in lowest terms. Squaring both sides tells us that $3 = c^2/d^2$, so that $3d^2 = c^2$. Can we use this equation to show that 3 must be a factor of both $c$ and $d$, similar to how we used the equation $2b^2 = a^2$ in Example 10 in Section 1.7 to show that 2 must be a factor of both $a$ and $b$? (Recall that an integer $s$ is a factor of the integer $t$ if $t/s$ is an integer. An integer $n$ is even if and only if 2 is a factor of $n$.) In turns out that we can, but we need some ammunition from number theory, which we will develop in Chapter 4. We sketch out the remainder of the proof, but leave the justification of these steps until Chapter 4. Because 3 is a factor of $c^2$, it must also be a factor of $c$. Furthermore, because 3 is a factor of $c$, 9 is a factor of $c^2$, which means that 9 is a factor of $3d^2$. This implies that 3 is a factor of $d^2$, which means that 3 is a factor of that $d$. This makes 3 a factor of both $c$ and $d$, which contradicts the assumption that $c/d$ is in lowest terms. After we have filled in the justification for these steps, we will have shown that $\sqrt{3}$ is irrational by adapting the proof that $\sqrt{2}$ is irrational. Note that this proof can be extended to show that $\sqrt{n}$ is irrational whenever $n$ is a positive integer that is not a perfect square. We leave the details of this to Chapter 4. ◀

A good tip is to look for existing proofs that you might adapt when you are confronted with proving a new theorem, particularly when the new theorem seems similar to one you have already proved.

## Looking for Counterexamples

In Section 1.7 we introduced the use of counterexamples to show that certain statements are false. When confronted with a conjecture, you might first try to prove this conjecture, and if your attempts are unsuccessful, you might try to find a counterexample, first by looking at the simplest, smallest examples. If you cannot find a counterexample, you might again try to prove the statement. In any case, looking for counterexamples is an extremely important pursuit, which often provides insights into problems. We will illustrate the role of counterexamples in Example 17.

**EXAMPLE 17** In Example 14 in Section 1.7 we showed that the statement "Every positive integer is the sum of two squares of integers" is false by finding a counterexample. That is, there are positive integers that cannot be written as the sum of the squares of two integers. Although we cannot write every positive integer as the sum of the squares of two integers, maybe we can write every positive integer as the sum of the squares of three integers. That is, is the statement "Every positive integer is the sum of the squares of three integers" true or false?

Extra Examples

*Solution:* Because we know that not every positive integer can be written as the sum of two squares of integers, we might initially be skeptical that every positive integer can be written as the sum of three squares of integers. So, we first look for a counterexample. That is, we can show that the statement "Every positive integer is the sum of three squares of integers" is false if we can find a particular integer that is not the sum of the squares of three integers. To look for a counterexample, we try to write successive positive integers as a sum of three squares. We find that $1 = 0^2 + 0^2 + 1^2$, $2 = 0^2 + 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 0^2 + 0^2 + 2^2$, $5 = 0^2 + 1^2 + 2^2$, $6 = 1^2 + 1^2 + 2^2$, but we cannot find a way to write 7 as the sum of three squares. To show that there are not three squares that add up to 7, we note that the only possible squares we can use are those not exceeding 7, namely, 0, 1, and 4. Because no three terms where each term is 0, 1, or 4 add up to 7, it follows that 7 is a counterexample. We conclude that the statement "Every positive integer is the sum of the squares of three integers" is false.

We have shown that not every positive integer is the sum of the squares of three integers. The next question to ask is whether every positive integer is the sum of the squares of four positive integers. Some experimentation provides evidence that the answer is yes. For example, $7 = 1^2 + 1^2 + 1^2 + 2^2$, $25 = 4^2 + 2^2 + 2^2 + 1^2$, and $87 = 9^2 + 2^2 + 1^2 + 1^2$. It turns out the conjecture "Every positive integer is the sum of the squares of four integers" is true. For a proof, see [Ro10]. ◀

## Proof Strategy in Action

Mathematics is generally taught as if mathematical facts were carved in stone. Mathematics texts (including the bulk of this book) formally present theorems and their proofs. Such presentations do not convey the discovery process in mathematics. This process begins with exploring concepts and examples, asking questions, formulating conjectures, and attempting to settle these conjectures either by proof or by counterexample. These are the day-to-day activities of mathematicians. Believe it or not, the material taught in textbooks was originally developed in this way.

Extra Examples

People formulate conjectures on the basis of many types of possible evidence. The examination of special cases can lead to a conjecture, as can the identification of possible patterns. Altering the hypotheses and conclusions of known theorems also can lead to plausible conjectures. At other times, conjectures are made based on intuition or a belief that a result holds. No matter how a conjecture was made, once it has been formulated, the goal is to prove or disprove it. When mathematicians believe that a conjecture may be true, they try to find a proof. If they cannot find a proof, they may look for a counterexample. When they cannot find a counterexample, they may switch gears and once again try to prove the conjecture. Although many conjectures are quickly settled, a few conjectures resist attack for hundreds of years and lead to

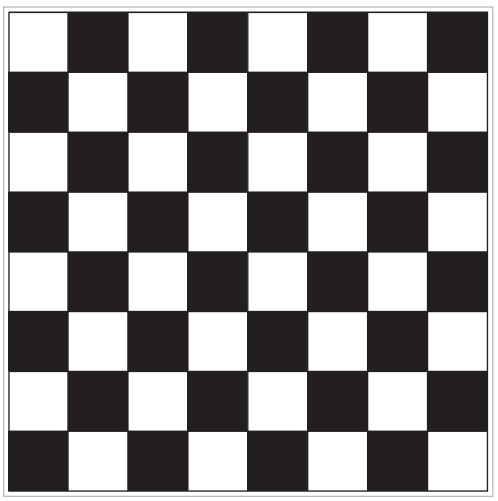


**FIGURE 2** **The Standard Checkerboard.**

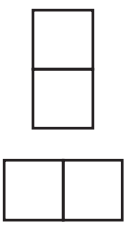


**FIGURE 3**
**Two Dominoes.**

the development of new parts of mathematics. We will mention a few famous conjectures later in this section.

## Tilings

We can illustrate aspects of proof strategy through a brief study of tilings of checkerboards. Looking at tilings of checkerboards is a fruitful way to quickly discover many different results and construct their proofs using a variety of proof methods. There are almost an endless number of conjectures that can be made and studied in this area too. To begin, we need to define some terms. A **checkerboard** is a rectangle divided into squares of the same size by horizontal and vertical lines. The game of checkers is played on a board with 8 rows and 8 columns; this board is called the **standard checkerboard** and is shown in Figure 2. In this section we use the term **board** to refer to a checkerboard of any rectangular size as well as parts of checkerboards obtained by removing one or more squares. A **domino** is a rectangular piece that is one square by two squares, as shown in Figure 3. We say that a board is **tiled** by dominoes when all its squares are covered with no overlapping dominoes and no dominoes overhanging the board. We now develop some results about tiling boards using dominoes.

**EXAMPLE 18** Can we tile the standard checkerboard using dominoes?

*Solution:* We can find many ways to tile the standard checkerboard using dominoes. For example, we can tile it by placing 32 dominoes horizontally, as shown in Figure 4. The existence of one such tiling completes a constructive existence proof. Of course, there are a large number of other ways to do this tiling. We can place 32 dominoes vertically on the board or we can place some tiles vertically and some horizontally. But for a constructive existence proof we needed to find just one such tiling. ◀

**EXAMPLE 19** Can we tile a board obtained by removing one of the four corner squares of a standard checkerboard?

*Solution:* To answer this question, note that a standard checkerboard has 64 squares, so removing a square produces a board with 63 squares. Now suppose that we could tile a board obtained from the standard checkerboard by removing a corner square. The board has an even number of

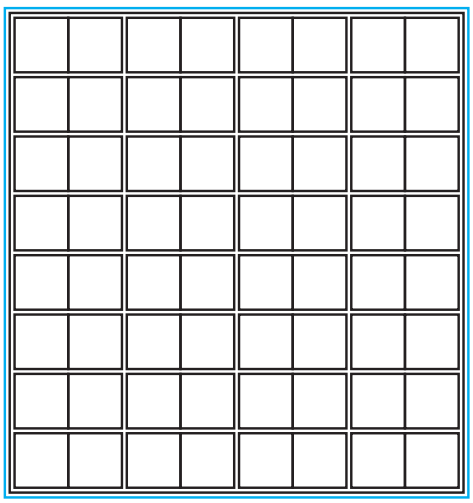


**FIGURE 4** **Tiling the Standard Checkerboard.**

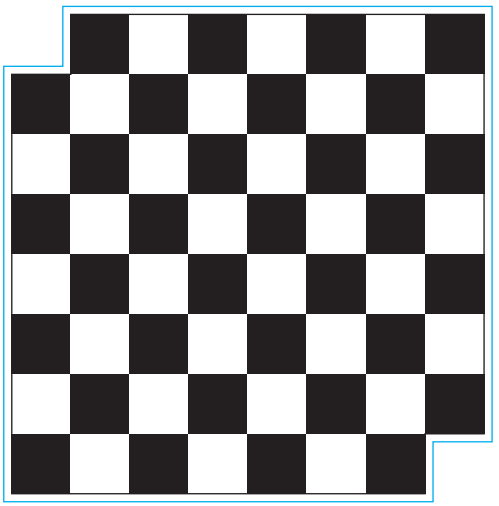


**FIGURE 5** **The Standard Checkerboard with the Upper Left and Lower Right Squares Removed.**

squares because each domino covers two squares and no two dominoes overlap and no dominoes overhang the board. Consequently, we can prove by contradiction that a standard checkerboard with one square removed cannot be tiled using dominoes because such a board has an odd number of squares. ◀

We now consider a trickier situation.

**EXAMPLE 20** Can we tile the board obtained by deleting the upper left and lower right corner squares of a standard checkerboard, shown in Figure 5?

*Solution:* A board obtained by deleting two squares of a standard checkerboard contains $64 - 2 = 62$ squares. Because 62 is even, we cannot quickly rule out the existence of a tiling of the standard checkerboard with its upper left and lower right squares removed, unlike Example 19, where we ruled out the existence of a tiling of the standard checkerboard with one corner square removed. Trying to construct a tiling of this board by successively placing dominoes might be a first approach, as the reader should attempt. However, no matter how much we try, we cannot find such a tiling. Because our efforts do not produce a tiling, we are led to conjecture that no tiling exists.

We might try to prove that no tiling exists by showing that we reach a dead end however we successively place dominoes on the board. To construct such a proof, we would have to consider all possible cases that arise as we run through all possible choices of successively placing dominoes. For example, we have two choices for covering the square in the second column of the first row, next to the removed top left corner. We could cover it with a horizontally placed tile or a vertically placed tile. Each of these two choices leads to further choices, and so on. It does not take long to see that this is not a fruitful plan of attack for a person, although a computer could be used to complete such a proof by exhaustion. (Exercise 45 asks you to supply such a proof to show that a $4 \times 4$ checkerboard with opposite corners removed cannot be tiled.)

We need another approach. Perhaps there is an easier way to prove there is no tiling of a standard checkerboard with two opposite corners removed. As with many proofs, a key observation can help. We color the squares of this checkerboard using alternating white and black squares, as in Figure 2. Observe that a domino in a tiling of such a board covers one white square and one black square. Next, note that this board has unequal numbers of white square and black

squares. We can use these observations to prove by contradiction that a standard checkerboard with opposite corners removed cannot be tiled using dominoes. We now present such a proof.

***Proof:*** Suppose we can use dominoes to tile a standard checkerboard with opposite corners removed. Note that the standard checkerboard with opposite corners removed contains $64 - 2 = 62$ squares. The tiling would use $62/2 = 31$ dominoes. Note that each domino in this tiling covers one white and one black square. Consequently, the tiling covers 31 white squares and 31 black squares. However, when we remove two opposite corner squares, either 32 of the remaining squares are white and 30 are black or else 30 are white and 32 are black. This contradicts the assumption that we can use dominoes to cover a standard checkerboard with opposite corners removed, completing the proof. ◀

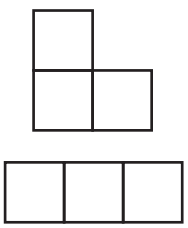


**FIGURE 6 A Right Triomino and a Straight Triomino.**

We can use other types of pieces besides dominoes in tilings. Instead of dominoes we can study tilings that use identically shaped pieces constructed from congruent squares that are connected along their edges. Such pieces are called **polyominoes**, a term coined in 1953 by the mathematician Solomon Golomb, the author of an entertaining book about them [Go94]. We will consider two polyominoes with the same number of squares the same if we can rotate and/or flip one of the polyominoes to get the other one. For example, there are two types of triominoes (see Figure 6), which are polyominoes made up of three squares connected by their sides. One type of triomino, the **straight triomino**, has three horizontally connected squares; the other type, **right triominoes**, resembles the letter L in shape, flipped and/or rotated, if necessary. We will study the tilings of a checkerboard by straight triominoes here; we will study tilings by right triominoes in Section 5.1.

**EXAMPLE 21** Can you use straight triominoes to tile a standard checkerboard?

*Solution:* The standard checkerboard contains 64 squares and each triomino covers three squares. Consequently, if triominoes tile a board, the number of squares of the board must be a multiple of 3. Because 64 is not a multiple of 3, triominoes cannot be used to cover an $8 \times 8$ checkerboard. ◀

In Example 22, we consider the problem of using straight triominoes to tile a standard checkerboard with one corner missing.

**EXAMPLE 22** Can we use straight triominoes to tile a standard checkerboard with one of its four corners removed? An $8 \times 8$ checkerboard with one corner removed contains $64 - 1 = 63$ squares. Any tiling by straight triominoes of one of these four boards uses $63/3 = 21$ triominoes. However, when we experiment, we cannot find a tiling of one of these boards using straight triominoes. A proof by exhaustion does not appear promising. Can we adapt our proof from Example 20 to prove that no such tiling exists?

*Solution:* We will color the squares of the checkerboard in an attempt to adapt the proof by contradiction we gave in Example 20 of the impossibility of using dominoes to tile a standard checkerboard with opposite corners removed. Because we are using straight triominoes rather than dominoes, we color the squares using three colors rather than two colors, as shown in Figure 7. Note that there are 21 blue squares, 21 black squares, and 22 white squares in this coloring. Next, we make the crucial observation that when a straight triomino covers three squares of the checkerboard, it covers one blue square, one black square, and one white square. Next, note that each of the three colors appears in a corner square. Thus without loss of generality, we may assume that we have rotated the coloring so that the missing square is colored blue. Therefore, we assume that the remaining board contains 20 blue squares, 21 black squares, and 22 white squares.

If we could tile this board using straight triominoes, then we would use $63/3 = 21$ straight triominoes. These triominoes would cover 21 blue squares, 21 black squares, and 21 white

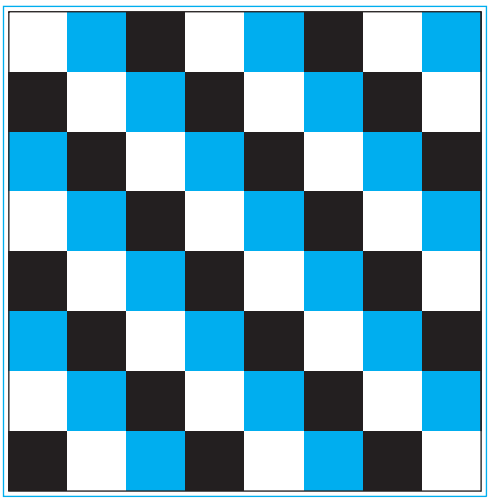


**FIGURE 7 Coloring the Squares of the Standard Checkerboard with Three Colors.**

squares. This contradicts the fact that this board contains 20 blue squares, 21 black squares, and 22 white squares. Therefore we cannot tile this board using straight triominoes. ◀

## The Role of Open Problems

Many advances in mathematics have been made by people trying to solve famous unsolved problems. In the past 20 years, many unsolved problems have finally been resolved, such as the proof of a conjecture in number theory made more than 300 years ago. This conjecture asserts the truth of the statement known as **Fermat's last theorem**.

**THEOREM 1**

**FERMAT'S LAST THEOREM** The equation

$$x^n + y^n = z^n$$

has no solutions in integers $x$, $y$, and $z$ with $xyz \neq 0$ whenever $n$ is an integer with $n > 2$.

Links

***Remark:*** The equation $x^2 + y^2 = z^2$ has infinitely many solutions in integers $x$, $y$, and $z$; these solutions are called Pythagorean triples and correspond to the lengths of the sides of right triangles with integer lengths. See Exercise 32.

This problem has a fascinating history. In the seventeenth century, Fermat jotted in the margin of his copy of the works of Diophantus that he had a "wondrous proof" that there are no integer solutions of $x^n + y^n = z^n$ when $n$ is an integer greater than 2 with $xyz \neq 0$. However, he never published a proof (Fermat published almost nothing), and no proof could be found in the papers he left when he died. Mathematicians looked for a proof for three centuries without success, although many people were convinced that a relatively simple proof could be found. (Proofs of special cases were found, such as the proof of the case when $n = 3$ by Euler and the proof of the $n = 4$ case by Fermat himself.) Over the years, several established mathematicians thought that they had proved this theorem. In the nineteenth century, one of these failed attempts led to the development of the part of number theory called algebraic number theory. A correct

proof, requiring hundreds of pages of advanced mathematics, was not found until the 1990s, when Andrew Wiles used recently developed ideas from a sophisticated area of number theory called the theory of elliptic curves to prove Fermat's last theorem. Wiles's quest to find a proof of Fermat's last theorem using this powerful theory, described in a program in the *Nova* series on public television, took close to ten years! Moreover, his proof was based on major contributions of many mathematicians. (The interested reader should consult [Ro10] for more information about Fermat's last theorem and for additional references concerning this problem and its resolution.)

We now state an open problem that is simple to describe, but that seems quite difficult to resolve.

**EXAMPLE 23** ***The 3x + 1 Conjecture*** Let $T$ be the transformation that sends an even integer $x$ to $x/2$ and an odd integer $x$ to $3x + 1$. A famous conjecture, sometimes known as the **3x + 1 conjecture**, states that for all positive integers $x$, when we repeatedly apply the transformation $T$, we will eventually reach the integer 1. For example, starting with $x = 13$, we find $T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$, $T(10) = 10/2 = 5$, $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 8$, $T(8) = 4$, $T(4) = 2$, and $T(2) = 1$. The $3x + 1$ conjecture has been verified using computers for all integers $x$ up to $5.6 \cdot 10^{13}$.

Links

The $3x + 1$ conjecture has an interesting history and has attracted the attention of mathematicians since the 1950s. The conjecture has been raised many times and goes by many other names, including the Collatz problem, Hasse's algorithm, Ulam's problem, the Syracuse problem, and Kakutani's problem. Many mathematicians have been diverted from their work to spend time attacking this conjecture. This led to the joke that this problem was part of a conspiracy to slow down American mathematical research. See the article by Jeffrey Lagarias [La10] for a fascinating discussion of this problem and the results that have been found by mathematicians attacking it. ◀

Watch out! Working on the $3x + 1$ problem can be addictive.

In Chapter 4 we will describe additional open questions about prime numbers. Students already familiar with the basic notions about primes might want to explore Section 4.3, where these open questions are discussed. We will mention other important open questions throughout the book.

## Additional Proof Methods

In this chapter we introduced the basic methods used in proofs. We also described how to leverage these methods to prove a variety of results. We will use these proof methods in all subsequent chapters. In particular, we will use them in Chapters 2, 3, and 4 to prove results about sets, functions, algorithms, and number theory and in Chapters 9, 10, and 11 to prove results in graph theory. Among the theorems we will prove is the famous halting theorem which states that there is a problem that cannot be solved using any procedure. However, there are many important proof methods besides those we have covered. We will introduce some of these methods later in this book. In particular, in Section 5.1 we will discuss mathematical induction, which is an extremely useful method for proving statements of the form $\forall n\, P(n)$, where the domain consists of all positive integers. In Section 5.3 we will introduce structural induction, which can be used to prove results about recursively defined sets. We will use the Cantor diagonalization method, which can be used to prove results about the size of infinite sets, in Section 2.5. In Chapter 6 we will introduce the notion of combinatorial proofs, which can be used to prove results by counting arguments. The reader should note that entire books have been devoted to the activities discussed in this section, including many excellent works by George Pólya ([Po61], [Po71], [Po90]).

Build up your arsenal of proof methods as you work through this book.

Finally, note that we have not given a procedure that can be used for proving theorems in mathematics. It is a deep theorem of mathematical logic that there is no such procedure.

## Exercises

**1.** Prove that $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$.

**2.** Prove that there are no positive perfect cubes less than 1000 that are the sum of the cubes of two positive integers.

**3.** Prove that if $x$ and $y$ are real numbers, then $\max(x, y) + \min(x, y) = x + y$. [*Hint:* Use a proof by cases, with the two cases corresponding to $x \geq y$ and $x < y$, respectively.]

**4.** Use a proof by cases to show that $\min(a, \min(b, c)) = \min(\min(a, b), c)$ whenever $a$, $b$, and $c$ are real numbers.

**5.** Prove using the notion of without loss of generality that $\min(x, y) = (x + y - |x - y|)/2$ and $\max(x, y) = (x + y + |x - y|)/2$ whenever $x$ and $y$ are real numbers.

**6.** Prove using the notion of without loss of generality that $5x + 5y$ is an odd integer when $x$ and $y$ are integers of opposite parity.

**7.** Prove the **triangle inequality**, which states that if $x$ and $y$ are real numbers, then $|x| + |y| \geq |x + y|$ (where $|x|$ represents the absolute value of $x$, which equals $x$ if $x \geq 0$ and equals $-x$ if $x < 0$).

**8.** Prove that there is a positive integer that equals the sum of the positive integers not exceeding it. Is your proof constructive or nonconstructive?

**9.** Prove that there are 100 consecutive positive integers that are not perfect squares. Is your proof constructive or nonconstructive?

**10.** Prove that either $2 \cdot 10^{500} + 15$ or $2 \cdot 10^{500} + 16$ is not a perfect square. Is your proof constructive or nonconstructive?

**11.** Prove that there exists a pair of consecutive integers such that one of these integers is a perfect square and the other is a perfect cube.

**12.** Show that the product of two of the numbers $65^{1000} - 8^{2001} + 3^{177}$, $79^{1212} - 9^{2399} + 2^{2001}$, and $24^{4493} - 5^{8192} + 7^{1777}$ is nonnegative. Is your proof constructive or nonconstructive? [*Hint:* Do not try to evaluate these numbers!]

**13.** Prove or disprove that there is a rational number $x$ and an irrational number $y$ such that $x^y$ is irrational.

**14.** Prove or disprove that if $a$ and $b$ are rational numbers, then $a^b$ is also rational.

**15.** Show that each of these statements can be used to express the fact that there is a unique element $x$ such that $P(x)$ is true. [Note that we can also write this statement as $\exists! x\, P(x)$.]

**a)** $\exists x \forall y (P(y) \leftrightarrow x = y)$

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

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

**16.** Show that if $a$, $b$, and $c$ are real numbers and $a \neq 0$, then there is a unique solution of the equation $ax + b = c$.

**17.** Suppose that $a$ and $b$ are odd integers with $a \neq b$. Show there is a unique integer $c$ such that $|a - c| = |b - c|$.

**18.** Show that if $r$ is an irrational number, there is a unique integer $n$ such that the distance between $r$ and $n$ is less than $1/2$.

**19.** Show that if $n$ is an odd integer, then there is a unique integer $k$ such that $n$ is the sum of $k - 2$ and $k + 3$.

**20.** Prove that given a real number $x$ there exist unique numbers $n$ and $\epsilon$ such that $x = n + \epsilon$, $n$ is an integer, and $0 \leq \epsilon < 1$.

**21.** Prove that given a real number $x$ there exist unique numbers $n$ and $\epsilon$ such that $x = n - \epsilon$, $n$ is an integer, and $0 \leq \epsilon < 1$.

**22.** Use forward reasoning to show that if $x$ is a nonzero real number, then $x^2 + 1/x^2 \geq 2$. [*Hint:* Start with the inequality $(x - 1/x)^2 \geq 0$ which holds for all nonzero real numbers $x$.]

**23.** The **harmonic mean** of two real numbers $x$ and $y$ equals $2xy/(x + y)$. By computing the harmonic and geometric means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

**24.** The **quadratic mean** of two real numbers $x$ and $y$ equals $\sqrt{(x^2 + y^2)/2}$. By computing the arithmetic and quadratic means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

***25.** Write the numbers $1, 2, \ldots, 2n$ on a blackboard, where $n$ is an odd integer. Pick any two of the numbers, $j$ and $k$, write $|j - k|$ on the board and erase $j$ and $k$. Continue this process until only one integer is written on the board. Prove that this integer must be odd.

***26.** Suppose that five ones and four zeros are arranged around a circle. Between any two equal bits you insert a 0 and between any two unequal bits you insert a 1 to produce nine new bits. Then you erase the nine original bits. Show that when you iterate this procedure, you can never get nine zeros. [*Hint:* Work backward, assuming that you did end up with nine zeros.]

**27.** Formulate a conjecture about the decimal digits that appear as the final decimal digit of the fourth power of an integer. Prove your conjecture using a proof by cases.

**28.** Formulate a conjecture about the final two decimal digits of the square of an integer. Prove your conjecture using a proof by cases.

**29.** Prove that there is no positive integer $n$ such that $n^2 + n^3 = 100$.

**30.** Prove that there are no solutions in integers $x$ and $y$ to the equation $2x^2 + 5y^2 = 14$.

**31.** Prove that there are no solutions in positive integers $x$ and $y$ to the equation $x^4 + y^4 = 625$.

**32.** Prove that there are infinitely many solutions in positive integers $x$, $y$, and $z$ to the equation $x^2 + y^2 = z^2$. [*Hint:* Let $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$, where $m$ and $n$ are integers.]

**33.** Adapt the proof in Example 4 in Section 1.7 to prove that if $n = abc$, where $a$, $b$, and $c$ are positive integers, then $a \leq \sqrt[3]{n}$, $b \leq \sqrt[3]{n}$, or $c \leq \sqrt[3]{n}$.

**34.** Prove that $\sqrt[3]{2}$ is irrational.

**35.** Prove that between every two rational numbers there is an irrational number.

**36.** Prove that between every rational number and every irrational number there is an irrational number.

***37.** Let $S = x_1y_1 + x_2y_2 + \cdots + x_ny_n$, where $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are orderings of two different sequences of positive real numbers, each containing $n$ elements.

**a)** Show that $S$ takes its maximum value over all orderings of the two sequences when both sequences are sorted (so that the elements in each sequence are in nondecreasing order).

**b)** Show that $S$ takes its minimum value over all orderings of the two sequences when one sequence is sorted into nondecreasing order and the other is sorted into nonincreasing order.

**38.** Prove or disprove that if you have an 8-gallon jug of water and two empty jugs with capacities of 5 gallons and 3 gallons, respectively, then you can measure 4 gallons by successively pouring some of or all of the water in a jug into another jug.

**39.** Verify the $3x + 1$ conjecture for these integers.

**a)** 6 **b)** 7 **c)** 17 **d)** 21

**40.** Verify the $3x + 1$ conjecture for these integers.

**a)** 16 **b)** 11 **c)** 35 **d)** 113

**41.** Prove or disprove that you can use dominoes to tile the standard checkerboard with two adjacent corners removed (that is, corners that are not opposite).

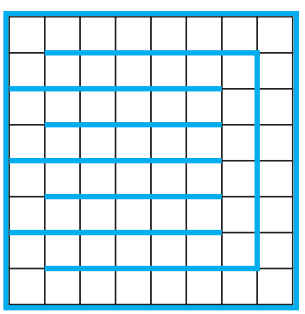
**42.** Prove or disprove that you can use dominoes to tile a standard checkerboard with all four corners removed.

**43.** Prove that you can use dominoes to tile a rectangular checkerboard with an even number of squares.

**44.** Prove or disprove that you can use dominoes to tile a $5 \times 5$ checkerboard with three corners removed.

**45.** Use a proof by exhaustion to show that a tiling using dominoes of a $4 \times 4$ checkerboard with opposite corners removed does not exist. [*Hint:* First show that you can assume that the squares in the upper left and lower right corners are removed. Number the squares of the original checkerboard from 1 to 16, starting in the first row, moving right in this row, then starting in the leftmost square in the second row and moving right, and so on. Remove squares 1 and 16. To begin the proof, note that square 2 is covered either by a domino laid horizontally, which covers squares 2 and 3, or vertically, which covers squares 2 and 6. Consider each of these cases separately, and work through all the subcases that arise.]

***46.** Prove that when a white square and a black square are removed from an $8 \times 8$ checkerboard (colored as in the text) you can tile the remaining squares of the checkerboard using dominoes. [*Hint:* Show that when one black and one white square are removed, each part of the partition of the remaining cells formed by inserting the barriers shown in the figure can be covered by dominoes.]



**47.** Show that by removing two white squares and two black squares from an $8 \times 8$ checkerboard (colored as in the text) you can make it impossible to tile the remaining squares using dominoes.

***48.** Find all squares, if they exist, on an $8 \times 8$ checkerboard such that the board obtained by removing one of these square can be tiled using straight triominoes. [*Hint:* First use arguments based on coloring and rotations to eliminate as many squares as possible from consideration.]

***49.** **a)** Draw each of the five different tetrominoes, where a tetromino is a polyomino consisting of four squares.

**b)** For each of the five different tetrominoes, prove or disprove that you can tile a standard checkerboard using these tetrominoes.

***50.** Prove or disprove that you can tile a $10 \times 10$ checkerboard using straight tetrominoes.

## Key Terms and Results

### TERMS

**proposition:** a statement that is true or false

**propositional variable:** a variable that represents a proposition

**truth value:** true or false

**$\neg p$ (negation of $p$):** the proposition with truth value opposite to the truth value of $p$

**logical operators:** operators used to combine propositions

**compound proposition:** a proposition constructed by combining propositions using logical operators

**truth table:** a table displaying all possible truth values of propositions

**$p \vee q$ (disjunction of $p$ and $q$):** the proposition "$p$ or $q$," which is true if and only if at least one of $p$ and $q$ is true

**$p \wedge q$ (conjunction of $p$ and $q$):** the proposition "$p$ and $q$," which is true if and only if both $p$ and $q$ are true

**$p \oplus q$ (exclusive or of $p$ and $q$):** the proposition "$p$ *XOR* $q$," which is true when exactly one of $p$ and $q$ is true

**$p \rightarrow q$ ($p$ implies $q$):** the proposition "if $p$, then $q$," which is false if and only if $p$ is true and $q$ is false

**converse of $p \rightarrow q$:** the conditional statement $q \rightarrow p$

**contrapositive of $p \rightarrow q$:** the conditional statement $\neg q \rightarrow \neg p$

**inverse of $p \rightarrow q$:** the conditional statement $\neg p \rightarrow \neg q$

**$p \leftrightarrow q$ (biconditional):** the proposition "$p$ if and only if $q$," which is true if and only if $p$ and $q$ have the same truth value

**bit:** either a 0 or a 1

**Boolean variable:** a variable that has a value of 0 or 1

**bit operation:** an operation on a bit or bits

**bit string:** a list of bits

**bitwise operations:** operations on bit strings that operate on each bit in one string and the corresponding bit in the other string

**logic gate:** a logic element that performs a logical operation on one or more bits to produce an output bit

**logic circuit:** a switching circuit made up of logic gates that produces one or more output bits

**tautology:** a compound proposition that is always true

**contradiction:** a compound proposition that is always false

**contingency:** a compound proposition that is sometimes true and sometimes false

**consistent compound propositions:** compound propositions for which there is an assignment of truth values to the variables that makes all these propositions true

**satisfiable compound proposition:** a compound proposition for which there is an assignment of truth values to its variables that makes it true

**logically equivalent compound propositions:** compound propositions that always have the same truth values

**predicate:** part of a sentence that attributes a property to the subject

**propositional function:** a statement containing one or more variables that becomes a proposition when each of its variables is assigned a value or is bound by a quantifier

**domain (or universe) of discourse:** the values a variable in a propositional function may take

**$\exists x\, P(x)$ (existential quantification of $P(x)$):** the proposition that is true if and only if there exists an $x$ in the domain such that $P(x)$ is true

**$\forall x P(x)$ (universal quantification of $P(x)$):** the proposition that is true if and only if $P(x)$ is true for every $x$ in the domain

**logically equivalent expressions:** expressions that have the same truth value no matter which propositional functions and domains are used

**free variable:** a variable not bound in a propositional function

**bound variable:** a variable that is quantified

**scope of a quantifier:** portion of a statement where the quantifier binds its variable

**argument:** a sequence of statements

**argument form:** a sequence of compound propositions involving propositional variables

**premise:** a statement, in an argument, or argument form, other than the final one

**conclusion:** the final statement in an argument or argument form

**valid argument form:** a sequence of compound propositions involving propositional variables where the truth of all the premises implies the truth of the conclusion

**valid argument:** an argument with a valid argument form

**rule of inference:** a valid argument form that can be used in the demonstration that arguments are valid

**fallacy:** an invalid argument form often used incorrectly as a rule of inference (or sometimes, more generally, an incorrect argument)

**circular reasoning or begging the question:** reasoning where one or more steps are based on the truth of the statement being proved

**theorem:** a mathematical assertion that can be shown to be true

**conjecture:** a mathematical assertion proposed to be true, but that has not been proved

**proof:** a demonstration that a theorem is true

**axiom:** a statement that is assumed to be true and that can be used as a basis for proving theorems

**lemma:** a theorem used to prove other theorems

**corollary:** a proposition that can be proved as a consequence of a theorem that has just been proved

**vacuous proof:** a proof that $p \rightarrow q$ is true based on the fact that $p$ is false

**trivial proof:** a proof that $p \rightarrow q$ is true based on the fact that $q$ is true

**direct proof:** a proof that $p \rightarrow q$ is true that proceeds by showing that $q$ must be true when $p$ is true

**proof by contraposition:** a proof that $p \rightarrow q$ is true that proceeds by showing that $p$ must be false when $q$ is false

**proof by contradiction:** a proof that $p$ is true based on the truth of the conditional statement $\neg p \rightarrow q$, where $q$ is a contradiction

**exhaustive proof:** a proof that establishes a result by checking a list of all possible cases

**proof by cases:** a proof broken into separate cases, where these cases cover all possibilities

**without loss of generality:** an assumption in a proof that makes it possible to prove a theorem by reducing the number of cases to consider in the proof

**counterexample:** an element $x$ such that $P(x)$ is false

**constructive existence proof:** a proof that an element with a specified property exists that explicitly finds such an element

**nonconstructive existence proof:** a proof that an element with a specified property exists that does not explicitly find such an element

**rational number:** a number that can be expressed as the ratio of two integers $p$ and $q$ such that $q \neq 0$

**uniqueness proof:** a proof that there is exactly one element satisfying a specified property

**RESULTS**

The logical equivalences given in Tables 6, 7, and 8 in Section 1.3.

De Morgan's laws for quantifiers.

Rules of inference for propositional calculus.

Rules of inference for quantified statements.

## Review Questions

**1. a)** Define the negation of a proposition.

**b)** What is the negation of "This is a boring course"?

**2. a)** Define (using truth tables) the disjunction, conjunction, exclusive or, conditional, and biconditional of the propositions $p$ and $q$.

**b)** What are the disjunction, conjunction, exclusive or, conditional, and biconditional of the propositions "I'll go to the movies tonight" and "I'll finish my discrete mathematics homework"?

**3. a)** Describe at least five different ways to write the conditional statement $p \rightarrow q$ in English.

**b)** Define the converse and contrapositive of a conditional statement.

**c)** State the converse and the contrapositive of the conditional statement "If it is sunny tomorrow, then I will go for a walk in the woods."

**4. a)** What does it mean for two propositions to be logically equivalent?

**b)** Describe the different ways to show that two compound propositions are logically equivalent.

**c)** Show in at least two different ways that the compound propositions $\neg p \vee (r \rightarrow \neg q)$ and $\neg p \vee \neg q \vee \neg r$ are equivalent.

**5.** *(Depends on the Exercise Set in Section 1.3)*

**a)** Given a truth table, explain how to use disjunctive normal form to construct a compound proposition with this truth table.

**b)** Explain why part (a) shows that the operators $\wedge$, $\vee$, and $\neg$ are functionally complete.

**c)** Is there an operator such that the set containing just this operator is functionally complete?

**6.** What are the universal and existential quantifications of a predicate $P(x)$? What are their negations?

**7. a)** What is the difference between the quantification $\exists x \forall y P(x, y)$ and $\forall y \exists x P(x, y)$, where $P(x, y)$ is a predicate?

**b)** Give an example of a predicate $P(x, y)$ such that $\exists x \forall y P(x, y)$ and $\forall y \exists x P(x, y)$ have different truth values.

**8.** Describe what is meant by a valid argument in propositional logic and show that the argument "If the earth is flat, then you can sail off the edge of the earth," "You cannot sail off the edge of the earth," therefore, "The earth is not flat" is a valid argument.

**9.** Use rules of inference to show that if the premises "All zebras have stripes" and "Mark is a zebra" are true, then the conclusion "Mark has stripes" is true.

**10. a)** Describe what is meant by a direct proof, a proof by contraposition, and a proof by contradiction of a conditional statement $p \rightarrow q$.

**b)** Give a direct proof, a proof by contraposition and a proof by contradiction of the statement: "If $n$ is even, then $n + 4$ is even."

**11. a)** Describe a way to prove the biconditional $p \leftrightarrow q$.

**b)** Prove the statement: "The integer $3n + 2$ is odd if and only if the integer $9n + 5$ is even, where $n$ is an integer."

**12.** To prove that the statements $p_1$, $p_2$, $p_3$, and $p_4$ are equivalent, is it sufficient to show that the conditional statements $p_4 \rightarrow p_2$, $p_3 \rightarrow p_1$, and $p_1 \rightarrow p_2$ are valid? If not, provide another collection of conditional statements that can be used to show that the four statements are equivalent.

**13. a)** Suppose that a statement of the form $\forall x P(x)$ is false. How can this be proved?

**b)** Show that the statement "For every positive integer $n$, $n^2 \geq 2n$" is false.

**14.** What is the difference between a constructive and nonconstructive existence proof? Give an example of each.

**15.** What are the elements of a proof that there is a unique element $x$ such that $P(x)$, where $P(x)$ is a propositional function?

**16.** Explain how a proof by cases can be used to prove a result about absolute values, such as the fact that $|xy| = |x||y|$ for all real numbers $x$ and $y$.

## Supplementary Exercises

**1.** Let $p$ be the proposition "I will do every exercise in this book" and $q$ be the proposition "I will get an "A" in this course." Express each of these as a combination of $p$ and $q$.

**a)** I will get an "A" in this course only if I do every exercise in this book.

**b)** I will get an "A" in this course and I will do every exercise in this book.

**c)** Either I will not get an "A" in this course or I will not do every exercise in this book.

**d)** For me to get an "A" in this course it is necessary and sufficient that I do every exercise in this book.

**2.** Find the truth table of the compound proposition $(p \vee q) \rightarrow (p \wedge \neg r)$.

**3.** Show that these compound propositions are tautologies.
**a)** $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
**b)** $((p \vee q) \wedge \neg p) \rightarrow q$

**4.** Give the converse, the contrapositive, and the inverse of these conditional statements.
**a)** If it rains today, then I will drive to work.
**b)** If $|x| = x$, then $x \geq 0$.
**c)** If $n$ is greater than 3, then $n^2$ is greater than 9.

**5.** Given a conditional statement $p \rightarrow q$, find the converse of its inverse, the converse of its converse, and the converse of its contrapositive.

**6.** Given a conditional statement $p \rightarrow q$, find the inverse of its inverse, the inverse of its converse, and the inverse of its contrapositive.

**7.** Find a compound proposition involving the propositional variables $p$, $q$, $r$, and $s$ that is true when exactly three of these propositional variables are true and is false otherwise.

**8.** Show that these statements are inconsistent: "If Sergei takes the job offer then he will get a signing bonus." "If Sergei takes the job offer, then he will receive a higher salary." "If Sergei gets a signing bonus, then he will not receive a higher salary." "Sergei takes the job offer."

**9.** Show that these statements are inconsistent: "If Miranda does not take a course in discrete mathematics, then she will not graduate." "If Miranda does not graduate, then she is not qualified for the job." "If Miranda reads this book, then she is qualified for the job." "Miranda does not take a course in discrete mathematics but she reads this book."

Teachers in the Middle Ages supposedly tested the realtime propositional logic ability of a student via a technique known as an **obligato game**. In an obligato game, a number of rounds is set and in each round the teacher gives the student successive assertions that the student must either accept or reject as they are given. When the student accepts an assertion, it is added as a commitment; when the student rejects an assertion its negation is added as a commitment. The student passes the test if the consistency of all commitments is maintained throughout the test.

**10.** Suppose that in a three-round obligato game, the teacher first gives the student the proposition $p \rightarrow q$, then the proposition $\neg(p \vee r) \vee q$, and finally the proposition $q$. For which of the eight possible sequences of three answers will the student pass the test?

**11.** Suppose that in a four-round obligato game, the teacher first gives the student the proposition $\neg(p \rightarrow (q \wedge r))$, then the proposition $p \vee \neg q$, then the proposition $\neg r$, and finally, the proposition $(p \wedge r) \vee (q \rightarrow p)$. For which of the 16 possible sequences of four answers will the student pass the test?

**12.** Explain why every obligato game has a winning strategy.

Exercises 13 and 14 are set on the island of knights and knaves described in Example 7 in Section 1.2.

**13.** Suppose that you meet three people Aaron, Bohan, and Crystal. Can you determine what Aaron, Bohan, and Crystal are if Aaron says "All of us are knaves" and Bohan says "Exactly one of us is a knave."?

**14.** Suppose that you meet three people, Anita, Boris, and Carmen. What are Anita, Boris, and Carmen if Anita says "I am a knave and Boris is a knight" and Boris says "Exactly one of the three of us is a knight"?

**15.** (Adapted from [Sm78]) Suppose that on an island there are three types of people, knights, knaves, and normals (also known as spies). Knights always tell the truth, knaves always lie, and normals sometimes lie and sometimes tell the truth. Detectives questioned three inhabitants of the island—Amy, Brenda, and Claire—as part of the investigation of a crime. The detectives knew that one of the three committed the crime, but not which one. They also knew that the criminal was a knight, and that the other two were not. Additionally, the detectives recorded these statements: Amy: "I am innocent." Brenda: "What Amy says is true." Claire: "Brenda is not a normal." After analyzing their information, the detectives positively identified the guilty party. Who was it?

**16.** Show that if $S$ is a proposition, where $S$ is the conditional statement "If $S$ is true, then unicorns live," then "Unicorns live" is true. Show that it follows that $S$ cannot be a proposition. (This paradox is known as *Löb's paradox*.)

**17.** Show that the argument with premises "The tooth fairy is a real person" and "The tooth fairy is not a real person" and conclusion "You can find gold at the end of the rainbow" is a valid argument. Does this show that the conclusion is true?

**18.** Suppose that the truth value of the proposition $p_i$ is **T** whenever $i$ is an odd positive integer and is **F** whenever $i$ is an even positive integer. Find the truth values of $\bigvee_{i=1}^{100}(p_i \wedge p_{i+1})$ and $\bigwedge_{i=1}^{100}(p_i \vee p_{i+1})$.

***19.** Model $16 \times 16$ Sudoku puzzles (with $4 \times 4$ blocks) as satisfiability problems.

**20.** Let $P(x)$ be the statement "Student $x$ knows calculus" and let $Q(y)$ be the statement "Class $y$ contains a student who knows calculus." Express each of these as quantifications of $P(x)$ and $Q(y)$.
**a)** Some students know calculus.
**b)** Not every student knows calculus.
**c)** Every class has a student in it who knows calculus.
**d)** Every student in every class knows calculus.
**e)** There is at least one class with no students who know calculus.

**21.** Let $P(m, n)$ be the statement "$m$ divides $n$," where the domain for both variables consists of all positive integers. (By "$m$ divides $n$" we mean that $n = km$ for some integer $k$.) Determine the truth values of each of these statements.
**a)** $P(4, 5)$ **b)** $P(2, 4)$
**c)** $\forall m \forall n\, P(m, n)$ **d)** $\exists m \forall n\, P(m, n)$
**e)** $\exists n \forall m\, P(m, n)$ **f)** $\forall n\, P(1, n)$

**22.** Find a domain for the quantifiers in $\exists x \exists y(x \neq y \wedge \forall z((z = x) \vee (z = y)))$ such that this statement is true.

**23.** Find a domain for the quantifiers in $\exists x \exists y(x \neq y \wedge \forall z((z = x) \vee (z = y)))$ such that this statement is false.

**24.** Use existential and universal quantifiers to express the statement "No one has more than three grandmothers" using the propositional function $G(x, y)$, which represents "$x$ is the grandmother of $y$."

**25.** Use existential and universal quantifiers to express the statement "Everyone has exactly two biological parents" using the propositional function $P(x, y)$, which represents "$x$ is the biological parent of $y$."

**26.** The quantifier $\exists_n$ denotes "there exists exactly $n$," so that $\exists_n x P(x)$ means there exist exactly $n$ values in the domain such that $P(x)$ is true. Determine the true value of these statements where the domain consists of all real numbers.

**a)** $\exists_0 x(x^2 = -1)$ **b)** $\exists_1 x(|x| = 0)$
**c)** $\exists_2 x(x^2 = 2)$ **d)** $\exists_3 x(x = |x|)$

**27.** Express each of these statements using existential and universal quantifiers and propositional logic where $\exists_n$ is defined in Exercise 26.

**a)** $\exists_0 x P(x)$ **b)** $\exists_1 x P(x)$
**c)** $\exists_2 x P(x)$ **d)** $\exists_3 x P(x)$

**28.** Let $P(x, y)$ be a propositional function. Show that $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$ is a tautology.

**29.** Let $P(x)$ and $Q(x)$ be propositional functions. Show that $\exists x (P(x) \rightarrow Q(x))$ and $\forall x P(x) \rightarrow \exists x Q(x)$ always have the same truth value.

**30.** If $\forall y \exists x P(x, y)$ is true, does it necessarily follow that $\exists x \forall y P(x, y)$ is true?

**31.** If $\forall x \exists y P(x, y)$ is true, does it necessarily follow that $\exists x \forall y P(x, y)$ is true?

**32.** Find the negations of these statements.

**a)** If it snows today, then I will go skiing tomorrow.
**b)** Every person in this class understands mathematical induction.
**c)** Some students in this class do not like discrete mathematics.
**d)** In every mathematics class there is some student who falls asleep during lectures.

**33.** Express this statement using quantifiers: "Every student in this class has taken some course in every department in the school of mathematical sciences."

**34.** Express this statement using quantifiers: "There is a building on the campus of some college in the United States in which every room is painted white."

**35.** Express the statement "There is exactly one student in this class who has taken exactly one mathematics class at this school" using the uniqueness quantifier. Then express this statement using quantifiers, without using the uniqueness quantifier.

**36.** Describe a rule of inference that can be used to prove that there are exactly two elements $x$ and $y$ in a domain such that $P(x)$ and $P(y)$ are true. Express this rule of inference as a statement in English.

**37.** Use rules of inference to show that if the premises $\forall x(P(x) \rightarrow Q(x))$, $\forall x(Q(x) \rightarrow R(x))$, and $\neg R(a)$, where $a$ is in the domain, are true, then the conclusion $\neg P(a)$ is true.

**38.** Prove that if $x^3$ is irrational, then $x$ is irrational.

**39.** Prove that if $x$ is irrational and $x \geq 0$, then $\sqrt{x}$ is irrational.

**40.** Prove that given a nonnegative integer $n$, there is a unique nonnegative integer $m$ such that $m^2 \leq n < (m + 1)^2$.

**41.** Prove that there exists an integer $m$ such that $m^2 > 10^{1000}$. Is your proof constructive or nonconstructive?

**42.** Prove that there is a positive integer that can be written as the sum of squares of positive integers in two different ways. (Use a computer or calculator to speed up your work.)

**43.** Disprove the statement that every positive integer is the sum of the cubes of eight nonnegative integers.

**44.** Disprove the statement that every positive integer is the sum of at most two squares and a cube of nonnegative integers.

**45.** Disprove the statement that every positive integer is the sum of 36 fifth powers of nonnegative integers.

**46.** Assuming the truth of the theorem that states that $\sqrt{n}$ is irrational whenever $n$ is a positive integer that is not a perfect square, prove that $\sqrt{2} + \sqrt{3}$ is irrational.

## Computer Projects

### Write programs with the specified input and output.

**1.** Given the truth values of the propositions $p$ and $q$, find the truth values of the conjunction, disjunction, exclusive or, conditional statement, and biconditional of these propositions.

**2.** Given two bit strings of length $n$, find the bitwise *AND*, bitwise *OR*, and bitwise *XOR* of these strings.

***3.** Give a compound proposition, determine whether it is satisfiable by checking its truth value for all positive assignments of truth values to its propositional variables.

**4.** Given the truth values of the propositions $p$ and $q$ in fuzzy logic, find the truth value of the disjunction and the conjunction of $p$ and $q$ (see Exercises 46 and 47 of Section 1.1).

***5.** Given positive integers $m$ and $n$, interactively play the game of Chomp.

***6.** Given a portion of a checkerboard, look for tilings of this checkerboard with various types of polyominoes, including dominoes, the two types of triominoes, and larger polyominoes.

## Computations and Explorations

### Use a computational program or programs you have written to do these exercises.

1. Look for positive integers that are not the sum of the cubes of nine different positive integers.
2. Look for positive integers greater than 79 that are not the sum of the fourth powers of 18 positive integers.
3. Find as many positive integers as you can that can be written as the sum of cubes of positive integers, in two different ways, sharing this property with 1729.
*4. Try to find winning strategies for the game of Chomp for different initial configurations of cookies.
5. Construct the 12 different pentominoes, where a pentomino is a polyomino consisting of five squares.
6. Find all the rectangles of 60 squares that can be tiled using every one of the 12 different pentominoes.

## Writing Projects

### Respond to these with essays using outside sources.

1. Discuss logical paradoxes, including the paradox of Epimenides the Cretan, Jourdain's card paradox, and the barber paradox, and how they are resolved.
2. Describe how fuzzy logic is being applied to practical applications. Consult one or more of the recent books on fuzzy logic written for general audiences.
3. Describe some of the practical problems that can be modeled as satisfiability problems.
4. Describe some of the techniques that have been devised to help people solve Sudoku puzzles without the use of a computer.
5. Describe the basic rules of *WFF'N PROOF*, *The Game of Modern Logic*, developed by Layman Allen. Give examples of some of the games included in *WFF'N PROOF*.
6. Read some of the writings of Lewis Carroll on symbolic logic. Describe in detail some of the models he used to represent logical arguments and the rules of inference he used in these arguments.
7. Extend the discussion of Prolog given in Section 1.4, explaining in more depth how Prolog employs resolution.
8. Discuss some of the techniques used in computational logic, including Skolem's rule.
9. "Automated theorem proving" is the task of using computers to mechanically prove theorems. Discuss the goals and applications of automated theorem proving and the progress made in developing automated theorem provers.
10. Describe how DNA computing has been used to solve instances of the satisfiability problem.
11. Look up some of the incorrect proofs of famous open questions and open questions that were solved since 1970 and describe the type of error made in each proof.
12. Discuss what is known about winning strategies in the game of Chomp.
13. Describe various aspects of proof strategy discussed by George Pólya in his writings on reasoning, including [Po62], [Po71], and [Po90].
14. Describe a few problems and results about tilings with polyominoes, as described in [Go94] and [Ma91], for example.

CHAPTER

# 2 Basic Structures: Sets, Functions, Sequences, Sums, and Matrices



Much of discrete mathematics is devoted to the study of discrete structures, used to represent discrete objects. Many important discrete structures are built using sets, which are collections of objects. Among the discrete structures built from sets are combinations, unordered collections of objects used extensively in counting; relations, sets of ordered pairs that represent relationships between objects; graphs, sets of vertices and edges that connect vertices; and finite state machines, used to model computing machines. These are some of the topics we will study in later chapters.

The concept of a function is extremely important in discrete mathematics. A function assigns to each element of a first set exactly one element of a second set, where the two sets are not necessarily distinct. Functions play important roles throughout discrete mathematics. They are used to represent the computational complexity of algorithms, to study the size of sets, to count objects, and in a myriad of other ways. Useful structures such as sequences and strings are special types of functions. In this chapter, we will introduce the notion of a sequence, which represents ordered lists of elements. Furthermore, we will introduce some important types of sequences and we will show how to define the terms of a sequence using earlier terms. We will also address the problem of identifying a sequence from its first few terms.

In our study of discrete mathematics, we will often add consecutive terms of a sequence of numbers. Because adding terms from a sequence, as well as other indexed sets of numbers, is such a common occurrence, a special notation has been developed for adding such terms. In this chapter, we will introduce the notation used to express summations. We will develop formulae for certain types of summations that appear throughout the study of discrete mathematics. For instance, we will encounter such summations in the analysis of the number of steps used by an algorithm to sort a list of numbers so that its terms are in increasing order.

The relative sizes of infinite sets can be studied by introducing the notion of the size, or cardinality, of a set. We say that a set is countable when it is finite or has the same size as the set of positive integers. In this chapter we will establish the surprising result that the set of rational numbers is countable, while the set of real numbers is not. We will also show how the concepts we discuss can be used to show that there are functions that cannot be computed using a computer program in any programming language.

Matrices are used in discrete mathematics to represent a variety of discrete structures. We will review the basic material about matrices and matrix arithmetic needed to represent relations and graphs. The matrix arithmetic we study will be used to solve a variety of problems involving these structures.

## 2.1 Sets

### Introduction

In this section, we study the fundamental discrete structure on which all other discrete structures are built, namely, the set. Sets are used to group objects together. Often, but not always, the objects in a set have similar properties. For instance, all the students who are currently enrolled in your school make up a set. Likewise, all the students currently taking a course in discrete mathematics at any school make up a set. In addition, those students enrolled in your school who are taking a course in discrete mathematics form a set that can be obtained by taking the elements common to the first two collections. The language of sets is a means to study such

collections in an organized fashion. We now provide a definition of a set. This definition is an intuitive definition, which is not part of a formal theory of sets.

**DEFINITION 1**

A *set* is an unordered collection of objects, called *elements* or *members* of the set. A set is said to *contain* its elements. We write $a \in A$ to denote that $a$ is an element of the set $A$. The notation $a \notin A$ denotes that $a$ is not an element of the set $A$.

It is common for sets to be denoted using uppercase letters. Lowercase letters are usually used to denote elements of sets.

There are several ways to describe a set. One way is to list all the members of a set, when this is possible. We use a notation where all members of the set are listed between braces. For example, the notation $\{a, b, c, d\}$ represents the set with the four elements $a$, $b$, $c$, and $d$. This way of describing a set is known as the **roster method**.

**EXAMPLE 1** The set $V$ of all vowels in the English alphabet can be written as $V = \{a, e, i, o, u\}$. ◀

**EXAMPLE 2** The set $O$ of odd positive integers less than 10 can be expressed by $O = \{1, 3, 5, 7, 9\}$. ◀

**EXAMPLE 3** Although sets are usually used to group together elements with common properties, there is nothing that prevents a set from having seemingly unrelated elements. For instance, {$a$, 2, Fred, New Jersey} is the set containing the four elements $a$, 2, Fred, and New Jersey. ◀

Sometimes the roster method is used to describe a set without listing all its members. Some members of the set are listed, and then *ellipses* (. . .) are used when the general pattern of the elements is obvious.

**EXAMPLE 4** The set of positive integers less than 100 can be denoted by $\{1, 2, 3, \ldots, 99\}$. ◀

Extra Examples

Another way to describe a set is to use **set builder** notation. We characterize all those elements in the set by stating the property or properties they must have to be members. For instance, the set $O$ of all odd positive integers less than 10 can be written as

$$O = \{x \mid x \text{ is an odd positive integer less than } 10\},$$

or, specifying the universe as the set of positive integers, as

$$O = \{x \in \mathbf{Z}^+ \mid x \text{ is odd and } x < 10\}.$$

We often use this type of notation to describe sets when it is impossible to list all the elements of the set. For instance, the set $\mathbf{Q}^+$ of all positive rational numbers can be written as

$$\mathbf{Q}^+ = \{x \in \mathbf{R} \mid x = \tfrac{p}{q}, \text{ for some positive integers } p \text{ and } q\}.$$

Beware that mathematicians disagree whether 0 is a natural number. We consider it quite natural.

These sets, each denoted using a boldface letter, play an important role in discrete mathematics:

$\mathbf{N} = \{0, 1, 2, 3, \ldots\}$, the set of **natural numbers**
$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of **integers**
$\mathbf{Z}^+ = \{1, 2, 3, \ldots\}$, the set of **positive integers**
$\mathbf{Q} = \{p/q \mid p \in \mathbf{Z}, q \in \mathbf{Z}, \text{ and } q \neq 0\}$, the set of **rational numbers**
$\mathbf{R}$, the set of **real numbers**
$\mathbf{R}^+$, the set of **positive real numbers**
$\mathbf{C}$, the set of **complex numbers**.

(Note that some people do not consider 0 a natural number, so be careful to check how the term *natural numbers* is used when you read other books.)

Recall the notation for **intervals** of real numbers. When $a$ and $b$ are real numbers with $a < b$, we write

$$[a, b] = \{x \mid a \leq x \leq b\}$$
$$[a, b) = \{x \mid a \leq x < b\}$$
$$(a, b] = \{x \mid a < x \leq b\}$$
$$(a, b) = \{x \mid a < x < b\}$$

Note that $[a, b]$ is called the **closed interval** from $a$ to $b$ and $(a, b)$ is called the **open interval** from $a$ to $b$.

Sets can have other sets as members, as Example 5 illustrates.

**EXAMPLE 5** The set $\{\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}\}$ is a set containing four elements, each of which is a set. The four elements of this set are $\mathbf{N}$, the set of natural numbers; $\mathbf{Z}$, the set of integers; $\mathbf{Q}$, the set of rational numbers; and $\mathbf{R}$, the set of real numbers. ◀

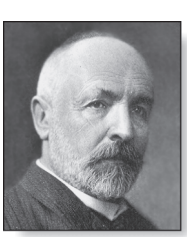
***Remark:*** Note that the concept of a datatype, or type, in computer science is built upon the concept of a set. In particular, a **datatype** or **type** is the name of a set, together with a set of operations that can be performed on objects from that set. For example, *boolean* is the name of the set $\{0, 1\}$ together with operators on one or more elements of this set, such as AND, OR, and NOT.

Because many mathematical statements assert that two differently specified collections of objects are really the same set, we need to understand what it means for two sets to be equal.

**DEFINITION 2** Two sets are *equal* if and only if they have the same elements. Therefore, if $A$ and $B$ are sets, then $A$ and $B$ are equal if and only if $\forall x(x \in A \leftrightarrow x \in B)$. We write $A = B$ if $A$ and $B$ are equal sets.

**EXAMPLE 6** The sets $\{1, 3, 5\}$ and $\{3, 5, 1\}$ are equal, because they have the same elements. Note that the order in which the elements of a set are listed does not matter. Note also that it does not matter if an element of a set is listed more than once, so $\{1, 3, 3, 3, 5, 5, 5, 5\}$ is the same as the set $\{1, 3, 5\}$ because they have the same elements. ◀

**Links**



GEORG CANTOR (1845–1918) Georg Cantor was born in St. Petersburg, Russia, where his father was a successful merchant. Cantor developed his interest in mathematics in his teens. He began his university studies in Zurich in 1862, but when his father died he left Zurich. He continued his university studies at the University of Berlin in 1863, where he studied under the eminent mathematicians Weierstrass, Kummer, and Kronecker. He received his doctor's degree in 1867, after having written a dissertation on number theory. Cantor assumed a position at the University of Halle in 1869, where he continued working until his death.

Cantor is considered the founder of set theory. His contributions in this area include the discovery that the set of real numbers is uncountable. He is also noted for his many important contributions to analysis. Cantor also was interested in philosophy and wrote papers relating his theory of sets with metaphysics.

Cantor married in 1874 and had five children. His melancholy temperament was balanced by his wife's happy disposition. Although he received a large inheritance from his father, he was poorly paid as a professor. To mitigate this, he tried to obtain a better-paying position at the University of Berlin. His appointment there was blocked by Kronecker, who did not agree with Cantor's views on set theory. Cantor suffered from mental illness throughout the later years of his life. He died in 1918 from a heart attack.

THE EMPTY SET There is a special set that has no elements. This set is called the **empty set**, or **null set**, and is denoted by ∅. The empty set can also be denoted by { } (that is, we represent the empty set with a pair of braces that encloses all the elements in this set). Often, a set of elements with certain properties turns out to be the null set. For instance, the set of all positive integers that are greater than their squares is the null set.

{∅} has one more element than ∅.

A set with one element is called a **singleton set**. A common error is to confuse the empty set ∅ with the set {∅}, which is a singleton set. The single element of the set {∅} is the empty set itself! A useful analogy for remembering this difference is to think of folders in a computer file system. The empty set can be thought of as an empty folder and the set consisting of just the empty set can be thought of as a folder with exactly one folder inside, namely, the empty folder.

Links

NAIVE SET THEORY Note that the term *object* has been used in the definition of a set, Definition 1, without specifying what an object is. This description of a set as a collection of objects, based on the intuitive notion of an object, was first stated in 1895 by the German mathematician Georg Cantor. The theory that results from this intuitive definition of a set, and the use of the intuitive notion that for any property whatever, there is a set consisting of exactly the objects with this property, leads to **paradoxes**, or logical inconsistencies. This was shown by the English philosopher Bertrand Russell in 1902 (see Exercise 46 for a description of one of these paradoxes). These logical inconsistencies can be avoided by building set theory beginning with axioms. However, we will use Cantor's original version of set theory, known as **naive set theory**, in this book because all sets considered in this book can be treated consistently using Cantor's original theory. Students will find familiarity with naive set theory helpful if they go on to learn about axiomatic set theory. They will also find the development of axiomatic set theory much more abstract than the material in this text. We refer the interested reader to [Su72] to learn more about axiomatic set theory.

## Venn Diagrams

Sets can be represented graphically using Venn diagrams, named after the English mathematician John Venn, who introduced their use in 1881. In Venn diagrams the **universal set** $U$, which contains all the objects under consideration, is represented by a rectangle. (Note that the universal set varies depending on which objects are of interest.) Inside this rectangle, circles or other geometrical figures are used to represent sets. Sometimes points are used to represent the particular elements of the set. Venn diagrams are often used to indicate the relationships between sets. We show how a Venn diagram can be used in Example 7.

Assessment

**EXAMPLE 7** Draw a Venn diagram that represents $V$, the set of vowels in the English alphabet.

*Solution:* We draw a rectangle to indicate the universal set $U$, which is the set of the 26 letters of the English alphabet. Inside this rectangle we draw a circle to represent $V$. Inside this circle we indicate the elements of $V$ with points (see Figure 1). ◀

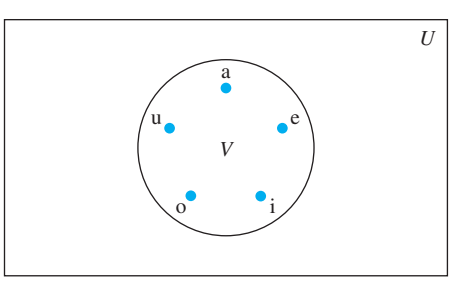



**FIGURE 1 Venn Diagram for the Set of Vowels.**

## Subsets

It is common to encounter situations where the elements of one set are also the elements of a second set. We now introduce some terminology and notation to express such relationships between sets.

**DEFINITION 3** The set $A$ is a *subset* of $B$ if and only if every element of $A$ is also an element of $B$. We use the notation $A \subseteq B$ to indicate that $A$ is a subset of the set $B$.

We see that $A \subseteq B$ if and only if the quantification

$$\forall x(x \in A \rightarrow x \in B)$$

is true. Note that to show that $A$ is not a subset of $B$ we need only find one element $x \in A$ with $x \notin B$. Such an $x$ is a counterexample to the claim that $x \in A$ implies $x \in B$.

We have these useful rules for determining whether one set is a subset of another:

*Showing that A is a Subset of B* To show that $A \subseteq B$, show that if $x$ belongs to $A$ then $x$ also belongs to $B$.

*Showing that A is Not a Subset of B* To show that $A \not\subseteq B$, find a single $x \in A$ such that $x \notin B$.

**EXAMPLE 8** The set of all odd positive integers less than 10 is a subset of the set of all positive integers less than 10, the set of rational numbers is a subset of the set of real numbers, the set of all computer science majors at your school is a subset of the set of all students at your school, and the set of all people in China is a subset of the set of all people in China (that is, it is a subset of itself). Each of these facts follows immediately by noting that an element that belongs to the first set in each pair of sets also belongs to the second set in that pair. ◀

**EXAMPLE 9** The set of integers with squares less than 100 is not a subset of the set of nonnegative integers because $-1$ is in the former set [as $(-1)^2 < 100$], but not the later set. The set of people who have taken discrete mathematics at your school is not a subset of the set of all computer science majors at your school if there is at least one student who has taken discrete mathematics who is not a computer science major. ◀

Links

BERTRAND RUSSELL (1872–1970) Bertrand Russell was born into a prominent English family active in the progressive movement and having a strong commitment to liberty. He became an orphan at an early age and was placed in the care of his father's parents, who had him educated at home. He entered Trinity College, Cambridge, in 1890, where he excelled in mathematics and in moral science. He won a fellowship on the basis of his work on the foundations of geometry. In 1910 Trinity College appointed him to a lectureship in logic and the philosophy of mathematics.

Russell fought for progressive causes throughout his life. He held strong pacifist views, and his protests against World War I led to dismissal from his position at Trinity College. He was imprisoned for 6 months in 1918 because of an article he wrote that was branded as seditious. Russell fought for women's suffrage in Great Britain. In 1961, at the age of 89, he was imprisoned for the second time for his protests advocating nuclear disarmament.

Russell's greatest work was in his development of principles that could be used as a foundation for all of mathematics. His most famous work is *Principia Mathematica,* written with Alfred North Whitehead, which attempts to deduce all of mathematics using a set of primitive axioms. He wrote many books on philosophy, physics, and his political ideas. Russell won the Nobel Prize for literature in 1950.

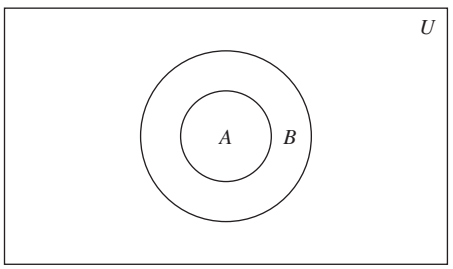



**FIGURE 2** **Venn Diagram Showing that $A$ Is a Subset of $B$.**

Theorem 1 shows that every nonempty set $S$ is guaranteed to have at least two subsets, the empty set and the set $S$ itself, that is, $\emptyset \subseteq S$ and $S \subseteq S$.

**THEOREM 1** For every set $S$, $(i)$ $\emptyset \subseteq S$ and $(ii)$ $S \subseteq S$.

*Proof:* We will prove $(i)$ and leave the proof of $(ii)$ as an exercise.

Let $S$ be a set. To show that $\emptyset \subseteq S$, we must show that $\forall x(x \in \emptyset \rightarrow x \in S)$ is true. Because the empty set contains no elements, it follows that $x \in \emptyset$ is always false. It follows that the conditional statement $x \in \emptyset \rightarrow x \in S$ is always true, because its hypothesis is always false and a conditional statement with a false hypothesis is true. Therefore, $\forall x(x \in \emptyset \rightarrow x \in S)$ is true. This completes the proof of $(i)$. Note that this is an example of a vacuous proof. ◁

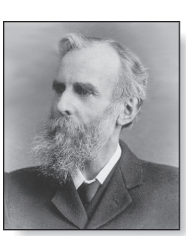
When we wish to emphasize that a set $A$ is a subset of a set $B$ but that $A \neq B$, we write $A \subset B$ and say that $A$ is a **proper subset** of $B$. For $A \subset B$ to be true, it must be the case that $A \subseteq B$ and there must exist an element $x$ of $B$ that is not an element of $A$. That is, $A$ is a proper subset of $B$ if and only if

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$$

is true. Venn diagrams can be used to illustrate that a set $A$ is a subset of a set $B$. We draw the universal set $U$ as a rectangle. Within this rectangle we draw a circle for $B$. Because $A$ is a subset of $B$, we draw the circle for $A$ within the circle for $B$. This relationship is shown in Figure 2.

A useful way to show that two sets have the same elements is to show that each set is a subset of the other. In other words, we can show that if $A$ and $B$ are sets with $A \subseteq B$ and $B \subseteq A$, then $A = B$. That is, $A = B$ if and only if $\forall x(x \in A \rightarrow x \in B)$ and $\forall x(x \in B \rightarrow x \in A)$ or equivalently if and only if $\forall x(x \in A \leftrightarrow x \in B)$, which is what it means for the $A$ and $B$ to be equal. Because this method of showing two sets are equal is so useful, we highlight it here.

Links



JOHN VENN (1834–1923) John Venn was born into a London suburban family noted for its philanthropy. He attended London schools and got his mathematics degree from Caius College, Cambridge, in 1857. He was elected a fellow of this college and held his fellowship there until his death. He took holy orders in 1859 and, after a brief stint of religious work, returned to Cambridge, where he developed programs in the moral sciences. Besides his mathematical work, Venn had an interest in history and wrote extensively about his college and family.

Venn's book *Symbolic Logic* clarifies ideas originally presented by Boole. In this book, Venn presents a systematic development of a method that uses geometric figures, known now as *Venn diagrams*. Today these diagrams are primarily used to analyze logical arguments and to illustrate relationships between sets. In addition to his work on symbolic logic, Venn made contributions to probability theory described in his widely used textbook on that subject.

*Showing Two Sets are Equal* To show that two sets $A$ and $B$ are equal, show that $A \subseteq B$ and $B \subseteq A$.

Sets may have other sets as members. For instance, we have the sets

$A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ and $B = \{x \mid x \text{ is a subset of the set } \{a, b\}\}$.

Note that these two sets are equal, that is, $A = B$. Also note that $\{a\} \in A$, but $a \notin A$.

## The Size of a Set

Sets are used extensively in counting problems, and for such applications we need to discuss the sizes of sets.

**DEFINITION 4** Let $S$ be a set. If there are exactly $n$ distinct elements in $S$ where $n$ is a nonnegative integer, we say that $S$ is a *finite set* and that $n$ is the *cardinality* of $S$. The cardinality of $S$ is denoted by $|S|$.

***Remark:*** The term *cardinality* comes from the common usage of the term *cardinal number* as the size of a finite set.

**EXAMPLE 10** Let $A$ be the set of odd positive integers less than 10. Then $|A| = 5$. ◀

**EXAMPLE 11** Let $S$ be the set of letters in the English alphabet. Then $|S| = 26$. ◀

**EXAMPLE 12** Because the null set has no elements, it follows that $|\emptyset| = 0$. ◀

We will also be interested in sets that are not finite.

**DEFINITION 5** A set is said to be *infinite* if it is not finite.

**EXAMPLE 13** The set of positive integers is infinite. ◀

Extra Examples

We will extend the notion of cardinality to infinite sets in Section 2.5, a challenging topic full of surprising results.

## Power Sets

Many problems involve testing all combinations of elements of a set to see if they satisfy some property. To consider all such combinations of elements of a set $S$, we build a new set that has as its members all the subsets of $S$.

**DEFINITION 6** Given a set $S$, the *power set* of $S$ is the set of all subsets of the set $S$. The power set of $S$ is denoted by $\mathcal{P}(S)$.

**EXAMPLE 14** What is the power set of the set $\{0, 1, 2\}$?

Extra Examples

*Solution:* The power set $\mathcal{P}(\{0, 1, 2\})$ is the set of all subsets of $\{0, 1, 2\}$. Hence,

$$\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

Note that the empty set and the set itself are members of this set of subsets. ◀

**EXAMPLE 15** What is the power set of the empty set? What is the power set of the set $\{\emptyset\}$?

*Solution:* The empty set has exactly one subset, namely, itself. Consequently,

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

The set $\{\emptyset\}$ has exactly two subsets, namely, $\emptyset$ and the set $\{\emptyset\}$ itself. Therefore,

$$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$ ◀

If a set has $n$ elements, then its power set has $2^n$ elements. We will demonstrate this fact in several ways in subsequent sections of the text.

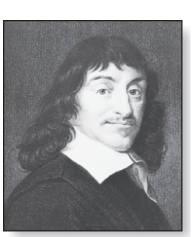
## Cartesian Products

The order of elements in a collection is often important. Because sets are unordered, a different structure is needed to represent ordered collections. This is provided by **ordered *n*-tuples**.

**DEFINITION 7** The *ordered n-tuple* $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has $a_1$ as its first element, $a_2$ as its second element, $\ldots$, and $a_n$ as its $n$th element.

We say that two ordered $n$-tuples are equal if and only if each corresponding pair of their elements is equal. In other words, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ if and only if $a_i = b_i$, for $i = 1, 2, \ldots, n$. In particular, ordered 2-tuples are called **ordered pairs**. The ordered pairs $(a, b)$ and $(c, d)$ are equal if and only if $a = c$ and $b = d$. Note that $(a, b)$ and $(b, a)$ are not equal unless $a = b$.

Links



RENÉ DESCARTES (1596–1650) René Descartes was born into a noble family near Tours, France, about 200 miles southwest of Paris. He was the third child of his father's first wife; she died several days after his birth. Because of René's poor health, his father, a provincial judge, let his son's formal lessons slide until, at the age of 8, René entered the Jesuit college at La Flèche. The rector of the school took a liking to him and permitted him to stay in bed until late in the morning because of his frail health. From then on, Descartes spent his mornings in bed; he considered these times his most productive hours for thinking.

Descartes left school in 1612, moving to Paris, where he spent 2 years studying mathematics. He earned a law degree in 1616 from the University of Poitiers. At 18 Descartes became disgusted with studying and decided to see the world. He moved to Paris and became a successful gambler. However, he grew tired of bawdy living and moved to the suburb of Saint-Germain, where he devoted himself to mathematical study. When his gambling friends found him, he decided to leave France and undertake a military career. However, he never did any fighting. One day, while escaping the cold in an overheated room at a military encampment, he had several feverish dreams, which revealed his future career as a mathematician and philosopher.

After ending his military career, he traveled throughout Europe. He then spent several years in Paris, where he studied mathematics and philosophy and constructed optical instruments. Descartes decided to move to Holland, where he spent 20 years wandering around the country, accomplishing his most important work. During this time he wrote several books, including the *Discours,* which contains his contributions to analytic geometry, for which he is best known. He also made fundamental contributions to philosophy.

In 1649 Descartes was invited by Queen Christina to visit her court in Sweden to tutor her in philosophy. Although he was reluctant to live in what he called "the land of bears amongst rocks and ice," he finally accepted the invitation and moved to Sweden. Unfortunately, the winter of 1649–1650 was extremely bitter. Descartes caught pneumonia and died in mid-February.

Many of the discrete structures we will study in later chapters are based on the notion of the *Cartesian product* of sets (named after René Descartes). We first define the Cartesian product of two sets.

**DEFINITION 8**

Let $A$ and $B$ be sets. The *Cartesian product* of $A$ and $B$, denoted by $A \times B$, is the set of all ordered pairs $(a, b)$, where $a \in A$ and $b \in B$. Hence,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

**EXAMPLE 16** Let $A$ represent the set of all students at a university, and let $B$ represent the set of all courses offered at the university. What is the Cartesian product $A \times B$ and how can it be used?

Extra Examples

*Solution:* The Cartesian product $A \times B$ consists of all the ordered pairs of the form $(a, b)$, where $a$ is a student at the university and $b$ is a course offered at the university. One way to use the set $A \times B$ is to represent all possible enrollments of students in courses at the university. ◀

**EXAMPLE 17** What is the Cartesian product of $A = \{1, 2\}$ and $B = \{a, b, c\}$?

*Solution:* The Cartesian product $A \times B$ is

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$ ◀

Note that the Cartesian products $A \times B$ and $B \times A$ are not equal, unless $A = \emptyset$ or $B = \emptyset$ (so that $A \times B = \emptyset$) or $A = B$ (see Exercises 31 and 38). This is illustrated in Example 18.

**EXAMPLE 18** Show that the Cartesian product $B \times A$ is not equal to the Cartesian product $A \times B$, where $A$ and $B$ are as in Example 17.

*Solution:* The Cartesian product $B \times A$ is

$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

This is not equal to $A \times B$, which was found in Example 17. ◀

The Cartesian product of more than two sets can also be defined.

**DEFINITION 9**

The *Cartesian product* of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered $n$-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i$ belongs to $A_i$ for $i = 1, 2, \ldots, n$. In other words,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}.$$

**EXAMPLE 19** What is the Cartesian product $A \times B \times C$, where $A = \{0, 1\}$, $B = \{1, 2\}$, and $C = \{0, 1, 2\}$?

*Solution:* The Cartesian product $A \times B \times C$ consists of all ordered triples $(a, b, c)$, where $a \in A$, $b \in B$, and $c \in C$. Hence,

$$A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}.$$ ◀

***Remark:*** Note that when $A$, $B$, and $C$ are sets, $(A \times B) \times C$ is not the same as $A \times B \times C$ (see Exercise 39).

We use the notation $A^2$ to denote $A \times A$, the Cartesian product of the set $A$ with itself. Similarly, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$, and so on. More generally,

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A \text{ for } i = 1, 2, \ldots, n\}.$$

**EXAMPLE 20** Suppose that $A = \{1, 2\}$. It follows that $A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ and $A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$. ◀

A subset $R$ of the Cartesian product $A \times B$ is called a **relation** from the set $A$ to the set $B$. The elements of $R$ are ordered pairs, where the first element belongs to $A$ and the second to $B$. For example, $R = \{(a, 0), (a, 1), (a, 3), (b, 1), (b, 2), (c, 0), (c, 3)\}$ is a relation from the set $\{a, b, c\}$ to the set $\{0, 1, 2, 3\}$. A relation from a set $A$ to itself is called a relation on $A$.

**EXAMPLE 21** What are the ordered pairs in the less than or equal to relation, which contains $(a, b)$ if $a \leq b$, on the set $\{0, 1, 2, 3\}$?

*Solution:* The ordered pair $(a, b)$ belongs to $R$ if and only if both $a$ and $b$ belong to $\{0, 1, 2, 3\}$ and $a \leq b$. Consequently, the ordered pairs in $R$ are (0,0), (0,1), (0,2), (0,3), (1,1), (1,2), (1,3), (2,2), (2, 3), and (3, 3). ◀

We will study relations and their properties at length in Chapter 9.

## Using Set Notation with Quantifiers

Sometimes we restrict the domain of a quantified statement explicitly by making use of a particular notation. For example, $\forall x \in S(P(x))$ denotes the universal quantification of $P(x)$ over all elements in the set $S$. In other words, $\forall x \in S(P(x))$ is shorthand for $\forall x(x \in S \rightarrow P(x))$. Similarly, $\exists x \in S(P(x))$ denotes the existential quantification of $P(x)$ over all elements in $S$. That is, $\exists x \in S(P(x))$ is shorthand for $\exists x(x \in S \wedge P(x))$.

**EXAMPLE 22** What do the statements $\forall x \in \mathbf{R}\ (x^2 \geq 0)$ and $\exists x \in \mathbf{Z}\ (x^2 = 1)$ mean?

*Solution:* The statement $\forall x \in \mathbf{R}(x^2 \geq 0)$ states that for every real number $x$, $x^2 \geq 0$. This statement can be expressed as "The square of every real number is nonnegative." This is a true statement.

The statement $\exists x \in \mathbf{Z}(x^2 = 1)$ states that there exists an integer $x$ such that $x^2 = 1$. This statement can be expressed as "There is an integer whose square is 1." This is also a true statement because $x = 1$ is such an integer (as is $-1$). ◀

## Truth Sets and Quantifiers

We will now tie together concepts from set theory and from predicate logic. Given a predicate $P$, and a domain $D$, we define the **truth set** of $P$ to be the set of elements $x$ in $D$ for which $P(x)$ is true. The truth set of $P(x)$ is denoted by $\{x \in D \mid P(x)\}$.

**EXAMPLE 23** What are the truth sets of the predicates $P(x)$, $Q(x)$, and $R(x)$, where the domain is the set of integers and $P(x)$ is "$|x| = 1$," $Q(x)$ is "$x^2 = 2$," and $R(x)$ is "$|x| = x$."

*Solution:* The truth set of $P$, $\{x \in \mathbf{Z} \mid |x| = 1\}$, is the set of integers for which $|x| = 1$. Because $|x| = 1$ when $x = 1$ or $x = -1$, and for no other integers $x$, we see that the truth set of $P$ is the set $\{-1, 1\}$.

The truth set of $Q$, $\{x \in \mathbf{Z} \mid x^2 = 2\}$, is the set of integers for which $x^2 = 2$. This is the empty set because there are no integers $x$ for which $x^2 = 2$.

The truth set of $R$, $\{x \in \mathbf{Z} \mid |x| = x\}$, is the set of integers for which $|x| = x$. Because $|x| = x$ if and only if $x \geq 0$, it follows that the truth set of $R$ is $\mathbf{N}$, the set of nonnegative integers. ◀

Note that $\forall x\, P(x)$ is true over the domain $U$ if and only if the truth set of $P$ is the set $U$. Likewise, $\exists x\, P(x)$ is true over the domain $U$ if and only if the truth set of $P$ is nonempty.

## Exercises

**1.** List the members of these sets.
- **a)** $\{x \mid x$ is a real number such that $x^2 = 1\}$
- **b)** $\{x \mid x$ is a positive integer less than 12$\}$
- **c)** $\{x \mid x$ is the square of an integer and $x < 100\}$
- **d)** $\{x \mid x$ is an integer such that $x^2 = 2\}$

**2.** Use set builder notation to give a description of each of these sets.
- **a)** $\{0, 3, 6, 9, 12\}$
- **b)** $\{-3, -2, -1, 0, 1, 2, 3\}$
- **c)** $\{m, n, o, p\}$

**3.** For each of these pairs of sets, determine whether the first is a subset of the second, the second is a subset of the first, or neither is a subset of the other.
- **a)** the set of airline flights from New York to New Delhi, the set of nonstop airline flights from New York to New Delhi
- **b)** the set of people who speak English, the set of people who speak Chinese
- **c)** the set of flying squirrels, the set of living creatures that can fly

**4.** For each of these pairs of sets, determine whether the first is a subset of the second, the second is a subset of the first, or neither is a subset of the other.
- **a)** the set of people who speak English, the set of people who speak English with an Australian accent
- **b)** the set of fruits, the set of citrus fruits
- **c)** the set of students studying discrete mathematics, the set of students studying data structures

**5.** Determine whether each of these pairs of sets are equal.
- **a)** $\{1, 3, 3, 3, 5, 5, 5, 5, 5\}, \{5, 3, 1\}$
- **b)** $\{\{1\}\}, \{1, \{1\}\}$
- **c)** $\emptyset, \{\emptyset\}$

**6.** Suppose that $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$, and $D = \{4, 6, 8\}$. Determine which of these sets are subsets of which other of these sets.

**7.** For each of the following sets, determine whether 2 is an element of that set.
- **a)** $\{x \in \mathbf{R} \mid x$ is an integer greater than 1$\}$
- **b)** $\{x \in \mathbf{R} \mid x$ is the square of an integer$\}$
- **c)** $\{2, \{2\}\}$
- **d)** $\{\{2\}, \{\{2\}\}\}$
- **e)** $\{\{2\}, \{2, \{2\}\}\}$
- **f)** $\{\{\{2\}\}\}$

**8.** For each of the sets in Exercise 7, determine whether $\{2\}$ is an element of that set.

**9.** Determine whether each of these statements is true or false.
- **a)** $0 \in \emptyset$
- **b)** $\emptyset \in \{0\}$
- **c)** $\{0\} \subset \emptyset$
- **d)** $\emptyset \subset \{0\}$
- **e)** $\{0\} \in \{0\}$
- **f)** $\{0\} \subset \{0\}$
- **g)** $\{\emptyset\} \subseteq \{\emptyset\}$

**10.** Determine whether these statements are true or false.
- **a)** $\emptyset \in \{\emptyset\}$
- **b)** $\emptyset \in \{\emptyset, \{\emptyset\}\}$
- **c)** $\{\emptyset\} \in \{\emptyset\}$
- **d)** $\{\emptyset\} \in \{\{\emptyset\}\}$
- **e)** $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$
- **f)** $\{\{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}\}$
- **g)** $\{\{\emptyset\}\} \subset \{\{\emptyset\}, \{\emptyset\}\}$

**11.** Determine whether each of these statements is true or false.
- **a)** $x \in \{x\}$
- **b)** $\{x\} \subseteq \{x\}$
- **c)** $\{x\} \in \{x\}$
- **d)** $\{x\} \in \{\{x\}\}$
- **e)** $\emptyset \subseteq \{x\}$
- **f)** $\emptyset \in \{x\}$

**12.** Use a Venn diagram to illustrate the subset of odd integers in the set of all positive integers not exceeding 10.

**13.** Use a Venn diagram to illustrate the set of all months of the year whose names do not contain the letter $R$ in the set of all months of the year.

**14.** Use a Venn diagram to illustrate the relationship $A \subseteq B$ and $B \subseteq C$.

**15.** Use a Venn diagram to illustrate the relationships $A \subset B$ and $B \subset C$.

**16.** Use a Venn diagram to illustrate the relationships $A \subset B$ and $A \subset C$.

**17.** Suppose that $A$, $B$, and $C$ are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.

**18.** Find two sets $A$ and $B$ such that $A \in B$ and $A \subseteq B$.

**19.** What is the cardinality of each of these sets?

**a)** $\{a\}$ **b)** $\{\{a\}\}$

**c)** $\{a, \{a\}\}$ **d)** $\{a, \{a\}, \{a, \{a\}\}\}$

**20.** What is the cardinality of each of these sets?

**a)** $\emptyset$ **b)** $\{\emptyset\}$

**c)** $\{\emptyset, \{\emptyset\}\}$ **d)** $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

**21.** Find the power set of each of these sets, where $a$ and $b$ are distinct elements.

**a)** $\{a\}$ **b)** $\{a, b\}$ **c)** $\{\emptyset, \{\emptyset\}\}$

**22.** Can you conclude that $A = B$ if $A$ and $B$ are two sets with the same power set?

**23.** How many elements does each of these sets have where $a$ and $b$ are distinct elements?

**a)** $\mathcal{P}(\{a, b, \{a, b\}\})$

**b)** $\mathcal{P}(\{\emptyset, a, \{a\}, \{\{a\}\}\})$

**c)** $\mathcal{P}(\mathcal{P}(\emptyset))$

**24.** Determine whether each of these sets is the power set of a set, where $a$ and $b$ are distinct elements.

**a)** $\emptyset$ **b)** $\{\emptyset, \{a\}\}$

**c)** $\{\emptyset, \{a\}, \{\emptyset, a\}\}$ **d)** $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

**25.** Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ if and only if $A \subseteq B$.

**26.** Show that if $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$

**27.** Let $A = \{a, b, c, d\}$ and $B = \{y, z\}$. Find

**a)** $A \times B$. **b)** $B \times A$.

**28.** What is the Cartesian product $A \times B$, where $A$ is the set of courses offered by the mathematics department at a university and $B$ is the set of mathematics professors at this university? Give an example of how this Cartesian product can be used.

**29.** What is the Cartesian product $A \times B \times C$, where $A$ is the set of all airlines and $B$ and $C$ are both the set of all cities in the United States? Give an example of how this Cartesian product can be used.

**30.** Suppose that $A \times B = \emptyset$, where $A$ and $B$ are sets. What can you conclude?

**31.** Let $A$ be a set. Show that $\emptyset \times A = A \times \emptyset = \emptyset$.

**32.** Let $A = \{a, b, c\}$, $B = \{x, y\}$, and $C = \{0, 1\}$. Find

**a)** $A \times B \times C$. **b)** $C \times B \times A$.

**c)** $C \times A \times B$. **d)** $B \times B \times B$.

**33.** Find $A^2$ if

**a)** $A = \{0, 1, 3\}$. **b)** $A = \{1, 2, a, b\}$.

**34.** Find $A^3$ if

**a)** $A = \{a\}$. **b)** $A = \{0, a\}$.

**35.** How many different elements does $A \times B$ have if $A$ has $m$ elements and $B$ has $n$ elements?

**36.** How many different elements does $A \times B \times C$ have if $A$ has $m$ elements, $B$ has $n$ elements, and $C$ has $p$ elements?

**37.** How many different elements does $A^n$ have when $A$ has $m$ elements and $n$ is a positive integer?

**38.** Show that $A \times B \neq B \times A$, when $A$ and $B$ are nonempty, unless $A = B$.

**39.** Explain why $A \times B \times C$ and $(A \times B) \times C$ are not the same.

**40.** Explain why $(A \times B) \times (C \times D)$ and $A \times (B \times C) \times D$ are not the same.

**41.** Translate each of these quantifications into English and determine its truth value.

**a)** $\forall x \in \mathbf{R}\ (x^2 \neq -1)$ **b)** $\exists x \in \mathbf{Z}\ (x^2 = 2)$

**c)** $\forall x \in \mathbf{Z}\ (x^2 > 0)$ **d)** $\exists x \in \mathbf{R}\ (x^2 = x)$

**42.** Translate each of these quantifications into English and determine its truth value.

**a)** $\exists x \in \mathbf{R}\ (x^3 = -1)$ **b)** $\exists x \in \mathbf{Z}\ (x + 1 > x)$

**c)** $\forall x \in \mathbf{Z}\ (x - 1 \in \mathbf{Z})$ **d)** $\forall x \in \mathbf{Z}\ (x^2 \in \mathbf{Z})$

**43.** Find the truth set of each of these predicates where the domain is the set of integers.

**a)** $P(x)$: $x^2 < 3$ **b)** $Q(x)$: $x^2 > x$

**c)** $R(x)$: $2x + 1 = 0$

**44.** Find the truth set of each of these predicates where the domain is the set of integers.

**a)** $P(x)$: $x^3 \geq 1$ **b)** $Q(x)$: $x^2 = 2$

**c)** $R(x)$: $x < x^2$

***45.** The defining property of an ordered pair is that two ordered pairs are equal if and only if their first elements are equal and their second elements are equal. Surprisingly, instead of taking the ordered pair as a primitive concept, we can construct ordered pairs using basic notions from set theory. Show that if we define the ordered pair $(a, b)$ to be $\{\{a\}, \{a, b\}\}$, then $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. [*Hint:* First show that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ if and only if $a = c$ and $b = d$.]

***46.** This exercise presents **Russell's paradox**. Let $S$ be the set that contains a set $x$ if the set $x$ does not belong to itself, so that $S = \{x \mid x \notin x\}$.

**a)** Show the assumption that $S$ is a member of $S$ leads to a contradiction.

**b)** Show the assumption that $S$ is not a member of $S$ leads to a contradiction.

By parts (a) and (b) it follows that the set $S$ cannot be defined as it was. This paradox can be avoided by restricting the types of elements that sets can have.

***47.** Describe a procedure for listing all the subsets of a finite set.

# 2.2 Set Operations

## Introduction

Two, or more, sets can be combined in many different ways. For instance, starting with the set of mathematics majors at your school and the set of computer science majors at your school, we can form the set of students who are mathematics majors or computer science majors, the set of students who are joint majors in mathematics and computer science, the set of all students not majoring in mathematics, and so on.

Links

**DEFINITION 1** Let $A$ and $B$ be sets. The *union* of the sets $A$ and $B$, denoted by $A \cup B$, is the set that contains those elements that are either in $A$ or in $B$, or in both.

An element $x$ belongs to the union of the sets $A$ and $B$ if and only if $x$ belongs to $A$ or $x$ belongs to $B$. This tells us that

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

The Venn diagram shown in Figure 1 represents the union of two sets $A$ and $B$. The area that represents $A \cup B$ is the shaded area within either the circle representing $A$ or the circle representing $B$.

We will give some examples of the union of sets.

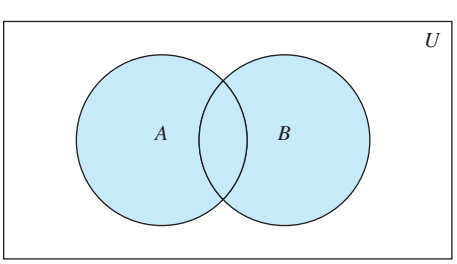
**EXAMPLE 1** The union of the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{1, 2, 3, 5\}$; that is, $\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$. ◀

**EXAMPLE 2** The union of the set of all computer science majors at your school and the set of all mathematics majors at your school is the set of students at your school who are majoring either in mathematics or in computer science (or in both). ◀

**DEFINITION 2** Let $A$ and $B$ be sets. The *intersection* of the sets $A$ and $B$, denoted by $A \cap B$, is the set containing those elements in both $A$ and $B$.

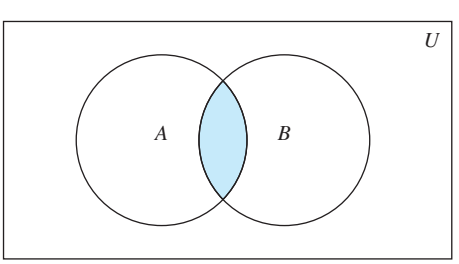
An element $x$ belongs to the intersection of the sets $A$ and $B$ if and only if $x$ belongs to $A$ and $x$ belongs to $B$. This tells us that

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$




$A \cup B$ is shaded.

**FIGURE 1** **Venn Diagram of the Union of $A$ and $B$.**




$A \cap B$ is shaded.

**FIGURE 2** **Venn Diagram of the Intersection of $A$ and $B$.**

The Venn diagram shown in Figure 2 represents the intersection of two sets $A$ and $B$. The shaded area that is within both the circles representing the sets $A$ and $B$ is the area that represents the intersection of $A$ and $B$.

We give some examples of the intersection of sets.

**EXAMPLE 3** The intersection of the sets $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{1, 3\}$; that is, $\{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$. ◀

**EXAMPLE 4** The intersection of the set of all computer science majors at your school and the set of all mathematics majors is the set of all students who are joint majors in mathematics and computer science. ◀

**DEFINITION 3** Two sets are called *disjoint* if their intersection is the empty set.

**EXAMPLE 5** Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{2, 4, 6, 8, 10\}$. Because $A \cap B = \emptyset$, $A$ and $B$ are disjoint. ◀

Be careful not to overcount!

We are often interested in finding the cardinality of a union of two finite sets $A$ and $B$. Note that $|A| + |B|$ counts each element that is in $A$ but not in $B$ or in $B$ but not in $A$ exactly once, and each element that is in both $A$ and $B$ exactly twice. Thus, if the number of elements that are in both $A$ and $B$ is subtracted from $|A| + |B|$, elements in $A \cap B$ will be counted only once. Hence,

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

The generalization of this result to unions of an arbitrary number of sets is called the **principle of inclusion–exclusion**. The principle of inclusion–exclusion is an important technique used in enumeration. We will discuss this principle and other counting techniques in detail in Chapters 6 and 8.

There are other important ways to combine sets.

**DEFINITION 4** Let $A$ and $B$ be sets. The *difference* of $A$ and $B$, denoted by $A - B$, is the set containing those elements that are in $A$ but not in $B$. The difference of $A$ and $B$ is also called the *complement of $B$ with respect to $A$*.

***Remark:*** The difference of sets $A$ and $B$ is sometimes denoted by $A \setminus B$.

An element $x$ belongs to the difference of $A$ and $B$ if and only if $x \in A$ and $x \notin B$. This tells us that

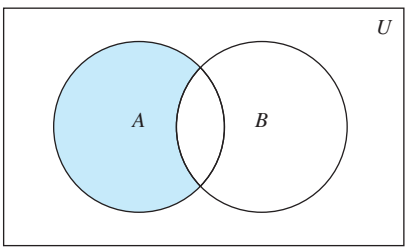
$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$

The Venn diagram shown in Figure 3 represents the difference of the sets $A$ and $B$. The shaded area inside the circle that represents $A$ and outside the circle that represents $B$ is the area that represents $A - B$.

We give some examples of differences of sets.

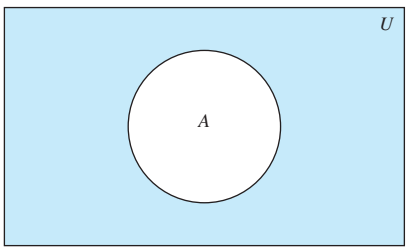
**EXAMPLE 6** The difference of $\{1, 3, 5\}$ and $\{1, 2, 3\}$ is the set $\{5\}$; that is, $\{1, 3, 5\} - \{1, 2, 3\} = \{5\}$. This is different from the difference of $\{1, 2, 3\}$ and $\{1, 3, 5\}$, which is the set $\{2\}$. ◀

**EXAMPLE 7** The difference of the set of computer science majors at your school and the set of mathematics majors at your school is the set of all computer science majors at your school who are not also mathematics majors. ◀




$A - B$ is shaded.

**FIGURE 3** **Venn Diagram for the Difference of $A$ and $B$.**




$\overline{A}$ is shaded.

**FIGURE 4** **Venn Diagram for the Complement of the Set $A$.**

Once the universal set $U$ has been specified, the **complement** of a set can be defined.

**DEFINITION 5** Let $U$ be the universal set. The *complement* of the set $A$, denoted by $\overline{A}$, is the complement of $A$ with respect to $U$. Therefore, the complement of the set $A$ is $U - A$.

An element belongs to $\overline{A}$ if and only if $x \notin A$. This tells us that

$$\overline{A} = \{x \in U \mid x \notin A\}.$$

In Figure 4 the shaded area outside the circle representing $A$ is the area representing $\overline{A}$.

We give some examples of the complement of a set.

**EXAMPLE 8** Let $A = \{a, e, i, o, u\}$ (where the universal set is the set of letters of the English alphabet). Then $\overline{A} = \{b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z\}$. ◀

**EXAMPLE 9** Let $A$ be the set of positive integers greater than 10 (with universal set the set of all positive integers). Then $\overline{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. ◀

It is left to the reader (Exercise 19) to show that we can express the difference of $A$ and $B$ as the intersection of $A$ and the complement of $B$. That is,

$$A - B = A \cap \overline{B}.$$

## Set Identities

Table 1 lists the most important set identities. We will prove several of these identities here, using three different methods. These methods are presented to illustrate that there are often many different approaches to the solution of a problem. The proofs of the remaining identities will be left as exercises. The reader should note the similarity between these set identities and the logical equivalences discussed in Section 1.3. (Compare Table 6 of Section 1.6 and Table 1.) In fact, the set identities given can be proved directly from the corresponding logical equivalences. Furthermore, both are special cases of identities that hold for Boolean algebra (discussed in Chapter 12).

Set identities and propositional equivalences are just special cases of identities for Boolean algebra.

One way to show that two sets are equal is to show that each is a subset of the other. Recall that to show that one set is a subset of a second set, we can show that if an element belongs to the first set, then it must also belong to the second set. We generally use a direct proof to do this. We illustrate this type of proof by establishing the first of De Morgan's laws.

**TABLE 1 Set Identities.**

| *Identity* | *Name* |
|---|---|
| $A \cap U = A$<br>$A \cup \emptyset = A$ | Identity laws |
| $A \cup U = U$<br>$A \cap \emptyset = \emptyset$ | Domination laws |
| $A \cup A = A$<br>$A \cap A = A$ | Idempotent laws |
| $\overline{(\overline{A})} = A$ | Complementation law |
| $A \cup B = B \cup A$<br>$A \cap B = B \cap A$ | Commutative laws |
| $A \cup (B \cup C) = (A \cup B) \cup C$<br>$A \cap (B \cap C) = (A \cap B) \cap C$ | Associative laws |
| $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$<br>$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ | Distributive laws |
| $\overline{A \cap B} = \overline{A} \cup \overline{B}$<br>$\overline{A \cup B} = \overline{A} \cap \overline{B}$ | De Morgan's laws |
| $A \cup (A \cap B) = A$<br>$A \cap (A \cup B) = A$ | Absorption laws |
| $A \cup \overline{A} = U$<br>$A \cap \overline{A} = \emptyset$ | Complement laws |

**EXAMPLE 10** Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

This identity says that the complement of the intersection of two sets is the union of their complements.

*Solution:* We will prove that the two sets $\overline{A \cap B}$ and $\overline{A} \cup \overline{B}$ are equal by showing that each set is a subset of the other.

First, we will show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. We do this by showing that if $x$ is in $\overline{A \cap B}$, then it must also be in $\overline{A} \cup \overline{B}$. Now suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, we see that the proposition $\neg((x \in A) \wedge (x \in B))$ is true.

By applying De Morgan's law for propositions, we see that $\neg(x \in A)$ or $\neg(x \in B)$. Using the definition of negation of propositions, we have $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, we see that this implies that $x \in \overline{A}$ or $x \in \overline{B}$. Consequently, by the definition of union, we see that $x \in \overline{A} \cup \overline{B}$. We have now shown that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

Extra Examples

Next, we will show that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. We do this by showing that if $x$ is in $\overline{A} \cup \overline{B}$, then it must also be in $\overline{A \cap B}$. Now suppose that $x \in \overline{A} \cup \overline{B}$. By the definition of union, we know that $x \in \overline{A}$ or $x \in \overline{B}$. Using the definition of complement, we see that $x \notin A$ or $x \notin B$. Consequently, the proposition $\neg(x \in A) \vee \neg(x \in B)$ is true.

By De Morgan's law for propositions, we conclude that $\neg((x \in A) \wedge (x \in B))$ is true. By the definition of intersection, it follows that $\neg(x \in A \cap B)$. We now use the definition of complement to conclude that $x \in \overline{A \cap B}$. This shows that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

Because we have shown that each set is a subset of the other, the two sets are equal, and the identity is proved. ◀

We can more succinctly express the reasoning used in Example 10 using set builder notation, as Example 11 illustrates.

**EXAMPLE 11** Use set builder notation and logical equivalences to establish the first De Morgan law $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

*Solution:* We can prove this identity with the following steps.

$$\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement}\\
&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol}\\
&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection}\\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences}\\
&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol}\\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement}\\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union}\\
&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}
\end{aligned}$$

Note that besides the definitions of complement, union, set membership, and set builder notation, this proof uses the second De Morgan law for logical equivalences. ◀

Proving a set identity involving more than two sets by showing each side of the identity is a subset of the other often requires that we keep track of different cases, as illustrated by the proof in Example 12 of one of the distributive laws for sets.

**EXAMPLE 12** Prove the second distributive law from Table 1, which states that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for all sets $A$, $B$, and $C$.

*Solution:* We will prove this identity by showing that each side is a subset of the other side.

Suppose that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. By the definition of union, it follows that $x \in A$, and $x \in B$ or $x \in C$ (or both). In other words, we know that the compound proposition $(x \in A) \wedge ((x \in B) \vee (x \in C))$ is true. By the distributive law for conjunction over disjunction, it follows that $((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))$. We conclude that either $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$. By the definition of intersection, it follows that $x \in A \cap B$ or $x \in A \cap C$. Using the definition of union, we conclude that $x \in (A \cap B) \cup (A \cap C)$. We conclude that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Now suppose that $x \in (A \cap B) \cup (A \cap C)$. Then, by the definition of union, $x \in A \cap B$ or $x \in A \cap C$. By the definition of intersection, it follows that $x \in A$ and $x \in B$ or that $x \in A$ and $x \in C$. From this we see that $x \in A$, and $x \in B$ or $x \in C$. Consequently, by the definition of union we see that $x \in A$ and $x \in B \cup C$. Furthermore, by the definition of intersection, it follows that $x \in A \cap (B \cup C)$. We conclude that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. This completes the proof of the identity. ◀

Set identities can also be proved using **membership tables**. We consider each combination of sets that an element can belong to and verify that elements in the same combinations of sets belong to both the sets in the identity. To indicate that an element is in a set, a 1 is used; to indicate that an element is not in a set, a 0 is used. (The reader should note the similarity between membership tables and truth tables.)

**EXAMPLE 13** Use a membership table to show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

*Solution:* The membership table for these combinations of sets is shown in Table 2. This table has eight rows. Because the columns for $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ are the same, the identity is valid. ◀

Additional set identities can be established using those that we have already proved. Consider Example 14.

**TABLE 2 A Membership Table for the Distributive Property.**

| $A$ | $B$ | $C$ | $B \cup C$ | $A \cap (B \cup C)$ | $A \cap B$ | $A \cap C$ | $(A \cap B) \cup (A \cap C)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**EXAMPLE 14** Let $A$, $B$, and $C$ be sets. Show that

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

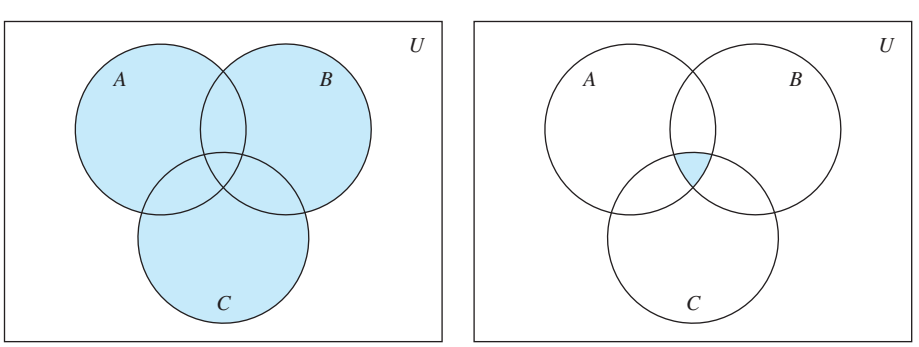
*Solution:* We have

$$\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap (\overline{B \cap C}) && \text{by the first De Morgan law} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{by the second De Morgan law} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{by the commutative law for intersections} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{by the commutative law for unions.}
\end{aligned}$$

◀

## Generalized Unions and Intersections

Because unions and intersections of sets satisfy associative laws, the sets $A \cup B \cup C$ and $A \cap B \cap C$ are well defined; that is, the meaning of this notation is unambiguous when $A$, $B$, and $C$ are sets. That is, we do not have to use parentheses to indicate which operation comes first because $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$. Note that $A \cup B \cup C$ contains those elements that are in at least one of the sets $A$, $B$, and $C$, and that $A \cap B \cap C$ contains those elements that are in all of $A$, $B$, and $C$. These combinations of the three sets, $A$, $B$, and $C$, are shown in Figure 5.




(a) $A \cup B \cup C$ is shaded. (b) $A \cap B \cap C$ is shaded.

**FIGURE 5 The Union and Intersection of $A$, $B$, and $C$.**

**EXAMPLE 15** Let $A = \{0, 2, 4, 6, 8\}$, $B = \{0, 1, 2, 3, 4\}$, and $C = \{0, 3, 6, 9\}$. What are $A \cup B \cup C$ and $A \cap B \cap C$?

*Solution:* The set $A \cup B \cup C$ contains those elements in at least one of $A$, $B$, and $C$. Hence,

$$A \cup B \cup C = \{0, 1, 2, 3, 4, 6, 8, 9\}.$$

The set $A \cap B \cap C$ contains those elements in all three of $A$, $B$, and $C$. Thus,

$$A \cap B \cap C = \{0\}.$$ ◀

We can also consider unions and intersections of an arbitrary number of sets. We introduce these definitions.

**DEFINITION 6** The *union* of a collection of sets is the set that contains those elements that are members of at least one set in the collection.

We use the notation

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

to denote the union of the sets $A_1, A_2, \ldots, A_n$.

**DEFINITION 7** The *intersection* of a collection of sets is the set that contains those elements that are members of all the sets in the collection.

We use the notation

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

to denote the intersection of the sets $A_1, A_2, \ldots, A_n$. We illustrate generalized unions and intersections with Example 16.

**EXAMPLE 16** For $i = 1, 2, \ldots$, let $A_i = \{i, i + 1, i + 2, \ldots\}$. Then,

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i + 1, i + 2, \ldots\} = \{1, 2, 3, \ldots\},$$

and

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i + 1, i + 2, \ldots\} = \{n, n + 1, n + 2, \ldots\} = A_n.$$ ◀

We can extend the notation we have introduced for unions and intersections to other families of sets. In particular, we use the notation

$$A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots = \bigcup_{i=1}^{\infty} A_i$$

to denote the union of the sets $A_1, A_2, \ldots, A_n, \ldots$. Similarly, the intersection of these sets is denoted by

$$A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots = \bigcap_{i=1}^{\infty} A_i.$$

More generally, when $I$ is a set, the notations $\bigcap_{i \in I} A_i$ and $\bigcup_{i \in I} A_i$ are used to denote the intersection and union of the sets $A_i$ for $i \in I$, respectively. Note that we have $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I\ (x \in A_i)\}$ and $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I\ (x \in A_i)\}$.

**EXAMPLE 17** Suppose that $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Then,

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \{1, 2, 3, \ldots\} = \mathbf{Z}^+$$

and

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \{1\}.$$

To see that the union of these sets is the set of positive integers, note that every positive integer $n$ is in at least one of the sets, because it belongs to $A_n = \{1, 2, \ldots, n\}$, and every element of the sets in the union is a positive integer. To see that the intersection of these sets is the set $\{1\}$, note that the only element that belongs to all the sets $A_1, A_2, \ldots$ is 1. To see this note that $A_1 = \{1\}$ and $1 \in A_i$ for $i = 1, 2, \ldots$. ◀

## Computer Representation of Sets

There are various ways to represent sets using a computer. One method is to store the elements of the set in an unordered fashion. However, if this is done, the operations of computing the union, intersection, or difference of two sets would be time-consuming, because each of these operations would require a large amount of searching for elements. We will present a method for storing elements using an arbitrary ordering of the elements of the universal set. This method of representing sets makes computing combinations of sets easy.

Assume that the universal set $U$ is finite (and of reasonable size so that the number of elements of $U$ is not larger than the memory size of the computer being used). First, specify an arbitrary ordering of the elements of $U$, for instance $a_1, a_2, \ldots, a_n$. Represent a subset $A$ of $U$ with the bit string of length $n$, where the $i$th bit in this string is 1 if $a_i$ belongs to $A$ and is 0 if $a_i$ does not belong to $A$. Example 18 illustrates this technique.

**EXAMPLE 18** Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and the ordering of elements of $U$ has the elements in increasing order; that is, $a_i = i$. What bit strings represent the subset of all odd integers in $U$, the subset of all even integers in $U$, and the subset of integers not exceeding 5 in $U$?

*Solution:* The bit string that represents the set of odd integers in $U$, namely, $\{1, 3, 5, 7, 9\}$, has a one bit in the first, third, fifth, seventh, and ninth positions, and a zero elsewhere. It is

10 1010 1010.

(We have split this bit string of length ten into blocks of length four for easy reading.) Similarly, we represent the subset of all even integers in $U$, namely, $\{2, 4, 6, 8, 10\}$, by the string

01 0101 0101.

The set of all integers in $U$ that do not exceed 5, namely, $\{1, 2, 3, 4, 5\}$, is represented by the string

11 1110 0000. ◀

Using bit strings to represent sets, it is easy to find complements of sets and unions, intersections, and differences of sets. To find the bit string for the complement of a set from the bit string for that set, we simply change each 1 to a 0 and each 0 to 1, because $x \in A$ if and only if $x \notin \overline{A}$. Note that this operation corresponds to taking the negation of each bit when we associate a bit with a truth value—with 1 representing true and 0 representing false.

**EXAMPLE 19** We have seen that the bit string for the set $\{1, 3, 5, 7, 9\}$ (with universal set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$) is

10 1010 1010.

What is the bit string for the complement of this set?

*Solution:* The bit string for the complement of this set is obtained by replacing 0s with 1s and vice versa. This yields the string

01 0101 0101,

which corresponds to the set $\{2, 4, 6, 8, 10\}$. ◀

To obtain the bit string for the union and intersection of two sets we perform bitwise Boolean operations on the bit strings representing the two sets. The bit in the $i$th position of the bit string of the union is 1 if either of the bits in the $i$th position in the two strings is 1 (or both are 1), and is 0 when both bits are 0. Hence, the bit string for the union is the bitwise *OR* of the bit strings for the two sets. The bit in the $i$th position of the bit string of the intersection is 1 when the bits in the corresponding position in the two strings are both 1, and is 0 when either of the two bits is 0 (or both are). Hence, the bit string for the intersection is the bitwise *AND* of the bit strings for the two sets.

**EXAMPLE 20** The bit strings for the sets $\{1, 2, 3, 4, 5\}$ and $\{1, 3, 5, 7, 9\}$ are 11 1110 0000 and 10 1010 1010, respectively. Use bit strings to find the union and intersection of these sets.

*Solution:* The bit string for the union of these sets is

$$11\ 1110\ 0000 \vee 10\ 1010\ 1010 = 11\ 1110\ 1010,$$

which corresponds to the set $\{1, 2, 3, 4, 5, 7, 9\}$. The bit string for the intersection of these sets is

$$11\ 1110\ 0000 \wedge 10\ 1010\ 1010 = 10\ 1010\ 0000,$$

which corresponds to the set $\{1, 3, 5\}$. ◀

## Exercises

**1.** Let $A$ be the set of students who live within one mile of school and let $B$ be the set of students who walk to classes. Describe the students in each of these sets.
**a)** $A \cap B$ **b)** $A \cup B$
**c)** $A - B$ **d)** $B - A$

**2.** Suppose that $A$ is the set of sophomores at your school and $B$ is the set of students in discrete mathematics at your school. Express each of these sets in terms of $A$ and $B$.
**a)** the set of sophomores taking discrete mathematics in your school
**b)** the set of sophomores at your school who are not taking discrete mathematics
**c)** the set of students at your school who either are sophomores or are taking discrete mathematics
**d)** the set of students at your school who either are not sophomores or are not taking discrete mathematics

**3.** Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 3, 6\}$. Find
**a)** $A \cup B$. **b)** $A \cap B$.
**c)** $A - B$. **d)** $B - A$.

**4.** Let $A = \{a, b, c, d, e\}$ and $B = \{a, b, c, d, e, f, g, h\}$. Find
**a)** $A \cup B$. **b)** $A \cap B$.
**c)** $A - B$. **d)** $B - A$.

In Exercises 5–10 assume that $A$ is a subset of some underlying universal set $U$.

**5.** Prove the complementation law in Table 1 by showing that $\overline{\overline{A}} = A$.

**6.** Prove the identity laws in Table 1 by showing that
**a)** $A \cup \emptyset = A$. **b)** $A \cap U = A$.

**7.** Prove the domination laws in Table 1 by showing that
**a)** $A \cup U = U$. **b)** $A \cap \emptyset = \emptyset$.

**8.** Prove the idempotent laws in Table 1 by showing that
**a)** $A \cup A = A$. **b)** $A \cap A = A$.

**9.** Prove the complement laws in Table 1 by showing that
**a)** $A \cup \overline{A} = U$. **b)** $A \cap \overline{A} = \emptyset$.

**10.** Show that
**a)** $A - \emptyset = A$. **b)** $\emptyset - A = \emptyset$.

**11.** Let $A$ and $B$ be sets. Prove the commutative laws from Table 1 by showing that
**a)** $A \cup B = B \cup A$.
**b)** $A \cap B = B \cap A$.

**12.** Prove the first absorption law from Table 1 by showing that if $A$ and $B$ are sets, then $A \cup (A \cap B) = A$.

**13.** Prove the second absorption law from Table 1 by showing that if $A$ and $B$ are sets, then $A \cap (A \cup B) = A$.

**14.** Find the sets $A$ and $B$ if $A - B = \{1, 5, 7, 8\}$, $B - A = \{2, 10\}$, and $A \cap B = \{3, 6, 9\}$.

**15.** Prove the second De Morgan law in Table 1 by showing that if $A$ and $B$ are sets, then $\overline{A \cup B} = \overline{A} \cap \overline{B}$
**a)** by showing each side is a subset of the other side.
**b)** using a membership table.

**16.** Let $A$ and $B$ be sets. Show that
**a)** $(A \cap B) \subseteq A$. **b)** $A \subseteq (A \cup B)$.
**c)** $A - B \subseteq A$. **d)** $A \cap (B - A) = \emptyset$.
**e)** $A \cup (B - A) = A \cup B$.

**17.** Show that if $A$, $B$, and $C$ are sets, then $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$
**a)** by showing each side is a subset of the other side.
**b)** using a membership table.

**18.** Let $A$, $B$, and $C$ be sets. Show that
**a)** $(A \cup B) \subseteq (A \cup B \cup C)$.
**b)** $(A \cap B \cap C) \subseteq (A \cap B)$.
**c)** $(A - B) - C \subseteq A - C$.
**d)** $(A - C) \cap (C - B) = \emptyset$.
**e)** $(B - A) \cup (C - A) = (B \cup C) - A$.

**19.** Show that if $A$ and $B$ are sets, then
**a)** $A - B = A \cap \overline{B}$.
**b)** $(A \cap B) \cup (A \cap \overline{B}) = A$.

**20.** Show that if $A$ and $B$ are sets with $A \subseteq B$, then
**a)** $A \cup B = B$.
**b)** $A \cap B = A$.

**21.** Prove the first associative law from Table 1 by showing that if $A$, $B$, and $C$ are sets, then $A \cup (B \cup C) = (A \cup B) \cup C$.

**22.** Prove the second associative law from Table 1 by showing that if $A$, $B$, and $C$ are sets, then $A \cap (B \cap C) = (A \cap B) \cap C$.

**23.** Prove the first distributive law from Table 1 by showing that if $A$, $B$, and $C$ are sets, then $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

**24.** Let $A$, $B$, and $C$ be sets. Show that $(A - B) - C = (A - C) - (B - C)$.

**25.** Let $A = \{0, 2, 4, 6, 8, 10\}$, $B = \{0, 1, 2, 3, 4, 5, 6\}$, and $C = \{4, 5, 6, 7, 8, 9, 10\}$. Find
**a)** $A \cap B \cap C$. **b)** $A \cup B \cup C$.
**c)** $(A \cup B) \cap C$. **d)** $(A \cap B) \cup C$.

**26.** Draw the Venn diagrams for each of these combinations of the sets $A$, $B$, and $C$.
**a)** $A \cap (B \cup C)$ **b)** $\overline{A} \cap \overline{B} \cap \overline{C}$
**c)** $(A - B) \cup (A - C) \cup (B - C)$

**27.** Draw the Venn diagrams for each of these combinations of the sets $A$, $B$, and $C$.
**a)** $A \cap (B - C)$ **b)** $(A \cap B) \cup (A \cap C)$
**c)** $(A \cap \overline{B}) \cup (A \cap \overline{C})$

**28.** Draw the Venn diagrams for each of these combinations of the sets $A$, $B$, $C$, and $D$.
**a)** $(A \cap B) \cup (C \cap D)$ **b)** $\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}$
**c)** $A - (B \cap C \cap D)$

**29.** What can you say about the sets $A$ and $B$ if we know that
**a)** $A \cup B = A$? **b)** $A \cap B = A$?
**c)** $A - B = A$? **d)** $A \cap B = B \cap A$?
**e)** $A - B = B - A$?

**30.** Can you conclude that $A = B$ if $A$, $B$, and $C$ are sets such that

**a)** $A \cup C = B \cup C$? **b)** $A \cap C = B \cap C$?

**c)** $A \cup C = B \cup C$ and $A \cap C = B \cap C$?

**31.** Let $A$ and $B$ be subsets of a universal set $U$. Show that $A \subseteq B$ if and only if $\overline{B} \subseteq \overline{A}$.

The **symmetric difference** of $A$ and $B$, denoted by $A \oplus B$, is the set containing those elements in either $A$ or $B$, but not in both $A$ and $B$.

**32.** Find the symmetric difference of $\{1, 3, 5\}$ and $\{1, 2, 3\}$.

**33.** Find the symmetric difference of the set of computer science majors at a school and the set of mathematics majors at this school.

**34.** Draw a Venn diagram for the symmetric difference of the sets $A$ and $B$.

**35.** Show that $A \oplus B = (A \cup B) - (A \cap B)$.

**36.** Show that $A \oplus B = (A - B) \cup (B - A)$.

**37.** Show that if $A$ is a subset of a universal set $U$, then

**a)** $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.

**c)** $A \oplus U = \overline{A}$. **d)** $A \oplus \overline{A} = U$.

**38.** Show that if $A$ and $B$ are sets, then

**a)** $A \oplus B = B \oplus A$. **b)** $(A \oplus B) \oplus B = A$.

**39.** What can you say about the sets $A$ and $B$ if $A \oplus B = A$?

***40.** Determine whether the symmetric difference is associative; that is, if $A$, $B$, and $C$ are sets, does it follow that $A \oplus (B \oplus C) = (A \oplus B) \oplus C$?

***41.** Suppose that $A$, $B$, and $C$ are sets such that $A \oplus C = B \oplus C$. Must it be the case that $A = B$?

**42.** If $A$, $B$, $C$, and $D$ are sets, does it follow that $(A \oplus B) \oplus (C \oplus D) = (A \oplus C) \oplus (B \oplus D)$?

**43.** If $A$, $B$, $C$, and $D$ are sets, does it follow that $(A \oplus B) \oplus (C \oplus D) = (A \oplus D) \oplus (B \oplus C)$?

**44.** Show that if $A$ and $B$ are finite sets, then $A \cup B$ is a finite set.

**45.** Show that if $A$ is an infinite set, then whenever $B$ is a set, $A \cup B$ is also an infinite set.

***46.** Show that if $A$, $B$, and $C$ are sets, then

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

(This is a special case of the inclusion–exclusion principle, which will be studied in Chapter 8.)

**47.** Let $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Find

**a)** $\bigcup_{i=1}^{n} A_i$. **b)** $\bigcap_{i=1}^{n} A_i$.

**48.** Let $A_i = \{\ldots, -2, -1, 0, 1, \ldots, i\}$. Find

**a)** $\bigcup_{i=1}^{n} A_i$. **b)** $\bigcap_{i=1}^{n} A_i$.

**49.** Let $A_i$ be the set of all nonempty bit strings (that is, bit strings of length at least one) of length not exceeding $i$. Find

**a)** $\bigcup_{i=1}^{n} A_i$. **b)** $\bigcap_{i=1}^{n} A_i$.

**50.** Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ if for every positive integer $i$,

**a)** $A_i = \{i, i + 1, i + 2, \ldots\}$.

**b)** $A_i = \{0, i\}$.

**c)** $A_i = (0, i)$, that is, the set of real numbers $x$ with $0 < x < i$.

**d)** $A_i = (i, \infty)$, that is, the set of real numbers $x$ with $x > i$.

**51.** Find $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ if for every positive integer $i$,

**a)** $A_i = \{-i, -i + 1, \ldots, -1, 0, 1, \ldots, i - 1, i\}$.

**b)** $A_i = \{-i, i\}$.

**c)** $A_i = [-i, i]$, that is, the set of real numbers $x$ with $-i \leq x \leq i$.

**d)** $A_i = [i, \infty)$, that is, the set of real numbers $x$ with $x \geq i$.

**52.** Suppose that the universal set is $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Express each of these sets with bit strings where the $i$th bit in the string is 1 if $i$ is in the set and 0 otherwise.

**a)** $\{3, 4, 5\}$

**b)** $\{1, 3, 6, 10\}$

**c)** $\{2, 3, 4, 7, 8, 9\}$

**53.** Using the same universal set as in the last problem, find the set specified by each of these bit strings.

**a)** 11 1100 1111

**b)** 01 0111 1000

**c)** 10 0000 0001

**54.** What subsets of a finite universal set do these bit strings represent?

**a)** the string with all zeros

**b)** the string with all ones

**55.** What is the bit string corresponding to the difference of two sets?

**56.** What is the bit string corresponding to the symmetric difference of two sets?

**57.** Show how bitwise operations on bit strings can be used to find these combinations of $A = \{a, b, c, d, e\}$, $B = \{b, c, d, g, p, t, v\}$, $C = \{c, e, i, o, u, x, y, z\}$, and $D = \{d, e, h, i, n, o, t, u, x, y\}$.

**a)** $A \cup B$ **b)** $A \cap B$

**c)** $(A \cup D) \cap (B \cup C)$ **d)** $A \cup B \cup C \cup D$

**58.** How can the union and intersection of $n$ sets that all are subsets of the universal set $U$ be found using bit strings?

The **successor** of the set $A$ is the set $A \cup \{A\}$.

**59.** Find the successors of the following sets.

**a)** $\{1, 2, 3\}$ **b)** $\emptyset$

**c)** $\{\emptyset\}$ **d)** $\{\emptyset, \{\emptyset\}\}$

**60.** How many elements does the successor of a set with $n$ elements have?

Sometimes the number of times that an element occurs in an unordered collection matters. **Multisets** are unordered collections of elements where an element can occur as a member more than once. The notation $\{m_1 \cdot a_1, m_2 \cdot a_2, \ldots, m_r \cdot a_r\}$ denotes the multiset with element $a_1$ occurring $m_1$ times, element $a_2$ occurring $m_2$ times, and so on. The numbers $m_i$, $i = 1, 2, \ldots, r$ are called the **multiplicities** of the elements $a_i$, $i = 1, 2, \ldots, r$.

Let $P$ and $Q$ be multisets. The **union** of the multisets $P$ and $Q$ is the multiset where the multiplicity of an element is the maximum of its multiplicities in $P$ and $Q$. The **intersection** of $P$ and $Q$ is the multiset where the multiplicity of an element is the minimum of its multiplicities in $P$ and $Q$. The **difference** of $P$ and $Q$ is the multiset where the multiplicity of an element is the multiplicity of the element in $P$ less its multiplicity in $Q$ unless this difference is negative, in which case the multiplicity is 0. The **sum** of $P$ and $Q$ is the multiset where the multiplicity of an element is the sum of multiplicities in $P$ and $Q$. The union, intersection, and difference of $P$ and $Q$ are denoted by $P \cup Q$, $P \cap Q$, and $P - Q$, respectively (where these operations should not be confused with the analogous operations for sets). The sum of $P$ and $Q$ is denoted by $P + Q$.

**61.** Let $A$ and $B$ be the multisets $\{3 \cdot a, 2 \cdot b, 1 \cdot c\}$ and $\{2 \cdot a, 3 \cdot b, 4 \cdot d\}$, respectively. Find

**a)** $A \cup B$. **b)** $A \cap B$. **c)** $A - B$.
**d)** $B - A$. **e)** $A + B$.

**62.** Suppose that $A$ is the multiset that has as its elements the types of computer equipment needed by one department of a university and the multiplicities are the number of pieces of each type needed, and $B$ is the analogous multiset for a second department of the university. For instance, $A$ could be the multiset $\{107 \cdot$ personal computers, $44 \cdot$ routers, $6 \cdot$ servers$\}$ and $B$ could be the multiset $\{14 \cdot$ personal computers, $6 \cdot$ routers, $2 \cdot$ mainframes$\}$.

**a)** What combination of $A$ and $B$ represents the equipment the university should buy assuming both departments use the same equipment?

**b)** What combination of $A$ and $B$ represents the equipment that will be used by both departments if both departments use the same equipment?

**c)** What combination of $A$ and $B$ represents the equipment that the second department uses, but the first department does not, if both departments use the same equipment?

**d)** What combination of $A$ and $B$ represents the equipment that the university should purchase if the departments do not share equipment?

**Fuzzy sets** are used in artificial intelligence. Each element in the universal set $U$ has a **degree of membership**, which is a real number between 0 and 1 (including 0 and 1), in a fuzzy set $S$. The fuzzy set $S$ is denoted by listing the elements with their degrees of membership (elements with 0 degree of membership are not listed). For instance, we write {0.6 Alice, 0.9 Brian, 0.4 Fred, 0.1 Oscar, 0.5 Rita} for the set $F$ (of famous people) to indicate that Alice has a 0.6 degree of membership in $F$, Brian has a 0.9 degree of membership in $F$, Fred has a 0.4 degree of membership in $F$, Oscar has a 0.1 degree of membership in $F$, and Rita has a 0.5 degree of membership in $F$ (so that Brian is the most famous and Oscar is the least famous of these people). Also suppose that $R$ is the set of rich people with $R = \{0.4$ Alice, 0.8 Brian, 0.2 Fred, 0.9 Oscar, 0.7 Rita$\}$.

**63.** The **complement** of a fuzzy set $S$ is the set $\overline{S}$, with the degree of the membership of an element in $\overline{S}$ equal to 1 minus the degree of membership of this element in $S$. Find $\overline{F}$ (the fuzzy set of people who are not famous) and $\overline{R}$ (the fuzzy set of people who are not rich).

**64.** The **union** of two fuzzy sets $S$ and $T$ is the fuzzy set $S \cup T$, where the degree of membership of an element in $S \cup T$ is the maximum of the degrees of membership of this element in $S$ and in $T$. Find the fuzzy set $F \cup R$ of rich or famous people.

**65.** The **intersection** of two fuzzy sets $S$ and $T$ is the fuzzy set $S \cap T$, where the degree of membership of an element in $S \cap T$ is the minimum of the degrees of membership of this element in $S$ and in $T$. Find the fuzzy set $F \cap R$ of rich and famous people.

# 2.3 Functions

## Introduction

In many instances we assign to each element of a set a particular element of a second set (which may be the same as the first). For example, suppose that each student in a discrete mathematics class is assigned a letter grade from the set $\{A, B, C, D, F\}$. And suppose that the grades are $A$ for Adams, $C$ for Chou, $B$ for Goodfriend, $A$ for Rodriguez, and $F$ for Stevens. This assignment of grades is illustrated in Figure 1.

This assignment is an example of a function. The concept of a function is extremely important in mathematics and computer science. For example, in discrete mathematics functions are used in the definition of such discrete structures as sequences and strings. Functions are also used to represent how long it takes a computer to solve problems of a given size. Many computer programs and subroutines are designed to calculate values of functions. Recursive functions,

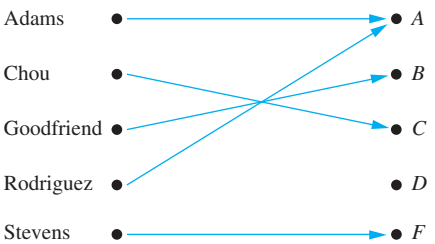



**FIGURE 1** **Assignment of Grades in a Discrete Mathematics Class.**

which are functions defined in terms of themselves, are used throughout computer science; they will be studied in Chapter 5. This section reviews the basic concepts involving functions needed in discrete mathematics.

**DEFINITION 1**

Let $A$ and $B$ be nonempty sets. A *function* $f$ from $A$ to $B$ is an assignment of exactly one element of $B$ to each element of $A$. We write $f(a) = b$ if $b$ is the unique element of $B$ assigned by the function $f$ to the element $a$ of $A$. If $f$ is a function from $A$ to $B$, we write $f : A \to B$.

***Remark:*** Functions are sometimes also called **mappings** or **transformations**.

Assessment

Functions are specified in many different ways. Sometimes we explicitly state the assignments, as in Figure 1. Often we give a formula, such as $f(x) = x + 1$, to define a function. Other times we use a computer program to specify a function.

A function $f : A \to B$ can also be defined in terms of a relation from $A$ to $B$. Recall from Section 2.1 that a relation from $A$ to $B$ is just a subset of $A \times B$. A relation from $A$ to $B$ that contains one, and only one, ordered pair $(a, b)$ for every element $a \in A$, defines a function $f$ from $A$ to $B$. This function is defined by the assignment $f(a) = b$, where $(a, b)$ is the unique ordered pair in the relation that has $a$ as its first element.

**DEFINITION 2**

If $f$ is a function from $A$ to $B$, we say that $A$ is the *domain* of $f$ and $B$ is the *codomain* of $f$. If $f(a) = b$, we say that $b$ is the *image* of $a$ and $a$ is a *preimage* of $b$. The *range*, or *image*, of $f$ is the set of all images of elements of $A$. Also, if $f$ is a function from $A$ to $B$, we say that $f$ *maps* $A$ to $B$.

Figure 2 represents a function $f$ from $A$ to $B$.

When we define a function we specify its domain, its codomain, and the mapping of elements of the domain to elements in the codomain. Two functions are **equal** when they have the same domain, have the same codomain, and map each element of their common domain to the same element in their common codomain. Note that if we change either the domain or the codomain

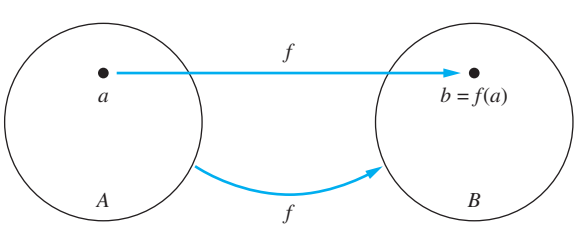



**FIGURE 2** **The Function $f$ Maps $A$ to $B$.**

of a function, then we obtain a different function. If we change the mapping of elements, then we also obtain a different function.

Examples 1–5 provide examples of functions. In each case, we describe the domain, the codomain, the range, and the assignment of values to elements of the domain.

**EXAMPLE 1** What are the domain, codomain, and range of the function that assigns grades to students described in the first paragraph of the introduction of this section?

*Solution:* Let $G$ be the function that assigns a grade to a student in our discrete mathematics class. Note that $G(\text{Adams}) = A$, for instance. The domain of $G$ is the set {Adams, Chou, Goodfriend, Rodriguez, Stevens}, and the codomain is the set $\{A, B, C, D, F\}$. The range of $G$ is the set $\{A, B, C, F\}$, because each grade except $D$ is assigned to some student. ◀

**EXAMPLE 2** Let $R$ be the relation with ordered pairs (Abdul, 22), (Brenda, 24), (Carla, 21), (Desire, 22), (Eddie, 24), and (Felicia, 22). Here each pair consists of a graduate student and this student's age. Specify a function determined by this relation.

*Solution:* If $f$ is a function specified by $R$, then $f(\text{Abdul}) = 22$, $f(\text{Brenda}) = 24$, $f(\text{Carla}) = 21$, $f(\text{Desire}) = 22$, $f(\text{Eddie}) = 24$, and $f(\text{Felicia}) = 22$. (Here, $f(x)$ is the age of $x$, where $x$ is a student.) For the domain, we take the set {Abdul, Brenda, Carla, Desire, Eddie, Felicia}. We also need to specify a codomain, which needs to contain all possible ages of students. Because it is highly likely that all students are less than 100 years old, we can take the set of positive integers less than 100 as the codomain. (Note that we could choose a different codomain, such as the set of all positive integers or the set of positive integers between 10 and 90, but that would change the function. Using this codomain will also allow us to extend the function by adding the names and ages of more students later.) The range of the function we have specified is the set of different ages of these students, which is the set {21, 22, 24}. ◀

**EXAMPLE 3** Let $f$ be the function that assigns the last two bits of a bit string of length 2 or greater to that string. For example, $f(11010) = 10$. Then, the domain of $f$ is the set of all bit strings of length 2 or greater, and both the codomain and range are the set {00, 01, 10, 11}. ◀


**EXAMPLE 4** Let $f: \mathbf{Z} \to \mathbf{Z}$ assign the square of an integer to this integer. Then, $f(x) = x^2$, where the domain of $f$ is the set of all integers, the codomain of $f$ is the set of all integers, and the range of $f$ is the set of all integers that are perfect squares, namely, $\{0, 1, 4, 9, \ldots\}$. ◀

**EXAMPLE 5** The domain and codomain of functions are often specified in programming languages. For instance, the Java statement

int **floor**(float real){. . .}

and the C++ function statement

int **function** (float $x$){. . .}

both tell us that the domain of the floor function is the set of real numbers (represented by floating point numbers) and its codomain is the set of integers. ◀

A function is called **real-valued** if its codomain is the set of real numbers, and it is called **integer-valued** if its codomain is the set of integers. Two real-valued functions or two integer-valued functions with the same domain can be added, as well as multiplied.

**DEFINITION 3**

Let $f_1$ and $f_2$ be functions from $A$ to $\mathbf{R}$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from $A$ to $\mathbf{R}$ defined for all $x \in A$ by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

Note that the functions $f_1 + f_2$ and $f_1 f_2$ have been defined by specifying their values at $x$ in terms of the values of $f_1$ and $f_2$ at $x$.

**EXAMPLE 6** Let $f_1$ and $f_2$ be functions from $\mathbf{R}$ to $\mathbf{R}$ such that $f_1(x) = x^2$ and $f_2(x) = x - x^2$. What are the functions $f_1 + f_2$ and $f_1 f_2$?

*Solution:* From the definition of the sum and product of functions, it follows that

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

and

$$(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4.$$ ◀

When $f$ is a function from $A$ to $B$, the image of a subset of $A$ can also be defined.

**DEFINITION 4**

Let $f$ be a function from $A$ to $B$ and let $S$ be a subset of $A$. The *image* of $S$ under the function $f$ is the subset of $B$ that consists of the images of the elements of $S$. We denote the image of $S$ by $f(S)$, so

$$f(S) = \{t \mid \exists s \in S\ (t = f(s))\}.$$

We also use the shorthand $\{f(s) \mid s \in S\}$ to denote this set.

***Remark:*** The notation $f(S)$ for the image of the set $S$ under the function $f$ is potentially ambiguous. Here, $f(S)$ denotes a set, and not the value of the function $f$ for the set $S$.

**EXAMPLE 7** Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3, 4\}$ with $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$, and $f(e) = 1$. The image of the subset $S = \{b, c, d\}$ is the set $f(S) = \{1, 4\}$. ◀

## One-to-One and Onto Functions

Some functions never assign the same value to two different domain elements. These functions are said to be **one-to-one**.

**DEFINITION 5**

A function $f$ is said to be *one-to-one,* or an *injunction,* if and only if $f(a) = f(b)$ implies that $a = b$ for all $a$ and $b$ in the domain of $f$. A function is said to be *injective* if it is one-to-one.

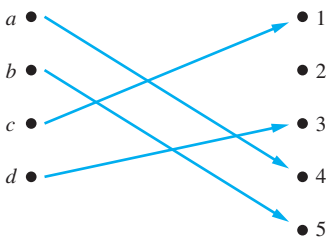



**FIGURE 3** **A One-to-One Function.**

Note that a function $f$ is one-to-one if and only if $f(a) \neq f(b)$ whenever $a \neq b$. This way of expressing that $f$ is one-to-one is obtained by taking the contrapositive of the implication in the definition.

***Remark:*** We can express that $f$ is one-to-one using quantifiers as $\forall a \forall b(f(a) = f(b) \rightarrow a = b)$ or equivalently $\forall a \forall b(a \neq b \rightarrow f(a) \neq f(b))$, where the universe of discourse is the domain of the function.

Assessment

We illustrate this concept by giving examples of functions that are one-to-one and other functions that are not one-to-one.

**EXAMPLE 8** Determine whether the function $f$ from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$ is one-to-one.

Extra Examples

*Solution:* The function $f$ is one-to-one because $f$ takes on different values at the four elements of its domain. This is illustrated in Figure 3. ◀

**EXAMPLE 9** Determine whether the function $f(x) = x^2$ from the set of integers to the set of integers is one-to-one.

*Solution:* The function $f(x) = x^2$ is not one-to-one because, for instance, $f(1) = f(-1) = 1$, but $1 \neq -1$.

Note that the function $f(x) = x^2$ with its domain restricted to $\mathbf{Z}^+$ is one-to-one. (Technically, when we restrict the domain of a function, we obtain a new function whose values agree with those of the original function for the elements of the restricted domain. The restricted function is not defined for elements of the original domain outside of the restricted domain.) ◀

**EXAMPLE 10** Determine whether the function $f(x) = x + 1$ from the set of real numbers to itself is one-to-one.

*Solution:* The function $f(x) = x + 1$ is a one-to-one function. To demonstrate this, note that $x + 1 \neq y + 1$ when $x \neq y$. ◀

**EXAMPLE 11** Suppose that each worker in a group of employees is assigned a job from a set of possible jobs, each to be done by a single worker. In this situation, the function $f$ that assigns a job to each worker is one-to-one. To see this, note that if $x$ and $y$ are two different workers, then $f(x) \neq f(y)$ because the two workers $x$ and $y$ must be assigned different jobs. ◀

We now give some conditions that guarantee that a function is one-to-one.

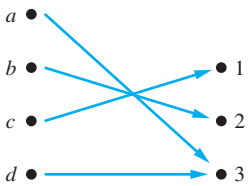



**FIGURE 4** **An Onto Function.**

**DEFINITION 6**

A function $f$ whose domain and codomain are subsets of the set of real numbers is called *increasing* if $f(x) \leq f(y)$, and *strictly increasing* if $f(x) < f(y)$, whenever $x < y$ and $x$ and $y$ are in the domain of $f$. Similarly, $f$ is called *decreasing* if $f(x) \geq f(y)$, and *strictly decreasing* if $f(x) > f(y)$, whenever $x < y$ and $x$ and $y$ are in the domain of $f$. (The word *strictly* in this definition indicates a strict inequality.)

***Remark:*** A function $f$ is increasing if $\forall x \forall y(x < y \rightarrow f(x) \leq f(y))$, strictly increasing if $\forall x \forall y(x < y \rightarrow f(x) < f(y))$, decreasing if $\forall x \forall y(x < y \rightarrow f(x) \geq f(y))$, and strictly decreasing if $\forall x \forall y(x < y \rightarrow f(x) > f(y))$, where the universe of discourse is the domain of $f$.

From these definitions, it can be shown (see Exercises 26 and 27) that a function that is either strictly increasing or strictly decreasing must be one-to-one. However, a function that is increasing, but not strictly increasing, or decreasing, but not strictly decreasing, is not one-to-one.

For some functions the range and the codomain are equal. That is, every member of the codomain is the image of some element of the domain. Functions with this property are called **onto** functions.

**DEFINITION 7**

A function $f$ from $A$ to $B$ is called *onto,* or a *surjection,* if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function $f$ is called *surjective* if it is onto.

***Remark:*** A function $f$ is onto if $\forall y \exists x(f(x) = y)$, where the domain for $x$ is the domain of the function and the domain for $y$ is the codomain of the function.

We now give examples of onto functions and functions that are not onto.

**EXAMPLE 12** Let $f$ be the function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is $f$ an onto function?

Extra Examples

*Solution:* Because all three elements of the codomain are images of elements in the domain, we see that $f$ is onto. This is illustrated in Figure 4. Note that if the codomain were $\{1, 2, 3, 4\}$, then $f$ would not be onto. ◀

**EXAMPLE 13** Is the function $f(x) = x^2$ from the set of integers to the set of integers onto?

*Solution:* The function $f$ is not onto because there is no integer $x$ with $x^2 = -1$, for instance. ◀

**EXAMPLE 14** Is the function $f(x) = x + 1$ from the set of integers to the set of integers onto?

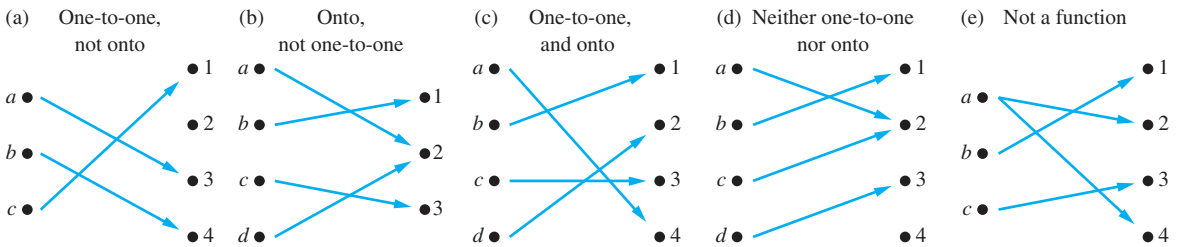



**FIGURE 5** **Examples of Different Types of Correspondences.**

*Solution:* This function is onto, because for every integer $y$ there is an integer $x$ such that $f(x) = y$. To see this, note that $f(x) = y$ if and only if $x + 1 = y$, which holds if and only if $x = y - 1$. ◀

**EXAMPLE 15** Consider the function $f$ in Example 11 that assigns jobs to workers. The function $f$ is onto if for every job there is a worker assigned this job. The function $f$ is not onto when there is at least one job that has no worker assigned it. ◀

**DEFINITION 8** The function $f$ is a *one-to-one correspondence,* or a *bijection,* if it is both one-to-one and onto. We also say that such a function is *bijective*.

Examples 16 and 17 illustrate the concept of a bijection.

**EXAMPLE 16** Let $f$ be the function from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ with $f(a) = 4$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is $f$ a bijection?

*Solution:* The function $f$ is one-to-one and onto. It is one-to-one because no two values in the domain are assigned the same function value. It is onto because all four elements of the codomain are images of elements in the domain. Hence, $f$ is a bijection. ◀

Figure 5 displays four functions where the first is one-to-one but not onto, the second is onto but not one-to-one, the third is both one-to-one and onto, and the fourth is neither one-to-one nor onto. The fifth correspondence in Figure 5 is not a function, because it sends an element to two different elements.

Suppose that $f$ is a function from a set $A$ to itself. If $A$ is finite, then $f$ is one-to-one if and only if it is onto. (This follows from the result in Exercise 72.) This is not necessarily the case if $A$ is infinite (as will be shown in Section 2.5).

**EXAMPLE 17** Let $A$ be a set. The *identity function* on $A$ is the function $\iota_A : A \to A$, where

$$\iota_A(x) = x$$

for all $x \in A$. In other words, the identity function $\iota_A$ is the function that assigns each element to itself. The function $\iota_A$ is one-to-one and onto, so it is a bijection. (Note that $\iota$ is the Greek letter iota.) ◀

For future reference, we summarize what needs be to shown to establish whether a function is one-to-one and whether it is onto. It is instructive to review Examples 8–17 in light of this summary.

Suppose that $f : A \to B$.

*To show that $f$ is injective* Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$.

*To show that $f$ is not injective* Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

*To show that $f$ is surjective* Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

*To show that $f$ is not surjective* Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

## Inverse Functions and Compositions of Functions

Now consider a one-to-one correspondence $f$ from the set $A$ to the set $B$. Because $f$ is an onto function, every element of $B$ is the image of some element in $A$. Furthermore, because $f$ is also a one-to-one function, every element of $B$ is the image of a *unique* element of $A$. Consequently, we can define a new function from $B$ to $A$ that reverses the correspondence given by $f$. This leads to Definition 9.

**DEFINITION 9**

Let $f$ be a one-to-one correspondence from the set $A$ to the set $B$. The *inverse function* of $f$ is the function that assigns to an element $b$ belonging to $B$ the unique element $a$ in $A$ such that $f(a) = b$. The inverse function of $f$ is denoted by $f^{-1}$. Hence, $f^{-1}(b) = a$ when $f(a) = b$.

***Remark:*** Be sure not to confuse the function $f^{-1}$ with the function $1/f$, which is the function that assigns to each $x$ in the domain the value $1/f(x)$. Notice that the latter makes sense only when $f(x)$ is a non-zero real number.

Figure 6 illustrates the concept of an inverse function.

If a function $f$ is not a one-to-one correspondence, we cannot define an inverse function of $f$. When $f$ is not a one-to-one correspondence, either it is not one-to-one or it is not onto. If $f$ is not one-to-one, some element $b$ in the codomain is the image of more than one element in the domain. If $f$ is not onto, for some element $b$ in the codomain, no element $a$ in the domain exists for which $f(a) = b$. Consequently, if $f$ is not a one-to-one correspondence, we cannot assign to each element $b$ in the codomain a unique element $a$ in the domain such that $f(a) = b$ (because for some $b$ there is either more than one such $a$ or no such $a$).

A one-to-one correspondence is called **invertible** because we can define an inverse of this function. A function is **not invertible** if it is not a one-to-one correspondence, because the inverse of such a function does not exist.

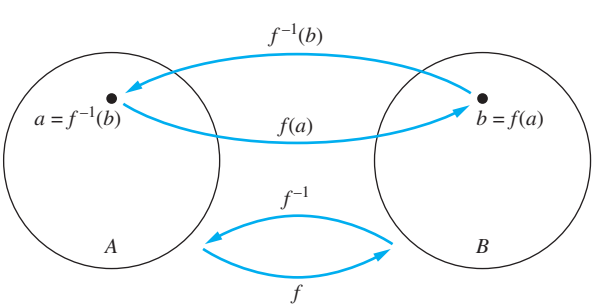



**FIGURE 6** **The Function $f^{-1}$ Is the Inverse of Function $f$.**

**EXAMPLE 18** Let $f$ be the function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, and $f(c) = 1$. Is $f$ invertible, and if it is, what is its inverse?

*Solution:* The function $f$ is invertible because it is a one-to-one correspondence. The inverse function $f^{-1}$ reverses the correspondence given by $f$, so $f^{-1}(1) = c$, $f^{-1}(2) = a$, and $f^{-1}(3) = b$. ◀

**EXAMPLE 19** Let $f : \mathbf{Z} \to \mathbf{Z}$ be such that $f(x) = x + 1$. Is $f$ invertible, and if it is, what is its inverse?

*Solution:* The function $f$ has an inverse because it is a one-to-one correspondence, as follows from Examples 10 and 14. To reverse the correspondence, suppose that $y$ is the image of $x$, so that $y = x + 1$. Then $x = y - 1$. This means that $y - 1$ is the unique element of $\mathbf{Z}$ that is sent to $y$ by $f$. Consequently, $f^{-1}(y) = y - 1$. ◀

**EXAMPLE 20** Let $f$ be the function from $\mathbf{R}$ to $\mathbf{R}$ with $f(x) = x^2$. Is $f$ invertible?

*Solution:* Because $f(-2) = f(2) = 4$, $f$ is not one-to-one. If an inverse function were defined, it would have to assign two elements to 4. Hence, $f$ is not invertible. (Note we can also show that $f$ is not invertible because it is not onto.) ◀

Sometimes we can restrict the domain or the codomain of a function, or both, to obtain an invertible function, as Example 21 illustrates.

**EXAMPLE 21** Show that if we restrict the function $f(x) = x^2$ in Example 20 to a function from the set of all nonnegative real numbers to the set of all nonnegative real numbers, then $f$ is invertible.

*Solution:* The function $f(x) = x^2$ from the set of nonnegative real numbers to the set of nonnegative real numbers is one-to-one. To see this, note that if $f(x) = f(y)$, then $x^2 = y^2$, so $x^2 - y^2 = (x + y)(x - y) = 0$. This means that $x + y = 0$ or $x - y = 0$, so $x = -y$ or $x = y$. Because both $x$ and $y$ are nonnegative, we must have $x = y$. So, this function is one-to-one. Furthermore, $f(x) = x^2$ is onto when the codomain is the set of all nonnegative real numbers, because each nonnegative real number has a square root. That is, if $y$ is a nonnegative real number, there exists a nonnegative real number $x$ such that $x = \sqrt{y}$, which means that $x^2 = y$. Because the function $f(x) = x^2$ from the set of nonnegative real numbers to the set of nonnegative real numbers is one-to-one and onto, it is invertible. Its inverse is given by the rule $f^{-1}(y) = \sqrt{y}$. ◀

**DEFINITION 10** Let $g$ be a function from the set $A$ to the set $B$ and let $f$ be a function from the set $B$ to the set $C$. The *composition* of the functions $f$ and $g$, denoted for all $a \in A$ by $f \circ g$, is defined by

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

In other words, $f \circ g$ is the function that assigns to the element $a$ of $A$ the element assigned by $f$ to $g(a)$. That is, to find $(f \circ g)(a)$ we first apply the function $g$ to $a$ to obtain $g(a)$ and then we apply the function $f$ to the result $g(a)$ to obtain $(f \circ g)(a) = f(g(a))$. Note that the composition $f \circ g$ cannot be defined unless the range of $g$ is a subset of the domain of $f$. In Figure 7 the composition of functions is shown.

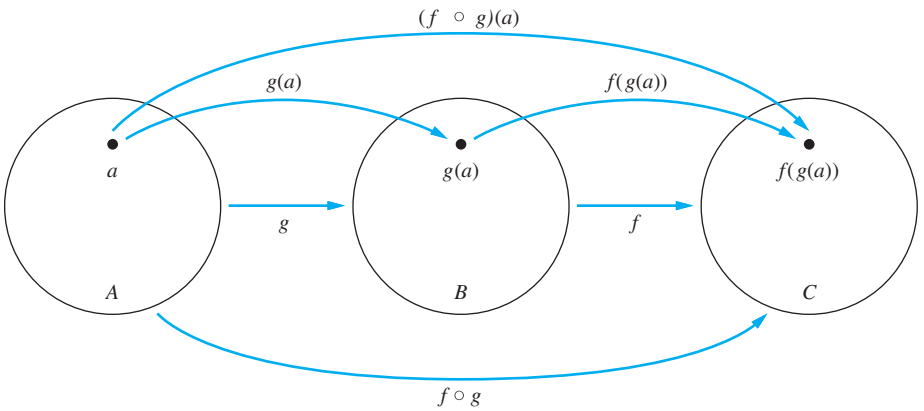



**FIGURE 7** **The Composition of the Functions $f$ and $g$.**

**EXAMPLE 22** Let $g$ be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b$, $g(b) = c$, and $g(c) = a$. Let $f$ be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3$, $f(b) = 2$, and $f(c) = 1$. What is the composition of $f$ and $g$, and what is the composition of $g$ and $f$?

*Solution:* The composition $f \circ g$ is defined by $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$.

Note that $g \circ f$ is not defined, because the range of $f$ is not a subset of the domain of $g$. ◀

**EXAMPLE 23** Let $f$ and $g$ be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of $f$ and $g$? What is the composition of $g$ and $f$?

*Solution:* Both the compositions $f \circ g$ and $g \circ f$ are defined. Moreover,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

and

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$ ◀

***Remark:*** Note that even though $f \circ g$ and $g \circ f$ are defined for the functions $f$ and $g$ in Example 23, $f \circ g$ and $g \circ f$ are not equal. In other words, the commutative law does not hold for the composition of functions.

When the composition of a function and its inverse is formed, in either order, an identity function is obtained. To see this, suppose that $f$ is a one-to-one correspondence from the set $A$ to the set $B$. Then the inverse function $f^{-1}$ exists and is a one-to-one correspondence from $B$ to $A$. The inverse function reverses the correspondence of the original function, so $f^{-1}(b) = a$ when $f(a) = b$, and $f(a) = b$ when $f^{-1}(b) = a$. Hence,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

and

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$$

Consequently $f^{-1} \circ f = \iota_A$ and $f \circ f^{-1} = \iota_B$, where $\iota_A$ and $\iota_B$ are the identity functions on the sets $A$ and $B$, respectively. That is, $(f^{-1})^{-1} = f$.

## The Graphs of Functions

We can associate a set of pairs in $A \times B$ to each function from $A$ to $B$. This set of pairs is called the **graph** of the function and is often displayed pictorially to aid in understanding the behavior of the function.

**DEFINITION 11** Let $f$ be a function from the set $A$ to the set $B$. The *graph* of the function $f$ is the set of ordered pairs $\{(a, b) \mid a \in A \text{ and } f(a) = b\}$.

From the definition, the graph of a function $f$ from $A$ to $B$ is the subset of $A \times B$ containing the ordered pairs with the second entry equal to the element of $B$ assigned by $f$ to the first entry. Also, note that the graph of a function $f$ from $A$ to $B$ is the same as the relation from $A$ to $B$ determined by the function $f$, as described on page 139.

**EXAMPLE 24** Display the graph of the function $f(n) = 2n + 1$ from the set of integers to the set of integers.

*Solution:* The graph of $f$ is the set of ordered pairs of the form $(n, 2n + 1)$, where $n$ is an integer. This graph is displayed in Figure 8. ◀

**EXAMPLE 25** Display the graph of the function $f(x) = x^2$ from the set of integers to the set of integers.

*Solution:* The graph of $f$ is the set of ordered pairs of the form $(x, f(x)) = (x, x^2)$, where $x$ is an integer. This graph is displayed in Figure 9. ◀

## Some Important Functions

Next, we introduce two important functions in discrete mathematics, namely, the floor and ceiling functions. Let $x$ be a real number. The floor function rounds $x$ down to the closest integer less than or equal to $x$, and the ceiling function rounds $x$ up to the closest integer greater than or equal to $x$. These functions are often used when objects are counted. They play an important role in the analysis of the number of steps used by procedures to solve problems of a particular size.

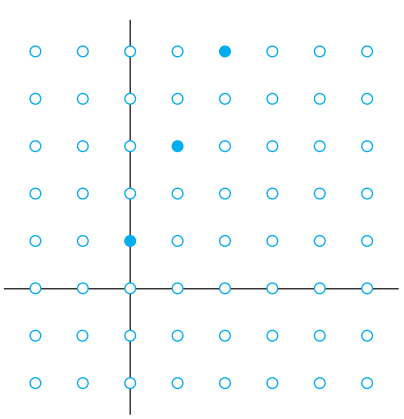


**FIGURE 8** **The Graph of $f(n) = 2n + 1$ from Z to Z.**

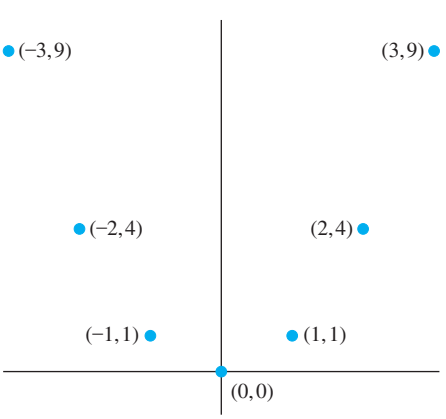



**FIGURE 9** **The Graph of $f(x) = x^2$ from Z to Z.**

**DEFINITION 12**

The *floor function* assigns to the real number $x$ the largest integer that is less than or equal to $x$. The value of the floor function at $x$ is denoted by $\lfloor x \rfloor$. The *ceiling function* assigns to the real number $x$ the smallest integer that is greater than or equal to $x$. The value of the ceiling function at $x$ is denoted by $\lceil x \rceil$.

***Remark:*** The floor function is often also called the *greatest integer function*. It is often denoted by $[x]$.

**EXAMPLE 26** These are some values of the floor and ceiling functions:

$$\lfloor \tfrac{1}{2} \rfloor = 0, \lceil \tfrac{1}{2} \rceil = 1, \lfloor -\tfrac{1}{2} \rfloor = -1, \lceil -\tfrac{1}{2} \rceil = 0, \lfloor 3.1 \rfloor = 3, \lceil 3.1 \rceil = 4, \lfloor 7 \rfloor = 7, \lceil 7 \rceil = 7. \blacktriangleleft$$

Links

We display the graphs of the floor and ceiling functions in Figure 10. In Figure 10(a) we display the graph of the floor function $\lfloor x \rfloor$. Note that this function has the same value throughout the interval $[n, n+1)$, namely $n$, and then it jumps up to $n+1$ when $x = n+1$. In Figure 10(b) we display the graph of the ceiling function $\lceil x \rceil$. Note that this function has the same value throughout the interval $(n, n+1]$, namely $n+1$, and then jumps to $n+2$ when $x$ is a little larger than $n+1$.

The floor and ceiling functions are useful in a wide variety of applications, including those involving data storage and data transmission. Consider Examples 27 and 28, typical of basic calculations done when database and data communications problems are studied.

**EXAMPLE 27** Data stored on a computer disk or transmitted over a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 100 bits of data?

*Solution:* To determine the number of bytes needed, we determine the smallest integer that is at least as large as the quotient when 100 is divided by 8, the number of bits in a byte. Consequently, $\lceil 100/8 \rceil = \lceil 12.5 \rceil = 13$ bytes are required. $\blacktriangleleft$

**EXAMPLE 28** In asynchronous transfer mode (ATM) (a communications protocol used on backbone networks), data are organized into cells of 53 bytes. How many ATM cells can be transmitted in 1 minute over a connection that transmits data at the rate of 500 kilobits per second?

*Solution:* In 1 minute, this connection can transmit $500{,}000 \cdot 60 = 30{,}000{,}000$ bits. Each ATM cell is 53 bytes long, which means that it is $53 \cdot 8 = 424$ bits long. To determine the number

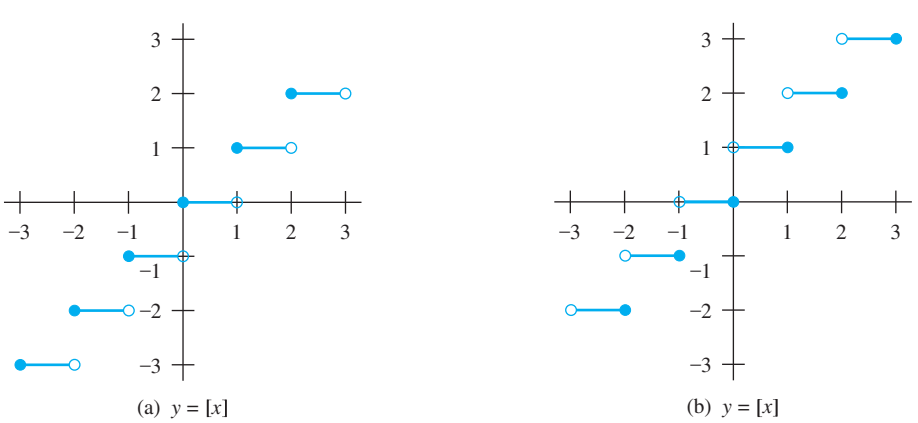



**FIGURE 10** **Graphs of the (a) Floor and (b) Ceiling Functions.**

**TABLE 1 Useful Properties of the Floor and Ceiling Functions.**
($n$ is an integer, $x$ is a real number)

| | |
|---|---|
| (1a) | $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$ |
| (1b) | $\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$ |
| (1c) | $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$ |
| (1d) | $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$ |
| (2) | $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$ |
| (3a) | $\lfloor -x \rfloor = -\lceil x \rceil$ |
| (3b) | $\lceil -x \rceil = -\lfloor x \rfloor$ |
| (4a) | $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ |
| (4b) | $\lceil x + n \rceil = \lceil x \rceil + n$ |

of cells that can be transmitted in 1 minute, we determine the largest integer not exceeding the quotient when 30,000,000 is divided by 424. Consequently, $\lfloor 30{,}000{,}000/424 \rfloor = 70{,}754$ ATM cells can be transmitted in 1 minute over a 500 kilobit per second connection. ◀

Table 1, with $x$ denoting a real number, displays some simple but important properties of the floor and ceiling functions. Because these functions appear so frequently in discrete mathematics, it is useful to look over these identities. Each property in this table can be established using the definitions of the floor and ceiling functions. Properties (1a), (1b), (1c), and (1d) follow directly from these definitions. For example, (1a) states that $\lfloor x \rfloor = n$ if and only if the integer $n$ is less than or equal to $x$ and $n + 1$ is larger than $x$. This is precisely what it means for $n$ to be the greatest integer not exceeding $x$, which is the definition of $\lfloor x \rfloor = n$. Properties (1b), (1c), and (1d) can be established similarly. We will prove property (4a) using a direct proof.

***Proof:*** Suppose that $\lfloor x \rfloor = m$, where $m$ is a positive integer. By property (1a), it follows that $m \leq x < m + 1$. Adding $n$ to all three quantities in this chain of two inequalities shows that $m + n \leq x + n < m + n + 1$. Using property (1a) again, we see that $\lfloor x + n \rfloor = m + n = \lfloor x \rfloor + n$. This completes the proof. Proofs of the other properties are left as exercises. ◁

The floor and ceiling functions enjoy many other useful properties besides those displayed in Table 1. There are also many statements about these functions that may appear to be correct, but actually are not. We will consider statements about the floor and ceiling functions in Examples 29 and 30.

A useful approach for considering statements about the floor function is to let $x = n + \epsilon$, where $n = \lfloor x \rfloor$ is an integer, and $\epsilon$, the fractional part of $x$, satisfies the inequality $0 \leq \epsilon < 1$. Similarly, when considering statements about the ceiling function, it is useful to write $x = n - \epsilon$, where $n = \lceil x \rceil$ is an integer and $0 \leq \epsilon < 1$.

**EXAMPLE 29** Prove that if $x$ is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Extra Examples

*Solution:* To prove this statement we let $x = n + \epsilon$, where $n$ is an integer and $0 \leq \epsilon < 1$. There are two cases to consider, depending on whether $\epsilon$ is less than, or greater than or equal to $\frac{1}{2}$. (The reason we choose these two cases will be made clear in the proof.)

We first consider the case when $0 \le \epsilon < \frac{1}{2}$. In this case, $2x = 2n + 2\epsilon$ and $\lfloor 2x \rfloor = 2n$ because $0 \le 2\epsilon < 1$. Similarly, $x + \frac{1}{2} = n + (\frac{1}{2} + \epsilon)$, so $\lfloor x + \frac{1}{2} \rfloor = n$, because $0 < \frac{1}{2} + \epsilon < 1$. Consequently, $\lfloor 2x \rfloor = 2n$ and $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + n = 2n$.

Next, we consider the case when $\frac{1}{2} \le \epsilon < 1$. In this case, $2x = 2n + 2\epsilon = (2n + 1) + (2\epsilon - 1)$. Because $0 \le 2\epsilon - 1 < 1$, it follows that $\lfloor 2x \rfloor = 2n + 1$. Because $\lfloor x + \frac{1}{2} \rfloor = \lfloor n + (\frac{1}{2} + \epsilon) \rfloor = \lfloor n + 1 + (\epsilon - \frac{1}{2}) \rfloor$ and $0 \le \epsilon - \frac{1}{2} < 1$, it follows that $\lfloor x + \frac{1}{2} \rfloor = n + 1$. Consequently, $\lfloor 2x \rfloor = 2n + 1$ and $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + (n + 1) = 2n + 1$. This concludes the proof. ◀

**EXAMPLE 30** Prove or disprove that $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ for all real numbers $x$ and $y$.

*Solution:* Although this statement may appear reasonable, it is false. A counterexample is supplied by $x = \frac{1}{2}$ and $y = \frac{1}{2}$. With these values we find that $\lceil x + y \rceil = \lceil \frac{1}{2} + \frac{1}{2} \rceil = \lceil 1 \rceil = 1$, but $\lceil x \rceil + \lceil y \rceil = \lceil \frac{1}{2} \rceil + \lceil \frac{1}{2} \rceil = 1 + 1 = 2$. ◀

There are certain types of functions that will be used throughout the text. These include polynomial, logarithmic, and exponential functions. A brief review of the properties of these functions needed in this text is given in Appendix 2. In this book the notation $\log x$ will be used to denote the logarithm to the base 2 of $x$, because 2 is the base that we will usually use for logarithms. We will denote logarithms to the base $b$, where $b$ is any real number greater than 1, by $\log_b x$, and the natural logarithm by $\ln x$.

Another function we will use throughout this text is the **factorial function** $f : \mathbf{N} \to \mathbf{Z}^+$, denoted by $f(n) = n!$. The value of $f(n) = n!$ is the product of the first $n$ positive integers, so $f(n) = 1 \cdot 2 \cdots (n - 1) \cdot n$ [and $f(0) = 0! = 1$].

**EXAMPLE 31** We have $f(1) = 1! = 1$, $f(2) = 2! = 1 \cdot 2 = 2$, $f(6) = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$, and $f(20) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 = 2{,}432{,}902{,}008{,}176{,}640{,}000$. ◀

Example 31 illustrates that the factorial function grows extremely rapidly as $n$ grows. The rapid growth of the factorial function is made clearer by Stirling's formula, a result from higher mathematics that tell us that $n! \sim \sqrt{2\pi n}(n/e)^n$. Here, we have used the notation $f(n) \sim g(n)$, which means that the ratio $f(n)/g(n)$ approaches 1 as $n$ grows without bound (that is, $\lim_{n\to\infty} f(n)/g(n) = 1$). The symbol $\sim$ is read "is asymptotic to." Stirling's formula is named after James Stirling, a Scottish mathematician of the eighteenth century.

Links

JAMES STIRLING (1692–1770) James Stirling was born near the town of Stirling, Scotland. His family strongly supported the Jacobite cause of the Stuarts as an alternative to the British crown. The first information known about James is that he entered Balliol College, Oxford, on a scholarship in 1711. However, he later lost his scholarship when he refused to pledge his allegiance to the British crown. The first Jacobean rebellion took place in 1715, and Stirling was accused of communicating with rebels. He was charged with cursing King George, but he was acquitted of these charges. Even though he could not graduate from Oxford because of his politics, he remained there for several years. Stirling published his first work, which extended Newton's work on plane curves, in 1717. He traveled to Venice, where a chair of mathematics had been promised to him, an appointment that unfortunately fell through. Nevertheless, Stirling stayed in Venice, continuing his mathematical work. He attended the University of Padua in 1721, and in 1722 he returned to Glasgow. Stirling apparently fled Italy after learning the secrets of the Italian glass industry, avoiding the efforts of Italian glass makers to assassinate him to protect their secrets.

In late 1724 Stirling moved to London, staying there 10 years teaching mathematics and actively engaging in research. In 1730 he published *Methodus Differentialis*, his most important work, presenting results on infinite series, summations, interpolation, and quadrature. It is in this book that his asymptotic formula for $n!$ appears. Stirling also worked on gravitation and the shape of the earth; he stated, but did not prove, that the earth is an oblate spheroid. Stirling returned to Scotland in 1735, when he was appointed manager of a Scottish mining company. He was very successful in this role and even published a paper on the ventilation of mine shafts. He continued his mathematical research, but at a reduced pace, during his years in the mining industry. Stirling is also noted for surveying the River Clyde with the goal of creating a series of locks to make it navigable. In 1752 the citizens of Glasgow presented him with a silver teakettle as a reward for this work.

## Partial Functions

A program designed to evaluate a function may not produce the correct value of the function for all elements in the domain of this function. For example, a program may not produce a correct value because evaluating the function may lead to an infinite loop or an overflow. Similarly, in abstract mathematics, we often want to discuss functions that are defined only for a subset of the real numbers, such as $1/x$, $\sqrt{x}$, and arcsin $(x)$. Also, we may want to use such notions as the "youngest child" function, which is undefined for a couple having no children, or the "time of sunrise," which is undefined for some days above the Arctic Circle. To study such situations, we use the concept of a partial function.

**DEFINITION 13**

A *partial function* $f$ from a set $A$ to a set $B$ is an assignment to each element $a$ in a subset of $A$, called the *domain of definition* of $f$, of a unique element $b$ in $B$. The sets $A$ and $B$ are called the *domain* and *codomain* of $f$, respectively. We say that $f$ is *undefined* for elements in $A$ that are not in the domain of definition of $f$. When the domain of definition of $f$ equals $A$, we say that $f$ is a *total function.*

***Remark:*** We write $f : A \to B$ to denote that $f$ is a partial function from $A$ to $B$. Note that this is the same notation as is used for functions. The context in which the notation is used determines whether $f$ is a partial function or a total function.

**EXAMPLE 32** The function $f : \mathbf{Z} \to \mathbf{R}$ where $f(n) = \sqrt{n}$ is a partial function from $\mathbf{Z}$ to $\mathbf{R}$ where the domain of definition is the set of nonnegative integers. Note that $f$ is undefined for negative integers. ◀

## Exercises

**1.** Why is $f$ not a function from $\mathbf{R}$ to $\mathbf{R}$ if
- **a)** $f(x) = 1/x$?
- **b)** $f(x) = \sqrt{x}$?
- **c)** $f(x) = \pm\sqrt{(x^2 + 1)}$?

**2.** Determine whether $f$ is a function from $\mathbf{Z}$ to $\mathbf{R}$ if
- **a)** $f(n) = \pm n$.
- **b)** $f(n) = \sqrt{n^2 + 1}$.
- **c)** $f(n) = 1/(n^2 - 4)$.

**3.** Determine whether $f$ is a function from the set of all bit strings to the set of integers if
- **a)** $f(S)$ is the position of a 0 bit in $S$.
- **b)** $f(S)$ is the number of 1 bits in $S$.
- **c)** $f(S)$ is the smallest integer $i$ such that the $i$th bit of $S$ is 1 and $f(S) = 0$ when $S$ is the empty string, the string with no bits.

**4.** Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
- **a)** the function that assigns to each nonnegative integer its last digit
- **b)** the function that assigns the next largest integer to a positive integer
- **c)** the function that assigns to a bit string the number of one bits in the string
- **d)** the function that assigns to a bit string the number of bits in the string

**5.** Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
- **a)** the function that assigns to each bit string the number of ones in the string minus the number of zeros in the string
- **b)** the function that assigns to each bit string twice the number of zeros in that string
- **c)** the function that assigns the number of bits left over when a bit string is split into bytes (which are blocks of 8 bits)
- **d)** the function that assigns to each positive integer the largest perfect square not exceeding this integer

**6.** Find the domain and range of these functions.
- **a)** the function that assigns to each pair of positive integers the first integer of the pair
- **b)** the function that assigns to each positive integer its largest decimal digit
- **c)** the function that assigns to a bit string the number of ones minus the number of zeros in the string
- **d)** the function that assigns to each positive integer the largest integer not exceeding the square root of the integer
- **e)** the function that assigns to a bit string the longest string of ones in the string

**7.** Find the domain and range of these functions.
   **a)** the function that assigns to each pair of positive integers the maximum of these two integers
   **b)** the function that assigns to each positive integer the number of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 that do not appear as decimal digits of the integer
   **c)** the function that assigns to a bit string the number of times the block 11 appears
   **d)** the function that assigns to a bit string the numerical position of the first 1 in the string and that assigns the value 0 to a bit string consisting of all 0s

**8.** Find these values.
   **a)** $\lfloor 1.1 \rfloor$ **b)** $\lceil 1.1 \rceil$
   **c)** $\lfloor -0.1 \rfloor$ **d)** $\lceil -0.1 \rceil$
   **e)** $\lceil 2.99 \rceil$ **f)** $\lceil -2.99 \rceil$
   **g)** $\lfloor \frac{1}{2} + \lceil \frac{1}{2} \rceil \rfloor$ **h)** $\lceil \lfloor \frac{1}{2} \rfloor + \lceil \frac{1}{2} \rceil + \frac{1}{2} \rceil$

**9.** Find these values.
   **a)** $\lceil \frac{3}{4} \rceil$ **b)** $\lfloor \frac{7}{8} \rfloor$
   **c)** $\lceil -\frac{3}{4} \rceil$ **d)** $\lfloor -\frac{7}{8} \rfloor$
   **e)** $\lceil 3 \rceil$ **f)** $\lfloor -1 \rfloor$
   **g)** $\lfloor \frac{1}{2} + \lceil \frac{3}{2} \rceil \rfloor$ **h)** $\lfloor \frac{1}{2} \cdot \lfloor \frac{5}{2} \rfloor \rfloor$

**10.** Determine whether each of these functions from $\{a, b, c, d\}$ to itself is one-to-one.
   **a)** $f(a) = b$, $f(b) = a$, $f(c) = c$, $f(d) = d$
   **b)** $f(a) = b$, $f(b) = b$, $f(c) = d$, $f(d) = c$
   **c)** $f(a) = d$, $f(b) = b$, $f(c) = c$, $f(d) = d$

**11.** Which functions in Exercise 10 are onto?

**12.** Determine whether each of these functions from $\mathbf{Z}$ to $\mathbf{Z}$ is one-to-one.
   **a)** $f(n) = n - 1$ **b)** $f(n) = n^2 + 1$
   **c)** $f(n) = n^3$ **d)** $f(n) = \lceil n/2 \rceil$

**13.** Which functions in Exercise 12 are onto?

**14.** Determine whether $f: \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ is onto if
   **a)** $f(m, n) = 2m - n$.
   **b)** $f(m, n) = m^2 - n^2$.
   **c)** $f(m, n) = m + n + 1$.
   **d)** $f(m, n) = |m| - |n|$.
   **e)** $f(m, n) = m^2 - 4$.

**15.** Determine whether the function $f: \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ is onto if
   **a)** $f(m, n) = m + n$.
   **b)** $f(m, n) = m^2 + n^2$.
   **c)** $f(m, n) = m$.
   **d)** $f(m, n) = |n|$.
   **e)** $f(m, n) = m - n$.

**16.** Consider these functions from the set of students in a discrete mathematics class. Under what conditions is the function one-to-one if it assigns to a student his or her
   **a)** mobile phone number.
   **b)** student identification number.
   **c)** final grade in the class.
   **d)** home town.

**17.** Consider these functions from the set of teachers in a school. Under what conditions is the function one-to-one if it assigns to a teacher his or her
   **a)** office.
   **b)** assigned bus to chaperone in a group of buses taking students on a field trip.
   **c)** salary.
   **d)** social security number.

**18.** Specify a codomain for each of the functions in Exercise 16. Under what conditions is each of these functions with the codomain you specified onto?

**19.** Specify a codomain for each of the functions in Exercise 17. Under what conditions is each of the functions with the codomain you specified onto?

**20.** Give an example of a function from $\mathbf{N}$ to $\mathbf{N}$ that is
   **a)** one-to-one but not onto.
   **b)** onto but not one-to-one.
   **c)** both onto and one-to-one (but different from the identity function).
   **d)** neither one-to-one nor onto.

**21.** Give an explicit formula for a function from the set of integers to the set of positive integers that is
   **a)** one-to-one, but not onto.
   **b)** onto, but not one-to-one.
   **c)** one-to-one and onto.
   **d)** neither one-to-one nor onto.

**22.** Determine whether each of these functions is a bijection from $\mathbf{R}$ to $\mathbf{R}$.
   **a)** $f(x) = -3x + 4$
   **b)** $f(x) = -3x^2 + 7$
   **c)** $f(x) = (x + 1)/(x + 2)$
   **d)** $f(x) = x^5 + 1$

**23.** Determine whether each of these functions is a bijection from $\mathbf{R}$ to $\mathbf{R}$.
   **a)** $f(x) = 2x + 1$
   **b)** $f(x) = x^2 + 1$
   **c)** $f(x) = x^3$
   **d)** $f(x) = (x^2 + 1)/(x^2 + 2)$

**24.** Let $f: \mathbf{R} \to \mathbf{R}$ and let $f(x) > 0$ for all $x \in \mathbf{R}$. Show that $f(x)$ is strictly increasing if and only if the function $g(x) = 1/f(x)$ is strictly decreasing.

**25.** Let $f: \mathbf{R} \to \mathbf{R}$ and let $f(x) > 0$ for all $x \in \mathbf{R}$. Show that $f(x)$ is strictly decreasing if and only if the function $g(x) = 1/f(x)$ is strictly increasing.

**26.** **a)** Prove that a strictly increasing function from $\mathbf{R}$ to itself is one-to-one.
   **b)** Give an example of an increasing function from $\mathbf{R}$ to itself that is not one-to-one.

**27.** **a)** Prove that a strictly decreasing function from $\mathbf{R}$ to itself is one-to-one.
   **b)** Give an example of a decreasing function from $\mathbf{R}$ to itself that is not one-to-one.

**28.** Show that the function $f(x) = e^x$ from the set of real numbers to the set of real numbers is not invertible, but if the codomain is restricted to the set of positive real numbers, the resulting function is invertible.

**29.** Show that the function $f(x) = |x|$ from the set of real numbers to the set of nonnegative real numbers is not invertible, but if the domain is restricted to the set of nonnegative real numbers, the resulting function is invertible.

**30.** Let $S = \{-1, 0, 2, 4, 7\}$. Find $f(S)$ if

**a)** $f(x) = 1$. **b)** $f(x) = 2x + 1$.

**c)** $f(x) = \lceil x/5 \rceil$. **d)** $f(x) = \lfloor (x^2 + 1)/3 \rfloor$.

**31.** Let $f(x) = \lfloor x^2/3 \rfloor$. Find $f(S)$ if

**a)** $S = \{-2, -1, 0, 1, 2, 3\}$.

**b)** $S = \{0, 1, 2, 3, 4, 5\}$.

**c)** $S = \{1, 5, 7, 11\}$.

**d)** $S = \{2, 6, 10, 14\}$.

**32.** Let $f(x) = 2x$ where the domain is the set of real numbers. What is

**a)** $f(\mathbf{Z})$? **b)** $f(\mathbf{N})$? **c)** $f(\mathbf{R})$?

**33.** Suppose that $g$ is a function from $A$ to $B$ and $f$ is a function from $B$ to $C$.

**a)** Show that if both $f$ and $g$ are one-to-one functions, then $f \circ g$ is also one-to-one.

**b)** Show that if both $f$ and $g$ are onto functions, then $f \circ g$ is also onto.

***34.** If $f$ and $f \circ g$ are one-to-one, does it follow that $g$ is one-to-one? Justify your answer.

***35.** If $f$ and $f \circ g$ are onto, does it follow that $g$ is onto? Justify your answer.

**36.** Find $f \circ g$ and $g \circ f$, where $f(x) = x^2 + 1$ and $g(x) = x + 2$, are functions from $\mathbf{R}$ to $\mathbf{R}$.

**37.** Find $f + g$ and $fg$ for the functions $f$ and $g$ given in Exercise 36.

**38.** Let $f(x) = ax + b$ and $g(x) = cx + d$, where $a, b, c$, and $d$ are constants. Determine necessary and sufficient conditions on the constants $a, b, c$, and $d$ so that $f \circ g = g \circ f$.

**39.** Show that the function $f(x) = ax + b$ from $\mathbf{R}$ to $\mathbf{R}$ is invertible, where $a$ and $b$ are constants, with $a \neq 0$, and find the inverse of $f$.

**40.** Let $f$ be a function from the set $A$ to the set $B$. Let $S$ and $T$ be subsets of $A$. Show that

**a)** $f(S \cup T) = f(S) \cup f(T)$.

**b)** $f(S \cap T) \subseteq f(S) \cap f(T)$.

**41.** **a)** Give an example to show that the inclusion in part (b) in Exercise 40 may be proper.

**b)** Show that if $f$ is one-to-one, the inclusion in part (b) in Exercise 40 is an equality.

Let $f$ be a function from the set $A$ to the set $B$. Let $S$ be a subset of $B$. We define the **inverse image** of $S$ to be the subset of $A$ whose elements are precisely all pre-images of all elements of $S$. We denote the inverse image of $S$ by $f^{-1}(S)$, so $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$. (*Beware:* The notation $f^{-1}$ is used in two different ways. Do not confuse the notation introduced here with the notation $f^{-1}(y)$ for the value at $y$ of the inverse of the invertible function $f$. Notice also that $f^{-1}(S)$, the inverse image of the set $S$, makes sense for all functions $f$, not just invertible functions.)

**42.** Let $f$ be the function from $\mathbf{R}$ to $\mathbf{R}$ defined by $f(x) = x^2$. Find

**a)** $f^{-1}(\{1\})$. **b)** $f^{-1}(\{x \mid 0 < x < 1\})$.

**c)** $f^{-1}(\{x \mid x > 4\})$.

**43.** Let $g(x) = \lfloor x \rfloor$. Find

**a)** $g^{-1}(\{0\})$. **b)** $g^{-1}(\{-1, 0, 1\})$.

**c)** $g^{-1}(\{x \mid 0 < x < 1\})$.

**44.** Let $f$ be a function from $A$ to $B$. Let $S$ and $T$ be subsets of $B$. Show that

**a)** $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$.

**b)** $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

**45.** Let $f$ be a function from $A$ to $B$. Let $S$ be a subset of $B$. Show that $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$.

**46.** Show that $\lfloor x + \frac{1}{2} \rfloor$ is the closest integer to the number $x$, except when $x$ is midway between two integers, when it is the larger of these two integers.

**47.** Show that $\lceil x - \frac{1}{2} \rceil$ is the closest integer to the number $x$, except when $x$ is midway between two integers, when it is the smaller of these two integers.

**48.** Show that if $x$ is a real number, then $\lceil x \rceil - \lfloor x \rfloor = 1$ if $x$ is not an integer and $\lceil x \rceil - \lfloor x \rfloor = 0$ if $x$ is an integer.

**49.** Show that if $x$ is a real number, then $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.

**50.** Show that if $x$ is a real number and $m$ is an integer, then $\lceil x + m \rceil = \lceil x \rceil + m$.

**51.** Show that if $x$ is a real number and $n$ is an integer, then

**a)** $x < n$ if and only if $\lfloor x \rfloor < n$.

**b)** $n < x$ if and only if $n < \lceil x \rceil$.

**52.** Show that if $x$ is a real number and $n$ is an integer, then

**a)** $x \leq n$ if and only if $\lceil x \rceil \leq n$.

**b)** $n \leq x$ if and only if $n \leq \lfloor x \rfloor$.

**53.** Prove that if $n$ is an integer, then $\lfloor n/2 \rfloor = n/2$ if $n$ is even and $(n - 1)/2$ if $n$ is odd.

**54.** Prove that if $x$ is a real number, then $\lfloor -x \rfloor = -\lceil x \rceil$ and $\lceil -x \rceil = -\lfloor x \rfloor$.

**55.** The function INT is found on some calculators, where $\text{INT}(x) = \lfloor x \rfloor$ when $x$ is a nonnegative real number and $\text{INT}(x) = \lceil x \rceil$ when $x$ is a negative real number. Show that this INT function satisfies the identity $\text{INT}(-x) = -\text{INT}(x)$.

**56.** Let $a$ and $b$ be real numbers with $a < b$. Use the floor and/or ceiling functions to express the number of integers $n$ that satisfy the inequality $a \leq n \leq b$.

**57.** Let $a$ and $b$ be real numbers with $a < b$. Use the floor and/or ceiling functions to express the number of integers $n$ that satisfy the inequality $a < n < b$.

**58.** How many bytes are required to encode $n$ bits of data where $n$ equals

**a)** 4? **b)** 10? **c)** 500? **d)** 3000?

**59.** How many bytes are required to encode $n$ bits of data where $n$ equals

**a)** 7? **b)** 17? **c)** 1001? **d)** 28,800?

**60.** How many ATM cells (described in Example 28) can be transmitted in 10 seconds over a link operating at the following rates?

**a)** 128 kilobits per second (1 kilobit = 1000 bits)
**b)** 300 kilobits per second
**c)** 1 megabit per second (1 megabit = 1,000,000 bits)

**61.** Data are transmitted over a particular Ethernet network in blocks of 1500 octets (blocks of 8 bits). How many blocks are required to transmit the following amounts of data over this Ethernet network? (Note that a byte is a synonym for an octet, a kilobyte is 1000 bytes, and a megabyte is 1,000,000 bytes.)

**a)** 150 kilobytes of data
**b)** 384 kilobytes of data
**c)** 1.544 megabytes of data
**d)** 45.3 megabytes of data

**62.** Draw the graph of the function $f(n) = 1 - n^2$ from $\mathbf{Z}$ to $\mathbf{Z}$.

**63.** Draw the graph of the function $f(x) = \lfloor 2x \rfloor$ from $\mathbf{R}$ to $\mathbf{R}$.

**64.** Draw the graph of the function $f(x) = \lfloor x/2 \rfloor$ from $\mathbf{R}$ to $\mathbf{R}$.

**65.** Draw the graph of the function $f(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor$ from $\mathbf{R}$ to $\mathbf{R}$.

**66.** Draw the graph of the function $f(x) = \lceil x \rceil + \lfloor x/2 \rfloor$ from $\mathbf{R}$ to $\mathbf{R}$.

**67.** Draw graphs of each of these functions.

**a)** $f(x) = \lfloor x + \frac{1}{2} \rfloor$ **b)** $f(x) = \lfloor 2x + 1 \rfloor$
**c)** $f(x) = \lceil x/3 \rceil$ **d)** $f(x) = \lceil 1/x \rceil$
**e)** $f(x) = \lceil x - 2 \rceil + \lfloor x + 2 \rfloor$
**f)** $f(x) = \lfloor 2x \rfloor \lceil x/2 \rceil$ **g)** $f(x) = \lceil \lfloor x - \frac{1}{2} \rfloor + \frac{1}{2} \rceil$

**68.** Draw graphs of each of these functions.

**a)** $f(x) = \lceil 3x - 2 \rceil$ **b)** $f(x) = \lceil 0.2x \rceil$
**c)** $f(x) = \lfloor -1/x \rfloor$ **d)** $f(x) = \lfloor x^2 \rfloor$
**e)** $f(x) = \lceil x/2 \rceil \lfloor x/2 \rfloor$ **f)** $f(x) = \lfloor x/2 \rfloor + \lceil x/2 \rceil$
**g)** $f(x) = \lfloor 2 \lceil x/2 \rceil + \frac{1}{2} \rfloor$

**69.** Find the inverse function of $f(x) = x^3 + 1$.

**70.** Suppose that $f$ is an invertible function from $Y$ to $Z$ and $g$ is an invertible function from $X$ to $Y$. Show that the inverse of the composition $f \circ g$ is given by $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

**71.** Let $S$ be a subset of a universal set $U$. The **characteristic function** $f_S$ of $S$ is the function from $U$ to the set $\{0, 1\}$ such that $f_S(x) = 1$ if $x$ belongs to $S$ and $f_S(x) = 0$ if $x$ does not belong to $S$. Let $A$ and $B$ be sets. Show that for all $x \in U$,

**a)** $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$
**b)** $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$
**c)** $f_{\overline{A}}(x) = 1 - f_A(x)$
**d)** $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2 f_A(x) f_B(x)$

☞ **72.** Suppose that $f$ is a function from $A$ to $B$, where $A$ and $B$ are finite sets with $|A| = |B|$. Show that $f$ is one-to-one if and only if it is onto.

**73.** Prove or disprove each of these statements about the floor and ceiling functions.

**a)** $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ for all real numbers $x$.
**b)** $\lfloor 2x \rfloor = 2 \lfloor x \rfloor$ whenever $x$ is a real number.
**c)** $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = 0$ or 1 whenever $x$ and $y$ are real numbers.
**d)** $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$ for all real numbers $x$ and $y$.
**e)** $\left\lceil \frac{x}{2} \right\rceil = \left\lfloor \frac{x+1}{2} \right\rfloor$ for all real numbers $x$.

**74.** Prove or disprove each of these statements about the floor and ceiling functions.

**a)** $\lfloor \lceil x \rceil \rfloor = \lceil x \rceil$ for all real numbers $x$.
**b)** $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ for all real numbers $x$ and $y$.
**c)** $\lceil \lceil x/2 \rceil / 2 \rceil = \lceil x/4 \rceil$ for all real numbers $x$.
**d)** $\lfloor \sqrt{\lceil x \rceil} \rfloor = \lfloor \sqrt{x} \rfloor$ for all positive real numbers $x$.
**e)** $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$ for all real numbers $x$ and $y$.

**75.** Prove that if $x$ is a positive real number, then

**a)** $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$.
**b)** $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$.

**76.** Let $x$ be a real number. Show that $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$.

**77.** For each of these partial functions, determine its domain, codomain, domain of definition, and the set of values for which it is undefined. Also, determine whether it is a total function.

**a)** $f : \mathbf{Z} \to \mathbf{R}$, $f(n) = 1/n$
**b)** $f : \mathbf{Z} \to \mathbf{Z}$, $f(n) = \lceil n/2 \rceil$
**c)** $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Q}$, $f(m, n) = m/n$
**d)** $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = mn$
**e)** $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = m - n$ if $m > n$

**78. a)** Show that a partial function from $A$ to $B$ can be viewed as a function $f^*$ from $A$ to $B \cup \{u\}$, where $u$ is not an element of $B$ and

$$f^*(a) = \begin{cases} f(a) & \text{if } a \text{ belongs to the domain} \\ & \text{of definition of } f \\ u & \text{if } f \text{ is undefined at } a. \end{cases}$$

**b)** Using the construction in (a), find the function $f^*$ corresponding to each partial function in Exercise 77.

☞ **79. a)** Show that if a set $S$ has cardinality $m$, where $m$ is a positive integer, then there is a one-to-one correspondence between $S$ and the set $\{1, 2, \ldots, m\}$.

**b)** Show that if $S$ and $T$ are two sets each with $m$ elements, where $m$ is a positive integer, then there is a one-to-one correspondence between $S$ and $T$.

***80.** Show that a set $S$ is infinite if and only if there is a proper subset $A$ of $S$ such that there is a one-to-one correspondence between $A$ and $S$.

CHAPTER

# 7 Discrete Probability



Combinatorics and probability theory share common origins. The theory of probability was first developed more than 300 years ago, when certain gambling games were analyzed. Although probability theory was originally invented to study gambling, it now plays an essential role in a wide variety of disciplines. For example, probability theory is extensively applied in the study of genetics, where it can be used to help understand the inheritance of traits. Of course, probability still remains an extremely popular part of mathematics because of its applicability to gambling, which continues to be an extremely popular human endeavor.

In computer science, probability theory plays an important role in the study of the complexity of algorithms. In particular, ideas and techniques from probability theory are used to determine the average-case complexity of algorithms. Probabilistic algorithms can be used to solve many problems that cannot be easily or practically solved by deterministic algorithms. In a probabilistic algorithm, instead of always following the same steps when given the same input, as a deterministic algorithm does, the algorithm makes one or more random choices, which may lead to different output. In combinatorics, probability theory can even be used to show that objects with certain properties exist. The probabilistic method, a technique in combinatorics introduced by Paul Erdős and Alfréd Rényi, shows that an object with a specified property exists by showing that there is a positive probability that a randomly constructed object has this property. Probability theory can help us answer questions that involve uncertainty, such as determining whether we should reject an incoming mail message as spam based on the words that appear in the message.

## 7.1 An Introduction to Discrete Probability

### Introduction

Probability theory dates back to 1526 when the Italian mathematician, physician, and gambler Girolamo Cardano wrote the first known systematic treatment of the subject in his book *Liber de Ludo Aleae* (*Book on Games of Chance*). (This book was not published until 1663, which may have held back the development of probability theory.) In the seventeenth century the French mathematician Blaise Pascal determined the odds of winning some popular bets based on the outcome when a pair of dice is repeatedly rolled. In the eighteenth century, the French mathematician Laplace, who also studied gambling, defined the probability of an event as the number of successful outcomes divided by the number of possible outcomes. For instance, the probability that a die comes up an odd number when it is rolled is the number of successful outcomes—namely, the number of ways it can come up odd—divided by the number of possible outcomes—namely, the number of different ways the die can come up. There are a total of six possible outcomes—namely, 1, 2, 3, 4, 5, and 6—and exactly three of these are successful outcomes—namely, 1, 3, and 5. Hence, the probability that the die comes up an odd number is $3/6 = 1/2$. (Note that it has been assumed that all possible outcomes are equally likely, or, in other words, that the die is fair.)

In this section we will restrict ourselves to experiments that have finitely many, equally likely, outcomes. This permits us to use Laplace's definition of the probability of an event. We will continue our study of probability in Section 7.2, where we will study experiments with finitely many outcomes that are not necessarily equally likely. In Section 7.2 we will also introduce

some key concepts in probability theory, including conditional probability, independence of events, and random variables. In Section 7.4 we will introduce the concepts of the expectation and variance of a random variable.

## Finite Probability

An **experiment** is a procedure that yields one of a given set of possible outcomes. The **sample space** of the experiment is the set of possible outcomes. An **event** is a subset of the sample space. Laplace's definition of the probability of an event with finitely many possible outcomes will now be stated.

**DEFINITION 1** If $S$ is a finite nonempty sample space of equally likely outcomes, and $E$ is an event, that is, a subset of $S$, then the *probability* of $E$ is $p(E) = \dfrac{|E|}{|S|}$.

The probability of an event can never be negative or more than one!

According to Laplace's definition, the probability of an event is between 0 and 1. To see this, note that if $E$ is an event from a finite sample space $S$, then $0 \leq |E| \leq |S|$, because $E \subseteq S$. Thus, $0 \leq p(E) = |E|/|S| \leq 1$.

Examples 1–7 illustrate how the probability of an event is found.

**EXAMPLE 1** An urn contains four blue balls and five red balls. What is the probability that a ball chosen at random from the urn is blue?

Extra Examples

*Solution:* To calculate the probability, note that there are nine possible outcomes, and four of these possible outcomes produce a blue ball. Hence, the probability that a blue ball is chosen is 4/9. ◀

**EXAMPLE 2** What is the probability that when two dice are rolled, the sum of the numbers on the two dice is 7?

*Solution:* There are a total of 36 equally likely possible outcomes when two dice are rolled. (The product rule can be used to see this; because each die has six possible outcomes, the total

Links

GIROLAMO CARDANO (1501–1576) Cardano, born in Pavia, Italy, was the illegitimate child of Fazio Cardano, a lawyer, mathematician, and friend of Leonardo da Vinci, and Chiara Micheria, a young widow. In spite of illness and poverty, Cardano was able to study at the universities of Pavia and Padua, from where he received his medical degree. Cardano was not accepted into Milan's College of Physicians because of his illegitimate birth, as well as his eccentricity and confrontational style. Nevertheless, his medical skills were highly regarded. One of his main accomplishments as a physician is the first description of typhoid fever.

Cardano published more than 100 books on a diverse range of subjects, including medicine, the natural sciences, mathematics, gambling, physical inventions and experiments, and astrology. He also wrote a fascinating autobiography. In mathematics, Cardano's book *Ars Magna*, published in 1545, established the foundations of abstract algebra. This was the most comprehensive book on abstract algebra for more than a century; it presents many novel ideas of Cardano and of others, including methods for solving cubic and quartic equations from their coefficients. Cardano also made several important contributions to cryptography. Cardano was an advocate of education for the deaf, believing, unlike his contemporaries, that deaf people could learn to read and write before learning to speak, and could use their minds just as well as hearing people.

Cardano was often short of money. However, he kept himself solvent through gambling and winning money by beating others at chess. His book about games of chance, *Liber de Ludo Aleae*, written in 1526 (but published in 1663), offers the first systematic treatment of probability; it also describes effective ways to cheat. Cardano was considered to be a man of dubious moral character; he was often described as a liar, gambler, lecher, and heretic.

number of outcomes when two dice are rolled is $6^2 = 36$.) There are six successful outcomes, namely, (1, 6), (2, 5), (3, 4), (4, 3), (5, 2), and (6, 1), where the values of the first and second dice are represented by an ordered pair. Hence, the probability that a seven comes up when two fair dice are rolled is $6/36 = 1/6$. ◀

Links

Lotteries are extremely popular throughout the world. We can easily compute the odds of winning different types of lotteries, as illustrated in Examples 3 and 4. (The odd of winning the popular Mega Millions and Powerball lotteries are studied in the supplementary exercises.)

**EXAMPLE 3** In a lottery, players win a large prize when they pick four digits that match, in the correct order, four digits selected by a random mechanical process. A smaller prize is won if only three digits are matched. What is the probability that a player wins the large prize? What is the probability that a player wins the small prize?

*Solution:* There is only one way to choose all four digits correctly. By the product rule, there are $10^4 = 10{,}000$ ways to choose four digits. Hence, the probability that a player wins the large prize is $1/10{,}000 = 0.0001$.

Players win the smaller prize when they correctly choose exactly three of the four digits. Exactly one digit must be wrong to get three digits correct, but not all four correct. By the sum rule, to find the number of ways to choose exactly three digits correctly, we add the number of ways to choose four digits matching the digits picked in all but the $i$th position, for $i = 1, 2, 3, 4$.

To count the number of successes with the first digit incorrect, note that there are nine possible choices for the first digit (all but the one correct digit), and one choice for each of the other digits, namely, the correct digits for these slots. Hence, there are nine ways to choose four digits where the first digit is incorrect, but the last three are correct. Similarly, there are nine ways to choose four digits where the second digit is incorrect, nine with the third digit incorrect, and nine with the fourth digit incorrect. Hence, there is a total of 36 ways to choose four digits with exactly three of the four digits correct. Thus, the probability that a player wins the smaller prize is $36/10{,}000 = 9/2500 = 0.0036$. ◀

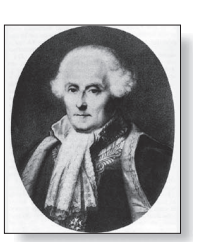
**EXAMPLE 4** There are many lotteries now that award enormous prizes to people who correctly choose a set of six numbers out of the first $n$ positive integers, where $n$ is usually between 30 and 60. What is the probability that a person picks the correct six numbers out of 40?

*Solution:* There is only one winning combination. The total number of ways to choose six numbers out of 40 is

$$C(40, 6) = \frac{40!}{34!\,6!} = 3{,}838{,}380.$$

Consequently, the probability of picking a winning combination is $1/3{,}838{,}380 \approx 0.00000026$. (Here the symbol $\approx$ means approximately equal to.) ◀

Links



PIERRE-SIMON LAPLACE (1749–1827) Pierre-Simon Laplace came from humble origins in Normandy. In his childhood he was educated in a school run by the Benedictines. At 16 he entered the University of Caen intending to study theology. However, he soon realized his true interests were in mathematics. After completing his studies, he was named a provisional professor at Caen, and in 1769 he became professor of mathematics at the Paris Military School.

Laplace is best known for his contributions to celestial mechanics, the study of the motions of heavenly bodies. His *Traité de Mécanique Céleste* is considered one of the greatest scientific works of the early nineteenth century. Laplace was one of the founders of probability theory and made many contributions to mathematical statistics. His work in this area is documented in his book *Théorie Analytique des Probabilités*, in which he defined the probability of an event as the ratio of the number of favorable outcomes to the total number of outcomes of an experiment.

Laplace was famous for his political flexibility. He was loyal, in succession, to the French Republic, Napoleon, and King Louis XVIII. This flexibility permitted him to be productive before, during, and after the French Revolution.


Poker, and other card games, are growing in popularity. To win at these games it helps to know the probability of different hands. We can find the probability of specific hands that arise in card games using the techniques developed so far. A deck of cards contains 52 cards. There are 13 different kinds of cards, with four cards of each kind. (Among the terms commonly used instead of "kind" are "rank," "face value," "denomination," and "value.") These kinds are twos, threes, fours, fives, sixes, sevens, eights, nines, tens, jacks, queens, kings, and aces. There are also four suits: spades, clubs, hearts, and diamonds, each containing 13 cards, with one card of each kind in a suit. In many poker games, a hand consists of five cards.

**EXAMPLE 5** Find the probability that a hand of five cards in poker contains four cards of one kind.

*Solution:* By the product rule, the number of hands of five cards with four cards of one kind is the product of the number of ways to pick one kind, the number of ways to pick the four of this kind out of the four in the deck of this kind, and the number of ways to pick the fifth card. This is

$$C(13, 1)C(4, 4)C(48, 1).$$

By Example 11 in Section 6.3 there are $C(52, 5)$ different hands of five cards. Hence, the probability that a hand contains four cards of one kind is

$$\frac{C(13, 1)C(4, 4)C(48, 1)}{C(52, 5)} = \frac{13 \cdot 1 \cdot 48}{2{,}598{,}960} \approx 0.00024.$$ ◀

**EXAMPLE 6** What is the probability that a poker hand contains a full house, that is, three of one kind and two of another kind?

*Solution:* By the product rule, the number of hands containing a full house is the product of the number of ways to pick two kinds in order, the number of ways to pick three out of four for the first kind, and the number of ways to pick two out of four for the second kind. (Note that the order of the two kinds matters, because, for instance, three queens and two aces is different from three aces and two queens.) We see that the number of hands containing a full house is

$$P(13, 2)C(4, 3)C(4, 2) = 13 \cdot 12 \cdot 4 \cdot 6 = 3744.$$

Because there are $C(52, 5) = 2{,}598{,}960$ poker hands, the probability of a full house is

$$\frac{3744}{2{,}598{,}960} \approx 0.0014.$$ ◀

**EXAMPLE 7** What is the probability that the numbers 11, 4, 17, 39, and 23 are drawn in that order from a bin containing 50 balls labeled with the numbers $1, 2, \ldots, 50$ if (a) the ball selected is not returned to the bin before the next ball is selected and (b) the ball selected is returned to the bin before the next ball is selected?

*Solution:* (a) By the product rule, there are $50 \cdot 49 \cdot 48 \cdot 47 \cdot 46 = 254{,}251{,}200$ ways to select the balls because each time a ball is drawn there is one fewer ball to choose from. Consequently, the probability that 11, 4, 17, 39, and 23 are drawn in that order is $1/254{,}251{,}200$. This is an example of **sampling without replacement**.

(b) By the product rule, there are $50^5 = 312{,}500{,}000$ ways to select the balls because there are 50 possible balls to choose from each time a ball is drawn. Consequently, the probability that 11, 4, 17, 39, and 23 are drawn in that order is $1/312{,}500{,}000$. This is an example of **sampling with replacement**. ◀

## Probabilities of Complements and Unions of Events

We can use counting techniques to find the probability of events derived from other events.

**THEOREM 1**

Let $E$ be an event in a sample space $S$. The probability of the event $\overline{E} = S - E$, the complementary event of $E$, is given by

$$p(\overline{E}) = 1 - p(E).$$

*Proof:* To find the probability of the event $\overline{E} = S - E$, note that $|\overline{E}| = |S| - |E|$. Hence,

$$p(\overline{E}) = \frac{|S| - |E|}{|S|} = 1 - \frac{|E|}{|S|} = 1 - p(E).$$

◁

There is an alternative strategy for finding the probability of an event when a direct approach does not work well. Instead of determining the probability of the event, the probability of its complement can be found. This is often easier to do, as Example 8 shows.

**EXAMPLE 8** A sequence of 10 bits is randomly generated. What is the probability that at least one of these bits is 0?

*Solution:* Let $E$ be the event that at least one of the 10 bits is 0. Then $\overline{E}$ is the event that all the bits are 1s. Because the sample space $S$ is the set of all bit strings of length 10, it follows that

$$\begin{aligned} p(E) &= 1 - p(\overline{E}) = 1 - \frac{|\overline{E}|}{|S|} = 1 - \frac{1}{2^{10}} \\ &= 1 - \frac{1}{1024} = \frac{1023}{1024}. \end{aligned}$$

Hence, the probability that the bit string will contain at least one 0 bit is $1023/1024$. It is quite difficult to find this probability directly without using Theorem 1. ◀

We can also find the probability of the union of two events.

**THEOREM 2**

Let $E_1$ and $E_2$ be events in the sample space $S$. Then

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2).$$

*Proof:* Using the formula given in Section 2.2 for the number of elements in the union of two sets, it follows that

$$|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|.$$

Hence,

$$\begin{aligned} p(E_1 \cup E_2) &= \frac{|E_1 \cup E_2|}{|S|} \\ &= \frac{|E_1| + |E_2| - |E_1 \cap E_2|}{|S|} \\ &= \frac{|E_1|}{|S|} + \frac{|E_2|}{|S|} - \frac{|E_1 \cap E_2|}{|S|} \\ &= p(E_1) + p(E_2) - p(E_1 \cap E_2). \end{aligned}$$

◁

**EXAMPLE 9** What is the probability that a positive integer selected at random from the set of positive integers not exceeding 100 is divisible by either 2 or 5?

Extra Examples

*Solution:* Let $E_1$ be the event that the integer selected at random is divisible by 2, and let $E_2$ be the event that it is divisible by 5. Then $E_1 \cup E_2$ is the event that it is divisible by either 2 or 5. Also, $E_1 \cap E_2$ is the event that it is divisible by both 2 and 5, or equivalently, that it is divisible by 10. Because $|E_1| = 50$, $|E_2| = 20$, and $|E_1 \cap E_2| = 10$, it follows that

$$\begin{aligned} p(E_1 \cup E_2) &= p(E_1) + p(E_2) - p(E_1 \cap E_2) \\ &= \frac{50}{100} + \frac{20}{100} - \frac{10}{100} = \frac{3}{5}. \end{aligned}$$

◀

## Probabilistic Reasoning

A common problem is determining which of two events is more likely. Analyzing the probabilities of such events can be tricky. Example 10 describes a problem of this type. It discusses a famous problem originating with the television game show *Let's Make a Deal* and named after the host of the show, Monty Hall.

**EXAMPLE 10** **The Monty Hall Three-Door Puzzle** Suppose you are a game show contestant. You have a chance to win a large prize. You are asked to select one of three doors to open; the large prize is behind one of the three doors and the other two doors are losers. Once you select a door, the game show host, who knows what is behind each door, does the following. First, whether or not you selected the winning door, he opens one of the other two doors that he knows is a losing door (selecting at random if both are losing doors). Then he asks you whether you would like to switch doors. Which strategy should you use? Should you change doors or keep your original selection, or does it not matter?

Links

*Solution:* The probability you select the correct door (before the host opens a door and asks you whether you want to change) is $1/3$, because the three doors are equally likely to be the correct door. The probability this is the correct door does not change once the game show host opens one of the other doors, because he will always open a door that the prize is not behind.

The probability that you selected incorrectly is the probability the prize is behind one of the two doors you did not select. Consequently, the probability that you selected incorrectly is $2/3$. If you selected incorrectly, when the game show host opens a door to show you that the prize is not behind it, the prize is behind the other door. You will always win if your initial choice was incorrect and you change doors. So, by changing doors, the probability you win is $2/3$. In other words, you should always change doors when given the chance to do so by the game show host. This doubles the probability that you will win. (A more rigorous treatment of this puzzle can be found in Exercise 15 of Section 7.3. For much more on this famous puzzle and its variations, see [Ro09].) ◀

## Exercises

**1.** What is the probability that a card selected at random from a standard deck of 52 cards is an ace?

**2.** What is the probability that a fair die comes up six when it is rolled?

**3.** What is the probability that a randomly selected integer chosen from the first 100 positive integers is odd?

**4.** What is the probability that a randomly selected day of a leap year (with 366 possible days) is in April?

**5.** What is the probability that the sum of the numbers on two dice is even when they are rolled?

**6.** What is the probability that a card selected at random from a standard deck of 52 cards is an ace or a heart?

**7.** What is the probability that when a coin is flipped six times in a row, it lands heads up every time?

**8.** What is the probability that a five-card poker hand contains the ace of hearts?

**9.** What is the probability that a five-card poker hand does not contain the queen of hearts?

**10.** What is the probability that a five-card poker hand contains the two of diamonds and the three of spades?

**11.** What is the probability that a five-card poker hand contains the two of diamonds, the three of spades, the six of hearts, the ten of clubs, and the king of hearts?

**12.** What is the probability that a five-card poker hand contains exactly one ace?

**13.** What is the probability that a five-card poker hand contains at least one ace?

**14.** What is the probability that a five-card poker hand contains cards of five different kinds?

**15.** What is the probability that a five-card poker hand contains two pairs (that is, two of each of two different kinds and a fifth card of a third kind)?

**16.** What is the probability that a five-card poker hand contains a flush, that is, five cards of the same suit?

**17.** What is the probability that a five-card poker hand contains a straight, that is, five cards that have consecutive kinds? (Note that an ace can be considered either the lowest card of an A-2-3-4-5 straight or the highest card of a 10-J-Q-K-A straight.)

**18.** What is the probability that a five-card poker hand contains a straight flush, that is, five cards of the same suit of consecutive kinds?

***19.** What is the probability that a five-card poker hand contains cards of five different kinds and does not contain a flush or a straight?

**20.** What is the probability that a five-card poker hand contains a royal flush, that is, the 10, jack, queen, king, and ace of one suit?

**21.** What is the probability that a fair die never comes up an even number when it is rolled six times?

**22.** What is the probability that a positive integer not exceeding 100 selected at random is divisible by 3?

**23.** What is the probability that a positive integer not exceeding 100 selected at random is divisible by 5 or 7?

**24.** Find the probability of winning a lottery by selecting the correct six integers, where the order in which these integers are selected does not matter, from the positive integers not exceeding

**a)** 30. **b)** 36. **c)** 42. **d)** 48.

**25.** Find the probability of winning a lottery by selecting the correct six integers, where the order in which these integers are selected does not matter, from the positive integers not exceeding

**a)** 50. **b)** 52. **c)** 56. **d)** 60.

**26.** Find the probability of selecting none of the correct six integers in a lottery, where the order in which these integers are selected does not matter, from the positive integers not exceeding

**a)** 40. **b)** 48. **c)** 56. **d)** 64.

**27.** Find the probability of selecting exactly one of the correct six integers in a lottery, where the order in which these integers are selected does not matter, from the positive integers not exceeding

**a)** 40. **b)** 48. **c)** 56. **d)** 64.

**28.** In a superlottery, a player selects 7 numbers out of the first 80 positive integers. What is the probability that a person wins the grand prize by picking 7 numbers that are among the 11 numbers selected at random by a computer.

**29.** In a superlottery, players win a fortune if they choose the eight numbers selected by a computer from the positive integers not exceeding 100. What is the probability that a player wins this superlottery?

**30.** What is the probability that a player of a lottery wins the prize offered for correctly choosing five (but not six) numbers out of six integers chosen at random from the integers between 1 and 40, inclusive?

**31.** Suppose that 100 people enter a contest and that different winners are selected at random for first, second, and third prizes. What is the probability that Michelle wins one of these prizes if she is one of the contestants?

**32.** Suppose that 100 people enter a contest and that different winners are selected at random for first, second, and third prizes. What is the probability that Kumar, Janice, and Pedro each win a prize if each has entered the contest?

**33.** What is the probability that Abby, Barry, and Sylvia win the first, second, and third prizes, respectively, in a drawing if 200 people enter a contest and

**a)** no one can win more than one prize.
**b)** winning more than one prize is allowed.

**34.** What is the probability that Bo, Colleen, Jeff, and Rohini win the first, second, third, and fourth prizes, respectively, in a drawing if 50 people enter a contest and

**a)** no one can win more than one prize.
**b)** winning more than one prize is allowed.

**35.** In roulette, a wheel with 38 numbers is spun. Of these, 18 are red, and 18 are black. The other two numbers, which are neither black nor red, are 0 and 00. The probability that when the wheel is spun it lands on any particular number is $1/38$.

**a)** What is the probability that the wheel lands on a red number?

**b)** What is the probability that the wheel lands on a black number twice in a row?

**c)** What is the probability that the wheel lands on 0 or 00?

**d)** What is the probability that in five spins the wheel never lands on either 0 or 00?

**e)** What is the probability that the wheel lands on one of the first six integers on one spin, but does not land on any of them on the next spin?

**36.** Which is more likely: rolling a total of 8 when two dice are rolled or rolling a total of 8 when three dice are rolled?

**37.** Which is more likely: rolling a total of 9 when two dice are rolled or rolling a total of 9 when three dice are rolled?

**38.** Two events $E_1$ and $E_2$ are called **independent** if $p(E_1 \cap E_2) = p(E_1)p(E_2)$. For each of the following pairs of events, which are subsets of the set of all possible outcomes when a coin is tossed three times, determine whether or not they are independent.

**a)** $E_1$: tails comes up with the coin is tossed the first time; $E_2$: heads comes up when the coin is tossed the second time.

**b)** $E_1$: the first coin comes up tails; $E_2$: two, and not three, heads come up in a row.

**c)** $E_1$: the second coin comes up tails; $E_2$: two, and not three, heads come up in a row.

(We will study independence of events in more depth in Section 7.2.)

**39.** Explain what is wrong with the statement that in the Monty Hall Three-Door Puzzle the probability that the prize is behind the first door you select and the probability that the prize is behind the other of the two doors that Monty does not open are both $1/2$, because there are two doors left.

**40.** Suppose that instead of three doors, there are four doors in the Monty Hall puzzle. What is the probability that you win by not changing once the host, who knows what is behind each door, opens a losing door and gives you the chance to change doors? What is the probability that you win by changing the door you select to one of the two remaining doors among the three that you did not select?

**41.** This problem was posed by the Chevalier de Méré and was solved by Blaise Pascal and Pierre de Fermat.

**a)** Find the probability of rolling at least one six when a fair die is rolled four times.

**b)** Find the probability that a double six comes up at least once when a pair of dice is rolled 24 times. Answer the query the Chevalier de Méré made to Pascal asking whether this probability was greater than $1/2$.

**c)** Is it more likely that a six comes up at least once when a fair die is rolled four times or that a double six comes up at least once when a pair of dice is rolled 24 times?

# 7.2 Probability Theory

## Introduction

Links

In Section 7.1 we introduced the notion of the probability of an event. (Recall that an event is a subset of the possible outcomes of an experiment.) We defined the probability of an event $E$ as Laplace did, that is,

$$p(E) = \frac{|E|}{|S|},$$

the number of outcomes in $E$ divided by the total number of outcomes. This definition assumes that all outcomes are equally likely. However, many experiments have outcomes that are not equally likely. For instance, a coin may be biased so that it comes up heads twice as often as tails. Similarly, the likelihood that the input of a linear search is a particular element in a list, or is not in the list, depends on how the input is generated. How can we model the likelihood of events in such situations? In this section we will show how to define probabilities of outcomes to study probabilities of experiments where outcomes may not be equally likely.

Suppose that a fair coin is flipped four times, and the first time it comes up heads. Given this information, what is the probability that heads comes up three times? To answer this and

similar questions, we will introduce the concept of *conditional probability*. Does knowing that the first flip comes up heads change the probability that heads comes up three times? If not, these two events are called *independent*, a concept studied later in this section.

Many questions address a particular numerical value associated with the outcome of an experiment. For instance, when we flip a coin 100 times, what is the probability that exactly 40 heads appear? How many heads should we expect to appear? In this section we will introduce *random variables*, which are functions that associate numerical values to the outcomes of experiments.

## Assigning Probabilities

Let $S$ be the sample space of an experiment with a finite or countable number of outcomes. We assign a probability $p(s)$ to each outcome $s$. We require that two conditions be met:

$(i)$ $0 \leq p(s) \leq 1$ for each $s \in S$

and

$(ii)$ $\displaystyle\sum_{s \in S} p(s) = 1.$

Condition $(i)$ states that the probability of each outcome is a nonnegative real number no greater than 1. Condition $(ii)$ states that the sum of the probabilities of all possible outcomes should be 1; that is, when we do the experiment, it is a certainty that one of these outcomes occurs. (Note that when the sample space is infinite, $\sum_{s \in S} p(s)$ is a convergent infinite series.) This is a generalization of Laplace's definition in which each of $n$ outcomes is assigned a probability of $1/n$. Indeed, conditions $(i)$ and $(ii)$ are met when Laplace's definition of probabilities of equally likely outcomes is used and $S$ is finite. (See Exercise 4.)

Note that when there are $n$ possible outcomes, $x_1, x_2, \ldots, x_n$, the two conditions to be met are

$(i)$ $0 \leq p(x_i) \leq 1$ for $i = 1, 2, \ldots, n$

and

$(ii)$ $\displaystyle\sum_{i=1}^{n} p(x_i) = 1.$

The function $p$ from the set of all outcomes of the sample space $S$ is called a **probability distribution**.

To model an experiment, the probability $p(s)$ assigned to an outcome $s$ should equal the limit of the number of times $s$ occurs divided by the number of times the experiment is performed, as this number grows without bound. (We will assume that all experiments discussed have outcomes that are predictable on the average, so that this limit exists. We also assume that the outcomes of successive trials of an experiment do not depend on past results.)

---

Links HISTORICAL NOTE The Chevalier de Méré was a French nobleman, a famous gambler, and a bon vivant. He was successful at making bets with odds slightly greater than 1/2 (such as having at least one six come up in four tosses of a fair die). His correspondence with Pascal asking about the probability of having at least one double six come up when a pair of dice is rolled 24 times led to the development of probability theory. According to one account, Pascal wrote to Fermat about the Chevalier saying something like "He's a good guy but, alas, he's no mathematician."

***Remark:*** We will not discuss probabilities of events when the set of outcomes is not finite or countable, such as when the outcome of an experiment can be any real number. In such cases, integral calculus is usually required for the study of the probabilities of events.

We can model experiments in which outcomes are either equally likely or not equally likely by choosing the appropriate function $p(s)$, as Example 1 illustrates.

**EXAMPLE 1** What probabilities should we assign to the outcomes $H$ (heads) and $T$ (tails) when a fair coin is flipped? What probabilities should be assigned to these outcomes when the coin is biased so that heads comes up twice as often as tails?

*Solution:* For a fair coin, the probability that heads comes up when the coin is flipped equals the probability that tails comes up, so the outcomes are equally likely. Consequently, we assign the probability $1/2$ to each of the two possible outcomes, that is, $p(H) = p(T) = 1/2$.

For the biased coin we have

$$p(H) = 2p(T).$$

Because

$$p(H) + p(T) = 1,$$

it follows that

$$2p(T) + p(T) = 3p(T) = 1.$$

We conclude that $p(T) = 1/3$ and $p(H) = 2/3$. ◀

**DEFINITION 1** Suppose that $S$ is a set with $n$ elements. The *uniform distribution* assigns the probability $1/n$ to each element of $S$.

We now define the probability of an event as the sum of the probabilities of the outcomes in this event.

**DEFINITION 2** The *probability* of the event $E$ is the sum of the probabilities of the outcomes in $E$. That is,

$$p(E) = \sum_{s \in E} p(s).$$

(Note that when $E$ is an infinite set, $\sum_{s \in E} p(s)$ is a convergent infinite series.)

Note that when there are $n$ outcomes in the event $E$, that is, if $E = \{a_1, a_2, \ldots, a_n\}$, then $p(E) = \sum_{i=1}^{n} p(a_i)$. Note also that the uniform distribution assigns the same probability to an event that Laplace's original definition of probability assigns to this event. The experiment of selecting an element from a sample space with a uniform distribution is called selecting an element of $S$ **at random**.

**EXAMPLE 2** Suppose that a die is biased (or loaded) so that 3 appears twice as often as each other number but that the other five outcomes are equally likely. What is the probability that an odd number appears when we roll this die?

*Solution:* We want to find the probability of the event $E = \{1, 3, 5\}$. By Exercise 2, we have

$$p(1) = p(2) = p(4) = p(5) = p(6) = 1/7;\ p(3) = 2/7.$$

It follows that

$$p(E) = p(1) + p(3) + p(5) = 1/7 + 2/7 + 1/7 = 4/7.$$ ◀

When possible outcomes are equally likely and there are a finite number of possible outcomes, the definition of the probability of an event given in this section (Definition 2) agrees with Laplace's definition (Definition 1 of Section 7.1). To see this, suppose that there are $n$ equally likely outcomes; each possible outcome has probability $1/n$, because the sum of their probabilities is 1. Suppose the event $E$ contains $m$ outcomes. According to Definition 2,

$$p(E) = \sum_{i=1}^{m} \frac{1}{n} = \frac{m}{n}.$$

Because $|E| = m$ and $|S| = n$, it follows that

$$p(E) = \frac{m}{n} = \frac{|E|}{|S|}.$$

This is Laplace's definition of the probability of the event $E$.

## Probabilities of Complements and Unions of Events

The formulae for probabilities of combinations of events in Section 7.1 continue to hold when we use Definition 2 to define the probability of an event. For example, Theorem 1 of Section 7.1 asserts that

$$p(\overline{E}) = 1 - p(E),$$

where $\overline{E}$ is the complementary event of the event $E$. This equality also holds when Definition 2 is used. To see this, note that because the sum of the probabilities of the $n$ possible outcomes is 1, and each outcome is either in $E$ or in $\overline{E}$, but not in both, we have

$$\sum_{s \in S} p(s) = 1 = p(E) + p(\overline{E}).$$

Hence, $p(\overline{E}) = 1 - p(E)$.

Under Laplace's definition, by Theorem 2 in Section 7.1, we have

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

whenever $E_1$ and $E_2$ are events in a sample space $S$. This also holds when we define the probability of an event as we do in this section. To see this, note that $p(E_1 \cup E_2)$ is the sum of the probabilities of the outcomes in $E_1 \cup E_2$. When an outcome $x$ is in one, but not both, of $E_1$ and $E_2$, $p(x)$ occurs in exactly one of the sums for $p(E_1)$ and $p(E_2)$. When an outcome $x$ is in both $E_1$ and $E_2$, $p(x)$ occurs in the sum for $p(E_1)$, in the sum for $p(E_2)$, and in the sum for $p(E_1 \cap E_2)$, so it occurs $1 + 1 - 1 = 1$ time on the right-hand side. Consequently, the left-hand side and right-hand side are equal.

Also, note that if the events $E_1$ and $E_2$ are disjoint, then $p(E_1 \cap E_2) = 0$, which implies that

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2) = p(E_1) + p(E_2).$$

Theorem 1 generalizes this last formula by providing a formula for the probability of the union of pairwise disjoint events.

**THEOREM 1**

If $E_1, E_2, \ldots$ is a sequence of pairwise disjoint events in a sample space $S$, then

$$p\left(\bigcup_i E_i\right) = \sum_i p(E_i).$$

(Note that this theorem applies when the sequence $E_1, E_2, \ldots$ consists of a finite number or a countably infinite number of pairwise disjoint events.)

We leave the proof of Theorem 1 to the reader (see Exercises 36 and 37).

## Conditional Probability

Links

Suppose that we flip a coin three times, and all eight possibilities are equally likely. Moreover, suppose we know that the event $F$, that the first flip comes up tails, occurs. Given this information, what is the probability of the event $E$, that an odd number of tails appears? Because the first flip comes up tails, there are only four possible outcomes: *TTT*, *TTH*, *THT*, and *THH*, where *H* and *T* represent heads and tails, respectively. An odd number of tails appears only for the outcomes *TTT* and *THH*. Because the eight outcomes have equal probability, each of the four possible outcomes, given that $F$ occurs, should also have an equal probability of $1/4$. This suggests that we should assign the probability of $2/4 = 1/2$ to $E$, given that $F$ occurs. This probability is called the **conditional probability** of $E$ given $F$.

In general, to find the conditional probability of $E$ given $F$, we use $F$ as the sample space. For an outcome from $E$ to occur, this outcome must also belong to $E \cap F$. With this motivation, we make Definition 3.

**DEFINITION 3**

Let $E$ and $F$ be events with $p(F) > 0$. The *conditional probability* of $E$ given $F$, denoted by $p(E \mid F)$, is defined as

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}.$$

**EXAMPLE 3**

Extra Examples

A bit string of length four is generated at random so that each of the 16 bit strings of length four is equally likely. What is the probability that it contains at least two consecutive 0s, given that its first bit is a 0? (We assume that 0 bits and 1 bits are equally likely.)

*Solution:* Let $E$ be the event that a bit string of length four contains at least two consecutive 0s, and let $F$ be the event that the first bit of a bit string of length four is a 0. The probability that a bit string of length four has at least two consecutive 0s, given that its first bit is a 0, equals

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}.$$

Because $E \cap F = \{0000, 0001, 0010, 0011, 0100\}$, we see that $p(E \cap F) = 5/16$. Because there are eight bit strings of length four that start with a 0, we have $p(F) = 8/16 = 1/2$. Consequently,

$$p(E \mid F) = \frac{5/16}{1/2} = \frac{5}{8}.$$

◀

**EXAMPLE 4** What is the conditional probability that a family with two children has two boys, given they have at least one boy? Assume that each of the possibilities $BB$, $BG$, $GB$, and $GG$ is equally likely, where $B$ represents a boy and $G$ represents a girl. (Note that $BG$ represents a family with an older boy and a younger girl while $GB$ represents a family with an older girl and a younger boy.)

*Solution:* Let $E$ be the event that a family with two children has two boys, and let $F$ be the event that a family with two children has at least one boy. It follows that $E = \{BB\}$, $F = \{BB, BG, GB\}$, and $E \cap F = \{BB\}$. Because the four possibilities are equally likely, it follows that $p(F) = 3/4$ and $p(E \cap F) = 1/4$. We conclude that

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)} = \frac{1/4}{3/4} = \frac{1}{3}.$$

◀

## Independence

Links

Suppose a coin is flipped three times, as described in the introduction to our discussion of conditional probability. Does knowing that the first flip comes up tails (event $F$) alter the probability that tails comes up an odd number of times (event $E$)? In other words, is it the case that $p(E \mid F) = p(E)$? This equality is valid for the events $E$ and $F$, because $p(E \mid F) = 1/2$ and $p(E) = 1/2$. Because this equality holds, we say that $E$ and $F$ are **independent events**. When two events are independent, the occurrence of one of the events gives no information about the probability that the other event occurs.

Because $p(E \mid F) = p(E \cap F)/p(F)$, asking whether $p(E \mid F) = p(E)$ is the same as asking whether $p(E \cap F) = p(E)p(F)$. This leads to Definition 4.

**DEFINITION 4** The events $E$ and $F$ are *independent* if and only if $p(E \cap F) = p(E)p(F)$.

**EXAMPLE 5** Suppose $E$ is the event that a randomly generated bit string of length four begins with a 1 and $F$ is the event that this bit string contains an even number of 1s. Are $E$ and $F$ independent, if the 16 bit strings of length four are equally likely?

Extra Examples

*Solution:* There are eight bit strings of length four that begin with a one: 1000, 1001, 1010, 1011, 1100, 1101, 1110, and 1111. There are also eight bit strings of length four that contain an even number of ones: 0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111. Because there are 16 bit strings of length four, it follows that

$$p(E) = p(F) = 8/16 = 1/2.$$

Because $E \cap F = \{1111, 1100, 1010, 1001\}$, we see that

$$p(E \cap F) = 4/16 = 1/4.$$

Because

$$p(E \cap F) = 1/4 = (1/2)(1/2) = p(E)p(F),$$

we conclude that $E$ and $F$ are independent. ◀

Probability has many applications to genetics, as Examples 6 and 7 illustrate.

**EXAMPLE 6** Assume, as in Example 4, that each of the four ways a family can have two children is equally likely. Are the events $E$, that a family with two children has two boys, and $F$, that a family with two children has at least one boy, independent?

*Solution:* Because $E = \{BB\}$, we have $p(E) = 1/4$. In Example 4 we showed that $p(F) = 3/4$ and that $p(E \cap F) = 1/4$. But $p(E)p(F) = \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$. Therefore $p(E \cap F) \neq p(E)p(F)$, so the events $E$ and $F$ are not independent. ◀

**EXAMPLE 7** Are the events $E$, that a family with three children has children of both sexes, and $F$, that this family has at most one boy, independent? Assume that the eight ways a family can have three children are equally likely.

*Solution:* By assumption, each of the eight ways a family can have three children, $BBB$, $BBG$, $BGB$, $BGG$, $GBB$, $GBG$, $GGB$, and $GGG$, has a probability of $1/8$. Because $E = \{BBG,\ BGB,\ BGG,\ GBB,\ GBG,\ GGB\}$, $F = \{BGG,\ GBG,\ GGB,\ GGG\}$, and $E \cap F = \{BGG,\ GBG,\ GGB\}$, it follows that $p(E) = 6/8 = 3/4$, $p(F) = 4/8 = 1/2$, and $p(E \cap F) = 3/8$. Because

$$p(E)p(F) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8},$$

it follows that $p(E \cap F) = p(E)p(F)$, so $E$ and $F$ are independent. (This conclusion may seem surprising. Indeed, if we change the number of children, the conclusion may no longer hold. See Exercise 27.) ◀

PAIRWISE AND MUTUAL INDEPENDENCE We can also define the independence of more than two events. However, there are two different types of independence, given in Definition 5.

**DEFINITION 5** The events $E_1, E_2, \ldots, E_n$ are *pairwise independent* if and only if $p(E_i \cap E_j) = p(E_i)p(E_j)$ for all pairs of integers $i$ and $j$ with $1 \leq i < j \leq n$. These events are *mutually independent* if $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})p(E_{i_2}) \cdots p(E_{i_m})$ whenever $i_j$, $j = 1, 2, \ldots, m$, are integers with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and $m \geq 2$.

From Definition 5, we see that every set of $n$ mutually independent events is also pairwise independent. However, $n$ pairwise independent events are not necessarily mutually independent, as we see in Exercise 25 in the Supplementary Exercises. Many theorems about $n$ events include the hypothesis that these events are mutually independent, and not just pairwise independent. We will introduce several such theorems later in this chapter.

## Bernoulli Trials and the Binomial Distribution

Links

Suppose that an experiment can have only two possible outcomes. For instance, when a bit is generated at random, the possible outcomes are 0 and 1. When a coin is flipped, the possible outcomes are heads and tails. Each performance of an experiment with two possible outcomes is called a **Bernoulli trial**, after James Bernoulli, who made important contributions to probability theory. In general, a possible outcome of a Bernoulli trial is called a **success** or a **failure**. If $p$ is the probability of a success and $q$ is the probability of a failure, it follows that $p + q = 1$.

Many problems can be solved by determining the probability of $k$ successes when an experiment consists of $n$ mutually independent Bernoulli trials. (Bernoulli trials are **mutually independent** if the conditional probability of success on any given trial is $p$, given any information whatsoever about the outcomes of the other trials.) Consider Example 8.

**EXAMPLE 8** A coin is biased so that the probability of heads is 2/3. What is the probability that exactly four heads come up when the coin is flipped seven times, assuming that the flips are independent?

*Solution:* There are $2^7 = 128$ possible outcomes when a coin is flipped seven times. The number of ways four of the seven flips can be heads is $C(7, 4)$. Because the seven flips are independent, the probability of each of these outcomes (four heads and three tails) is $(2/3)^4(1/3)^3$. Consequently, the probability that exactly four heads appear is

$$C(7, 4)(2/3)^4(1/3)^3 = \frac{35 \cdot 16}{3^7} = \frac{560}{2187}.$$ ◀

Following the same reasoning as was used in Example 8, we can find the probability of $k$ successes in $n$ independent Bernoulli trials.

**THEOREM 2**

The probability of exactly $k$ successes in $n$ independent Bernoulli trials, with probability of success $p$ and probability of failure $q = 1 - p$, is

$$C(n, k)p^k q^{n-k}.$$

*Proof:* When $n$ Bernoulli trials are carried out, the outcome is an $n$-tuple $(t_1, t_2, \ldots, t_n)$, where $t_i = S$ (for success) or $t_i = F$ (for failure) for $i = 1, 2, \ldots, n$. Because the $n$ trials are independent, the probability of each outcome of $n$ trials consisting of $k$ successes and $n - k$ failures (in any order) is $p^k q^{n-k}$. Because there are $C(n, k)$ $n$-tuples of $S$'s and $F$'s that contain exactly $k$ $S$'s, the probability of exactly $k$ successes is

$$C(n, k)p^k q^{n-k}.$$ ◁

We denote by $b(k; n, p)$ the probability of $k$ successes in $n$ independent Bernoulli trials with probability of success $p$ and probability of failure $q = 1 - p$. Considered as a function of $k$, we call this function the **binomial distribution**. Theorem 2 tells us that $b(k; n, p) = C(n, k)p^k q^{n-k}$.

**EXAMPLE 9** Extra Examples

Suppose that the probability that a 0 bit is generated is 0.9, that the probability that a 1 bit is generated is 0.1, and that bits are generated independently. What is the probability that exactly eight 0 bits are generated when 10 bits are generated?

*Solution:* By Theorem 2, the probability that exactly eight 0 bits are generated is

$$b(8; 10, 0.9) = C(10, 8)(0.9)^8(0.1)^2 = 0.1937102445.$$ ◀

Links

JAMES BERNOULLI (1654–1705) James Bernoulli (also known as Jacob I), was born in Basel, Switzerland. He is one of the eight prominent mathematicians in the Bernoulli family (see Section 10.1 for the Bernoulli family tree of mathematicians). Following his father's wish, James studied theology and entered the ministry. But contrary to the desires of his parents, he also studied mathematics and astronomy. He traveled throughout Europe from 1676 to 1682, learning about the latest discoveries in mathematics and the sciences. Upon returning to Basel in 1682, he founded a school for mathematics and the sciences. He was appointed professor of mathematics at the University of Basel in 1687, remaining in this position for the rest of his life.

James Bernoulli is best known for the work *Ars Conjectandi*, published eight years after his death. In this work, he described the known results in probability theory and in enumeration, often providing alternative proofs of known results. This work also includes the application of probability theory to games of chance and his introduction of the theorem known as the **law of large numbers**. This law states that if $\epsilon > 0$, as $n$ becomes arbitrarily large the probability approaches 1 that the fraction of times an event $E$ occurs during $n$ trials is within $\epsilon$ of $p(E)$.

Note that the sum of the probabilities that there are $k$ successes when $n$ independent Bernoulli trials are carried out, for $k = 0, 1, 2, \ldots, n$, equals

$$\sum_{k=0}^{n} C(n, k)p^k q^{n-k} = (p + q)^n = 1,$$

as should be the case. The first equality in this string of equalities is a consequence of the binomial theorem (see Section 6.4). The second equality follows because $q = 1 - p$.

## Random Variables

Many problems are concerned with a numerical value associated with the outcome of an experiment. For instance, we may be interested in the total number of one bits in a randomly generated string of 10 bits; or in the number of times tails come up when a coin is flipped 20 times. To study problems of this type we introduce the concept of a random variable.

**DEFINITION 6**

A *random variable* is a function from the sample space of an experiment to the set of real numbers. That is, a random variable assigns a real number to each possible outcome.

***Remark:*** Note that a random variable is a function. It is not a variable, and it is not random! The name *random variable* (the translation of *variabile casuale*) was introduced by the Italian mathematician F. P. Cantelli in 1916. In the late 1940s, the mathematicians, W. Feller and J. L. Doob flipped a coin to see whether both would use "random variable" or the more fitting term "chance variable." Feller won; unfortunately "random varible" was used in both books and ever since.

**EXAMPLE 10** Suppose that a coin is flipped three times. Let $X(t)$ be the random variable that equals the number of heads that appear when $t$ is the outcome. Then $X(t)$ takes on the following values:

$$\begin{aligned} X(HHH) &= 3, \\ X(HHT) &= X(HTH) = X(THH) = 2, \\ X(TTH) &= X(THT) = X(HTT) = 1, \\ X(TTT) &= 0. \end{aligned}$$

◀

**DEFINITION 7**

The *distribution* of a random variable $X$ on a sample space $S$ is the set of pairs $(r, p(X = r))$ for all $r \in X(S)$, where $p(X = r)$ is the probability that $X$ takes the value $r$. (The set of pairs in this distribution is determined by the probabilities $p(X = r)$ for $r \in X(S)$.)

**EXAMPLE 11** Each of the eight possible outcomes when a fair coin is flipped three times has probability $1/8$. So, the distribution of the random variable $X(t)$ in Example 10 is determined by the probabilities $P(X = 3) = 1/8$, $P(X = 2) = 3/8$, $P(X = 1) = 3/8$, and $P(X = 0) = 1/8$. Consequently, the distribution of $X(t)$ in Example 10 is the set of pairs $(3, 1/8)$, $(2, 3/8)$, $(1, 3/8)$, and $(0, 1/8)$. ◀

**EXAMPLE 12** Let $X$ be the sum of the numbers that appear when a pair of dice is rolled. What are the values of this random variable for the 36 possible outcomes $(i, j)$, where $i$ and $j$ are the numbers that appear on the first die and the second die, respectively, when these two dice are rolled?

*Solution:* The random variable $X$ takes on the following values:

$$
\begin{aligned}
&X((1, 1)) = 2,\\
&X((1, 2)) = X((2, 1)) = 3,\\
&X((1, 3)) = X((2, 2)) = X((3, 1)) = 4,\\
&X((1, 4)) = X((2, 3)) = X((3, 2)) = X((4, 1)) = 5,\\
&X((1, 5)) = X((2, 4)) = X((3, 3)) = X((4, 2)) = X((5, 1)) = 6,\\
&X((1, 6)) = X((2, 5)) = X((3, 4)) = X((4, 3)) = X((5, 2)) = X((6, 1)) = 7,\\
&X((2, 6)) = X((3, 5)) = X((4, 4)) = X((5, 3)) = X((6, 2)) = 8,\\
&X((3, 6)) = X((4, 5)) = X((5, 4)) = X((6, 3)) = 9,\\
&X((4, 6)) = X((5, 5)) = X((6, 4)) = 10,\\
&X((5, 6)) = X((6, 5)) = 11,\\
&X((6, 6)) = 12.
\end{aligned}
$$

◀

We will continue our study of random variables in Section 7.4, where we will show how they can be used in a variety of applications.

## The Birthday Problem

A famous puzzle asks for the smallest number of people needed in a room so that it is more likely than not that at least two of them have the same day of the year as their birthday. Most people find the answer, which we determine in Example 13, to be surprisingly small. After we solve this famous problem, we will show how similar reasoning can be adapted to solve a question about hashing functions.

**EXAMPLE 13** Links

**The Birthday Problem** What is the minimum number of people who need to be in a room so that the probability that at least two of them have the same birthday is greater than $1/2$?

*Solution:* First, we state some assumptions. We assume that the birthdays of the people in the room are independent. Furthermore, we assume that each birthday is equally likely and that there are 366 days in the year. (In reality, more people are born on some days of the year than others, such as days nine months after some holidays including New Year's Eve, and only leap years have 366 days.)

To find the probability that at least two of $n$ people in a room have the same birthday, we first calculate the probability $p_n$ that these people all have different birthdays. Then, the probability that at least two people have the same birthday is $1 - p_n$. To compute $p_n$, we consider the birthdays of the $n$ people in some fixed order. Imagine them entering the room one at a time; we will compute the probability that each successive person entering the room has a birthday different from those of the people already in the room.

The birthday of the first person certainly does not match the birthday of someone already in the room. The probability that the birthday of the second person is different from that of the first person is $365/366$ because the second person has a different birthday when he or she was born on one of the 365 days of the year other than the day the first person was born. (The assumption that it is equally likely for someone to be born on any of the 366 days of the year enters into this and subsequent steps.)

The probability that the third person has a birthday different from both the birthdays of the first and second people given that these two people have different birthdays is $364/366$. In general, the probability that the $j$th person, with $2 \leq j \leq 366$, has a birthday different from the

birthdays of the $j-1$ people already in the room given that these $j-1$ people have different birthdays is

$$\frac{366-(j-1)}{366} = \frac{367-j}{366}.$$

Because we have assumed that the birthdays of the people in the room are independent, we can conclude that the probability that the $n$ people in the room have different birthdays is

$$p_n = \frac{365}{366}\,\frac{364}{366}\,\frac{363}{366}\cdots\frac{367-n}{366}.$$

It follows that the probability that among $n$ people there are at least two people with the same birthday is

$$1-p_n = 1-\frac{365}{366}\,\frac{364}{366}\,\frac{363}{366}\cdots\frac{367-n}{366}.$$

To determine the minimum number of people in the room so that the probability that at least two of them have the same birthday is greater than $1/2$, we use the formula we have found for $1-p_n$ to compute it for increasing values of $n$ until it becomes greater than $1/2$. (There are more sophisticated approaches using calculus that can eliminate this computation, but we will not use them here.) After considerable computation we find that for $n=22$, $1-p_n \approx 0.475$, while for $n=23$, $1-p_n \approx 0.506$. Consequently, the minimum number of people needed so that the probability that at least two people have the same birthday is greater than $1/2$ is 23. ◀

The solution to the birthday problem leads to the solution of the question in Example 14 about hashing functions.

**EXAMPLE 14** **Probability of a Collision in Hashing Functions** Recall from Section 4.5 that a hashing function $h(k)$ is a mapping of the keys (of the records that are to be stored in a database) to storage locations. Hashing functions map a large universe of keys (such as the approximately 300 million Social Security numbers in the United States) to a much smaller set of storage locations. A good hashing function yields few **collisions**, which are mappings of two different keys to the same memory location, when relatively few of the records are in play in a given application. What is the probability that no two keys are mapped to the same location by a hashing function, or, in other words, that there are no collisions?

*Solution:* To calculate this probability, we assume that the probability that a randomly selected key is mapped to a location is $1/m$, where $m$ is the number of available locations, that is, the hashing function distributes keys uniformly. (In practice, hashing functions may not satisfy this assumption. However, for a good hashing function, this assumption should be close to correct.) Furthermore, we assume that the keys of the records selected have an equal probability to be any of the elements of the key universe and that these keys are independently selected.

Suppose that the keys are $k_1, k_2, \ldots, k_n$. When we add the second record, the probability that it is mapped to a location different from the location of the first record, that $h(k_2) \neq h(k_1)$, is $(m-1)/m$ because there are $m-1$ free locations after the first record has been placed. The probability that the third record is mapped to a free location after the first and second records have been placed without a collision is $(m-2)/m$. In general, the probability that the $j$th record is mapped to a free location after the first $j-1$ records have been mapped to locations $h(k_1)$, $h(k_2), \ldots, h(k_{j-1})$ without collisions is $(m-(j-1))/m$ because $j-1$ of the $m$ locations are taken.

Because the keys are independent, the probability that all $n$ keys are mapped to different locations is

$$p_n = \frac{m-1}{m}\cdot\frac{m-2}{m}\cdot\cdots\cdot\frac{m-n+1}{m}.$$

It follows that the probability that there is at least one collision, that is, at least two keys are mapped to the same location, is

$$1 - p_n = 1 - \frac{m-1}{m} \cdot \frac{m-2}{m} \cdot \cdots \cdot \frac{m-n+1}{m}.$$

Techniques from calculus can be used to find the smallest value of $n$ given a value of $m$ such that the probability of a collision is greater than a particular threshold. It can be shown that the smallest integer $n$ such that the probability of a collision is greater than $1/2$ is approximately $n = 1.177\sqrt{m}$. For example, when $m = 1{,}000{,}000$, the smallest integer $n$ such that the probability of a collision is greater than $1/2$ is 1178. ◀

## Monte Carlo Algorithms

The algorithms discussed so far in this book are all deterministic. That is, each algorithm always proceeds in the same way whenever given the same input. However, there are many situations where we would like an algorithm to make a random choice at one or more steps. Such a situation arises when a deterministic algorithm would have to go through a huge number, or even an unknown number, of possible cases. Algorithms that make random choices at one or more steps are called **probabilistic algorithms**. We will discuss a particular class of probabilistic algorithms in this section, namely, **Monte Carlo algorithms**, for decision problems. Monte Carlo algorithms always produce answers to problems, but a small probability remains that these answers may be incorrect. However, the probability that the answer is incorrect decreases rapidly when the algorithm carries out sufficient computation. Decision problems have either "true" or "false" as their answer. The designation "Monte Carlo" is a reference to the famous casino in Monaco; the use of randomness and the repetitive processes in these algorithms make them similar to some gambling games. This name was introduced by the inventors of Monte Carlo methods, including Stan Ulam, Enrico Fermi, and John von Neumann.

Monte Carlo methods were invented to help develop the first nuclear weapons.

A Monte Carlo algorithm for a decision problem uses a sequence of tests. The probability that the algorithm answers the decision problem correctly increases as more tests are carried out. At each step of the algorithm, possible responses are "true," which means that the answer is "true" and no additional iterations are needed, or "unknown," which means that the answer could be either "true" or "false." After running all the iterations in such an algorithm, the final answer produced is "true" if at least one iteration yields the answer "true," and the answer is "false" if every iteration yields the answer "unknown." If the correct answer is "false," then the algorithm answers "false," because every iteration will yield "unknown." However, if the correct answer is "true," then the algorithm could answer either "true" or "false," because it may be possible that each iteration produced the response "unknown" even though the correct response was "true." We will show that this possibility becomes extremely unlikely as the number of tests increases.

Suppose that $p$ is the probability that the response of a test is "true," given that the answer is "true." It follows that $1-p$ is the probability that the response is "unknown," given that the answer is "true." Because the algorithm answers "false" when all $n$ iterations yield the answer "unknown" and the iterations perform independent tests, the probability of error is $(1-p)^n$. When $p \neq 0$, this probability approaches 0 as the number of tests increases. Consequently, the probability that the algorithm answers "true" when the answer is "true" approaches 1.

**EXAMPLE 15** **Quality Control** (This example is adapted from [AhUl95].) Suppose that a manufacturer orders processor chips in batches of size $n$, where $n$ is a positive integer. The chip maker has tested only some of these batches to make sure that all the chips in the batch are good (replacing any bad chips found during testing with good ones). In previously untested batches, the probability that a particular chip is bad has been observed to be 0.1 when random testing is done. The PC manufacturer wants to decide whether all the chips in a batch are good. To

do this, the PC manufacturer can test each chip in a batch to see whether it is good. However, this requires $n$ tests. Assuming that each test can be carried out in constant time, these tests require $O(n)$ seconds. Can the PC manufacturer determine whether a batch of chips has been tested by the chip maker using less time?

*Solution:* We can use a Monte Carlo algorithm to determine whether a batch of chips has been tested by the chip maker as long as we are willing to accept some probability of error. The algorithm is set up to answer the question: "Has this batch of chips not been tested by the chip maker?" It proceeds by successively selecting chips at random from the batch and testing them one by one. When a bad chip is encountered, the algorithm answers "true" and stops. If a tested chip is good, the algorithm answers "unknown" and goes on to the next chip. After the algorithm has tested a specified number of chips, say $k$ chips, without getting an answer of "true," the algorithm terminates with the answer "false"; that is, the algorithm concludes that the batch is good, that is, that the chip maker has tested all the chips in the batch.

The only way for this algorithm to answer incorrectly is for it to conclude that an untested batch of chips has been tested by the chip maker. The probability that a chip is good, but that it came from an untested batch, is $1 - 0.1 = 0.9$. Because the events of testing different chips from a batch are independent, the probability that all $k$ steps of the algorithm produce the answer "unknown," given that the batch of chips is untested, is $0.9^k$.

By taking $k$ large enough, we can make this probability as small as we like. For example, by testing 66 chips, the probability that the algorithm decides a batch has been tested by the chip maker is $0.9^{66}$, which is less than 0.001. That is, the probability is less than 1 in 1000 that the algorithm has answered incorrectly. Note that this probability is independent of $n$, the number of chips in a batch. That is, the Monte Carlo algorithm uses a constant number, or $O(1)$, tests and requires $O(1)$ seconds, no matter how many chips are in a batch. As long as the PC manufacturer can live with an error rate of less than 1 in 1000, the Monte Carlo algorithm will save the PC manufacturer a lot of testing. If a smaller error rate is needed, the PC manufacturer can test more chips in each batch; the reader can verify that 132 tests lower the error rate to less than 1 in 1,000,000. ◀

**EXAMPLE 16** **Probabilistic Primality Testing** In Chapter 4 we remarked that a composite integer, that is, an integer greater than one that is not prime, passes Miller's test (see the preamble to Exercise 44 in Section 4.4) for fewer than $n/4$ bases $b$ with $1 < b < n$. This observation is the basis for a Monte Carlo algorithm to determine whether an integer greater than one is prime. Because large primes play an essential role in public-key cryptography (see Section 4.6), being able to generate large primes quickly has become extremely important.

The goal of the algorithm is to decide the question "Is $n$ composite?" Given an integer $n$ greater than one, we select an integer $b$ at random with $1 < b < n$ and determine whether $n$ passes Miller's test to the base $b$. If $n$ fails the test, the answer is "true" because $n$ must be composite, and the algorithm ends. Otherwise, we perform the test $k$ times, where $k$ is a positive integer. Each time we select a random integer $b$ and determine whether $n$ passes Miller's test to the base $b$. If the answer is "unknown" at each step, the algorithm answers "false," that is, it says that $n$ is not composite, so that it is prime. The only possibility for the algorithm to return an incorrect answer occurs when $n$ is composite, and the answer "unknown" is the output at each of the $k$ iterations. The probability that a composite integer $n$ passes Miller's test for a randomly selected base $b$ is less than $1/4$. Because the integer $b$ with $1 < b < n$ is selected at random at each iteration and these iterations are independent, the probability that $n$ is composite but the algorithm responds that $n$ is prime is less than $(1/4)^k$. By taking $k$ to be sufficiently large, we can make this probability extremely small. For example, with 10 iterations, the probability that the algorithm decides that $n$ is prime when it really is composite is less than 1 in 1,000,000. With 30 iterations, this probability drops to less than 1 in $10^{18}$, an extremely unlikely event.

A number that passes many iterations of a probabilistic primality test is called an *industrial strength prime*, even though it may be composite.

To generate large primes, say with 200 digits, we randomly choose an integer $n$ with 200 digits and run this algorithm, with 30 iterations. If the algorithm decides that $n$ is prime, we

can use it as one of the two primes used in an encryption key for the RSA cryptosystem. If $n$ is actually composite and is used as part of the key, the procedures used to decrypt messages will not produce the original encrypted message. The key is then discarded and two new possible primes are used. ◀

## The Probabilistic Method

We discussed existence proofs in Chapter 1 and illustrated the difference between constructive existence proofs and nonconstructive existence proofs. The probabilistic method, introduced by Paul Erdős and Alfréd Rényi, is a powerful technique that can be used to create nonconstructive existence proofs. To use the probabilistic method to prove results about a set $S$, such as the existence of an element in $S$ with a specified property, we assign probabilities to the elements of $S$. We then use methods from probability theory to prove results about the elements of $S$. In particular, we can show that an element with a specified property exists by showing that the probability an element $x \in S$ has this property is positive. The probabilistic method is based on the equivalent statement in Theorem 3.

**THEOREM 3** **THE PROBABILISTIC METHOD** If the probability that an element chosen at random from a $S$ does not have a particular property is less than 1, there exists an element in $S$ with this property.

An existence proof based on the probabilistic method is nonconstructive because it does not find a particular element with the desired property.

We illustrate the power of the probabilistic method by finding a lower bound for the Ramsey number $R(k, k)$. Recall from Section 6.2 that $R(k, k)$ equals the minimum number of people at a party needed to ensure that there are at least $k$ mutual friends or $k$ mutual enemies (assuming that any two people are friends or enemies).

**THEOREM 4** If $k$ is an integer with $k \geq 2$, then $R(k, k) \geq 2^{k/2}$.

*Proof:* We note that the theorem holds for $k = 2$ and $k = 3$ because $R(2, 2) = 2$ and $R(3, 3) = 6$, as was shown in Section 6.2. Now suppose that $k \geq 4$. We will use the probabilistic method to show that if there are fewer than $2^{k/2}$ people at a party, it is possible that no $k$ of them are mutual friends or mutual enemies. This will show that $R(k, k)$ is at least $2^{k/2}$.

To use the probabilistic method, we assume that it is equally likely for two people to be friends or enemies. (Note that this assumption does not have to be realistic.) Suppose there are $n$ people at the party. It follows that there are $\binom{n}{k}$ different sets of $k$ people at this party, which we list as $S_1, S_2, \ldots, S_{\binom{n}{k}}$. Let $E_i$ be the event that all $k$ people in $S_i$ are either mutual friends or mutual enemies. The probability that there are either $k$ mutual friends or $k$ mutual enemies among the $n$ people equals $p(\bigcup_{i=1}^{\binom{n}{k}} E_i)$.

According to our assumption it is equally likely for two people to be friends or enemies. The probability that two people are friends equals the probability that they are enemies; both probabilities equal $1/2$. Furthermore, there are $\binom{k}{2} = k(k-1)/2$ pairs of people in $S_i$ because there are $k$ people in $S_i$. Hence, the probability that all $k$ people in $S_i$ are mutual friends and the probability that all $k$ people in $S_i$ are mutual enemies both equal $(1/2)^{k(k-1)/2}$. It follows that $p(E_i) = 2(1/2)^{k(k-1)/2}$.

The probability that there are either $k$ mutual friends or $k$ mutual enemies in the group of $n$ people equals $p(\bigcup_{i=1}^{\binom{n}{k}} E_i)$. Using Boole's inequality (Exercise 15), it follows that

$$p\left(\bigcup_{i=1}^{\binom{n}{k}} E_i\right) \leq \sum_{i=1}^{\binom{n}{k}} p(E_i) = \binom{n}{k} \cdot 2\left(\frac{1}{2}\right)^{k(k-1)/2}.$$

By Exercise 17 in Section 6.4, we have $\binom{n}{k} \leq n^k/2^{k-1}$. Hence,

$$\binom{n}{k} 2\left(\frac{1}{2}\right)^{k(k-1)/2} \leq \frac{n^k}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2}.$$

Now if $n < 2^{k/2}$, we have

$$\frac{n^k}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2} < \frac{2^{k(k/2)}}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2} = 2^{2-(k/2)} \leq 1,$$

where the last step follows because $k \geq 4$.

We can now conclude that $p(\bigcup_{i=1}^{\binom{n}{k}} E_i) < 1$ when $k \geq 4$. Hence, the probability of the complementary event, that there is no set of either $k$ mutual friends or mutual enemies at the party, is greater than 0. It follows that if $n < 2^{k/2}$, there is at least one set such that no subset of $k$ people are mutual friends or mutual enemies. ◁

## Exercises

**1.** What probability should be assigned to the outcome of heads when a biased coin is tossed, if heads is three times as likely to come up as tails? What probability should be assigned to the outcome of tails?

**2.** Find the probability of each outcome when a loaded die is rolled, if a 3 is twice as likely to appear as each of the other five numbers on the die.

**3.** Find the probability of each outcome when a biased die is rolled, if rolling a 2 or rolling a 4 is three times as likely as rolling each of the other four numbers on the die and it is equally likely to roll a 2 or a 4.

**4.** Show that conditions (*i*) and (*ii*) are met under Laplace's definition of probability, when outcomes are equally likely.

**5.** A pair of dice is loaded. The probability that a 4 appears on the first die is $2/7$, and the probability that a 3 appears on the second die is $2/7$. Other outcomes for each die appear with probability $1/7$. What is the probability of 7 appearing as the sum of the numbers when the two dice are rolled?

**6.** What is the probability of these events when we randomly select a permutation of $\{1, 2, 3\}$?
- **a)** 1 precedes 3.
- **b)** 3 precedes 1.
- **c)** 3 precedes 1 and 3 precedes 2.

**7.** What is the probability of these events when we randomly select a permutation of $\{1, 2, 3, 4\}$?
- **a)** 1 precedes 4.
- **b)** 4 precedes 1.
- **c)** 4 precedes 1 and 4 precedes 2.
- **d)** 4 precedes 1, 4 precedes 2, and 4 precedes 3.
- **e)** 4 precedes 3 and 2 precedes 1.

**8.** What is the probability of these events when we randomly select a permutation of $\{1, 2, \ldots, n\}$ where $n \geq 4$?
- **a)** 1 precedes 2.
- **b)** 2 precedes 1.
- **c)** 1 immediately precedes 2.
- **d)** $n$ precedes 1 and $n-1$ precedes 2.
- **e)** $n$ precedes 1 and $n$ precedes 2.

**9.** What is the probability of these events when we randomly select a permutation of the 26 lowercase letters of the English alphabet?
- **a)** The permutation consists of the letters in reverse alphabetic order.
- **b)** $z$ is the first letter of the permutation.
- **c)** $z$ precedes $a$ in the permutation.
- **d)** $a$ immediately precedes $z$ in the permutation.
- **e)** $a$ immediately precedes $m$, which immediately precedes $z$ in the permutation.
- **f)** $m$, $n$, and $o$ are in their original places in the permutation.

**10.** What is the probability of these events when we randomly select a permutation of the 26 lowercase letters of the English alphabet?
- **a)** The first 13 letters of the permutation are in alphabetical order.
- **b)** $a$ is the first letter of the permutation and $z$ is the last letter.
- **c)** $a$ and $z$ are next to each other in the permutation.
- **d)** $a$ and $b$ are not next to each other in the permutation.
- **e)** $a$ and $z$ are separated by at least 23 letters in the permutation.
- **f)** $z$ precedes both $a$ and $b$ in the permutation.

**11.** Suppose that $E$ and $F$ are events such that $p(E) = 0.7$ and $p(F) = 0.5$. Show that $p(E \cup F) \geq 0.7$ and $p(E \cap F) \geq 0.2$.

**12.** Suppose that $E$ and $F$ are events such that $p(E) = 0.8$ and $p(F) = 0.6$. Show that $p(E \cup F) \geq 0.8$ and $p(E \cap F) \geq 0.4$.

**13.** Show that if $E$ and $F$ are events, then $p(E \cap F) \geq p(E) + p(F) - 1$. This is known as **Bonferroni's inequality**.

**14.** Use mathematical induction to prove the following generalization of Bonferroni's inequality:

$$p(E_1 \cap E_2 \cap \cdots \cap E_n) \geq p(E_1) + p(E_2) + \cdots + p(E_n) - (n-1),$$

where $E_1, E_2, \ldots, E_n$ are $n$ events.

**15.** Show that if $E_1, E_2, \ldots, E_n$ are events from a finite sample space, then

$$p(E_1 \cup E_2 \cup \cdots \cup E_n) \leq p(E_1) + p(E_2) + \cdots + p(E_n).$$

This is known as **Boole's inequality**.

**16.** Show that if $E$ and $F$ are independent events, then $\overline{E}$ and $\overline{F}$ are also independent events.

**17.** If $E$ and $F$ are independent events, prove or disprove that $\overline{E}$ and $F$ are necessarily independent events.

In Exercises 18, 20, and 21 assume that the year has 366 days and all birthdays are equally likely. In Exercise 19 assume it is equally likely that a person is born in any given month of the year.

**18.**
- **a)** What is the probability that two people chosen at random were born on the same day of the week?
- **b)** What is the probability that in a group of $n$ people chosen at random, there are at least two born on the same day of the week?
- **c)** How many people chosen at random are needed to make the probability greater than $1/2$ that there are at least two people born on the same day of the week?

**19.**
- **a)** What is the probability that two people chosen at random were born during the same month of the year?
- **b)** What is the probability that in a group of $n$ people chosen at random, there are at least two born in the same month of the year?
- **c)** How many people chosen at random are needed to make the probability greater than $1/2$ that there are at least two people born in the same month of the year?

**20.** Find the smallest number of people you need to choose at random so that the probability that at least one of them has a birthday today exceeds $1/2$.

**21.** Find the smallest number of people you need to choose at random so that the probability that at least two of them were both born on April 1 exceeds $1/2$.

***22.** February 29 occurs only in leap years. Years divisible by 4, but not by 100, are always leap years. Years divisible by 100, but not by 400, are not leap years, but years divisible by 400 are leap years.
- **a)** What probability distribution for birthdays should be used to reflect how often February 29 occurs?
- **b)** Using the probability distribution from part (a), what is the probability that in a group of $n$ people at least two have the same birthday?

**23.** What is the conditional probability that exactly four heads appear when a fair coin is flipped five times, given that the first flip came up heads?

**24.** What is the conditional probability that exactly four heads appear when a fair coin is flipped five times, given that the first flip came up tails?

**25.** What is the conditional probability that a randomly generated bit string of length four contains at least two consecutive 0s, given that the first bit is a 1? (Assume the probabilities of a 0 and a 1 are the same.)

**26.** Let $E$ be the event that a randomly generated bit string of length three contains an odd number of 1s, and let $F$ be the event that the string starts with 1. Are $E$ and $F$ independent?

**27.** Let $E$ and $F$ be the events that a family of $n$ children has children of both sexes and has at most one boy, respectively. Are $E$ and $F$ independent if
- **a)** $n = 2$? **b)** $n = 4$? **c)** $n = 5$?

**28.** Assume that the probability a child is a boy is 0.51 and that the sexes of children born into a family are independent. What is the probability that a family of five children has
- **a)** exactly three boys?
- **b)** at least one boy?
- **c)** at least one girl?
- **d)** all children of the same sex?

**29.** A group of six people play the game of "odd person out" to determine who will buy refreshments. Each person flips a fair coin. If there is a person whose outcome is not the same as that of any other member of the group, this person has to buy the refreshments. What is the probability that there is an odd person out after the coins are flipped once?

**30.** Find the probability that a randomly generated bit string of length 10 does not contain a 0 if bits are independent and if
- **a)** a 0 bit and a 1 bit are equally likely.
- **b)** the probability that a bit is a 1 is 0.6.
- **c)** the probability that the $i$th bit is a 1 is $1/2^i$ for $i = 1, 2, 3, \ldots, 10$.

**31.** Find the probability that a family with five children does not have a boy, if the sexes of children are independent and if

**a)** a boy and a girl are equally likely.

**b)** the probability of a boy is 0.51.

**c)** the probability that the $i$th child is a boy is $0.51 - (i/100)$.

**32.** Find the probability that a randomly generated bit string of length 10 begins with a 1 or ends with a 00 for the same conditions as in parts (a), (b), and (c) of Exercise 30, if bits are generated independently.

**33.** Find the probability that the first child of a family with five children is a boy or that the last two children of the family are girls, for the same conditions as in parts (a), (b), and (c) of Exercise 31.

**34.** Find each of the following probabilities when $n$ independent Bernoulli trials are carried out with probability of success $p$.

**a)** the probability of no successes

**b)** the probability of at least one success

**c)** the probability of at most one success

**d)** the probability of at least two successes

**35.** Find each of the following probabilities when $n$ independent Bernoulli trials are carried out with probability of success $p$.

**a)** the probability of no failures

**b)** the probability of at least one failure

**c)** the probability of at most one failure

**d)** the probability of at least two failures

**36.** Use mathematical induction to prove that if $E_1, E_2, \ldots, E_n$ is a sequence of $n$ pairwise disjoint events in a sample space $S$, where $n$ is a positive integer, then $p(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} p(E_i)$.

***37.** (*Requires calculus*) Show that if $E_1, E_2, \ldots$ is an infinite sequence of pairwise disjoint events in a sample space $S$, then $p(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} p(E_i)$. [*Hint:* Use Exercise 36 and take limits.]

**38.** A pair of dice is rolled in a remote location and when you ask an honest observer whether at least one die came up six, this honest observer answers in the affirmative.

**a)** What is the probability that the sum of the numbers that came up on the two dice is seven, given the information provided by the honest observer?

**b)** Suppose that the honest observer tells us that at least one die came up five. What is the probability the sum of the numbers that came up on the dice is seven, given this information?

****39.** This exercise employs the probabilistic method to prove a result about round-robin tournaments. In a **round-robin tournament** with $m$ players, every two players play one game in which one player wins and the other loses.

We want to find conditions on positive integers $m$ and $k$ with $k < m$ such that it is possible for the outcomes of the tournament to have the property that for every set of $k$ players, there is a player who beats every member in this set. So that we can use probabilistic reasoning to draw conclusions about round-robin tournaments, we assume that when two players compete it is equally likely that either player wins the game and we assume that the outcomes of different games are independent. Let $E$ be the event that for every set $S$ with $k$ players, where $k$ is a positive integer less than $m$, there is a player who has beaten all $k$ players in $S$.

**a)** Show that $p(\overline{E}) \leq \sum_{j=1}^{\binom{m}{k}} p(F_j)$, where $F_j$ is the event that there is no player who beats all $k$ players from the $j$th set in a list of the $\binom{m}{k}$ sets of $k$ players.

**b)** Show that the probability of $F_j$ is $(1-2^{-k})^{m-k}$.

**c)** Conclude from parts (a) and (b) that $p(\overline{E}) \leq \binom{m}{k}(1-2^{-k})^{m-k}$ and, therefore, that there must be a tournament with the described property if $\binom{m}{k}(1-2^{-k})^{m-k} < 1$.

**d)** Use part (c) to find values of $m$ such that there is a tournament with $m$ players such that for every set $S$ of two players, there is a player who has beaten both players in $S$. Repeat for sets of three players.

***40.** Devise a Monte Carlo algorithm that determines whether a permutation of the integers 1 through $n$ has already been sorted (that is, it is in increasing order), or instead, is a random permutation. A step of the algorithm should answer "true" if it determines the list is not sorted and "unknown" otherwise. After $k$ steps, the algorithm decides that the integers are sorted if the answer is "unknown" in each step. Show that as the number of steps increases, the probability that the algorithm produces an incorrect answer is extremely small. [*Hint:* For each step, test whether certain elements are in the correct order. Make sure these tests are independent.]

**41.** Use pseudocode to write out the probabilistic primality test described in Example 16.

# 7.3 Bayes' Theorem

## Introduction

There are many times when we want to assess the probability that a particular event occurs on the basis of partial evidence. For example, suppose we know the percentage of people who have a particular disease for which there is a very accurate diagnostic test. People who test positive for

this disease would like to know the likelihood that they actually have the disease. In this section we introduce a result that can be used to determine this probability, namely, the probability that a person has the disease given that this person tests positive for it. To use this result, we will need to know the percentage of people who do not have the disease but test positive for it and the percentage of people who have the disease but test negative for it.

Similarly, suppose we know the percentage of incoming e-mail messages that are spam. We will see that we can determine the likelihood that an incoming e-mail message is spam using the occurrence of words in the message. To determine this likelihood, we need to know the percentage of incoming messages that are spam, the percentage of spam messages in which each of these words occurs, and the percentage of messages that are not spam in which each of these words occurs.

The result that we can use to answer questions such as these is called Bayes' theorem and dates back to the eighteenth century. In the past two decades, Bayes' theorem has been extensively applied to estimate probabilities based on partial evidence in areas as diverse as medicine, law, machine learning, engineering, and software development.

## Bayes' Theorem

We illustrate the idea behind Bayes' theorem with an example that shows that when extra information is available, we can derive a more realistic estimate that a particular event occurs. That is, suppose we know $p(F)$, the probability that an event $F$ occurs, but we have knowledge that an event $E$ occurs. Then the conditional probability that $F$ occurs given that $E$ occurs, $p(F \mid E)$, is a more realistic estimate than $p(F)$ that $F$ occurs. In Example 1 we will see that we can find $p(F \mid E)$ when we know $p(F)$, $p(E \mid F)$, and $p(E \mid \overline{F})$.

**EXAMPLE 1** We have two boxes. The first contains two green balls and seven red balls; the second contains four green balls and three red balls. Bob selects a ball by first choosing one of the two boxes at random. He then selects one of the balls in this box at random. If Bob has selected a red ball, what is the probability that he selected a ball from the first box?

*Solution:* Let $E$ be the event that Bob has chosen a red ball; $\overline{E}$ is the event that Bob has chosen a green ball. Let $F$ be the event that Bob has chosen a ball from the first box; $\overline{F}$ is the event that Bob has chosen a ball from the second box. We want to find $p(F \mid E)$, the probability that the ball Bob selected came from the first box, given that it is red. By the definition of conditional probability, we have $p(F \mid E) = p(F \cap E)/p(E)$. Can we use the information provided to determine both $p(F \cap E)$ and $p(E)$ so that we can find $p(F \mid E)$?

First, note that because the first box contains seven red balls out of a total of nine balls, we know that $p(E \mid F) = 7/9$. Similarly, because the second box contains three red balls out of a total of seven balls, we know that $p(E \mid \overline{F}) = 3/7$. We assumed that Bob selects a box at random, so $p(F) = p(\overline{F}) = 1/2$. Because $p(E \mid F) = p(E \cap F)/p(F)$, it follows that $p(E \cap F) = p(E \mid F)p(F) = \frac{7}{9} \cdot \frac{1}{2} = \frac{7}{18}$ [as we remarked earlier, this is one of the quantities we need to find to determine $p(F \mid E)$]. Similarly, because $p(E \mid \overline{F}) = p(E \cap \overline{F})/p(\overline{F})$, it follows that $p(E \cap \overline{F}) = p(E \mid \overline{F})p(\overline{F}) = \frac{3}{7} \cdot \frac{1}{2} = \frac{3}{14}$.

We can now find $p(E)$. Note that $E = (E \cap F) \cup (E \cap \overline{F})$, where $E \cap F$ and $E \cap \overline{F}$ are disjoint sets. (If $x$ belongs to both $E \cap F$ and $E \cap \overline{F}$, then $x$ belongs to both $F$ and $\overline{F}$, which is impossible.) It follows that

$$p(E) = p(E \cap F) + p(E \cap \overline{F}) = \frac{7}{18} + \frac{3}{14} = \frac{49}{126} + \frac{27}{126} = \frac{76}{126} = \frac{38}{63}.$$

We have now found both $p(F \cap E) = 7/18$ and $p(E) = 38/63$. We conclude that

$$p(F \mid E) = \frac{p(F \cap E)}{p(E)} = \frac{7/18}{38/63} = \frac{49}{76} \approx 0.645.$$

Before we had any extra information, we assumed that the probability that Bob selected the first box was 1/2. However, with the extra information that the ball selected at random is red, this probability has increased to approximately 0.645. That is, the probability that Bob selected a ball from the first box increased from 1/2, when no extra information was available, to 0.645 once we knew that the ball selected was red. ◀

Using the same type of reasoning as in Example 1, we can find the conditional probability that an event $F$ occurs, given that an event $E$ has occurred, when we know $p(E \mid F)$, $p(E \mid \overline{F})$, and $p(F)$. The result we can obtain is called **Bayes' theorem**; it is named after Thomas Bayes, an eighteenth-century British mathematician and minister who introduced this result.

**THEOREM 1**

**BAYES' THEOREM** Suppose that $E$ and $F$ are events from a sample space $S$ such that $p(E) \neq 0$ and $p(F) \neq 0$. Then

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}.$$

*Proof:* The definition of conditional probability tells us that $p(F \mid E) = p(E \cap F)/p(E)$ and $p(E \mid F) = p(E \cap F)/p(F)$. Therefore, $p(E \cap F) = p(F \mid E)p(E)$ and $p(E \cap F) = p(E \mid F)p(F)$. Equating these two expressions for $p(E \cap F)$ shows that

$$p(F \mid E)p(E) = p(E \mid F)p(F).$$

Dividing both sides by $p(E)$, we find that

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E)}.$$

Next, we show that $p(E) = p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})$. To see this, first note that $E = E \cap S = E \cap (F \cup \overline{F}) = (E \cap F) \cup (E \cap \overline{F})$. Furthermore, $E \cap F$ and $E \cap \overline{F}$ are disjoint, because if $x \in E \cap F$ and $x \in E \cap \overline{F}$, then $x \in F \cap \overline{F} = \emptyset$. Consequently, $p(E) = p(E \cap F) + p(E \cap \overline{F})$. We have already shown that $p(E \cap F) = p(E \mid F)p(F)$. Moreover, we have $p(E \mid \overline{F}) = p(E \cap \overline{F})/p(\overline{F})$, which shows that $p(E \cap \overline{F}) = p(E \mid \overline{F})p(\overline{F})$. It now follows that

$$p(E) = p(E \cap F) + p(E \cap \overline{F}) = p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F}).$$

To complete the proof we insert this expression for $p(E)$ into the equation $p(F \mid E) = p(E \mid F)p(F)/p(E)$. We have proved that

Links

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}.$$

◁

APPLYING BAYES' THEOREM Bayes' theorem can be used to solve problems that arise in many disciplines. Next, we will discuss an application of Bayes' theorem to medicine. In particular, we will illustrate how Bayes' theorem can be used to assess the probability that someone testing positive for a disease actually has this disease. The results obtained from Bayes' theorem are often somewhat surprising, as Example 2 shows.

**EXAMPLE 2** Suppose that one person in 100,000 has a particular rare disease for which there is a fairly accurate diagnostic test. This test is correct 99.0% of the time when given to a person selected at random who has the disease; it is correct 99.5% of the time when given to a person selected at random who does not have the disease. Given this information can we find

(a) the probability that a person who tests positive for the disease has the disease?

(b) the probability that a person who tests negative for the disease does not have the disease?

Should a person who tests positive be very concerned that he or she has the disease?

*Solution:* (a) Let $F$ be the event that a person selected at random has the disease, and let $E$ be the event that a person selected at random tests positive for the disease. We want to compute $p(F \mid E)$. To use Bayes' theorem to compute $p(F \mid E)$ we need to find $p(E \mid F)$, $p(E \mid \overline{F})$, $p(F)$, and $p(\overline{F})$.

We know that one person in 100,000 has this disease, so $p(F) = 1/100{,}000 = 0.00001$ and $p(\overline{F}) = 1 - 0.00001 = 0.99999$. Because a person who has the disease tests positive 99% of the time, we know that $p(E \mid F) = 0.99$; this is the probability of a true positive, that a person with the disease tests positive. It follows that $p(\overline{E} \mid F) = 1 - p(E \mid F) = 1 - 0.99 = 0.01$; this is the probability of a false negative, that a person who has the disease tests negative.

Furthermore, because a person who does not have the disease tests negative 99.5% of the time, we know that $p(\overline{E} \mid \overline{F}) = 0.995$. This is the probability of a true negative, that a person without the disease tests negative. Finally, we see that $p(E \mid \overline{F}) = 1 - p(\overline{E} \mid \overline{F}) = 1 - 0.995 = 0.005$; this is the probability of a false positive, that a person without the disease tests positive.

The probability that a person who tests positive for the disease actually has the disease is $p(F \mid E)$. By Bayes' theorem, we know that

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}$$

$$= \frac{(0.99)(0.00001)}{(0.99)(0.00001) + (0.005)(0.99999)} \approx 0.002.$$

(b) The probability that someone who tests negative for the disease does not have the disease is $p(\overline{F} \mid \overline{E})$. By Bayes' theorem, we know that

$$p(\overline{F} \mid \overline{E}) = \frac{p(\overline{E} \mid \overline{F})p(\overline{F})}{p(\overline{E} \mid \overline{F})p(\overline{F}) + p(\overline{E} \mid F)p(F)}$$

$$= \frac{(0.995)(0.99999)}{(0.995)(0.99999) + (0.01)(0.00001)} \approx 0.9999999.$$

Consequently, 99.99999% of the people who test negative really do not have the disease.

In part (a) we showed that only 0.2% of people who test positive for the disease actually have the disease. Because the disease is extremely rare, the number of false positives on the diagnostic test is far greater than the number of true positives, making the percentage of people who test positive who actually have the disease extremely small. People who test positive for the diseases should not be overly concerned that they actually have the disease. ◀

**GENERALIZING BAYES' THEOREM** Note that in the statement of Bayes' theorem, the events $F$ and $\overline{F}$ are mutually exclusive and cover the entire sample space $S$ (that is, $F \cup \overline{F} = S$). We can extend Bayes' theorem to any collection of mutually exclusive events that cover the entire sample space $S$, in the following way.

**THEOREM 2**

**GENERALIZED BAYES' THEOREM** Suppose that $E$ is an event from a sample space $S$ and that $F_1, F_2, \ldots, F_n$ are mutually exclusive events such that $\bigcup_{i=1}^{n} F_i = S$. Assume that $p(E) \neq 0$ and $p(F_i) \neq 0$ for $i = 1, 2, \ldots, n$. Then

$$p(F_j \mid E) = \frac{p(E \mid F_j)p(F_j)}{\sum_{i=1}^{n} p(E \mid F_i)p(F_i)}.$$

We leave the proof of this generalized version of Bayes' theorem as Exercise 17.

## Bayesian Spam Filters

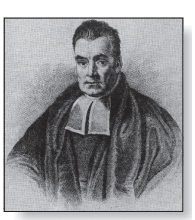
Most electronic mailboxes receive a flood of unwanted and unsolicited messages, known as **spam**. Because spam threatens to overwhelm electronic mail systems, a tremendous amount of work has been devoted to filtering it out. Some of the first tools developed for eliminating spam were based on Bayes' theorem, such as **Bayesian spam filters**.

A Bayesian spam filter uses information about previously seen e-mail messages to guess whether an incoming e-mail message is spam. Bayesian spam filters look for occurrences of particular words in messages. For a particular word $w$, the probability that $w$ appears in a spam e-mail message is estimated by determining the number of times $w$ appears in a message from a large set of messages known to be spam and the number of times it appears in a large set of messages known not to be spam. When we examine e-mail messages to determine whether they might be spam, we look at words that might be indicators of spam, such as "offer," "special," or "opportunity," as well as words that might indicate that a message is not spam, such as "mom," "lunch," or "Jan" (where Jan is one of your friends). Unfortunately, spam filters sometimes fail to identify a spam message as spam; this is called a false negative. And they sometimes identify a message that is not spam as spam; this is called a false positive. When testing for spam, it is important to minimize false positives, because filtering out wanted e-mail is much worse than letting some spam through.

Links

The use of the word *spam* for unsolicited e-mail comes from a Monty Python comedy sketch about a cafe where the food product Spam comes with everything regardless of whether customers want it.

Links



THOMAS BAYES (1702–1761) Thomas Bayes was the son a minister in a religious sect known as the Nonconformists. This sect was considered heretical in eighteenth-century Great Britain. Because of the secrecy of the Nonconformists, little is known of Thomas Bayes' life. When Thomas was young, his family moved to London. Thomas was likely educated privately; Nonconformist children generally did not attend school. In 1719 Bayes entered the University of Edinburgh, where he studied logic and theology. He was ordained as a Nonconformist minister like his father and began his work as a minister assisting his father. In 1733 he became minister of the Presbyterian Chapel in Tunbridge Wells, southeast of London, where he remained minister until 1752.

Bayes is best known for his essay on probability published in 1764, three years after his death. This essay was sent to the Royal Society by a friend who found it in the papers left behind when Bayes died. In the introduction to this essay, Bayes stated that his goal was to find a method that could measure the probability that an event happens, assuming that we know nothing about it, but that, under the same circumstances, it has happened a certain proportion of times. Bayes' conclusions were accepted by the great French mathematician Laplace but were later challenged by Boole, who questioned them in his book *Laws of Thought*. Since then Bayes' techniques have been subject to controversy.

Bayes also wrote an article that was published posthumously: "An Introduction to the Doctrine of Fluxions, and a Defense of the Mathematicians Against the Objections of the Author of The Analyst," which supported the logical foundations of calculus. Bayes was elected a Fellow of the Royal Society in 1742, with the support of important members of the Society, even though at that time he had no published mathematical works. Bayes' sole known publication during his lifetime was allegedly a mystical book entitled *Divine Benevolence*, discussing the original causation and ultimate purpose of the universe. Although the book is commonly attributed to Bayes, no author's name appeared on the title page, and the entire work is thought to be of dubious provenance. Evidence for Bayes' mathematical talents comes from a notebook that was almost certainly written by Bayes, which contains much mathematical work, including discussions of probability, trigonometry, geometry, solutions of equations, series, and differential calculus. There are also sections on natural philosophy, in which Bayes looks at topics that include electricity, optics, and celestial mechanics. Bayes is also the author of a mathematical publication on asymptotic series, which appeared after his death.

We will develop some basic Bayesian spam filters. First, suppose we have a set $B$ of messages known to be spam and a set $G$ of messages known not to be spam. (For example, users could classify messages as spam when they examine them in their inboxes.) We next identify the words that occur in $B$ and in $G$. We count the number of messages in the set containing each word to find $n_B(w)$ and $n_G(w)$, the number of messages containing the word $w$ in the sets $B$ and $G$, respectively. Then, the empirical probability that a spam message contains the word $w$ is $p(w) = n_B(w)/|B|$, and the empirical probability that a message that is not spam contains the word $w$ is $q(w) = n_G(w)/|G|$. We note that $p(w)$ and $q(w)$ estimate the probabilities that an incoming spam message, and an incoming message that is not spam, contain the word $w$, respectively.

Now suppose we receive a new e-mail message containing the word $w$. Let $S$ be the event that the message is spam. Let $E$ be the event that the message contains the word $w$. The events $S$, that the message is spam, and $\overline{S}$, that the message is not spam, partition the set of all messages. Hence, by Bayes' theorem, the probability that the message is spam, given that it contains the word $w$, is

$$p(S \mid E) = \frac{p(E \mid S)p(S)}{p(E \mid S)p(S) + p(E \mid \overline{S})p(\overline{S})}.$$

To apply this formula, we first estimate $p(S)$, the probability that an incoming message is spam, as well as $p(\overline{S})$, the probability that the incoming message is not spam. Without prior knowledge about the likelihood that an incoming message is spam, for simplicity we assume that the message is equally likely to be spam as it is not to be spam. That is, we assume that $p(S) = p(\overline{S}) = 1/2$. Using this assumption, we find that the probability that a message is spam, given that it contains the word $w$, is

$$p(S \mid E) = \frac{p(E \mid S)}{p(E \mid S) + p(E \mid \overline{S})}.$$

(Note that if we have some empirical data about the ratio of spam messages to messages that are not spam, we can change this assumption to produce a better estimate for $p(S)$ and for $p(\overline{S})$; see Exercise 22.)

Next, we estimate $p(E \mid S)$, the conditional probability that the message contains the word $w$ given that the message is spam, by $p(w)$. Similarly, we estimate $p(E \mid \overline{S})$, the conditional probability that the message contains the word $w$, given that the message is not spam, by $q(w)$. Inserting these estimates for $p(E \mid S)$ and $p(E \mid \overline{S})$ tells us that $p(S \mid E)$ can be estimated by

$$r(w) = \frac{p(w)}{p(w) + q(w)};$$

that is, $r(w)$ estimates the probability that the message is spam, given that it contains the word $w$. If $r(w)$ is greater than a threshold that we set, such as 0.9, then we classify the message as spam.

**EXAMPLE 3** Suppose that we have found that the word "Rolex" occurs in 250 of 2000 messages known to be spam and in 5 of 1000 messages known not to be spam. Estimate the probability that an incoming message containing the word "Rolex" is spam, assuming that it is equally likely that an incoming message is spam or not spam. If our threshold for rejecting a message as spam is 0.9, will we reject such messages?

*Solution:* We use the counts that the word "Rolex" appears in spam messages and messages that are not spam to find that $p(\text{Rolex}) = 250/2000 = 0.125$ and $q(\text{Rolex}) = 5/1000 = 0.005$.

Because we are assuming that it is equally likely for an incoming message to be spam as it is not to be spam, we can estimate the probability that an incoming message containing the word "Rolex" is spam by

$$r(\text{Rolex}) = \frac{p(\text{Rolex})}{p(\text{Rolex}) + q(\text{Rolex})} = \frac{0.125}{0.125 + 0.005} = \frac{0.125}{0.130} \approx 0.962.$$

Because $r(\text{Rolex})$ is greater than the threshold 0.9, we reject such messages as spam. ◀

Detecting spam based on the presence of a single word can lead to excessive false positives and false negatives. Consequently, spam filters look at the presence of multiple words. For example, suppose that the message contains the words $w_1$ and $w_2$. Let $E_1$ and $E_2$ denote the events that the message contains the words $w_1$ and $w_2$, respectively. To make our computations simpler, we assume that $E_1$ and $E_2$ are independent events and that $E_1 \mid S$ and $E_2 \mid S$ are independent events and that we have no prior knowledge regarding whether or not the message is spam. (The assumptions that $E_1$ and $E_2$ are independent and that $E_1 \mid S$ and $E_2 \mid S$ are independent may introduce some error into our computations; we assume that this error is small.) Using Bayes' theorem and our assumptions, we can show (see Exercise 23) that $p(S \mid E_1 \cap E_2)$, the probability that the message is spam given that it contains both $w_1$ and $w_2$, is

$$p(S \mid E_1 \cap E_2) = \frac{p(E_1 \mid S)p(E_2 \mid S)}{p(E_1 \mid S)p(E_2 \mid S) + p(E_1 \mid \overline{S})p(E_2 \mid \overline{S})}.$$

We estimate the probability $p(S \mid E_1 \cap E_2)$ by

$$r(w_1, w_2) = \frac{p(w_1)p(w_2)}{p(w_1)p(w_2) + q(w_1)q(w_2)}.$$

That is, $r(w_1, w_2)$ estimates the probability that the message is spam, given that it contains the words $w_1$ and $w_2$. When $r(w_1, w_2)$ is greater than a preset threshold, such as 0.9, we determine that the message is likely spam.

**EXAMPLE 4** Suppose that we train a Bayesian spam filter on a set of 2000 spam messages and 1000 messages that are not spam. The word "stock" appears in 400 spam messages and 60 messages that are not spam, and the word "undervalued" appears in 200 spam messages and 25 messages that are not spam. Estimate the probability that an incoming message containing both the words "stock" and "undervalued" is spam, assuming that we have no prior knowledge about whether it is spam. Will we reject such messages as spam when we set the threshold at 0.9?

*Solution:* Using the counts of each of these two words in messages known to be spam or known not to be spam, we obtain the following estimates: $p(\text{stock}) = 400/2000 = 0.2$, $q(\text{stock}) = 60/1000 = 0.06$, $p(\text{undervalued}) = 200/2000 = 0.1$, and $q(\text{undervalued}) = 25/1000 = 0.025$. Using these probabilities, we can estimate the probability that the message is spam by

$$r(\text{stock}, \text{undervalued}) = \frac{p(\text{stock})p(\text{undervalued})}{p(\text{stock})p(\text{undervalued}) + q(\text{stock})q(\text{undervalued})}$$

$$= \frac{(0.2)(0.1)}{(0.2)(0.1) + (0.06)(0.025)} \approx 0.930.$$

Because we have set the threshold for rejecting messages at 0.9, such messages will be rejected by the filter. ◀

The more words we use to estimate the probability that an incoming mail message is spam, the better is our chance that we correctly determine whether it is spam. In general, if $E_i$ is the

event that the message contains word $w_i$, assuming that the number of incoming spam messages is approximately the same as the number of incoming messages that are not spam, and that the events $E_i \mid S$ are independent, then by Bayes' theorem the probability that a message containing all the words $w_1, w_2, \ldots, w_k$ is spam is

$$p(S \mid \bigcap_{i=1}^{k} E_i) = \frac{\prod_{i=1}^{k} p(E_i \mid S)}{\prod_{i=1}^{k} p(E_i \mid S) + \prod_{i=1}^{k} p(E_i \mid \overline{S})}.$$

We can estimate this probability by

$$r(w_1, w_2, \ldots, w_k) = \frac{\prod_{i=1}^{k} p(w_i)}{\prod_{i=1}^{k} p(w_i) + \prod_{i=1}^{k} q(w_i)}.$$

For the most effective spam filter, we choose words for which the probability that each of these words appears in spam is either very high or very low. When we compute this value for a particular message, we reject the message as spam if $r(w_1, w_2, \ldots, w_k)$ exceeds a preset threshold, such as 0.9.

*Bayesian poisoning*, the insertion of extra words to defeat spam filters, can use random or purposefully selected words.

Another way to improve the performance of a Bayesian spam filter is to look at the probabilities that particular pairs of words appear in spam and in messages that are not spam. We then treat appearances of these pairs of words as appearance of a single block, rather than as the appearance of two separate words. For example, the pair of words "enhance performance" most likely indicates spam, while "operatic performance" indicates a message that is not spam. Similarly, we can assess the likelihood that a message is spam by examining the structure of a message to determine where words appear in it. Also, spam filters look at appearances of certain types of strings of characters rather than just words. For example, a message with the valid e-mail address of one of your friends is less likely to be spam (if not sent by a worm) than one containing an e-mail address that came from a country known to originate a lot of spam. There is an ongoing war between people who create spam and those trying to filter their messages out. This leads to the introduction of many new techniques to defeat spam filters, including inserting into spam messages long strings of words that appear in messages that are not spam, as well as including words inside pictures. The techniques we have discussed here are only the first steps in fighting this war on spam.

## Exercises

**1.** Suppose that $E$ and $F$ are events in a sample space and $p(E) = 1/3$, $p(F) = 1/2$, and $p(E \mid F) = 2/5$. Find $p(F \mid E)$.

**2.** Suppose that $E$ and $F$ are events in a sample space and $p(E) = 2/3$, $p(F) = 3/4$, and $p(F \mid E) = 5/8$. Find $p(E \mid F)$.

**3.** Suppose that Frida selects a ball by first picking one of two boxes at random and then selecting a ball from this box at random. The first box contains two white balls and three blue balls, and the second box contains four white balls and one blue ball. What is the probability that Frida picked a ball from the first box if she has selected a blue ball?

**4.** Suppose that Ann selects a ball by first picking one of two boxes at random and then selecting a ball from this box. The first box contains three orange balls and four black balls, and the second box contains five orange balls and six black balls. What is the probability that Ann picked a ball from the second box if she has selected an orange ball?

**5.** Suppose that 8% of all bicycle racers use steroids, that a bicyclist who uses steroids tests positive for steroids 96% of the time, and that a bicyclist who does not use steroids tests positive for steroids 9% of the time. What is the probability that a randomly selected bicyclist who tests positive for steroids actually uses steroids?

**6.** When a test for steroids is given to soccer players, 98% of the players taking steroids test positive and 12% of the players not taking steroids test positive. Suppose that 5% of soccer players take steroids. What is the probability that a soccer player who tests positive takes steroids?

**7.** Suppose that a test for opium use has a 2% false positive rate and a 5% false negative rate. That is, 2% of people who do not use opium test positive for opium, and

5% of opium users test negative for opium. Furthermore, suppose that 1% of people actually use opium.

**a)** Find the probability that someone who tests negative for opium use does not use opium.

**b)** Find the probability that someone who tests positive for opium use actually uses opium.

**8.** Suppose that one person in 10,000 people has a rare genetic disease. There is an excellent test for the disease; 99.9% of people with the disease test positive and only 0.02% who do not have the disease test positive.

**a)** What is the probability that someone who tests positive has the genetic disease?

**b)** What is the probability that someone who tests negative does not have the disease?

**9.** Suppose that 8% of the patients tested in a clinic are infected with HIV. Furthermore, suppose that when a blood test for HIV is given, 98% of the patients infected with HIV test positive and that 3% of the patients not infected with HIV test positive. What is the probability that

**a)** a patient testing positive for HIV with this test is infected with it?

**b)** a patient testing positive for HIV with this test is not infected with it?

**c)** a patient testing negative for HIV with this test is infected with it?

**d)** a patient testing negative for HIV with this test is not infected with it?

**10.** Suppose that 4% of the patients tested in a clinic are infected with avian influenza. Furthermore, suppose that when a blood test for avian influenza is given, 97% of the patients infected with avian influenza test positive and that 2% of the patients not infected with avian influenza test positive. What is the probability that

**a)** a patient testing positive for avian influenza with this test is infected with it?

**b)** a patient testing positive for avian influenza with this test is not infected with it?

**c)** a patient testing negative for avian influenza with this test is infected with it?

**d)** a patient testing negative for avian influenza with this test is not infected with it?

**11.** An electronics company is planning to introduce a new camera phone. The company commissions a marketing report for each new product that predicts either the success or the failure of the product. Of new products introduced by the company, 60% have been successes. Furthermore, 70% of their successful products were predicted to be successes, while 40% of failed products were predicted to be successes. Find the probability that this new camera phone will be successful if its success has been predicted.

***12.** A space probe near Neptune communicates with Earth using bit strings. Suppose that in its transmissions it sends a 1 one-third of the time and a 0 two-thirds of the time. When a 0 is sent, the probability that it is received correctly is 0.9, and the probability that it is received incorrectly (as a 1) is 0.1. When a 1 is sent, the probability that it is received correctly is 0.8, and the probability that it is received incorrectly (as a 0) is 0.2.

**a)** Find the probability that a 0 is received.

**b)** Use Bayes' theorem to find the probability that a 0 was transmitted, given that a 0 was received.

**13.** Suppose that $E$, $F_1$, $F_2$, and $F_3$ are events from a sample space $S$ and that $F_1$, $F_2$, and $F_3$ are pairwise disjoint and their union is $S$. Find $p(F_1 \mid E)$ if $p(E \mid F_1) = 1/8$, $p(E \mid F_2) = 1/4$, $p(E \mid F_3) = 1/6$, $p(F_1) = 1/4$, $p(F_2) = 1/4$, and $p(F_3) = 1/2$.

**14.** Suppose that $E$, $F_1$, $F_2$, and $F_3$ are events from a sample space $S$ and that $F_1$, $F_2$, and $F_3$ are pairwise disjoint and their union is $S$. Find $p(F_2 \mid E)$ if $p(E \mid F_1) = 2/7$, $p(E \mid F_2) = 3/8$, $p(E \mid F_3) = 1/2$, $p(F_1) = 1/6$, $p(F_2) = 1/2$, and $p(F_3) = 1/3$.

**15.** In this exercise we will use Bayes' theorem to solve the Monty Hall puzzle (Example 10 in Section 7.1). Recall that in this puzzle you are asked to select one of three doors to open. There is a large prize behind one of the three doors and the other two doors are losers. After you select a door, Monty Hall opens one of the two doors you did not select that he knows is a losing door, selecting at random if both are losing doors. Monty asks you whether you would like to switch doors. Suppose that the three doors in the puzzle are labeled 1, 2, and 3. Let $W$ be the random variable whose value is the number of the winning door; assume that $p(W = k) = 1/3$ for $k = 1, 2, 3$. Let $M$ denote the random variable whose value is the number of the door that Monty opens. Suppose you choose door $i$.

**a)** What is the probability that you will win the prize if the game ends without Monty asking you whether you want to change doors?

**b)** Find $p(M = j \mid W = k)$ for $j = 1, 2, 3$ and $k = 1, 2, 3$.

**c)** Use Bayes' theorem to find $p(W = j \mid M = k)$ where $i$ and $j$ and $k$ are distinct values.

**d)** Explain why the answer to part (c) tells you whether you should change doors when Monty gives you the chance to do so.

**16.** Ramesh can get to work in three different ways: by bicycle, by car, or by bus. Because of commuter traffic, there is a 50% chance that he will be late when he drives his car. When he takes the bus, which uses a special lane reserved for buses, there is a 20% chance that he will be late. The probability that he is late when he rides his bicycle is only 5%. Ramesh arrives late one day. His boss wants to estimate the probability that he drove his car to work that day.

**a)** Suppose the boss assumes that there is a 1/3 chance that Ramesh takes each of the three ways he can get to work. What estimate for the probability that Ramesh drove his car does the boss obtain from Bayes' theorem under this assumption?

**b)** Suppose the boss knows that Ramesh drives 30% of the time, takes the bus only 10% of the time, and takes his bicycle 60% of the time. What estimate for the probability that Ramesh drove his car does the boss obtain from Bayes' theorem using this information?

***17.** Prove Theorem 2, the extended form of Bayes' theorem. That is, suppose that $E$ is an event from a sample space $S$ and that $F_1, F_2, \ldots, F_n$ are mutually exclusive events such that $\bigcup_{i=1}^{n} F_i = S$. Assume that $p(E) \neq 0$ and $p(F_i) \neq 0$ for $i = 1, 2, \ldots, n$. Show that

$$p(F_j \mid E) = \frac{p(E \mid F_j)p(F_j)}{\sum_{i=1}^{n} p(E \mid F_i)p(F_i)}.$$

[*Hint:* Use the fact that $E = \bigcup_{i=1}^{n}(E \cap F_i)$.]

**18.** Suppose that a Bayesian spam filter is trained on a set of 500 spam messages and 200 messages that are not spam. The word "exciting" appears in 40 spam messages and in 25 messages that are not spam. Would an incoming message be rejected as spam if it contains the word "exciting" and the threshold for rejecting spam is 0.9?

**19.** Suppose that a Bayesian spam filter is trained on a set of 1000 spam messages and 400 messages that are not spam. The word "opportunity" appears in 175 spam messages and 20 messages that are not spam. Would an incoming message be rejected as spam if it contains the word "opportunity" and the threshold for rejecting a message is 0.9?

**20.** Would we reject a message as spam in Example 4

**a)** using just the fact that the word "undervalued" occurs in the message?

**b)** using just the fact that the word "stock" occurs in the message?

**21.** Suppose that a Bayesian spam filter is trained on a set of 10,000 spam messages and 5000 messages that are not spam. The word "enhancement" appears in 1500 spam messages and 20 messages that are not spam, while the word "herbal" appears in 800 spam messages and 200 messages that are not spam. Estimate the probability that a received message containing both the words "enhancement" and "herbal" is spam. Will the message be rejected as spam if the threshold for rejecting spam is 0.9?

**22.** Suppose that we have prior information concerning whether a random incoming message is spam. In particular, suppose that over a time period, we find that $s$ spam messages arrive and $h$ messages arrive that are not spam.

**a)** Use this information to estimate $p(S)$, the probability that an incoming message is spam, and $p(\overline{S})$, the probability an incoming message is not spam.

**b)** Use Bayes' theorem and part (a) to estimate the probability that an incoming message containing the word $w$ is spam, where $p(w)$ is the probability that $w$ occurs in a spam message and $q(w)$ is the probability that $w$ occurs in a message that is not spam.

**23.** Suppose that $E_1$ and $E_2$ are the events that an incoming mail message contains the words $w_1$ and $w_2$, respectively. Assuming that $E_1$ and $E_2$ are independent events and that $E_1 \mid S$ and $E_2 \mid S$ are independent events, where $S$ is the event that an incoming message is spam, and that we have no prior knowledge regarding whether or not the message is spam, show that

$$p(S \mid E_1 \cap E_2) = \frac{p(E_1 \mid S)p(E_2 \mid S)}{p(E_1 \mid S)p(E_2 \mid S) + p(E_1 \mid \overline{S})p(E_2 \mid \overline{S})}.$$

# 7.4 Expected Value and Variance

## Introduction

The **expected value** of a random variable is the sum over all elements in a sample space of the product of the probability of the element and the value of the random variable at this element. Consequently, the expected value is a weighted average of the values of a random variable. The expected value of a random variable provides a central point for the distribution of values of this random variable. We can solve many problems using the notion of the expected value of a random variable, such as determining who has an advantage in gambling games and computing the average-case complexity of algorithms. Another useful measure of a random variable is its **variance**, which tells us how spread out the values of this random variable are. We can use the variance of a random variable to help us estimate the probability that a random variable takes values far removed from its expected value.

## Expected Values


Many questions can be formulated in terms of the value we expect a random variable to take, or more precisely, the average value of a random variable when an experiment is performed a large number of times. Questions of this kind include: How many heads are expected to appear

when a coin is flipped 100 times? What is the expected number of comparisons used to find an element in a list using a linear search? To study such questions we introduce the concept of the expected value of a random variable.

**DEFINITION 1**

The *expected value*, also called the *expectation* or *mean*, of the random variable $X$ on the sample space $S$ is equal to

$$E(X) = \sum_{s \in S} p(s)X(s).$$

The *deviation* of $X$ at $s \in S$ is $X(s) - E(X)$, the difference between the value of $X$ and the mean of $X$.

Note that when the sample space $S$ has $n$ elements $S = \{x_1, x_2, \ldots, x_n\}$, $E(X) = \sum_{i=1}^{n} p(x_i)X(x_i)$.

***Remark:*** When there are infinitely many elements of the sample space, the expectation is defined only when the infinite series in the definition is absolutely convergent. In particular, the expectation of a random variable on an infinite sample space is finite if it exists.

**EXAMPLE 1** **Expected Value of a Die** Let $X$ be the number that comes up when a fair die is rolled. What is the expected value of $X$?

*Solution:* The random variable $X$ takes the values 1, 2, 3, 4, 5, or 6, each with probability 1/6. It follows that

$$E(X) = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \frac{1}{6} \cdot 4 + \frac{1}{6} \cdot 5 + \frac{1}{6} \cdot 6 = \frac{21}{6} = \frac{7}{2}.$$ ◀

**EXAMPLE 2** A fair coin is flipped three times. Let $S$ be the sample space of the eight possible outcomes, and let $X$ be the random variable that assigns to an outcome the number of heads in this outcome. What is the expected value of $X$?

Extra Examples

*Solution:* In Example 10 of Section 7.2 we listed the values of $X$ for the eight possible outcomes when a coin is flipped three times. Because the coin is fair and the flips are independent, the probability of each outcome is 1/8. Consequently,

$$\begin{aligned} E(X) &= \frac{1}{8}[X(HHH) + X(HHT) + X(HTH) + X(THH) + X(TTH) \\ &\quad + X(THT) + X(HTT) + X(TTT)] \\ &= \frac{1}{8}(3 + 2 + 2 + 2 + 1 + 1 + 1 + 0) = \frac{12}{8} \\ &= \frac{3}{2}. \end{aligned}$$

Consequently, the expected number of heads that come up when a fair coin is flipped three times is 3/2. ◀

When an experiment has relatively few outcomes, we can compute the expected value of a random variable directly from its definition, as was done in Example 2. However, when an experiment has a large number of outcomes, it may be inconvenient to compute the expected value of a random variable directly from its definition. Instead, we can find the expected value

of a random variable by grouping together all outcomes assigned the same value by the random variable, as Theorem 1 shows.

**THEOREM 1**

If $X$ is a random variable and $p(X = r)$ is the probability that $X = r$, so that $p(X = r) = \sum_{s \in S, X(s)=r} p(s)$, then

$$E(X) = \sum_{r \in X(S)} p(X = r)r.$$

*Proof:* Suppose that $X$ is a random variable with range $X(S)$, and let $p(X = r)$ be the probability that the random variable $X$ takes the value $r$. Consequently, $p(X = r)$ is the sum of the probabilities of the outcomes $s$ such that $X(s) = r$. It follows that

$$E(X) = \sum_{r \in X(S)} p(X = r)r.$$

◁

Example 3 and the proof of Theorem 2 will illustrate the use of this formula. In Example 3 we will find the expected value of the sum of the numbers that appear on two fair dice when they are rolled. In Theorem 2 we will find the expected value of the number of successes when $n$ Bernoulli trials are performed.

**EXAMPLE 3** What is the expected value of the sum of the numbers that appear when a pair of fair dice is rolled?

*Solution:* Let $X$ be the random variable equal to the sum of the numbers that appear when a pair of dice is rolled. In Example 12 of Section 7.2 we listed the value of $X$ for the 36 outcomes of this experiment. The range of $X$ is $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. By Example 12 of Section 7.2 we see that

$$\begin{aligned}
&p(X = 2) = p(X = 12) = 1/36,\\
&p(X = 3) = p(X = 11) = 2/36 = 1/18,\\
&p(X = 4) = p(X = 10) = 3/36 = 1/12,\\
&p(X = 5) = p(X = 9) = 4/36 = 1/9,\\
&p(X = 6) = p(X = 8) = 5/36,\\
&p(X = 7) = 6/36 = 1/6.
\end{aligned}$$

Substituting these values in the formula, we have

$$\begin{aligned}
E(X) &= 2 \cdot \frac{1}{36} + 3 \cdot \frac{1}{18} + 4 \cdot \frac{1}{12} + 5 \cdot \frac{1}{9} + 6 \cdot \frac{5}{36} + 7 \cdot \frac{1}{6}\\
&\quad + 8 \cdot \frac{5}{36} + 9 \cdot \frac{1}{9} + 10 \cdot \frac{1}{12} + 11 \cdot \frac{1}{18} + 12 \cdot \frac{1}{36}\\
&= 7.
\end{aligned}$$

◀

**THEOREM 2**

The expected number of successes when $n$ mutually independent Bernoulli trials are performed, where $p$ is the probability of success on each trial, is $np$.

*Proof:* Let $X$ be the random variable equal to the number of successes in $n$ trials. By Theorem 2 of Section 7.2 we see that $p(X = k) = C(n, k)p^k q^{n-k}$. Hence, we have

$$\begin{aligned}
E(X) &= \sum_{k=1}^{n} kp(X = k) && \text{by Theorem 1}\\
&= \sum_{k=1}^{n} kC(n, k)p^k q^{n-k} && \text{by Theorem 2 in Section 7.2}\\
&= \sum_{k=1}^{n} nC(n-1, k-1)p^k q^{n-k} && \text{by Exercise 21 in Section 6.4}\\
&= np \sum_{k=1}^{n} C(n-1, k-1)p^{k-1} q^{n-k} && \text{factoring } np \text{ from each term}\\
&= np \sum_{j=0}^{n-1} C(n-1, j)p^j q^{n-1-j} && \text{shifting index of summation with } j = k-1\\
&= np(p+q)^{n-1} && \text{by the binomial theorem}\\
&= np. && \text{because } p + q = 1
\end{aligned}$$

This completes the proof because it shows that the expected number of successes in $n$ mutually independent Bernoulli trials is $np$. ◁

We will also show that the hypothesis that the Bernoulli trials are mutually independent in Theorem 2 is not necessary.

## Linearity of Expectations

Theorem 3 tells us that expected values are linear. For example, the expected value of the sum of random variables is the sum of their expected values. We will find this property exceedingly useful.

**THEOREM 3**

If $X_i$, $i = 1, 2, \ldots, n$ with $n$ a positive integer, are random variables on $S$, and if $a$ and $b$ are real numbers, then

(*i*) $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$

(*ii*) $E(aX + b) = aE(X) + b$.

*Proof:* Part *(i)* follows for $n = 2$ directly from the definition of expected value, because

$$\begin{aligned}
E(X_1 + X_2) &= \sum_{s \in S} p(s)(X_1(s) + X_2(s))\\
&= \sum_{s \in S} p(s)X_1(s) + \sum_{s \in S} p(s)X_2(s)\\
&= E(X_1) + E(X_2).
\end{aligned}$$

The case for $n$ random variables follows easily by mathematical induction using the case of two random variables. (We leave it to the reader to complete the proof.)

To prove part *(ii)*, note that

$$\begin{aligned} E(aX+b) &= \textstyle\sum_{s\in S} p(s)(aX(s)+b) \\ &= a\textstyle\sum_{s\in S} p(s)X(s) + b\sum_{s\in S} p(s) \\ &= aE(X) + b \text{ because } \textstyle\sum_{s\in S} p(s) = 1. \end{aligned}$$

◁

Examples 4 and 5 illustrate how to use Theorem 3.

**EXAMPLE 4** Use Theorem 3 to find the expected value of the sum of the numbers that appear when a pair of fair dice is rolled. (This was done in Example 3 without the benefit of this theorem.)

*Solution:* Let $X_1$ and $X_2$ be the random variables with $X_1((i, j)) = i$ and $X_2((i, j)) = j$, so that $X_1$ is the number appearing on the first die and $X_2$ is the number appearing on the second die. It is easy to see that $E(X_1) = E(X_2) = 7/2$ because both equal $(1 + 2 + 3 + 4 + 5 + 6)/6 = 21/6 = 7/2$. The sum of the two numbers that appear when the two dice are rolled is the sum $X_1 + X_2$. By Theorem 3, the expected value of the sum is $E(X_1 + X_2) = E(X_1) + E(X_2) = 7/2 + 7/2 = 7$. ◀

**EXAMPLE 5** In the proof of Theorem 2 we found the expected value of the number of successes when $n$ independent Bernoulli trials are performed, where $p$ is the probability of success on each trial by direct computation. Show how Theorem 3 can be used to derive this result where the Bernoulli trials are not necessarily independent.

*Solution:* Let $X_i$ be the random variable with $X_i((t_1, t_2, \ldots, t_n)) = 1$ if $t_i$ is a success and $X_i((t_1, t_2, \ldots, t_n)) = 0$ if $t_i$ is a failure. The expected value of $X_i$ is $E(X_i) = 1 \cdot p + 0 \cdot (1 - p) = p$ for $i = 1, 2, \ldots, n$. Let $X = X_1 + X_2 + \cdots + X_n$, so that $X$ counts the number of successes when these $n$ Bernoulli trials are performed. Theorem 3, applied to the sum of $n$ random variables, shows that $E(X) = E(X_1) + E(X_2) + \cdots + E(X_n) = np$. ◀

We can take advantage of the linearity of expectations to find the solutions of many seemingly difficult problems. The key step is to express a random variable whose expectation we wish to find as the sum of random variables whose expectations are easy to find. Examples 6 and 7 illustrate this technique.

**EXAMPLE 6** **Expected Value in the Hatcheck Problem** A new employee checks the hats of $n$ people at a restaurant, forgetting to put claim check numbers on the hats. When customers return for their hats, the checker gives them back hats chosen at random from the remaining hats. What is the expected number of hats that are returned correctly?

*Solution:* Let $X$ be the random variable that equals the number of people who receive the correct hat from the checker. Let $X_i$ be the random variable with $X_i = 1$ if the $i$th person receives the correct hat and $X_i = 0$ otherwise. It follows that

$$X = X_1 + X_2 + \cdots + X_n.$$

Because it is equally likely that the checker returns any of the hats to this person, it follows that the probability that the $i$th person receives the correct hat is $1/n$. Consequently, by Theorem 1, for all $i$ we have

$$E(X_i) = 1 \cdot p(X_i = 1) + 0 \cdot p(X_i = 0) = 1 \cdot 1/n + 0 = 1/n.$$

By the linearity of expectations (Theorem 3), it follows that

$$E(X) = E(X_1) + E(X_2) + \cdots + E(X_n) = n \cdot 1/n = 1.$$

Consequently, the average number of people who receive the correct hat is exactly 1. Note that this answer is independent of the number of people who have checked their hats! (We will find an explicit formula for the probability that no one receives the correct hat in Example 4 of Section 8.6.) ◀

**EXAMPLE 7** **Expected Number of Inversions in a Permutation** The ordered pair $(i, j)$ is called an **inversion** in a permutation of the first $n$ positive integers if $i < j$ but $j$ precedes $i$ in the permutation. For instance, there are six inversions in the permutation 3, 5, 1, 4, 2; these inversions are

$$(1, 3), (1, 5), (2, 3), (2, 4), (2, 5), (4, 5).$$

Let $I_{i,j}$ be the random variable on the set of all permutations of the first $n$ positive integers with $I_{i,j} = 1$ if $(i, j)$ is an inversion of the permutation and $I_{i,j} = 0$ otherwise. It follows that if $X$ is the random variable equal to the number of inversions in the permutation, then

$$X = \sum_{1 \le i < j \le n} I_{i,j}.$$

Note that it is equally likely for $i$ to precede $j$ in a randomly chosen permutation as it is for $j$ to precede $i$. (To see this, note that there are an equal number of permutations with each of these properties.) Consequently, for all pairs $i$ and $j$ we have

$$E(I_{i,j}) = 1 \cdot p(I_{i,j} = 1) + 0 \cdot p(I_{i,j} = 0) = 1 \cdot 1/2 + 0 = 1/2.$$

Because there are $\binom{n}{2}$ pairs $i$ and $j$ with $1 \le i < j \le n$ and by the linearity of expectations (Theorem 3), we have

$$E(X) = \sum_{1 \le i < j \le n} E(I_{i,j}) = \binom{n}{2} \cdot \frac{1}{2} = \frac{n(n-1)}{4}.$$

It follows that there are an average of $n(n-1)/4$ inversions in a permutation of the first $n$ positive integers. ◀

## Average-Case Computational Complexity


Computing the average-case computational complexity of an algorithm can be interpreted as computing the expected value of a random variable. Let the sample space of an experiment be the set of possible inputs $a_j$, $j = 1, 2, \ldots, n$, and let $X$ be the random variable that assigns to $a_j$ the number of operations used by the algorithm when given $a_j$ as input. Based on our knowledge of the input, we assign a probability $p(a_j)$ to each possible input value $a_j$. Then, the average-case complexity of the algorithm is

$$E(X) = \sum_{j=1}^{n} p(a_j) X(a_j).$$

This is the expected value of $X$.

Finding the average-case computational complexity of an algorithm is usually much more difficult than finding its worst-case computational complexity, and often involves the use of sophisticated methods. However, there are some algorithms for which the analysis required to find the average-case computational complexity is not difficult. For instance, in Example 8 we will illustrate how to find the average-case computational complexity of the linear search algorithm under different assumptions concerning the probability that the element for which we search is an element of the list.

**EXAMPLE 8** **Average-Case Complexity of the Linear Search Algorithm** We are given a real number $x$ and a list of $n$ distinct real numbers. The linear search algorithm, described in Section 3.1, locates $x$ by successively comparing it to each element in the list, terminating when $x$ is located or when all the elements have been examined and it has been determined that $x$ is not in the list. What is the average-case computational complexity of the linear search algorithm if the probability that $x$ is in the list is $p$ and it is equally likely that $x$ is any of the $n$ elements in the list? (There are $n + 1$ possible types of input: one type for each of the $n$ numbers in the list and a last type for numbers not in the list, which we treat as a single input.)

*Solution:* In Example 4 of Section 3.3 we showed that $2i + 1$ comparisons are used if $x$ equals the $i$th element of the list and, in Example 2 of Section 3.3, we showed that $2n + 2$ comparisons are used if $x$ is not in the list. The probability that $x$ equals $a_i$, the $i$th element in the list, is $p/n$, and the probability that $x$ is not in the list is $q = 1 - p$. It follows that the average-case computational complexity of the linear search algorithm is

$$\begin{aligned} E &= \frac{3p}{n} + \frac{5p}{n} + \cdots + \frac{(2n+1)p}{n} + (2n+2)q \\ &= \frac{p}{n}(3 + 5 + \cdots + (2n+1)) + (2n+2)q \\ &= \frac{p}{n}((n+1)^2 - 1) + (2n+2)q \\ &= p(n+2) + (2n+2)q. \end{aligned}$$

(The third equality follows from Example 2 of Section 5.1.) For instance, when $x$ is guaranteed to be in the list, we have $p = 1$ (so the probability that $x = a_i$ is $1/n$ for each $i$) and $q = 0$. Then $E = n + 2$, as we showed in Example 4 in Section 3.3.

When $p$, the probability that $x$ is in the list, is $1/2$, it follows that $q = 1 - p = 1/2$, so $E = (n + 2)/2 + n + 1 = (3n + 4)/2$. Similarly, if the probability that $x$ is in the list is $3/4$, we have $p = 3/4$ and $q = 1/4$, so $E = 3(n + 2)/4 + (n + 1)/2 = (5n + 8)/4$.

Finally, when $x$ is guaranteed not to be in the list, we have $p = 0$ and $q = 1$. It follows that $E = 2n + 2$, which is not surprising because we have to search the entire list. ◀

Example 9 illustrates how the linearity of expectations can help us find the average-case complexity of a sorting algorithm, the insertion sort.

**EXAMPLE 9** **Average-Case Complexity of the Insertion Sort** What is the average number of comparisons used by the insertion sort to sort $n$ distinct elements?

*Solution:* We first suppose that $X$ is the random variable equal to the number of comparisons used by the insertion sort (described in Section 3.1) to sort a list $a_1, a_2, \ldots, a_n$ of $n$ distinct elements. Then $E(X)$ is the average number of comparisons used. (Recall that at step $i$ for $i = 2, \ldots, n$, the insertion sort inserts the $i$th element in the original list into the correct position in the sorted list of the first $i - 1$ elements of the original list.)

We let $X_i$ be the random variable equal to the number of comparisons used to insert $a_i$ into the proper position after the first $i-1$ elements $a_1, a_2, \ldots, a_{i-1}$ have been sorted. Because

$$X = X_2 + X_3 + \cdots + X_n,$$

we can use the linearity of expectations to conclude that

$$E(X) = E(X_2 + X_3 + \cdots + X_n) = E(X_2) + E(X_3) + \cdots + E(X_n).$$

To find $E(X_i)$ for $i = 2, 3, \ldots, n$, let $p_j(k)$ denote the probability that the largest of the first $j$ elements in the list occurs at the $k$th position, that is, that $\max(a_1, a_2, \ldots, a_j) = a_k$, where $1 \leq k \leq j$. Because the elements of the list are randomly distributed, it is equally likely for the largest element among the first $j$ elements to occur at any position. Consequently, $p_j(k) = 1/j$. If $X_i(k)$ equals the number of comparisons used by the insertion sort if $a_i$ is inserted into the $k$th position in the list once $a_1, a_2, \ldots, a_{i-1}$ have been sorted, it follows that $X_i(k) = k$. Because it is possible that $a_i$ is inserted in any of the first $i$ positions, we find that

$$E(X_i) = \sum_{k=1}^{i} p_i(k) \cdot X_i(k) = \sum_{k=1}^{i} \frac{1}{i} \cdot k = \frac{1}{i} \cdot \sum_{k=1}^{i} k = \frac{1}{i} \cdot \frac{i(i+1)}{2} = \frac{i+1}{2}.$$

It follows that

$$\begin{aligned} E(X) &= \sum_{i=2}^{n} E(X_i) = \sum_{i=2}^{n} \frac{i+1}{2} = \frac{1}{2} \sum_{j=3}^{n+1} j \\ &= \frac{1}{2} \frac{(n+1)(n+2)}{2} - \frac{1}{2}(1+2) = \frac{n^2 + 3n - 4}{4}. \end{aligned}$$

To obtain the third of these equalities we shifted the index of summation, setting $j = i + 1$. To obtain the fourth equality, we used the formula $\sum_{k=1}^{m} k = m(m+1)/2$ (from Table 2 in Section 2.4) with $m = n + 1$, subtracting off the missing terms with $j = 1$ and $j = 2$. We conclude that the average number of comparisons used by the insertion sort to sort $n$ elements equals $(n^2 + 3n - 4)/4$, which is $\Theta(n^2)$. ◀

## The Geometric Distribution

We now turn our attention to a random variable with infinitely many possible outcomes.

**EXAMPLE 10** Suppose that the probability that a coin comes up tails is $p$. This coin is flipped repeatedly until it comes up tails. What is the expected number of flips until this coin comes up tails?

Links

*Solution:* We first note that the sample space consists of all sequences that begin with any number of heads, denoted by $H$, followed by a tail, denoted by $T$. Therefore, the sample space is the set $\{T, HT, HHT, HHHT, HHHHT, \ldots\}$. Note that this is an infinite sample space. We can determine the probability of an element of the sample space by noting that the coin flips are independent and that the probability of a head is $1 - p$. Therefore, $p(T) = p$, $p(HT) = (1-p)p$, $p(HHT) = (1-p)^2 p$, and in general the probability that the coin is flipped $n$ times before a tail comes up, that is, that $n-1$ heads come up followed by a tail, is $(1-p)^{n-1} p$. (Exercise 14 asks for a verification that the sum of the probabilities of the points in the sample space is 1.)

Now let $X$ be the random variable equal to the number of flips in an element in the sample space. That is, $X(T) = 1$, $X(HT) = 2$, $X(HHT) = 3$, and so on. Note that $p(X = j) = (1 - p)^{j-1}p$. The expected number of flips until the coin comes up tails equals $E(X)$.

Using Theorem 1, we find that

$$E(X) = \sum_{j=1}^{\infty} j \cdot p(X = j) = \sum_{j=1}^{\infty} j(1 - p)^{j-1}p = p\sum_{j=1}^{\infty} j(1 - p)^{j-1} = p \cdot \frac{1}{p^2} = \frac{1}{p}.$$

[The third equality in this chain follows from Table 2 in Section 2.4, which tells us that $\sum_{j=1}^{\infty} j(1 - p)^{j-1} = 1/(1 - (1 - p))^2 = 1/p^2$.] It follows that the expected number of times the coin is flipped until tails comes up is $1/p$. Note that when the coin is fair we have $p = 1/2$, so the expected number of flips until it comes up tails is $1/(1/2) = 2$. ◀

The random variable $X$ that equals the number of flips expected before a coin comes up tails is an example of a random variable with a **geometric distribution**.

**DEFINITION 2**

A random variable $X$ has a *geometric distribution with parameter* $p$ if $p(X = k) = (1 - p)^{k-1}p$ for $k = 1, 2, 3, \ldots$, where $p$ is a real number with $0 \leq p \leq 1$.

Geometric distributions arise in many applications because they are used to study the time required before a particular event happens, such as the time required before we find an object with a certain property, the number of attempts before an experiment succeeds, the number of times a product can be used before it fails, and so on.

When we computed the expected value of the number of flips required before a coin comes up tails, we proved Theorem 4.

**THEOREM 4**

If the random variable $X$ has the geometric distribution with parameter $p$, then $E(X) = 1/p$.

## Independent Random Variables

We have already discussed independent events. We will now define what it means for two random variables to be independent.

**DEFINITION 3**

The random variables $X$ and $Y$ on a sample space $S$ are *independent* if

$$p(X = r_1 \text{ and } Y = r_2) = p(X = r_1) \cdot p(Y = r_2),$$

or in words, if the probability that $X = r_1$ and $Y = r_2$ equals the product of the probabilities that $X = r_1$ and $Y = r_2$, for all real numbers $r_1$ and $r_2$.

**EXAMPLE 11** Are the random variables $X_1$ and $X_2$ from Example 4 independent?

Extra Examples

*Solution:* Let $S = \{1, 2, 3, 4, 5, 6\}$, and let $i \in S$ and $j \in S$. Because there are 36 possible outcomes when the pair of dice is rolled and each is equally likely, we have

$$p(X_1 = i \text{ and } X_2 = j) = 1/36.$$

Furthermore, $p(X_1 = i) = 1/6$ and $p(X_2 = j) = 1/6$, because the probability that $i$ appears on the first die and the probability that $j$ appears on the second die are both $1/6$. It follows that

$$p(X_1 = i \text{ and } X_2 = j) = \frac{1}{36} \quad \text{and} \quad p(X_1 = i)p(X_2 = j) = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36},$$

so $X_1$ and $X_2$ are independent. ◀

**EXAMPLE 12** Show that the random variables $X_1$ and $X = X_1 + X_2$, where $X_1$ and $X_2$ are as defined in Example 4, are not independent.

*Solution:* Note that $p(X_1 = 1 \text{ and } X = 12) = 0$, because $X_1 = 1$ means the number appearing on the first die is 1, which implies that the sum of the numbers appearing on the two dice cannot equal 12. On the other hand, $p(X_1 = 1) = 1/6$ and $p(X = 12) = 1/36$. Hence $p(X_1 = 1 \text{ and } X = 12) \neq p(X_1 = 1) \cdot p(X = 12)$. This counterexample shows that $X_1$ and $X$ are not independent. ◀

The expected value of the product of two independent random variables is the product of their expected values, as Theorem 5 shows.

**THEOREM 5** If $X$ and $Y$ are independent random variables on a sample space $S$, then $E(XY) = E(X)E(Y)$.

***Proof:*** To prove this formula, we use the key observation that the event $XY = r$ is the disjoint union of the events $X = r_1$ and $Y = r_2$ over all $r_1 \in X(S)$ and $r_2 \in Y(S)$ with $r = r_1 r_2$. We have

$$\begin{aligned}
E(XY) &= \sum_{r \in XY(S)} r \cdot p(XY = r) && \text{by Theorem 1} \\
&= \sum_{r_1 \in X(S), r_2 \in Y(S)} r_1 r_2 \cdot p(X = r_1 \text{ and } Y = r_2) && \text{expressing } XY = r \text{ as a disjoint union} \\
&= \sum_{r_1 \in X(S)} \sum_{r_2 \in Y(S)} r_1 r_2 \cdot p(X = r_1 \text{ and } Y = r_2) && \text{using a double sum to order the terms} \\
&= \sum_{r_1 \in X(S)} \sum_{r_2 \in Y(S)} r_1 r_2 \cdot p(X = r_1) \cdot p(Y = r_2) && \text{by the independence of } X \text{ and } Y \\
&= \sum_{r_1 \in X(S)} \left( r_1 \cdot p(X = r_1) \cdot \sum_{r_2 \in Y(S)} r_2 \cdot p(Y = r_2) \right) && \text{by factoring out } r_1 \cdot p(X = r_1) \\
&= \sum_{r_1 \in X(S)} r_1 \cdot p(X = r_1) \cdot E(Y) && \text{by the definition of } E(Y) \\
&= E(Y) \left( \sum_{r_1 \in X(S)} r_1 \cdot p(X = r_1) \right) && \text{by factoring out } E(Y) \\
&= E(Y)E(X) && \text{by the definition of } E(X)
\end{aligned}$$

We complete the proof by noting that $E(Y)E(X) = E(X)E(Y)$, which is a consequence of the commutative law for multiplication. ◁

Note that when $X$ and $Y$ are random variables that are not independent, we cannot conclude that $E(XY) = E(X)E(Y)$, as Example 13 shows.

**EXAMPLE 13** Let $X$ and $Y$ be random variables that count the number of heads and the number of tails when a coin is flipped twice. Because $p(X = 2) = 1/4$, $p(X = 1) = 1/2$, and $p(X = 0) = 1/4$, by Theorem 1 we have

$$E(X) = 2 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} + 0 \cdot \frac{1}{4} = 1.$$

A similar computation shows that $E(Y) = 1$. We note that $XY = 0$ when either two heads and no tails or two tails and no heads come up and that $XY = 1$ when one head and one tail come up. Hence,

$$E(XY) = 1 \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{1}{2}.$$

It follows that

$$E(XY) \neq E(X)E(Y).$$

This does not contradict Theorem 5 because $X$ and $Y$ are not independent, as the reader should verify (see Exercise 16). ◀

## Variance


The expected value of a random variable tells us its average value, but nothing about how widely its values are distributed. For example, if $X$ and $Y$ are the random variables on the set $S = \{1, 2, 3, 4, 5, 6\}$, with $X(s) = 0$ for all $s \in S$ and $Y(s) = -1$ if $s \in \{1, 2, 3\}$ and $Y(s) = 1$ if $s \in \{4, 5, 6\}$, then the expected values of $X$ and $Y$ are both zero. However, the random variable $X$ never varies from 0, while the random variable $Y$ always differs from 0 by 1. The variance of a random variable helps us characterize how widely a random variable is distributed. In particular, it provides a measure of how widely $X$ is distributed about its expected value.

**DEFINITION 4** Let $X$ be a random variable on a sample space $S$. The *variance* of $X$, denoted by $V(X)$, is

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s).$$

That is, $V(X)$ is the weighted average of the square of the deviation of $X$. The *standard deviation* of $X$, denoted $\sigma(X)$, is defined to be $\sqrt{V(X)}$.

Theorem 6 provides a useful simple expression for the variance of a random variable.

**THEOREM 6** If $X$ is a random variable on a sample space $S$, then $V(X) = E(X^2) - E(X)^2$.

***Proof:*** Note that

$$\begin{aligned} V(X) &= \sum_{s \in S} (X(s) - E(X))^2 p(s) \\ &= \sum_{s \in S} X(s)^2 p(s) - 2E(X) \sum_{s \in S} X(s) p(s) + E(X)^2 \sum_{s \in S} p(s) \\ &= E(X^2) - 2E(X)E(X) + E(X)^2 \\ &= E(X^2) - E(X)^2. \end{aligned}$$

We have used the fact that $\sum_{s \in S} p(s) = 1$ in the next-to-last step. ◁

We can use Theorems 3 and 6 to derive an alternative formula for $V(X)$ that provides some insight into the meaning of the variance of a random variable.

**COROLLARY 1** If $X$ is a random variable on a sample space $S$ and $E(X) = \mu$, then $V(X) = E((X - \mu)^2)$.

$\mu$ is the Greek letter mu.

***Proof:*** If $X$ is a random variable with $E(X) = \mu$, then

$$\begin{aligned}
E((X-\mu)^2) &= E(X^2 - 2\mu X + \mu^2) && \text{expanding } (X-\mu)^2 \\
&= E(X^2) - E(2\mu X) + E(\mu^2) && \text{by part } (i) \text{ of Theorem 3} \\
&= E(X^2) - 2\mu E(X) + E(\mu^2) && \text{by part } (ii) \text{ of Theorem 3, noting that } \mu \text{ is a constant} \\
&= E(X^2) - 2\mu E(X) + \mu^2 && \text{as } E(\mu^2) = \mu^2, \text{ because } \mu^2 \text{ is a constant} \\
&= E(X^2) - 2\mu^2 + \mu^2 && \text{because } E(X) = \mu \\
&= E(X^2) - \mu^2 && \text{simplifying} \\
&= V(X) && \text{by Theorem 6 and noting that } E(X) = \mu.
\end{aligned}$$

This completes the proof. ◁

Corollary 1 tells us that the variance of a random variable $X$ is the expected value of the square of the difference between $X$ and its own expected value. This is commonly expressed as saying that the variance of $X$ is the mean of the square of its deviation. We also say that the standard deviation of $X$ is the square root of the mean of the square of its deviation (often read as the "root mean square" of the deviation).

We now compute the variance of some random variables.

**EXAMPLE 14** What is the variance of the random variable $X$ with $X(t) = 1$ if a Bernoulli trial is a success and $X(t) = 0$ if it is a failure, where $p$ is the probability of success and $q$ is the probability of failure?

Extra Examples

*Solution:* Because $X$ takes only the values 0 and 1, it follows that $X^2(t) = X(t)$. Hence,

$$V(X) = E(X^2) - E(X)^2 = p - p^2 = p(1-p) = pq.$$ ◀

**EXAMPLE 15** **Variance of the Value of a Die** What is the variance of the random variable $X$, where $X$ is the number that comes up when a fair die is rolled?

*Solution:* We have $V(X) = E(X^2) - E(X)^2$. By Example 1 we know that $E(X) = 7/2$. To find $E(X^2)$ note that $X^2$ takes the values $i^2$, $i = 1, 2, \ldots, 6$, each with probability $1/6$. It follows that

$$E(X^2) = \frac{1}{6}(1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2) = \frac{91}{6}.$$

We conclude that

$$V(X) = \frac{91}{6} - \left(\frac{7}{2}\right)^2 = \frac{35}{12}.$$ ◀

**EXAMPLE 16** What is the variance of the random variable $X((i, j)) = 2i$, where $i$ is the number appearing on the first die and $j$ is the number appearing on the second die, when two fair dice are rolled?

*Solution:* We will use Theorem 6 to find the variance of $X$. To do so, we need to find the expected values of $X$ and $X^2$. Note that because $p(X = k)$ is $1/6$ for $k = 2, 4, 6, 8, 10, 12$ and is 0 otherwise,

$$E(X) = (2 + 4 + 6 + 8 + 10 + 12)/6 = 7,$$

and

$$E(X^2) = (2^2 + 4^2 + 6^2 + 8^2 + 10^2 + 12^2)/6 = 182/3.$$

It follows from Theorem 6 that

$$V(X) = E(X^2) - E(X)^2 = 182/3 - 49 = 35/3.$$ ◀

Another useful property is that the variance of the sum of two or more independent random variables is the sum of their variances. The formula that expresses this property is known as **Bienaymé's formula**, after Irenée-Jules Bienaymé, the French mathematician who discovered it in 1853. Bienaymé's formula is useful for computing the variance of the result of $n$ independent Bernoulli trials, for instance.

**THEOREM 7**

**BIENAYMÉ'S FORMULA** If $X$ and $Y$ are two independent random variables on a sample space $S$, then $V(X + Y) = V(X) + V(Y)$. Furthermore, if $X_i, i = 1, 2, \ldots, n$, with $n$ a positive integer, are pairwise independent random variables on $S$, then $V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$.

Links

IRENÉE-JULES BIENAYMÉ (1796–1878) Bienaymé, born in Paris, moved with his family to Bruges in 1803 when his father became a government administrator. Bienaymé attended the Lycée impérial in Bruges, and when his family returned to Paris in 1811, the Lycée Louis-le-Grand. As a teenager, he helped defend Paris during the 1814 Napoleonic Wars; in 1815, he became a student at the École Polytechnique. In 1816 he joined the Ministry of Finances to help support his family. In 1819, he left the civil service, taking a job lecturing mathematics at the Académie militaire de Saint-Cyr. Unhappy with conditions there, he soon returned to the Ministry of Finances. He attained the position of inspector general, remaining until forced to retire in 1848 for political reasons. He was able to return as inspector general in 1850, but he retired a second time in 1852. In 1851 he briefly was professor at the Sorbonne and also served as an expert statistician for Napoleon III. Bienaymé was one of the founders of the Société Mathématique de France, and in 1875 was its president.

Bienaymé was noted for his ingenuity, but his papers frustrated readers by omitting important proofs. He published sparsely, often in obscure journals. However, he made important contributions to probability and statistics, and to their applications to the social sciences and to finance. Among his important contributions are the Bienaymé-Chebyshev inequality, which provides a simple proof of the law of large numbers, a generalization of Laplace's least square method, and Bienaymé's formula for the variance of a sum of random variables. He studied the extinction of aristocratic families, declining despite general population growth. Bienaymé was a skilled linguist; he translated the works of Chebyshev, a close friend, from Russian to French. It has been suggested that his relative obscurity results from his modesty, his lack of interest in asserting the priority of his discoveries, and the fact that his work was often ahead of its time. He and his brother married two sisters who were daughters of a family friend. Bienaymé and his wife had two sons and three daughters.

*Proof:* From Theorem 6, we have

$$V(X+Y) = E((X+Y)^2) - E(X+Y)^2.$$

It follows that

$$\begin{aligned} V(X+Y) &= E(X^2 + 2XY + Y^2) - (E(X) + E(Y))^2 \\ &= E(X^2) + 2E(XY) + E(Y^2) - E(X)^2 - 2E(X)E(Y) - E(Y)^2. \end{aligned}$$

Because $X$ and $Y$ are independent, by Theorem 5 we have $E(XY) = E(X)E(Y)$. It follows that

$$\begin{aligned} V(X+Y) &= (E(X^2) - E(X)^2) + (E(Y^2) - E(Y)^2) \\ &= V(X) + V(Y). \end{aligned}$$

We leave the proof of the case for $n$ pairwise independent random variables to the reader (Exercise 34). Such a proof can be constructed by generalizing the proof we have given for the case for two random variables. Note that it is not possible to use mathematical induction in a straightforward way to prove the general case (see Exercise 33). ◁

**EXAMPLE 17** Find the variance and standard deviation of the random variable $X$ whose value when two fair dice are rolled is $X((i, j)) = i + j$, where $i$ is the number appearing on the first die and $j$ is the number appearing on the second die.

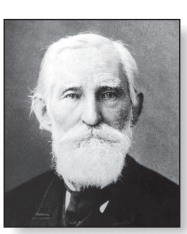
*Solution:* Let $X_1$ and $X_2$ be the random variables defined by $X_1((i, j)) = i$ and $X_2((i, j)) = j$ for a roll of the dice. Then $X = X_1 + X_2$, and $X_1$ and $X_2$ are independent, as Example 11 showed. From Theorem 7 it follows that $V(X) = V(X_1) + V(X_2)$. A simple computation as in Example 16, together with Exercise 29 in the Supplementary Exercises, tells us that $V(X_1) = V(X_2) = 35/12$. Hence, $V(X) = 35/12 + 35/12 = 35/6$ and $\sigma(X) = \sqrt{35/6}$. ◀

We will now find the variance of the random variable that counts the number of successes when $n$ independent Bernoulli trials are carried out.

**EXAMPLE 18** What is the variance of the number of successes when $n$ independent Bernoulli trials are performed, where, on each trial, $p$ is the probability of success and $q$ is the probability of failure?

*Solution:* Let $X_i$ be the random variable with $X_i((t_1, t_2, \ldots, t_n)) = 1$ if trial $t_i$ is a success and $X_i((t_1, t_2, \ldots, t_n)) = 0$ if trial $t_i$ is a failure. Let $X = X_1 + X_2 + \cdots + X_n$. Then $X$ counts the number of successes in the $n$ trials. From Theorem 7 it follows that $V(X) = V(X_1) + V(X_2) + \cdots + V(X_n)$. Using Example 14 we have $V(X_i) = pq$ for $i = 1, 2, \ldots, n$. It follows that $V(X) = npq$. ◀

Links



PAFNUTY LVOVICH CHEBYSHEV (1821–1894) Chebyshev was born into the gentry in Okatovo, Russia. His father was a retired army officer who had fought against Napoleon. In 1832 the family, with its nine children, moved to Moscow, where Pafnuty completed his high school education at home. He entered the Department of Physics and Mathematics at Moscow University. As a student, he developed a new method for approximating the roots of equations. He graduated from Moscow University in 1841 with a degree in mathematics, and he continued his studies, passing his master's exam in 1843 and completing his master's thesis in 1846.

Chebyshev was appointed in 1847 to a position as an assistant at the University of St. Petersburg. He wrote and defended a thesis in 1847. He became a professor at St. Petersburg in 1860, a position he held until 1882. His book on the theory of congruences written in 1849 was influential in the development of number theory. His work on the distribution of prime numbers was seminal. He proved Bertrand's conjecture that for every integer $n > 3$, there is a prime between $n$ and $2n - 2$. Chebyshev helped develop ideas that were later used to prove the prime number theorem. Chebyshev's work on the approximation of functions using polynomials is used extensively when computers are used to find values of functions. Chebyshev was also interested in mechanics. He studied the conversion of rotary motion into rectilinear motion by mechanical coupling. The Chebyshev parallel motion is three linked bars approximating rectilinear motion.

## Chebyshev's Inequality

How likely is it that a random variable takes a value far from its expected value? Theorem 8, called Chebyshev's inequality, helps answer this question by providing an upper bound on the probability that the value of a random variable differs from the expected value of the random variable by more than a specified amount.

**THEOREM 8**

**CHEBYSHEV'S INEQUALITY** Let $X$ be a random variable on a sample space $S$ with probability function $p$. If $r$ is a positive real number, then

$$p(|X(s) - E(X)| \geq r) \leq V(X)/r^2.$$

*Proof:* Let $A$ be the event

$$A = \{s \in S \,|\, |X(s) - E(X)| \geq r\}.$$

What we want to prove is that $p(A) \leq V(X)/r^2$. Note that

$$\begin{aligned} V(X) &= \sum_{s \in S} (X(s) - E(X))^2 p(s) \\ &= \sum_{s \in A} (X(s) - E(X))^2 p(s) + \sum_{s \notin A} (X(s) - E(X))^2 p(s). \end{aligned}$$

The second sum in this expression is nonnegative, because each of its summands is nonnegative. Also, because for each element $s$ in $A$, $(X(s) - E(X))^2 \geq r^2$, the first sum in this expression is at least $\sum_{s \in A} r^2 p(s)$. Hence, $V(X) \geq \sum_{s \in A} r^2 p(s) = r^2 p(A)$. It follows that $V(X)/r^2 \geq p(A)$, so $p(A) \leq V(X)/r^2$, completing the proof. ◁

**EXAMPLE 19** **Deviation from the Mean when Counting Tails** Suppose that $X$ is the random variable that counts the number of tails when a fair coin is tossed $n$ times. Note that $X$ is the number of successes when $n$ independent Bernoulli trials, each with probability of success $1/2$, are performed. It follows that $E(X) = n/2$ (by Theorem 2) and $V(X) = n/4$ (by Example 18). Applying Chebyshev's inequality with $r = \sqrt{n}$ shows that

$$p(|X(s) - n/2| \geq \sqrt{n}) \leq (n/4)/(\sqrt{n})^2 = 1/4.$$

Consequently, the probability is no more than $1/4$ that the number of tails that come up when a fair coin is tossed $n$ times deviates from the mean by more than $\sqrt{n}$. ◀

Chebyshev's inequality, although applicable to any random variable, often fails to provide a practical estimate for the probability that the value of a random variable exceeds its mean by a large amount. This is illustrated by Example 20.

**EXAMPLE 20** Let $X$ be the random variable whose value is the number appearing when a fair die is rolled. We have $E(X) = 7/2$ (see Example 1) and $V(X) = 35/12$ (see Example 15). Because the only possible values of $X$ are 1, 2, 3, 4, 5, and 6, $X$ cannot take a value more than $5/2$ from its mean, $E(X) = 7/2$. Hence, $p(|X - 7/2| \geq r) = 0$ if $r > 5/2$. By Chebyshev's inequality we know that $p(|X - 7/2| \geq r) \leq (35/12)/r^2$.

For example, when $r = 3$, Chebyshev's inequality tells us that $p(|X - 7/2| \geq 3) \leq (35/12)/9 = 35/108 \approx 0.324$, which is a poor estimate, because $p(|X - 7/2| \geq 3) = 0$. ◀

## Exercises

**1.** What is the expected number of heads that come up when a fair coin is flipped five times?

**2.** What is the expected number of heads that come up when a fair coin is flipped 10 times?

**3.** What is the expected number of times a 6 appears when a fair die is rolled 10 times?

**4.** A coin is biased so that the probability a head comes up when it is flipped is 0.6. What is the expected number of heads that come up when it is flipped 10 times?

**5.** What is the expected sum of the numbers that appear on two dice, each biased so that a 3 comes up twice as often as each other number?

**6.** What is the expected value when a \$1 lottery ticket is bought in which the purchaser wins exactly \$10 million if the ticket contains the six winning numbers chosen from the set $\{1, 2, 3, \ldots, 50\}$ and the purchaser wins nothing otherwise?

**7.** The final exam of a discrete mathematics course consists of 50 true/false questions, each worth two points, and 25 multiple-choice questions, each worth four points. The probability that Linda answers a true/false question correctly is 0.9, and the probability that she answers a multiple-choice question correctly is 0.8. What is her expected score on the final?

**8.** What is the expected sum of the numbers that appear when three fair dice are rolled?

**9.** Suppose that the probability that $x$ is in a list of $n$ distinct integers is $2/3$ and that it is equally likely that $x$ equals any element in the list. Find the average number of comparisons used by the linear search algorithm to find $x$ or to determine that it is not in the list.

**10.** Suppose that we flip a fair coin until either it comes up tails twice or we have flipped it six times. What is the expected number of times we flip the coin?

**11.** Suppose that we roll a fair die until a 6 comes up or we have rolled it 10 times. What is the expected number of times we roll the die?

**12.** Suppose that we roll a fair die until a 6 comes up.

**a)** What is the probability that we roll the die $n$ times?

**b)** What is the expected number of times we roll the die?

**13.** Suppose that we roll a pair of fair dice until the sum of the numbers on the dice is seven. What is the expected number of times we roll the dice?

**14.** Show that the sum of the probabilities of a random variable with geometric distribution with parameter $p$, where $0 < p \leq 1$, equals 1.

**15.** Show that if the random variable $X$ has the geometric distribution with parameter $p$, and $j$ is a positive integer, then $p(X \geq j) = (1 - p)^{j-1}$.

**16.** Let $X$ and $Y$ be the random variables that count the number of heads and the number of tails that come up when two fair coins are flipped. Show that $X$ and $Y$ are not independent.

**17.** Estimate the expected number of integers with 1000 digits that need to be selected at random to find a prime, if the probability a number with 1000 digits is prime is approximately $1/2302$.

**18.** Suppose that $X$ and $Y$ are random variables and that $X$ and $Y$ are nonnegative for all points in a sample space $S$. Let $Z$ be the random variable defined by $Z(s) = \max(X(s), Y(s))$ for all elements $s \in S$. Show that $E(Z) \leq E(X) + E(Y)$.

**19.** Let $X$ be the number appearing on the first die when two fair dice are rolled and let $Y$ be the sum of the numbers appearing on the two dice. Show that $E(X)E(Y) \neq E(XY)$.

***20.** Show that if $X_1, X_2, \ldots, X_n$ are mutually independent random variables, then $E(\prod_{i=1}^{n} X_i) = \prod_{i=1}^{n} E(X_i)$.

The **conditional expectation** of the random variable $X$ given the event $A$ from the sample space $S$ is $E(X|A) = \sum_{r \in X(S)} r \cdot P(X = r|A)$.

**21.** What is expected value of the sum of the numbers appearing on two fair dice when they are rolled given that the sum of these numbers is at least nine. That is, what is $E(X|A)$ where $X$ is the sum of the numbers appearing on the two dice and $A$ is the event that $X \geq 9$?

The **law of total expectation** states that if the sample space $S$ is the disjoint union of the events $S_1, S_2, \ldots, S_n$ and $X$ is a random variable, then $E(X) = \sum_{j=1}^{n} E(X|S_j)P(S_j)$.

**22.** Prove the law of total expectations.

**23.** Use the law of total expectation to find the average weight of a breeding elephant seal, given that 12% of the breeding elephant seals are male and the rest are female, and the expected weights of a breeding elephant seal is 4,200 pounds for a male and 1,100 pounds for a female.

**24.** Let $A$ be an event. Then $I_A$, the **indicator random variable** of $A$, equals 1 if $A$ occurs and equals 0 otherwise. Show that the expectation of the indicator random variable of $A$ equals the probability of $A$, that is, $E(I_A) = p(A)$.

**25.** A **run** is a maximal sequence of successes in a sequence of Bernoulli trials. For example, in the sequence $S, S, S, F, S, S, F, F, S$, where $S$ represents success and $F$ represents failure, there are three runs consisting of three successes, two successes, and one success, respectively. Let $R$ denote the random variable on the set of sequences of $n$ independent Bernoulli trials that counts the number of runs in this sequence. Find $E(R)$. [*Hint:* Show that $R = \sum_{j=1}^{n} I_j$, where $I_j = 1$ if a run begins at the $j$th Bernoulli trial and $I_j = 0$ otherwise. Find $E(I_1)$ and then find $E(I_j)$, where $1 < j \leq n$.]

**26.** Let $X(s)$ be a random variable, where $X(s)$ is a nonnegative integer for all $s \in S$, and let $A_k$ be the event that $X(s) \geq k$. Show that $E(X) = \sum_{k=1}^{\infty} p(A_k)$.

**27.** What is the variance of the number of heads that come up when a fair coin is flipped 10 times?

**28.** What is the variance of the number of times a 6 appears when a fair die is rolled 10 times?

**29.** Let $X_n$ be the random variable that equals the number of tails minus the number of heads when $n$ fair coins are flipped.

**a)** What is the expected value of $X_n$?

**b)** What is the variance of $X_n$?

**30.** Show that if $X$ and $Y$ are independent random variables, then $V(XY) = E(X)^2V(Y) + E(Y)^2V(X) + V(X)V(Y)$

**31.** Let $A(X) = E(|X - E(X)|)$, the expected value of the absolute value of the deviation of $X$, where $X$ is a random variable. Prove or disprove that $A(X + Y) = A(X) + A(Y)$ for all random variables $X$ and $Y$.

**32.** Provide an example that shows that the variance of the sum of two random variables is not necessarily equal to the sum of their variances when the random variables are not independent.

**33.** Suppose that $X_1$ and $X_2$ are independent Bernoulli trials each with probability $1/2$, and let $X_3 = (X_1 + X_2) \bmod 2$.

**a)** Show that $X_1$, $X_2$, and $X_3$ are pairwise independent, but $X_3$ and $X_1 + X_2$ are not independent.

**b)** Show that $V(X_1 + X_2 + X_3) = V(X_1) + V(X_2) + V(X_3)$.

**c)** Explain why a proof by mathematical induction of Theorem 7 does not work by considering the random variables $X_1$, $X_2$, and $X_3$.

***34.** Prove the general case of Theorem 7. That is, show that if $X_1, X_2, \ldots, X_n$ are pairwise independent random variables on a sample space $S$, where $n$ is a positive integer, then $V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$. [*Hint:* Generalize the proof given in Theorem 7 for two random variables. Note that a proof using mathematical induction does not work; see Exercise 33.]

**35.** Use Chebyshev's inequality to find an upper bound on the probability that the number of tails that come up when a fair coin is tossed $n$ times deviates from the mean by more than $5\sqrt{n}$.

**36.** Use Chebyshev's inequality to find an upper bound on the probability that the number of tails that come up when a biased coin with probability of heads equal to 0.6 is tossed $n$ times deviates from the mean by more than $\sqrt{n}$.

**37.** Let $X$ be a random variable on a sample space $S$ such that $X(s) \geq 0$ for all $s \in S$. Show that $p(X(s) \geq a) \leq E(X)/a$ for every positive real number $a$. This inequality is called **Markov's inequality**.

**38.** Suppose that the number of cans of soda pop filled in a day at a bottling plant is a random variable with an expected value of 10,000 and a variance of 1000.

**a)** Use Markov's inequality (Exercise 37) to obtain an upper bound on the probability that the plant will fill more than 11,000 cans on a particular day.

**b)** Use Chebyshev's inequality to obtain a lower bound on the probability that the plant will fill between 9000 and 11,000 cans on a particular day.

**39.** Suppose that the number of tin cans recycled in a day at a recycling center is a random variable with an expected value of 50,000 and a variance of 10,000.

**a)** Use Markov's inequality (Exercise 37) to find an upper bound on the probability that the center will recycle more than 55,000 cans on a particular day.

**b)** Use Chebyshev's inequality to provide a lower bound on the probability that the center will recycle 40,000 to 60,000 cans on a certain day.

***40.** Suppose the probability that $x$ is the $i$th element in a list of $n$ distinct integers is $i/[n(n + 1)]$. Find the average number of comparisons used by the linear search algorithm to find $x$ or to determine that it is not in the list.

***41.** In this exercise we derive an estimate of the average-case complexity of the variant of the bubble sort algorithm that terminates once a pass has been made with no interchanges. Let $X$ be the random variable on the set of permutations of a set of $n$ distinct integers $\{a_1, a_2, \ldots, a_n\}$ with $a_1 < a_2 < \cdots < a_n$ such that $X(P)$ equals the number of comparisons used by the bubble sort to put these integers into increasing order.

**a)** Show that, under the assumption that the input is equally likely to be any of the $n!$ permutations of these integers, the average number of comparisons used by the bubble sort equals $E(X)$.

**b)** Use Example 5 in Section 3.3 to show that $E(X) \leq n(n - 1)/2$.

**c)** Show that the sort makes at least one comparison for every inversion of two integers in the input.

**d)** Let $I(P)$ be the random variable that equals the number of inversions in the permutation $P$. Show that $E(X) \geq E(I)$.

**e)** Let $I_{j,k}$ be the random variable with $I_{j,k}(P) = 1$ if $a_k$ precedes $a_j$ in $P$ and $I_{j,k} = 0$ otherwise. Show that $I(P) = \sum_k \sum_{j<k} I_{j,k}(P)$.

**f)** Show that $E(I) = \sum_k \sum_{j<k} E(I_{j,k})$.

**g)** Show that $E(I_{j,k}) = 1/2$. [*Hint:* Show that $E(I_{j,k}) =$ probability that $a_k$ precedes $a_j$ in a permutation $P$. Then show it is equally likely for $a_k$ to precede $a_j$ as it is for $a_j$ to precede $a_k$ in a permutation.]

**h)** Use parts (f) and (g) to show that $E(I) = n(n - 1)/4$.

**i)** Conclude from parts (b), (d), and (h) that the average number of comparisons used to sort $n$ integers is $\Theta(n^2)$.

***42.** In this exercise we find the average-case complexity of the quick sort algorithm, described in the preamble to Exercise 50 in Section 5.4, assuming a uniform distribution on the set of permutations.

**a)** Let $X$ be the number of comparisons used by the quick sort algorithm to sort a list of $n$ distinct integers. Show that the average number of comparisons used by the quick sort algorithm is $E(X)$ (where the sample space is the set of all $n!$ permutations of $n$ integers).

**b)** Let $I_{j,k}$ denote the random variable that equals 1 if the $j$th smallest element and the $k$th smallest element of the initial list are ever compared as the quick sort algorithm sorts the list and equals 0 otherwise. Show that $X = \sum_{k=2}^{n} \sum_{j=1}^{k-1} I_{j,k}$.

**c)** Show that $E(X) = \sum_{k=2}^{n} \sum_{j=1}^{k-1} p(\text{the } j\text{th smallest element and the } k\text{th smallest element are compared})$.

**d)** Show that $p(\text{the } j\text{th smallest element and the } k\text{th smallest element are compared})$, where $k > j$, equals $2/(k - j + 1)$.

**e)** Use parts (c) and (d) to show that $E(X) = 2(n + 1)(\sum_{i=2}^{n} 1/i) - 2(n - 1)$.

**f)** Conclude from part (e) and the fact that $\sum_{j=1}^{n} 1/j \approx \ln n + \gamma$, where $\gamma = 0.57721\ldots$ is Euler's constant, that the average number of comparisons used by the quick sort algorithm is $\Theta(n \log n)$.

***43.** What is the variance of the number of **fixed elements**, that is, elements left in the same position, of a randomly selected permutation of $n$ elements? [*Hint:* Let $X$ denote the number of fixed points of a random permutation. Write $X = X_1 + X_2 + \cdots + X_n$, where $X_i = 1$ if the permutation fixes the $i$th element and $X_i = 0$ otherwise.]

The **covariance** of two random variables $X$ and $Y$ on a sample space $S$, denoted by $\text{Cov}(X, Y)$, is defined to be the expected value of the random variable $(X - E(X))(Y - E(Y))$. That is, $\text{Cov}(X, Y) = E((X - E(X))(Y - E(Y)))$.

**44.** Show that $\text{Cov}(X, Y) = E(XY) - E(X)E(Y)$, and use this result to conclude that $\text{Cov}(X, Y) = 0$ if $X$ and $Y$ are independent random variables.

**45.** Show that $V(X + Y) = V(X) + V(Y) + 2\,\text{Cov}(X, Y)$.

**46.** Find $\text{Cov}(X, Y)$ if $X$ and $Y$ are the random variables with $X((i, j)) = 2i$ and $Y((i, j)) = i + j$, where $i$ and $j$ are the numbers that appear on the first and second of two dice when they are rolled.

**47.** When $m$ balls are distributed into $n$ bins uniformly at random, what is the probability that the first bin remains empty?

**48.** What is the expected number of balls that fall into the first bin when $m$ balls are distributed into $n$ bins uniformly at random?

**49.** What is the expected number of bins that remain empty when $m$ balls are distributed into $n$ bins uniformly at random?

## Key Terms and Results

### TERMS

**sample space:** the set of possible outcomes of an experiment

**event:** a subset of the sample space of an experiment

**probability of an event (Laplace's definition):** the number of successful outcomes of this event divided by the number of possible outcomes

**probability distribution:** a function $p$ from the set of all outcomes of a sample space $S$ for which $0 \le p(x_i) \le 1$ for $i = 1, 2, \ldots, n$ and $\sum_{i=1}^{n} p(x_i) = 1$, where $x_1, \ldots, x_n$ are the possible outcomes

**probability of an event $E$:** the sum of the probabilities of the outcomes in $E$

**$p(E|F)$ (conditional probability of $E$ given $F$):** the ratio $p(E \cap F)/p(F)$

**independent events:** events $E$ and $F$ such that $p(E \cap F) = p(E)p(F)$

**pairwise independent events:** events $E_1, E_2, \ldots, E_n$ such that $p(E_i \cap E_j) = p(E_i)p(E_j)$ for all pairs of integers $i$ and $j$ with $1 \le j < k \le n$

**mutually independent events:** events $E_1, E_2, \ldots, E_n$ such that $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})p(E_{i_2}) \cdots p(E_{i_m})$ whenever $i_j$, $j = 1, 2, \ldots, m$, are integers with $1 \le i_1 < i_2 < \cdots < i_m \le n$ and $m \ge 2$

**random variable:** a function that assigns a real number to each possible outcome of an experiment

**distribution of a random variable $X$:** the set of pairs $(r, p(X = r))$ for $r \in X(S)$

**uniform distribution:** the assignment of equal probabilities to the elements of a finite set

**expected value of a random variable:** the weighted average of a random variable, with values of the random variable weighted by the probability of outcomes, that is, $E(X) = \sum_{s \in S} p(s)X(s)$

**geometric distribution:** the distribution of a random variable $X$ such that $p(X = k) = (1 - p)^{k-1}p$ for $k = 1, 2, \ldots$ for some real number $p$ with $0 \le p \le 1$.

**independent random variables:** random variables $X$ and $Y$ such that $p(X = r_1 \text{ and } Y = r_2) = p(X = r_1)p(Y = r_2)$ for all real numbers $r_1$ and $r_2$

**variance of a random variable $X$:** the weighted average of the square of the difference between the value of $X$ and its expected value $E(X)$, with weights given by the probability of outcomes, that is, $V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s)$

**standard deviation of a random variable $X$:** the square root of the variance of $X$, that is, $\sigma(X) = \sqrt{V(X)}$

**Bernoulli trial:** an experiment with two possible outcomes

**probabilistic (or Monte Carlo) algorithm:** an algorithm in which random choices are made at one or more steps

**probabilistic method:** a technique for proving the existence of objects in a set with certain properties that proceeds by assigning probabilities to objects and showing that the probability that an object has these properties is positive

### RESULTS

The probability of exactly $k$ successes when $n$ independent Bernoulli trials are carried out equals $C(n, k)p^k q^{n-k}$, where $p$ is the probability of success and $q = 1 - p$ is the probability of failure.

**Bayes' theorem:** If $E$ and $F$ are events from a sample space $S$ such that $p(E) \neq 0$ and $p(F) \neq 0$, then

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}.$$

$E(X) = \sum_{r \in X(S)} p(X = r)r$.

**linearity of expectations:** $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$ if $X_1, X_2, \ldots, X_n$ are random variables

If $X$ and $Y$ are independent random variables, then $E(XY) = E(X)E(Y)$.

**Bienaymé's formula:** If $X_1, X_2, \ldots, X_n$ are independent random variables, then $V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$.

**Chebyshev's inequality:** $p(|X(s) - E(X)| \geq r) \leq V(X)/r^2$, where $X$ is a random variable with probability function $p$ and $r$ is a positive real number.

## Review Questions

1. **a)** Define the probability of an event when all outcomes are equally likely.
   **b)** What is the probability that you select the six winning numbers in a lottery if the six different winning numbers are selected from the first 50 positive integers?
2. **a)** What conditions should be met by the probabilities assigned to the outcomes from a finite sample space?
   **b)** What probabilities should be assigned to the outcome of heads and the outcome of tails if heads comes up three times as often as tails?
3. **a)** Define the conditional probability of an event $E$ given an event $F$.
   **b)** Suppose $E$ is the event that when a die is rolled it comes up an even number, and $F$ is the event that when a die is rolled it comes up 1, 2, or 3. What is the probability of $F$ given $E$?
4. **a)** When are two events $E$ and $F$ independent?
   **b)** Suppose $E$ is the event that an even number appears when a fair die is rolled, and $F$ is the event that a 5 or 6 comes up. Are $E$ and $F$ independent?
5. **a)** What is a random variable?
   **b)** What are the possible values assigned by the random variable $X$ that assigns to a roll of two dice the larger number that appears on the two dice?
6. **a)** Define the expected value of a random variable $X$.
   **b)** What is the expected value of the random variable $X$ that assigns to a roll of two dice the larger number that appears on the two dice?
7. **a)** Explain how the average-case computational complexity of an algorithm, with finitely many possible input values, can be interpreted as an expected value.
   **b)** What is the average-case computational complexity of the linear search algorithm, if the probability that the element for which we search is in the list is $1/3$, and it is equally likely that this element is any of the $n$ elements in the list?
8. **a)** What is meant by a Bernoulli trial?
   **b)** What is the probability of $k$ successes in $n$ independent Bernoulli trials?
   **c)** What is the expected value of the number of successes in $n$ independent Bernoulli trials?
9. **a)** What does the linearity of expectations of random variables mean?
   **b)** How can the linearity of expectations help us find the expected number of people who receive the correct hat when a hatcheck person returns hats at random?
10. **a)** How can probability be used to solve a decision problem, if a small probability of error is acceptable?
    **b)** How can we quickly determine whether a positive integer is prime, if we are willing to accept a small probability of making an error?
11. State Bayes' theorem and use it to find $p(F \mid E)$ if $p(E \mid F) = 1/3$, $p(E \mid \overline{F}) = 1/4$, and $p(F) = 2/3$, where $E$ and $F$ are events from a sample space $S$.
12. **a)** What does it mean to say that a random variable has a geometric distribution with parameter $p$?
    **b)** What is the mean of a geometric distribution with parameter $p$?
13. **a)** What is the variance of a random variable?
    **b)** What is the variance of a Bernoulli trial with probability $p$ of success?
14. **a)** What is the variance of the sum of $n$ independent random variables?
    **b)** What is the variance of the number of successes when $n$ independent Bernoulli trials, each with probability $p$ of success, are carried out?
15. What does Chebyshev's inequality tell us about the probability that a random variable deviates from its mean by more than a specified amount?

## Supplementary Exercises

**1.** What is the probability that six consecutive integers will be chosen as the winning numbers in a lottery where each number chosen is an integer between 1 and 40 (inclusive)?

**2.** A player in the Mega Millions lottery picks five different integers between 1 and 56, inclusive, and a sixth integer between 1 and 46, which may duplicate one of the earlier five integers. The player wins the jackpot if the first five numbers picked match the first five numbers drawn and the sixth number matches the sixth number drawn.
**a)** What is the probability that a player wins the jackpot?
**b)** What is the probability that a player wins \$250,000, which is the prize for matching the first five numbers, but not the sixth number, drawn?
**c)** What is the probability that a player wins \$150 by matching exactly three of the first five numbers and the sixth number or by matching four of the first five numbers but not the sixth number?
**d)** What is the probability that a player wins a prize, if a prize is given when the player matches at least three of the first five numbers or the last number.

**3.** A player in the Powerball lottery picks five different integers between 1 and 59, inclusive, and a sixth integer between 1 and 39, which may duplicate one of the earlier five integers. The player wins the jackpot if the first five numbers picked match the first five number drawn and the sixth number matches the sixth number drawn.
**a)** What is the probability that a player wins the jackpot?
**b)** What is the probability that a player wins \$200,000, which is the prize for matching the first five numbers, but not the sixth number, drawn?
**c)** What is the probability that a player wins \$100 by matching exactly three of the first five and the sixth numbers or four of the first five numbers but not the sixth number?
**d)** What is the probability that a player wins a prize, if a prize is given when the player matches at least three of the first five numbers or the last number.

**4.** What is the probability that a hand of 13 cards contains no pairs?

**5.** What is the probability that a 13-card bridge hand contains
**a)** all 13 hearts?
**b)** 13 cards of the same suit?
**c)** seven spades and six clubs?
**d)** seven cards of one suit and six cards of a second suit?
**e)** four diamonds, six hearts, two spades, and one club?
**f)** four cards of one suit, six cards of a second suit, two cards of a third suit, and one card of the fourth suit?

**6.** What is the probability that a seven-card poker hand contains
**a)** four cards of one kind and three cards of a second kind?
**b)** three cards of one kind and pairs of each of two different kinds?
**c)** pairs of each of three different kinds and a single card of a fourth kind?
**d)** pairs of each of two different kinds and three cards of a third, fourth, and fifth kind?
**e)** cards of seven different kinds?
**f)** a seven-card flush?
**g)** a seven-card straight?
**h)** a seven-card straight flush?

An **octahedral die** has eight faces that are numbered 1 through 8.

**7.** **a)** What is the expected value of the number that comes up when a fair octahedral die is rolled?
**b)** What is the variance of the number that comes up when a fair octahedral die is rolled?

A **dodecahedral die** has 12 faces that are numbered 1 through 12.

**8.** **a)** What is the expected value of the number that comes up when a fair dodecahedral die is rolled?
**b)** What is the variance of the number that comes up when a fair dodecahedral die is rolled?

**9.** Suppose that a pair of fair octahedral dice is rolled.
**a)** What is the expected value of the sum of the numbers that come up?
**b)** What is the variance of the sum of the numbers that come up?

**10.** Suppose that a pair of fair dodecahedral dice is rolled.
**a)** What is the expected value of the sum of the numbers that come up?
**b)** What is the variance of the sum of the numbers that come up?

**11.** Suppose that a fair standard (cubic) die and a fair octahedral die are rolled together.
**a)** What is the expected value of the sum of the numbers that come up?
**b)** What is the variance of the sum of the numbers that come up?

**12.** Suppose that a fair octahedral die and a fair dodecahedral die are rolled together.
**a)** What is the expected value of the sum of the numbers that come up?
**b)** What is the variance of the sum of the numbers that come up?

**13.** Suppose $n$ people, $n \geq 3$, play "odd person out" to decide who will buy the next round of refreshments. The $n$ people each flip a fair coin simultaneously. If all the coins but one come up the same, the person whose coin comes up different buys the refreshments. Otherwise, the people flip the coins again and continue until just one coin comes up different from all the others.
**a)** What is the probability that the odd person out is decided in just one coin flip?

**b)** What is the probability that the odd person out is decided with the $k$th flip?

**c)** What is the expected number of flips needed to decide odd person out with $n$ people?

**14.** Suppose that $p$ and $q$ are primes and $n = pq$. What is the probability that a randomly chosen positive integer less than $n$ is not divisible by either $p$ or $q$?

***15.** Suppose that $m$ and $n$ are positive integers. What is the probability that a randomly chosen positive integer less than $mn$ is not divisible by either $m$ or $n$?

**16.** Suppose that $E_1, E_2, \ldots, E_n$ are $n$ events with $p(E_i) > 0$ for $i = 1, 2, \ldots, n$. Show that

$$p(E_1 \cap E_2 \cap \cdots \cap E_n) = p(E_1)p(E_2 \mid E_1)p(E_3 \mid E_1 \cap E_2) \cdots p(E_n \mid E_1 \cap E_2 \cap \cdots \cap E_{n-1}).$$

**17.** There are three cards in a box. Both sides of one card are black, both sides of one card are red, and the third card has one black side and one red side. We pick a card at random and observe only one side.

**a)** If the side is black, what is the probability that the other side is also black?

**b)** What is the probability that the opposite side is the same color as the one we observed?

**18.** What is the probability that when a fair coin is flipped $n$ times an equal number of heads and tails appear?

**19.** What is the probability that a randomly selected bit string of length 10 is a palindrome?

**20.** What is the probability that a randomly selected bit string of length 11 is a palindrome?

**21.** Consider the following game. A person flips a coin repeatedly until a head comes up. This person receives a payment of $2^n$ dollars if the first head comes up at the $n$th flip.

**a)** Let $X$ be a random variable equal to the amount of money the person wins. Show that the expected value of $X$ does not exist (that is, it is infinite). Show that a rational gambler, that is, someone willing to pay to play the game as long as the price to play is not more than the expected payoff, should be willing to wager any amount of money to play this game. (This is known as the **St. Petersburg paradox**. Why do you suppose it is called a paradox?)

**b)** Suppose that the person receives $2^n$ dollars if the first head comes up on the $n$th flip where $n < 8$ and $2^8 = 256$ dollars if the first head comes up on or after the eighth flip. What is the expected value of the amount of money the person wins? How much money should a person be willing to pay to play this game?

**22.** Suppose that $n$ balls are tossed into $b$ bins so that each ball is equally likely to fall into any of the bins and that the tosses are independent.

**a)** Find the probability that a particular ball lands in a specified bin.

**b)** What is the expected number of balls that land in a particular bin?

**c)** What is the expected number of balls tossed until a particular bin contains a ball?

***d)** What is the expected number of balls tossed until all bins contain a ball? [*Hint:* Let $X_i$ denote the number of tosses required to have a ball land in an $i$th bin once $i - 1$ bins contain a ball. Find $E(X_i)$ and use the linearity of expectations.]

**23.** Suppose that $A$ and $B$ are events with probabilities $p(A) = 3/4$ and $p(B) = 1/3$.

**a)** What is the largest $p(A \cap B)$ can be? What is the smallest it can be? Give examples to show that both extremes for $p(A \cap B)$ are possible.

**b)** What is the largest $p(A \cup B)$ can be? What is the smallest it can be? Give examples to show that both extremes for $p(A \cup B)$ are possible.

**24.** Suppose that $A$ and $B$ are events with probabilities $p(A) = 2/3$ and $p(B) = 1/2$.

**a)** What is the largest $p(A \cap B)$ can be? What is the smallest it can be? Give examples to show that both extremes for $p(A \cap B)$ are possible.

**b)** What is the largest $p(A \cup B)$ can be? What is the smallest it can be? Give examples to show that both extremes for $p(A \cup B)$ are possible.

**25.** Recall from Definition 5 in Section 7.2 that the events $E_1, E_2, \ldots, E_n$ are **mutually independent** if $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})p(E_{i_2}) \cdots p(E_{i_m})$ whenever $i_j$, $j = 1, 2, \ldots, m$, are integers with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and $m \geq 2$.

**a)** Write out the conditions required for three events $E_1$, $E_2$, and $E_3$ to be mutually independent.

**b)** Let $E_1$, $E_2$, and $E_3$ be the events that the first flip comes up heads, that the second flip comes up tails, and that the third flip comes up tails, respectively, when a fair coin is flipped three times. Are $E_1$, $E_2$, and $E_3$ mutually independent?

**c)** Let $E_1$, $E_2$, and $E_3$ be the events that the first flip comes up heads, that the third flip comes up heads, and that an even number of heads come up, respectively, when a fair coin is flipped three times. Are $E_1$, $E_2$, and $E_3$ pairwise independent? Are they mutually independent?

**d)** Let $E_1$, $E_2$, and $E_3$ be the events that the first flip comes up heads, that the third flip comes up heads, and that exactly one of the first flip and third flip come up heads, respectively, when a fair coin is flipped three times. Are $E_1$, $E_2$, and $E_3$ pairwise independent? Are they mutually independent?

**e)** How many conditions must be checked to show that $n$ events are mutually independent?

**26.** Suppose that $A$ and $B$ are events from a sample space $S$ such that $p(A) \neq 0$ and $p(B) \neq 0$. Show that if $p(B \mid A) < p(B)$, then $p(A \mid B) < p(A)$.

In Exercise 27 we consider the **two children problem**, introduced in 1959 by Martin Garnder is his Mathematical Games column in *Scientific American*. A version of the puzzle asks: "We meet Mr. Smith as he is walking down the street with a young child whom he introduces as his son. He also tells us that he has two children. What is the probability that his other child is a son?" We will show that this puzzle is ambiguous, leading to a paradox, by showing that there are two reasonable answers to this problem and we will describe how to make the puzzle unambiguous.

***27.** **a)** Solve this puzzle in two different ways. First, answer the problem by considering the probability of the gender of the second child. Then, determine the probability differently, by considering the four different possibilities for a family of two children.

**b)** Show that the answer to the puzzle becomes unambiguous if we also know that Mr. Smith chose his walking companion at random from his two children.

**c)** Another variation of this puzzle asks "When we meet Mr. Smith, he tells us that he has two children and at least one is a son. What is the probability that his other child is a son?" Solve this variation of the puzzle, explaining why it is unambiguous.

**28.** In 2010, the puzzle designer Gary Foshee posed this problem: "Mr. Smith has two children, one of whom is a son born on a Tuesday. What is the probability that Mr. Smith has two sons?" Show that there are two different answers to this puzzle, depending on whether Mr. Smith specifically mentioned his son because he was born on a Tuesday or whether he randomly chose a child and reported its gender and birth day of the week. [*Hint:* For the first possibility, enumerate all the equally likely possibilities for the gender and birth day of the week of the other child. To do, this consider first the cases where the older child is a boy born on a Tuesday and then the case where the older child is not a boy born on a Tuesday.]

**29.** Let $X$ be a random variable on a sample space $S$. Show that $V(aX + b) = a^2V(X)$ whenever $a$ and $b$ are real numbers.

**30.** Use Chebyshev's inequality to show that the probability that more than 10 people get the correct hat back when a hatcheck person returns hats at random does not exceed $1/100$ no matter how many people check their hats. [*Hint:* Use Example 6 and Exercise 43 in Section 7.4.]

**31.** Suppose that at least one of the events $E_j$, $j = 1, 2, \ldots, m$, is guaranteed to occur and no more than two can occur. Show that if $p(E_j) = q$ for $j = 1, 2, \ldots, m$ and $p(E_j \cap E_k) = r$ for $1 \leq j < k \leq m$, then $q \geq 1/m$ and $r \leq 2/m$.

**32.** Show that if $m$ is a positive integer, then the probability that the $m$th success occurs on the $(m + n)$th trial when independent Bernoulli trials, each with probability $p$ of success, are run, is $\binom{n+m-1}{n} q^n p^m$.

**33.** There are $n$ different types of collectible cards you can get as prizes when you buy a particular product. Suppose that every time you buy this product it is equally likely that you get any type of these cards. Let $X$ be the random variable equal to the number of products that need to be purchased to obtain at least one of each type of card and let $X_j$ be the random variable equal to the number of additional products that must be purchased after $j$ different cards have been collected until a new card is obtained for $j = 0, 1, \ldots, n - 1$.

**a)** Show that $X = \sum_{j=0}^{n-1} X_j$.

**b)** Show that after $j$ distinct types of cards have been obtained, the card obtained with the next purchase will be a card of a new type with probability $(n - j)/n$.

**c)** Show that $X_j$ has a geometric distribution with parameter $(n - j)/n$.

**d)** Use parts (a) and (c) to show that $E(X) = n \sum_{j=1}^{n} 1/j$.

**e)** Use the approximation $\sum_{j=1}^{n} 1/j \approx \ln n + \gamma$, where $\gamma = 0.57721\ldots$ is Euler's constant, to find the expected number of products that you need to buy to get one card of each type if there are 50 different types of cards.

**34.** The **maximum satisfiability problem** asks for an assignment of truth values to the variables in a compound proposition in conjunctive normal form (which expresses a compound proposition as the conjunction of clauses where each clause is the disjunction of two or more variables or their negations) that makes as many of these clauses true as possible. For example, three but not four of the clauses in

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

can be made true by an assignment of truth values to $p, q$, and $r$. We will show that probabilistic methods can provide a lower bound for the number of clauses that can be made true by an assignment of truth values to the variables.

**a)** Suppose that there are $n$ variables in a compound proposition in conjunctive normal form. If we pick a truth value for each variable randomly by flipping a coin and assigning true to the variable if the coin comes up heads and false if it comes up tails, what is the probability of each possible assignment of truth values to the $n$ variables?

**b)** Assuming that each clause is the disjunction of exactly two distinct variables or their negations, what is the probability that a given clause is true, given the random assignment of truth values from part (a)?

**c)** Suppose that there are $D$ clauses in the compound proposition. What is the expected number of these clauses that are true, given the random assignment of truth values of the variables?

**d)** Use part (c) to show that for every compound proposition in conjunctive normal form there is an assignment of truth values to the variables that makes at least 3/4 of the clauses true.

**35.** What is the probability that each player has a hand containing an ace when the 52 cards of a standard deck are dealt to four players?

***36.** The following method can be used to generate a random permutation of a sequence of $n$ terms. First, interchange the $n$th term and the $r(n)$th term where $r(n)$ is a randomly selected integer with $1 \leq r(n) \leq n$. Next, interchange the $(n-1)$st term of the resulting sequence with its $r(n-1)$st term where $r(n-1)$ is a randomly selected integer with $1 \leq r(n-1) \leq n-1$. Continue this process until $j = n$, where at the $j$th step you interchange the $(n-j+1)$st term of the resulting sequence with its $r(n-j+1)$st term, where $r(n-j+1)$ is a randomly selected integer with $1 \leq r(n-j+1) \leq n-j+1$. Show that when this method is followed, each of the $n!$ different permutations of the terms of the sequence is equally likely to be generated. [*Hint:* Use mathematical induction, assuming that the probability that each of the permutations of $n-1$ terms produced by this procedure for a sequence of $n-1$ terms is $1/(n-1)!$.]

## Computer Projects

### Write programs with these input and output.

1. Given a real number $p$ with $0 \leq p \leq 1$, generate random numbers taken from a Bernoulli distribution with probability $p$.
2. Given a positive integer $n$, generate a random permutation of the set $\{1, 2, 3, \ldots, n\}$. (See Exercise 36 in the Supplementary Exercises.)
3. Given positive integers $m$ and $n$, generate $m$ random permutations of the first $n$ positive integers. Find the number of inversions in each permutation and determine the average number of these inversions.
4. Given a positive integer $n$, simulate $n$ repeated flips of a biased coin with probability $p$ of heads and determine the number of heads that come up. Display the cumulative results.
5. Given positive integers $n$ and $m$, generate $m$ random permutations of the first $n$ positive integers. Sort each permutation using the insertion sort, counting the number of comparisons used. Determine the average number of comparisons used over all $m$ permutations.
6. Given positive integers $n$ and $m$, generate $m$ random permutations of the first $n$ positive integers. Sort each permutation using the version of the bubble sort that terminates when a pass has been made with no interchanges, counting the number of comparisons used. Determine the average number of comparisons used over all $m$ permutations.
7. Given a positive integer $m$, simulate the collection of cards that come with the purchase of products to find the number of products that must be purchased to obtain a full set of $m$ different collector cards. (See Supplementary Exercise 33.)
8. Given positive integers $m$ and $n$, simulate the placement of $n$ keys, where a record with key $k$ is placed at location $h(k) = k \bmod m$ and determine whether there is at least one collision.
9. Given a positive integer $n$, find the probability of selecting the six integers from the set $\{1, 2, \ldots, n\}$ that were mechanically selected in a lottery.
10. Simulate repeated trials of the Monty Hall Three-Door problem (Example 10 in Section 7.1) to calculate the probability of winning with each strategy.
11. Given a list of words and the empirical probabilities they occur in spam e-mails and in e-mails that are not spam, determine the probability that a new e-mail message is spam.

## Computations and Explorations

### Use a computational program or programs you have written to do these exercises.

1. Find the probabilities of each type of hand in five-card poker and rank the types of hands by their probability.
2. Find some conditions such that the expected value of buying a \$1 lottery ticket in the New Jersey Pick-6 lottery has an expected value of more than \$1. To win you have to select the six numbers drawn, where order does not matter, from the positive integers 1 to 49, inclusive. The winnings are split evenly among holders of winning tickets. Be sure to consider the total size of the pot going into the drawing and the number of people buying tickets.
3. Estimate the probability that two integers selected at random are relatively prime by testing a large number of randomly selected pairs of integers. Look up the theorem that gives this probability and compare your results with the correct probability.
4. Determine the number of people needed to ensure that the probability at least two of them have the same day of the year as their birthday is at least 70%, at least 80%, at least 90%, at least 95%, at least 98%, and at least 99%.

5. Generate a list of 100 randomly selected permutations of the set of the first 100 positive integers. (See Exercise 36 in the Supplementary Exercises.)
6. Given a collection of e-mail messages, each determined to be spam or not to be spam, develop a Bayesian filter based on the appearance of particular words in these messages.
7. Simulate the odd-person-out procedure (described in Exercise 13 of the Supplementary Exercises) for $n$ people with $3 \leq n \leq 10$. Run a large number of trials for each value of $n$ and use the results to estimate the expected number of flips needed to find the odd person out. Does your result agree with that found in Exercise 29 in Section 7.2? Vary the problem by supposing that exactly one person has a biased coin with probability of heads $p \neq 0.5$.
8. Given a positive integer $n$, simulate a hatcheck person randomly giving hats back to people. Determine the number of people who get the correct hat back.

## Writing Projects

**Respond to these with essays using outside sources.**

1. Describe the origins of probability theory and the first uses of this theory, including those by Cardano, Pascal, and Laplace.
2. Describe the different bets you can make when you play roulette. Find the probability of each of these bets in the American version where the wheel contains the numbers 0 and 00. Which is the best bet and which is the worst for you?
3. Discuss the probability of winning when you play the game of blackjack versus a casino. Is there a winning strategy for the person playing against the house?
4. Investigate the game of craps and discuss the probability that the shooter wins and how close to a fair game it is.
5. Discuss issues involved in developing successful spam filters and the current situation in the war between spammers and people trying to filter spam out.
6. Discuss the history and solution of what is known as the Newton–Pepys problem, which asks which is most likely: rolling at least one six when six dice are rolled, rolling at least two sixes when 12 dice are rolled, or rolling at least three sixes when 18 dice are rolled.
7. Explain how Erdős and Rényi first used the probabilistic method and describe some other applications of this method.
8. Discuss the different types of probabilistic algorithms and describe some examples of each type.

CHAPTER

# 9 Relations



Relationships between elements of sets occur in many contexts. Every day we deal with relationships such as those between a business and its telephone number, an employee and his or her salary, a person and a relative, and so on. In mathematics we study relationships such as those between a positive integer and one that it divides, an integer and one that it is congruent to modulo 5, a real number and one that is larger than it, a real number $x$ and the value $f(x)$ where $f$ is a function, and so on. Relationships such as that between a program and a variable it uses, and that between a computer language and a valid statement in this language often arise in computer science.

Relationships between elements of sets are represented using the structure called a relation, which is just a subset of the Cartesian product of the sets. Relations can be used to solve problems such as determining which pairs of cities are linked by airline flights in a network, finding a viable order for the different phases of a complicated project, or producing a useful way to store information in computer databases.

In some computer languages, only the first 31 characters of the name of a variable matter. The relation consisting of ordered pairs of strings where the first string has the same initial 31 characters as the second string is an example of a special type of relation, known as an equivalence relation. Equivalence relations arise throughout mathematics and computer science. We will study equivalence relations, and other special types of relations, in this chapter.

## 9.1 Relations and Their Properties

### Introduction

Links

The most direct way to express a relationship between elements of two sets is to use ordered pairs made up of two related elements. For this reason, sets of ordered pairs are called binary relations. In this section we introduce the basic terminology used to describe binary relations. Later in this chapter we will use relations to solve problems involving communications networks, project scheduling, and identifying elements in sets with common properties.

**DEFINITION 1** Let $A$ and $B$ be sets. A *binary relation from $A$ to $B$* is a subset of $A \times B$.

In other words, a binary relation from $A$ to $B$ is a set $R$ of ordered pairs where the first element of each ordered pair comes from $A$ and the second element comes from $B$. We use the notation $a\,R\,b$ to denote that $(a, b) \in R$ and $a \not R\, b$ to denote that $(a, b) \notin R$. Moreover, when $(a, b)$ belongs to $R$, $a$ is said to be **related to** $b$ by $R$.

Binary relations represent relationships between the elements of two sets. We will introduce $n$-ary relations, which express relationships among elements of more than two sets, later in this chapter. We will omit the word *binary* when there is no danger of confusion.

Examples 1–3 illustrate the notion of a relation.

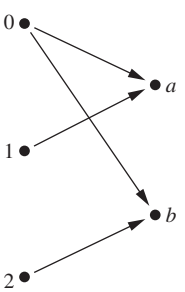
**EXAMPLE 1** Let $A$ be the set of students in your school, and let $B$ be the set of courses. Let $R$ be the relation that consists of those pairs $(a, b)$, where $a$ is a student enrolled in course $b$. For instance, if Jason Goodfriend and Deborah Sherman are enrolled in CS518, the pairs

(Jason Goodfriend, CS518) and (Deborah Sherman, CS518) belong to $R$. If Jason Goodfriend is also enrolled in CS510, then the pair (Jason Goodfriend, CS510) is also in $R$. However, if Deborah Sherman is not enrolled in CS510, then the pair (Deborah Sherman, CS510) is not in $R$.

Note that if a student is not currently enrolled in any courses there will be no pairs in $R$ that have this student as the first element. Similarly, if a course is not currently being offered there will be no pairs in $R$ that have this course as their second element. ◀

**EXAMPLE 2** Let $A$ be the set of cities in the U.S.A., and let $B$ be the set of the 50 states in the U.S.A. Define the relation $R$ by specifying that $(a, b)$ belongs to $R$ if a city with name $a$ is in the state $b$. For instance, (Boulder, Colorado), (Bangor, Maine), (Ann Arbor, Michigan), (Middletown, New Jersey), (Middletown, New York), (Cupertino, California), and (Red Bank, New Jersey) are in $R$. ◀

**EXAMPLE 3** Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. Then $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from $A$ to $B$. This means, for instance, that $0\,R\,a$, but that $1 \not R\, b$. Relations can be represented graphically, as shown in Figure 1, using arrows to represent ordered pairs. Another way to represent this relation is to use a table, which is also done in Figure 1. We will discuss representations of relations in more detail in Section 9.3. ◀




| $R$ | $a$ | $b$ |
|---|---|---|
| 0 | × | × |
| 1 | × | |
| 2 | | × |

**FIGURE 1** **Displaying the Ordered Pairs in the Relation $R$ from Example 3.**

## Functions as Relations

Recall that a function $f$ from a set $A$ to a set $B$ (as defined in Section 2.3) assigns exactly one element of $B$ to each element of $A$. The graph of $f$ is the set of ordered pairs $(a, b)$ such that $b = f(a)$. Because the graph of $f$ is a subset of $A \times B$, it is a relation from $A$ to $B$. Moreover, the graph of a function has the property that every element of $A$ is the first element of exactly one ordered pair of the graph.

Conversely, if $R$ is a relation from $A$ to $B$ such that every element in $A$ is the first element of exactly one ordered pair of $R$, then a function can be defined with $R$ as its graph. This can be done by assigning to an element $a$ of $A$ the unique element $b \in B$ such that $(a, b) \in R$. (Note that the relation $R$ in Example 2 is not the graph of a function because Middletown occurs more than once as the first element of an ordered pair in $R$.)

A relation can be used to express a one-to-many relationship between the elements of the sets $A$ and $B$ (as in Example 2), where an element of $A$ may be related to more than one element of $B$. A function represents a relation where exactly one element of $B$ is related to each element of $A$.

Relations are a generalization of graphs of functions; they can be used to express a much wider class of relationships between sets. (Recall that the graph of the function $f$ from $A$ to $B$ is the set of ordered pairs $(a, f(a))$ for $a \in A$.)

## Relations on a Set

Relations from a set $A$ to itself are of special interest.

**DEFINITION 2** A *relation on a set* $A$ is a relation from $A$ to $A$.

In other words, a relation on a set $A$ is a subset of $A \times A$.

**EXAMPLE 4** Let $A$ be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a \text{ divides } b\}$?

*Solution:* Because $(a, b)$ is in $R$ if and only if $a$ and $b$ are positive integers not exceeding 4 such that $a$ divides $b$, we see that

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

The pairs in this relation are displayed both graphically and in tabular form in Figure 2. ◀

Next, some examples of relations on the set of integers will be given in Example 5.

**EXAMPLE 5** Consider these relations on the set of integers:

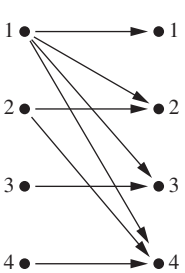
$$R_1 = \{(a, b) \mid a \leq b\},$$
$$R_2 = \{(a, b) \mid a > b\},$$
$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$
$$R_4 = \{(a, b) \mid a = b\},$$
$$R_5 = \{(a, b) \mid a = b + 1\},$$
$$R_6 = \{(a, b) \mid a + b \leq 3\}.$$

Which of these relations contain each of the pairs $(1, 1)$, $(1, 2)$, $(2, 1)$, $(1, -1)$, and $(2, 2)$?

***Remark:*** Unlike the relations in Examples 1–4, these are relations on an infinite set.

*Solution:* The pair $(1, 1)$ is in $R_1$, $R_3$, $R_4$, and $R_6$; $(1, 2)$ is in $R_1$ and $R_6$; $(2, 1)$ is in $R_2$, $R_5$, and $R_6$; $(1, -1)$ is in $R_2$, $R_3$, and $R_6$; and finally, $(2, 2)$ is in $R_1$, $R_3$, and $R_4$. ◀

It is not hard to determine the number of relations on a finite set, because a relation on a set $A$ is simply a subset of $A \times A$.




| $R$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | × | × | × | × |
| 2 | | × | | × |
| 3 | | | × | |
| 4 | | | | × |

**FIGURE 2** **Displaying the Ordered Pairs in the Relation $R$ from Example 4.**

**EXAMPLE 6** How many relations are there on a set with $n$ elements?

*Solution:* A relation on a set $A$ is a subset of $A \times A$. Because $A \times A$ has $n^2$ elements when $A$ has $n$ elements, and a set with $m$ elements has $2^m$ subsets, there are $2^{n^2}$ subsets of $A \times A$. Thus, there are $2^{n^2}$ relations on a set with $n$ elements. For example, there are $2^{3^2} = 2^9 = 512$ relations on the set $\{a, b, c\}$. ◀

## Properties of Relations

There are several properties that are used to classify relations on a set. We will introduce the most important of these here.

In some relations an element is always related to itself. For instance, let $R$ be the relation on the set of all people consisting of pairs $(x, y)$ where $x$ and $y$ have the same mother and the same father. Then $x\,R\,x$ for every person $x$.

**DEFINITION 3** A relation $R$ on a set $A$ is called *reflexive* if $(a, a) \in R$ for every element $a \in A$.

***Remark:*** Using quantifiers we see that the relation $R$ on the set $A$ is reflexive if $\forall a((a, a) \in R)$, where the universe of discourse is the set of all elements in $A$.

We see that a relation on $A$ is reflexive if every element of $A$ is related to itself. Examples 7–9 illustrate the concept of a reflexive relation.

**EXAMPLE 7** Consider the following relations on $\{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$
$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$
$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$
$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$
$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$
$$R_6 = \{(3, 4)\}.$$

Which of these relations are reflexive?

*Solution:* The relations $R_3$ and $R_5$ are reflexive because they both contain all pairs of the form $(a, a)$, namely, $(1, 1)$, $(2, 2)$, $(3, 3)$, and $(4, 4)$. The other relations are not reflexive because they do not contain all of these ordered pairs. In particular, $R_1$, $R_2$, $R_4$, and $R_6$ are not reflexive because $(3, 3)$ is not in any of these relations. ◀

**EXAMPLE 8** Which of the relations from Example 5 are reflexive?

*Solution:* The reflexive relations from Example 5 are $R_1$ (because $a \leq a$ for every integer $a$), $R_3$, and $R_4$. For each of the other relations in this example it is easy to find a pair of the form $(a, a)$ that is not in the relation. (This is left as an exercise for the reader.) ◀

**EXAMPLE 9** Is the "divides" relation on the set of positive integers reflexive?

*Solution:* Because $a \mid a$ whenever $a$ is a positive integer, the "divides" relation is reflexive. (Note that if we replace the set of positive integers with the set of all integers the relation is not reflexive because by definition 0 does not divide 0.) ◀

In some relations an element is related to a second element if and only if the second element is also related to the first element. The relation consisting of pairs $(x, y)$, where $x$ and $y$ are students at your school with at least one common class has this property. Other relations have the property that if an element is related to a second element, then this second element is not related to the first. The relation consisting of the pairs $(x, y)$, where $x$ and $y$ are students at your school, where $x$ has a higher grade point average than $y$ has this property.

**DEFINITION 4** A relation $R$ on a set $A$ is called *symmetric* if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$. A relation $R$ on a set $A$ such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called *antisymmetric*.

***Remark:*** Using quantifiers, we see that the relation $R$ on the set $A$ is symmetric if $\forall a \forall b((a, b) \in R \rightarrow (b, a) \in R)$. Similarly, the relation $R$ on the set $A$ is antisymmetric if $\forall a \forall b(((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b))$.

That is, a relation is symmetric if and only if $a$ is related to $b$ implies that $b$ is related to $a$. A relation is antisymmetric if and only if there are no pairs of distinct elements $a$ and $b$ with $a$ related to $b$ and $b$ related to $a$. That is, the only way to have $a$ related to $b$ and $b$ related to $a$ is for $a$ and $b$ to be the same element. The terms *symmetric* and *antisymmetric* are not opposites, because a relation can have both of these properties or may lack both of them (see Exercise 10). A relation cannot be both symmetric and antisymmetric if it contains some pair of the form $(a, b)$, where $a \neq b$.

***Remark:*** Although relatively few of the $2^{n^2}$ relations on a set with $n$ elements are symmetric or antisymmetric, as counting arguments can show, many important relations have one of these properties. (See Exercise 47.)

**EXAMPLE 10** Which of the relations from Example 7 are symmetric and which are antisymmetric?

Extra Examples

*Solution:* The relations $R_2$ and $R_3$ are symmetric, because in each case $(b, a)$ belongs to the relation whenever $(a, b)$ does. For $R_2$, the only thing to check is that both $(2, 1)$ and $(1, 2)$ are in the relation. For $R_3$, it is necessary to check that both $(1, 2)$ and $(2, 1)$ belong to the relation, and $(1, 4)$ and $(4, 1)$ belong to the relation. The reader should verify that none of the other relations is symmetric. This is done by finding a pair $(a, b)$ such that it is in the relation but $(b, a)$ is not.

$R_4$, $R_5$, and $R_6$ are all antisymmetric. For each of these relations there is no pair of elements $a$ and $b$ with $a \neq b$ such that both $(a, b)$ and $(b, a)$ belong to the relation. The reader should verify that none of the other relations is antisymmetric. This is done by finding a pair $(a, b)$ with $a \neq b$ such that $(a, b)$ and $(b, a)$ are both in the relation. ◀

**EXAMPLE 11** Which of the relations from Example 5 are symmetric and which are antisymmetric?

*Solution:* The relations $R_3$, $R_4$, and $R_6$ are symmetric. $R_3$ is symmetric, for if $a = b$ or $a = -b$, then $b = a$ or $b = -a$. $R_4$ is symmetric because $a = b$ implies that $b = a$. $R_6$ is symmetric because $a + b \leq 3$ implies that $b + a \leq 3$. The reader should verify that none of the other relations is symmetric.

The relations $R_1$, $R_2$, $R_4$, and $R_5$ are antisymmetric. $R_1$ is antisymmetric because the inequalities $a \leq b$ and $b \leq a$ imply that $a = b$. $R_2$ is antisymmetric because it is impossible that $a > b$ and $b > a$. $R_4$ is antisymmetric, because two elements are related with respect to $R_4$ if and only if they are equal. $R_5$ is antisymmetric because it is impossible that $a = b + 1$ and $b = a + 1$. The reader should verify that none of the other relations is antisymmetric. ◀

**EXAMPLE 12** Is the "divides" relation on the set of positive integers symmetric? Is it antisymmetric?

*Solution:* This relation is not symmetric because $1 \mid 2$, but $2 \nmid 1$. It is antisymmetric, for if $a$ and $b$ are positive integers with $a \mid b$ and $b \mid a$, then $a = b$ (the verification of this is left as an exercise for the reader). ◀

Let $R$ be the relation consisting of all pairs $(x, y)$ of students at your school, where $x$ has taken more credits than $y$. Suppose that $x$ is related to $y$ and $y$ is related to $z$. This means that $x$ has taken more credits than $y$ and $y$ has taken more credits than $z$. We can conclude that $x$ has taken more credits than $z$, so that $x$ is related to $z$. What we have shown is that $R$ has the transitive property, which is defined as follows.

**DEFINITION 5** A relation $R$ on a set $A$ is called *transitive* if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

***Remark:*** Using quantifiers we see that the relation $R$ on a set $A$ is transitive if we have $\forall a \forall b \forall c(((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R)$.

**EXAMPLE 13** Which of the relations in Example 7 are transitive?

Extra Examples

*Solution:* $R_4$, $R_5$, and $R_6$ are transitive. For each of these relations, we can show that it is transitive by verifying that if $(a, b)$ and $(b, c)$ belong to this relation, then $(a, c)$ also does. For instance, $R_4$ is transitive, because (3, 2) and (2, 1), (4, 2) and (2, 1), (4, 3) and (3, 1), and (4, 3) and (3, 2) are the only such sets of pairs, and (3, 1), (4, 1), and (4, 2) belong to $R_4$. The reader should verify that $R_5$ and $R_6$ are transitive.

$R_1$ is not transitive because (3, 4) and (4, 1) belong to $R_1$, but (3, 1) does not. $R_2$ is not transitive because (2, 1) and (1, 2) belong to $R_2$, but (2, 2) does not. $R_3$ is not transitive because (4, 1) and (1, 2) belong to $R_3$, but (4, 2) does not. ◀

**EXAMPLE 14** Which of the relations in Example 5 are transitive?

*Solution:* The relations $R_1$, $R_2$, $R_3$, and $R_4$ are transitive. $R_1$ is transitive because $a \leq b$ and $b \leq c$ imply that $a \leq c$. $R_2$ is transitive because $a > b$ and $b > c$ imply that $a > c$. $R_3$ is transitive because $a = \pm b$ and $b = \pm c$ imply that $a = \pm c$. $R_4$ is clearly transitive, as the reader should verify. $R_5$ is not transitive because (2, 1) and (1, 0) belong to $R_5$, but (2, 0) does not. $R_6$ is not transitive because (2, 1) and (1, 2) belong to $R_6$, but (2, 2) does not. ◀

**EXAMPLE 15** Is the "divides" relation on the set of positive integers transitive?

*Solution:* Suppose that $a$ divides $b$ and $b$ divides $c$. Then there are positive integers $k$ and $l$ such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so $a$ divides $c$. It follows that this relation is transitive. ◀

We can use counting techniques to determine the number of relations with specific properties. Finding the number of relations with a particular property provides information about how common this property is in the set of all relations on a set with $n$ elements.

**EXAMPLE 16** How many reflexive relations are there on a set with $n$ elements?

*Solution:* A relation $R$ on a set $A$ is a subset of $A \times A$. Consequently, a relation is determined by specifying whether each of the $n^2$ ordered pairs in $A \times A$ is in $R$. However, if $R$ is reflexive, each of the $n$ ordered pairs $(a, a)$ for $a \in A$ must be in $R$. Each of the other $n(n - 1)$ ordered

pairs of the form $(a, b)$, where $a \neq b$, may or may not be in $R$. Hence, by the product rule for counting, there are $2^{n(n-1)}$ reflexive relations [this is the number of ways to choose whether each element $(a, b)$, with $a \neq b$, belongs to $R$]. ◀

Formulas for the number of symmetric relations and the number of antisymmetric relations on a set with $n$ elements can be found using reasoning similar to that in Example 16 (see Exercise 47). However, no general formula is known that counts the transitive relations on a set with $n$ elements. Currently, $T(n)$, the number of transitive relations on a set with $n$ elements, is known only for $n \leq 17$. For example, $T(4) = 3{,}994$, $T(5) = 154{,}303$, and $T(6) = 9{,}415{,}189$.

## Combining Relations

Because relations from $A$ to $B$ are subsets of $A \times B$, two relations from $A$ to $B$ can be combined in any way two sets can be combined. Consider Examples 17–19.

**EXAMPLE 17** Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4\}$. The relations $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ and $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$ can be combined to obtain

$$R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\},$$
$$R_1 \cap R_2 = \{(1, 1)\},$$
$$R_1 - R_2 = \{(2, 2), (3, 3)\},$$
$$R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}.$$

◀

**EXAMPLE 18** Let $A$ and $B$ be the set of all students and the set of all courses at a school, respectively. Suppose that $R_1$ consists of all ordered pairs $(a, b)$, where $a$ is a student who has taken course $b$, and $R_2$ consists of all ordered pairs $(a, b)$, where $a$ is a student who requires course $b$ to graduate. What are the relations $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 \oplus R_2$, $R_1 - R_2$, and $R_2 - R_1$?

*Solution:* The relation $R_1 \cup R_2$ consists of all ordered pairs $(a, b)$, where $a$ is a student who either has taken course $b$ or needs course $b$ to graduate, and $R_1 \cap R_2$ is the set of all ordered pairs $(a, b)$, where $a$ is a student who has taken course $b$ and needs this course to graduate. Also, $R_1 \oplus R_2$ consists of all ordered pairs $(a, b)$, where student $a$ has taken course $b$ but does not need it to graduate or needs course $b$ to graduate but has not taken it. $R_1 - R_2$ is the set of ordered pairs $(a, b)$, where $a$ has taken course $b$ but does not need it to graduate; that is, $b$ is an elective course that $a$ has taken. $R_2 - R_1$ is the set of all ordered pairs $(a, b)$, where $b$ is a course that $a$ needs to graduate but has not taken. ◀

**EXAMPLE 19** Let $R_1$ be the "less than" relation on the set of real numbers and let $R_2$ be the "greater than" relation on the set of real numbers, that is, $R_1 = \{(x, y) \mid x < y\}$ and $R_2 = \{(x, y) \mid x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

*Solution:* We note that $(x, y) \in R_1 \cup R_2$ if and only if $(x, y) \in R_1$ or $(x, y) \in R_2$. Hence, $(x, y) \in R_1 \cup R_2$ if and only if $x < y$ or $x > y$. Because the condition $x < y$ or $x > y$ is the same as the condition $x \neq y$, it follows that $R_1 \cup R_2 = \{(x, y) \mid x \neq y\}$. In other words, the union of the "less than" relation and the "greater than" relation is the "not equals" relation.

Next, note that it is impossible for a pair $(x, y)$ to belong to both $R_1$ and $R_2$ because it is impossible that $x < y$ and $x > y$. It follows that $R_1 \cap R_2 = \emptyset$. We also see that $R_1 - R_2 = R_1$, $R_2 - R_1 = R_2$, and $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(x, y) \mid x \neq y\}$. ◀

There is another way that relations are combined that is analogous to the composition of functions.

**DEFINITION 6** Let $R$ be a relation from a set $A$ to a set $B$ and $S$ a relation from $B$ to a set $C$. The *composite* of $R$ and $S$ is the relation consisting of ordered pairs $(a, c)$, where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. We denote the composite of $R$ and $S$ by $S \circ R$.

Computing the composite of two relations requires that we find elements that are the second element of ordered pairs in the first relation and the first element of ordered pairs in the second relation, as Examples 20 and 21 illustrate.

**EXAMPLE 20** What is the composite of the relations $R$ and $S$, where $R$ is the relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ with $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$ and $S$ is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$?

*Solution:* $S \circ R$ is constructed using all ordered pairs in $R$ and ordered pairs in $S$, where the second element of the ordered pair in $R$ agrees with the first element of the ordered pair in $S$. For example, the ordered pairs $(2, 3)$ in $R$ and $(3, 1)$ in $S$ produce the ordered pair $(2, 1)$ in $S \circ R$. Computing all the ordered pairs in the composite, we find

$$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}.$$ ◀

**EXAMPLE 21** **Composing the Parent Relation with Itself** Let $R$ be the relation on the set of all people such that $(a, b) \in R$ if person $a$ is a parent of person $b$. Then $(a, c) \in R \circ R$ if and only if there is a person $b$ such that $(a, b) \in R$ and $(b, c) \in R$, that is, if and only if there is a person $b$ such that $a$ is a parent of $b$ and $b$ is a parent of $c$. In other words, $(a, c) \in R \circ R$ if and only if $a$ is a grandparent of $c$. ◀

The powers of a relation $R$ can be recursively defined from the definition of a composite of two relations.

**DEFINITION 7** Let $R$ be a relation on the set $A$. The powers $R^n$, $n = 1, 2, 3, \ldots$, are defined recursively by

$$R^1 = R \qquad \text{and} \qquad R^{n+1} = R^n \circ R.$$

The definition shows that $R^2 = R \circ R$, $R^3 = R^2 \circ R = (R \circ R) \circ R$, and so on.

**EXAMPLE 22** Let $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$. Find the powers $R^n$, $n = 2, 3, 4, \ldots$.

*Solution:* Because $R^2 = R \circ R$, we find that $R^2 = \{(1, 1), (2, 1), (3, 1), (4, 2)\}$. Furthermore, because $R^3 = R^2 \circ R$, $R^3 = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$. Additional computation shows that $R^4$ is the same as $R^3$, so $R^4 = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$. It also follows that $R^n = R^3$ for $n = 5, 6, 7, \ldots$. The reader should verify this. ◀

The following theorem shows that the powers of a transitive relation are subsets of this relation. It will be used in Section 9.4.

**THEOREM 1** The relation $R$ on a set $A$ is transitive if and only if $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$.

***Proof:*** We first prove the "if" part of the theorem. We suppose that $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$. In particular, $R^2 \subseteq R$. To see that this implies $R$ is transitive, note that if $(a, b) \in R$ and $(b, c) \in R$, then by the definition of composition, $(a, c) \in R^2$. Because $R^2 \subseteq R$, this means that $(a, c) \in R$. Hence, $R$ is transitive.

We will use mathematical induction to prove the only if part of the theorem. Note that this part of the theorem is trivially true for $n = 1$.

Assume that $R^n \subseteq R$, where $n$ is a positive integer. This is the inductive hypothesis. To complete the inductive step we must show that this implies that $R^{n+1}$ is also a subset of $R$. To show this, assume that $(a, b) \in R^{n+1}$. Then, because $R^{n+1} = R^n \circ R$, there is an element $x$ with $x \in A$ such that $(a, x) \in R$ and $(x, b) \in R^n$. The inductive hypothesis, namely, that $R^n \subseteq R$, implies that $(x, b) \in R$. Furthermore, because $R$ is transitive, and $(a, x) \in R$ and $(x, b) \in R$, it follows that $(a, b) \in R$. This shows that $R^{n+1} \subseteq R$, completing the proof. ◁

## Exercises

**1.** List the ordered pairs in the relation $R$ from $A = \{0, 1, 2, 3, 4\}$ to $B = \{0, 1, 2, 3\}$, where $(a, b) \in R$ if and only if

**a)** $a = b$. **b)** $a + b = 4$.
**c)** $a > b$. **d)** $a \mid b$.
**e)** $\gcd(a, b) = 1$. **f)** $\text{lcm}(a, b) = 2$.

**2. a)** List all the ordered pairs in the relation $R = \{(a, b) \mid a \text{ divides } b\}$ on the set $\{1, 2, 3, 4, 5, 6\}$.
**b)** Display this relation graphically, as was done in Example 4.
**c)** Display this relation in tabular form, as was done in Example 4.

**3.** For each of these relations on the set $\{1, 2, 3, 4\}$, decide whether it is reflexive, whether it is symmetric, whether it is antisymmetric, and whether it is transitive.

**a)** $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$
**b)** $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$
**c)** $\{(2, 4), (4, 2)\}$
**d)** $\{(1, 2), (2, 3), (3, 4)\}$
**e)** $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$
**f)** $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$

**4.** Determine whether the relation $R$ on the set of all people is reflexive, symmetric, antisymmetric, and/or transitive, where $(a, b) \in R$ if and only if

**a)** $a$ is taller than $b$.
**b)** $a$ and $b$ were born on the same day.
**c)** $a$ has the same first name as $b$.
**d)** $a$ and $b$ have a common grandparent.

**5.** Determine whether the relation $R$ on the set of all Web pages is reflexive, symmetric, antisymmetric, and/or transitive, where $(a, b) \in R$ if and only if

**a)** everyone who has visited Web page $a$ has also visited Web page $b$.
**b)** there are no common links found on both Web page $a$ and Web page $b$.
**c)** there is at least one common link on Web page $a$ and Web page $b$.
**d)** there is a Web page that includes links to both Web page $a$ and Web page $b$.

**6.** Determine whether the relation $R$ on the set of all real numbers is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

**a)** $x + y = 0$. **b)** $x = \pm y$.
**c)** $x - y$ is a rational number.
**d)** $x = 2y$. **e)** $xy \geq 0$.
**f)** $xy = 0$. **g)** $x = 1$.
**h)** $x = 1$ or $y = 1$.

**7.** Determine whether the relation $R$ on the set of all integers is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

**a)** $x \neq y$. **b)** $xy \geq 1$.
**c)** $x = y + 1$ or $x = y - 1$.
**d)** $x \equiv y \pmod 7$. **e)** $x$ is a multiple of $y$.
**f)** $x$ and $y$ are both negative or both nonnegative.
**g)** $x = y^2$. **h)** $x \geq y^2$.

**8.** Show that the relation $R = \emptyset$ on a nonempty set $S$ is symmetric and transitive, but not reflexive.

**9.** Show that the relation $R = \emptyset$ on the empty set $S = \emptyset$ is reflexive, symmetric, and transitive.

**10.** Give an example of a relation on a set that is

**a)** both symmetric and antisymmetric.
**b)** neither symmetric nor antisymmetric.

A relation $R$ on the set $A$ is **irreflexive** if for every $a \in A$, $(a, a) \notin R$. That is, $R$ is irreflexive if no element in $A$ is related to itself.

**11.** Which relations in Exercise 3 are irreflexive?

**12.** Which relations in Exercise 4 are irreflexive?

**13.** Which relations in Exercise 5 are irreflexive?

**14.** Which relations in Exercise 6 are irreflexive?

**15.** Can a relation on a set be neither reflexive nor irreflexive?

**16.** Use quantifiers to express what it means for a relation to be irreflexive.

**17.** Give an example of an irreflexive relation on the set of all people.

A relation $R$ is called **asymmetric** if $(a, b) \in R$ implies that $(b, a) \notin R$. Exercises 18–24 explore the notion of an asymmetric relation. Exercise 22 focuses on the difference between asymmetry and antisymmetry.

**18.** Which relations in Exercise 3 are asymmetric?

**19.** Which relations in Exercise 4 are asymmetric?

**20.** Which relations in Exercise 5 are asymmetric?

**21.** Which relations in Exercise 6 are asymmetric?

**22.** Must an asymmetric relation also be antisymmetric? Must an antisymmetric relation be asymmetric? Give reasons for your answers.

**23.** Use quantifiers to express what it means for a relation to be asymmetric.

**24.** Give an example of an asymmetric relation on the set of all people.

**25.** How many different relations are there from a set with $m$ elements to a set with $n$ elements?

☞ Let $R$ be a relation from a set $A$ to a set $B$. The **inverse relation** from $B$ to $A$, denoted by $R^{-1}$, is the set of ordered pairs $\{(b, a) \mid (a, b) \in R\}$. The **complementary relation** $\overline{R}$ is the set of ordered pairs $\{(a, b) \mid (a, b) \notin R\}$.

**26.** Let $R$ be the relation $R = \{(a, b) \mid a < b\}$ on the set of integers. Find

**a)** $R^{-1}$. **b)** $\overline{R}$.

**27.** Let $R$ be the relation $R = \{(a, b) \mid a \text{ divides } b\}$ on the set of positive integers. Find

**a)** $R^{-1}$. **b)** $\overline{R}$.

**28.** Let $R$ be the relation on the set of all states in the United States consisting of pairs $(a, b)$ where state $a$ borders state $b$. Find

**a)** $R^{-1}$. **b)** $\overline{R}$.

**29.** Suppose that the function $f$ from $A$ to $B$ is a one-to-one correspondence. Let $R$ be the relation that equals the graph of $f$. That is, $R = \{(a, f(a)) \mid a \in A\}$. What is the inverse relation $R^{-1}$?

**30.** Let $R_1 = \{(1, 2), (2, 3), (3, 4)\}$ and $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (3, 4)\}$ be relations from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$. Find

**a)** $R_1 \cup R_2$. **b)** $R_1 \cap R_2$.

**c)** $R_1 - R_2$. **d)** $R_2 - R_1$.

**31.** Let $A$ be the set of students at your school and $B$ the set of books in the school library. Let $R_1$ and $R_2$ be the relations consisting of all ordered pairs $(a, b)$, where student $a$ is required to read book $b$ in a course, and where student $a$ has read book $b$, respectively. Describe the ordered pairs in each of these relations.

**a)** $R_1 \cup R_2$ **b)** $R_1 \cap R_2$

**c)** $R_1 \oplus R_2$ **d)** $R_1 - R_2$

**e)** $R_2 - R_1$

**32.** Let $R$ be the relation $\{(1, 2), (1, 3), (2, 3), (2, 4), (3, 1)\}$, and let $S$ be the relation $\{(2, 1), (3, 1), (3, 2), (4, 2)\}$. Find $S \circ R$.

**33.** Let $R$ be the relation on the set of people consisting of pairs $(a, b)$, where $a$ is a parent of $b$. Let $S$ be the relation on the set of people consisting of pairs $(a, b)$, where $a$ and $b$ are siblings (brothers or sisters). What are $S \circ R$ and $R \circ S$?

Exercises 34–37 deal with these relations on the set of real numbers:

$R_1 = \{(a, b) \in \mathbf{R}^2 \mid a > b\}$, the "greater than" relation,

$R_2 = \{(a, b) \in \mathbf{R}^2 \mid a \geq b\}$, the "greater than or equal to" relation,

$R_3 = \{(a, b) \in \mathbf{R}^2 \mid a < b\}$, the "less than" relation,

$R_4 = \{(a, b) \in \mathbf{R}^2 \mid a \leq b\}$, the "less than or equal to" relation,

$R_5 = \{(a, b) \in \mathbf{R}^2 \mid a = b\}$, the "equal to" relation,

$R_6 = \{(a, b) \in \mathbf{R}^2 \mid a \neq b\}$, the "unequal to" relation.

**34.** Find

**a)** $R_1 \cup R_3$. **b)** $R_1 \cup R_5$.

**c)** $R_2 \cap R_4$. **d)** $R_3 \cap R_5$.

**e)** $R_1 - R_2$. **f)** $R_2 - R_1$.

**g)** $R_1 \oplus R_3$. **h)** $R_2 \oplus R_4$.

**35.** Find

**a)** $R_2 \cup R_4$. **b)** $R_3 \cup R_6$.

**c)** $R_3 \cap R_6$. **d)** $R_4 \cap R_6$.

**e)** $R_3 - R_6$. **f)** $R_6 - R_3$.

**g)** $R_2 \oplus R_6$. **h)** $R_3 \oplus R_5$.

**36.** Find

**a)** $R_1 \circ R_1$. **b)** $R_1 \circ R_2$.

**c)** $R_1 \circ R_3$. **d)** $R_1 \circ R_4$.

**e)** $R_1 \circ R_5$. **f)** $R_1 \circ R_6$.

**g)** $R_2 \circ R_3$. **h)** $R_3 \circ R_3$.

**37.** Find

**a)** $R_2 \circ R_1$. **b)** $R_2 \circ R_2$.

**c)** $R_3 \circ R_5$. **d)** $R_4 \circ R_1$.

**e)** $R_5 \circ R_3$. **f)** $R_3 \circ R_6$.

**g)** $R_4 \circ R_6$. **h)** $R_6 \circ R_6$.

**38.** Let $R$ be the parent relation on the set of all people (see Example 21). When is an ordered pair in the relation $R^3$?

**39.** Let $R$ be the relation on the set of people with doctorates such that $(a, b) \in R$ if and only if $a$ was the thesis advisor of $b$. When is an ordered pair $(a, b)$ in $R^2$? When is an ordered pair $(a, b)$ in $R^n$, when $n$ is a positive integer? (Assume that every person with a doctorate has a thesis advisor.)

**40.** Let $R_1$ and $R_2$ be the "divides" and "is a multiple of" relations on the set of all positive integers, respectively. That is, $R_1 = \{(a, b) \mid a \text{ divides } b\}$ and $R_2 = \{(a, b) \mid a \text{ is a multiple of } b\}$. Find

**a)** $R_1 \cup R_2$. **b)** $R_1 \cap R_2$.

**c)** $R_1 - R_2$. **d)** $R_2 - R_1$.

**e)** $R_1 \oplus R_2$.

**41.** Let $R_1$ and $R_2$ be the "congruent modulo 3" and the "congruent modulo 4" relations, respectively, on the set of integers. That is, $R_1 = \{(a, b) \mid a \equiv b \pmod 3\}$ and $R_2 = \{(a, b) \mid a \equiv b \pmod 4\}$. Find

**a)** $R_1 \cup R_2$. **b)** $R_1 \cap R_2$.
**c)** $R_1 - R_2$. **d)** $R_2 - R_1$.
**e)** $R_1 \oplus R_2$.

**42.** List the 16 different relations on the set $\{0, 1\}$.

**43.** How many of the 16 different relations on $\{0, 1\}$ contain the pair $(0, 1)$?

**44.** Which of the 16 relations on $\{0, 1\}$, which you listed in Exercise 42, are

**a)** reflexive? **b)** irreflexive?
**c)** symmetric? **d)** antisymmetric?
**e)** asymmetric? **f)** transitive?

**45. a)** How many relations are there on the set $\{a, b, c, d\}$?
**b)** How many relations are there on the set $\{a, b, c, d\}$ that contain the pair $(a, a)$?

**46.** Let $S$ be a set with $n$ elements and let $a$ and $b$ be distinct elements of $S$. How many relations $R$ are there on $S$ such that

**a)** $(a, b) \in R$? **b)** $(a, b) \notin R$?
**c)** no ordered pair in $R$ has $a$ as its first element?
**d)** at least one ordered pair in $R$ has $a$ as its first element?
**e)** no ordered pair in $R$ has $a$ as its first element or $b$ as its second element?
**f)** at least one ordered pair in $R$ either has $a$ as its first element or has $b$ as its second element?

***47.** How many relations are there on a set with $n$ elements that are

**a)** symmetric? **b)** antisymmetric?
**c)** asymmetric? **d)** irreflexive?
**e)** reflexive and symmetric?
**f)** neither reflexive nor irreflexive?

***48.** How many transitive relations are there on a set with $n$ elements if

**a)** $n = 1$? **b)** $n = 2$? **c)** $n = 3$?

**49.** Find the error in the "proof" of the following "theorem."

"*Theorem*": Let $R$ be a relation on a set $A$ that is symmetric and transitive. Then $R$ is reflexive.

"*Proof*": Let $a \in A$. Take an element $b \in A$ such that $(a, b) \in R$. Because $R$ is symmetric, we also have $(b, a) \in R$. Now using the transitive property, we can conclude that $(a, a) \in R$ because $(a, b) \in R$ and $(b, a) \in R$.

**50.** Suppose that $R$ and $S$ are reflexive relations on a set $A$. Prove or disprove each of these statements.

**a)** $R \cup S$ is reflexive.
**b)** $R \cap S$ is reflexive.
**c)** $R \oplus S$ is irreflexive.
**d)** $R - S$ is irreflexive.
**e)** $S \circ R$ is reflexive.

**51.** Show that the relation $R$ on a set $A$ is symmetric if and only if $R = R^{-1}$, where $R^{-1}$ is the inverse relation.

**52.** Show that the relation $R$ on a set $A$ is antisymmetric if and only if $R \cap R^{-1}$ is a subset of the diagonal relation $\Delta = \{(a, a) \mid a \in A\}$.

**53.** Show that the relation $R$ on a set $A$ is reflexive if and only if the inverse relation $R^{-1}$ is reflexive.

**54.** Show that the relation $R$ on a set $A$ is reflexive if and only if the complementary relation $\overline{R}$ is irreflexive.

**55.** Let $R$ be a relation that is reflexive and transitive. Prove that $R^n = R$ for all positive integers $n$.

**56.** Let $R$ be the relation on the set $\{1, 2, 3, 4, 5\}$ containing the ordered pairs $(1, 1), (1, 2), (1, 3), (2, 3), (2, 4), (3, 1), (3, 4), (3, 5), (4, 2), (4, 5), (5, 1), (5, 2)$, and $(5, 4)$. Find

**a)** $R^2$. **b)** $R^3$. **c)** $R^4$. **d)** $R^5$.

**57.** Let $R$ be a reflexive relation on a set $A$. Show that $R^n$ is reflexive for all positive integers $n$.

***58.** Let $R$ be a symmetric relation. Show that $R^n$ is symmetric for all positive integers $n$.

**59.** Suppose that the relation $R$ is irreflexive. Is $R^2$ necessarily irreflexive? Give a reason for your answer.

# 9.2 $n$-ary Relations and Their Applications

## Introduction

Relationships among elements of more than two sets often arise. For instance, there is a relationship involving the name of a student, the student's major, and the student's grade point average. Similarly, there is a relationship involving the airline, flight number, starting point, destination, departure time, and arrival time of a flight. An example of such a relationship in mathematics involves three integers, where the first integer is larger than the second integer, which is larger than the third. Another example is the betweenness relationship involving points on a line, such that three points are related when the second point is between the first and the third.

We will study relationships among elements from more than two sets in this section. These relationships are called ***n*-ary relations**. These relations are used to represent computer databases. These representations help us answer queries about the information stored in databases, such as: Which flights land at O'Hare Airport between 3 A.M. and 4 A.M.? Which students at your

school are sophomores majoring in mathematics or computer science and have greater than a 3.0 average? Which employees of a company have worked for the company less than 5 years and make more than $50,000?

## *n*-ary Relations

We begin with the basic definition on which the theory of relational databases rests.

**DEFINITION 1** Let $A_1, A_2, \ldots, A_n$ be sets. An *n-ary relation* on these sets is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The sets $A_1, A_2, \ldots, A_n$ are called the *domains* of the relation, and $n$ is called its *degree*.

**EXAMPLE 1** Let $R$ be the relation on $\mathbf{N} \times \mathbf{N} \times \mathbf{N}$ consisting of triples $(a, b, c)$, where $a$, $b$, and $c$ are integers with $a < b < c$. Then $(1, 2, 3) \in R$, but $(2, 4, 3) \notin R$. The degree of this relation is 3. Its domains are all equal to the set of natural numbers. ◀

**EXAMPLE 2** Let $R$ be the relation on $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$ consisting of all triples of integers $(a, b, c)$ in which $a$, $b$, and $c$ form an arithmetic progression. That is, $(a, b, c) \in R$ if and only if there is an integer $k$ such that $b = a + k$ and $c = a + 2k$, or equivalently, such that $b - a = k$ and $c - b = k$. Note that $(1, 3, 5) \in R$ because $3 = 1 + 2$ and $5 = 1 + 2 \cdot 2$, but $(2, 5, 9) \notin R$ because $5 - 2 = 3$ while $9 - 5 = 4$. This relation has degree 3 and its domains are all equal to the set of integers. ◀

**EXAMPLE 3** Let $R$ be the relation on $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}^+$ consisting of triples $(a, b, m)$, where $a$, $b$, and $m$ are integers with $m \geq 1$ and $a \equiv b \pmod{m}$. Then $(8, 2, 3)$, $(-1, 9, 5)$, and $(14, 0, 7)$ all belong to $R$, but $(7, 2, 3)$, $(-2, -8, 5)$, and $(11, 0, 6)$ do not belong to $R$ because $8 \equiv 2 \pmod 3$, $-1 \equiv 9 \pmod 5$, and $14 \equiv 0 \pmod 7$, but $7 \not\equiv 2 \pmod 3$, $-2 \not\equiv -8 \pmod 5$, and $11 \not\equiv 0 \pmod 6$. This relation has degree 3 and its first two domains are the set of all integers and its third domain is the set of positive integers. ◀

**EXAMPLE 4** Let $R$ be the relation consisting of 5-tuples $(A, N, S, D, T)$ representing airplane flights, where $A$ is the airline, $N$ is the flight number, $S$ is the starting point, $D$ is the destination, and $T$ is the departure time. For instance, if Nadir Express Airlines has flight 963 from Newark to Bangor at 15:00, then (Nadir, 963, Newark, Bangor, 15:00) belongs to $R$. The degree of this relation is 5, and its domains are the set of all airlines, the set of flight numbers, the set of cities, the set of cities (again), and the set of times. ◀

## Databases and Relations

Links

The time required to manipulate information in a database depends on how this information is stored. The operations of adding and deleting records, updating records, searching for records, and combining records from overlapping databases are performed millions of times each day in a large database. Because of the importance of these operations, various methods for representing databases have been developed. We will discuss one of these methods, called the **relational data model**, based on the concept of a relation.

A database consists of **records**, which are $n$-tuples, made up of **fields**. The fields are the entries of the $n$-tuples. For instance, a database of student records may be made up of fields containing the name, student number, major, and grade point average of the student. The relational data model represents a database of records as an $n$-ary relation. Thus, student records

**TABLE 1** **Students.**

| *Student_name* | *ID_number* | *Major* | *GPA* |
|---|---|---|---|
| Ackermann | 231455 | Computer Science | 3.88 |
| Adams | 888323 | Physics | 3.45 |
| Chou | 102147 | Computer Science | 3.49 |
| Goodfriend | 453876 | Mathematics | 3.45 |
| Rao | 678543 | Mathematics | 3.90 |
| Stevens | 786576 | Psychology | 2.99 |

are represented as 4-tuples of the form (*Student_name, ID_number, Major, GPA*). A sample database of six such records is

(Ackermann, 231455, Computer Science, 3.88)
(Adams, 888323, Physics, 3.45)
(Chou, 102147, Computer Science, 3.49)
(Goodfriend, 453876, Mathematics, 3.45)
(Rao, 678543, Mathematics, 3.90)
(Stevens, 786576, Psychology, 2.99).

Relations used to represent databases are also called **tables**, because these relations are often displayed as tables. Each column of the table corresponds to an *attribute* of the database. For instance, the same database of students is displayed in Table 1. The attributes of this database are Student Name, ID Number, Major, and GPA.

A domain of an $n$-ary relation is called a **primary key** when the value of the $n$-tuple from this domain determines the $n$-tuple. That is, a domain is a primary key when no two $n$-tuples in the relation have the same value from this domain.

Records are often added to or deleted from databases. Because of this, the property that a domain is a primary key is time-dependent. Consequently, a primary key should be chosen that remains one whenever the database is changed. The current collection of $n$-tuples in a relation is called the **extension** of the relation. The more permanent part of a database, including the name and attributes of the database, is called its **intension**. When selecting a primary key, the goal should be to select a key that can serve as a primary key for all possible extensions of the database. To do this, it is necessary to examine the intension of the database to understand the set of possible $n$-tuples that can occur in an extension.

**EXAMPLE 5** Which domains are primary keys for the $n$-ary relation displayed in Table 1, assuming that no $n$-tuples will be added in the future?

*Solution:* Because there is only one 4-tuple in this table for each student name, the domain of student names is a primary key. Similarly, the ID numbers in this table are unique, so the domain of ID numbers is also a primary key. However, the domain of major fields of study is not a primary key, because more than one 4-tuple contains the same major field of study. The domain of grade point averages is also not a primary key, because there are two 4-tuples containing the same GPA. ◀

Combinations of domains can also uniquely identify $n$-tuples in an $n$-ary relation. When the values of a set of domains determine an $n$-tuple in a relation, the Cartesian product of these domains is called a **composite key**.

**EXAMPLE 6** Is the Cartesian product of the domain of major fields of study and the domain of GPAs a composite key for the $n$-ary relation from Table 1, assuming that no $n$-tuples are ever added?

*Solution:* Because no two 4-tuples from this table have both the same major and the same GPA, this Cartesian product is a composite key. ◀

Because primary and composite keys are used to identify records uniquely in a database, it is important that keys remain valid when new records are added to the database. Hence, checks should be made to ensure that every new record has values that are different in the appropriate field, or fields, from all other records in this table. For instance, it makes sense to use the student identification number as a key for student records if no two students ever have the same student identification number. A university should not use the name field as a key, because two students may have the same name (such as John Smith).

## Operations on $n$-ary Relations

There are a variety of operations on $n$-ary relations that can be used to form new $n$-ary relations. Applied together, these operations can answer queries on databases that ask for all $n$-tuples that satisfy certain conditions.

The most basic operation on an $n$-ary relation is determining all $n$-tuples in the $n$-ary relation that satisfy certain conditions. For example, we may want to find all the records of all computer science majors in a database of student records. We may want to find all students who have a grade point average above 3.5. We may want to find the records of all computer science majors who have a grade point average above 3.5. To perform such tasks we use the selection operator.

**DEFINITION 2** Let $R$ be an $n$-ary relation and $C$ a condition that elements in $R$ may satisfy. Then the *selection operator* $s_C$ maps the $n$-ary relation $R$ to the $n$-ary relation of all $n$-tuples from $R$ that satisfy the condition $C$.

**EXAMPLE 7** To find the records of computer science majors in the $n$-ary relation $R$ shown in Table 1, we use the operator $s_{C_1}$, where $C_1$ is the condition Major = "Computer Science." The result is the two 4-tuples (Ackermann, 231455, Computer Science, 3.88) and (Chou, 102147, Computer Science, 3.49). Similarly, to find the records of students who have a grade point average above 3.5 in this database, we use the operator $s_{C_2}$, where $C_2$ is the condition GPA $> 3.5$. The result is the two 4-tuples (Ackermann, 231455, Computer Science, 3.88) and (Rao, 678543, Mathematics, 3.90). Finally, to find the records of computer science majors who have a GPA above 3.5, we use the operator $s_{C_3}$, where $C_3$ is the condition (Major = "Computer Science" $\wedge$ GPA $> 3.5$). The result consists of the single 4-tuple (Ackermann, 231455, Computer Science, 3.88). ◀

Projections are used to form new $n$-ary relations by deleting the same fields in every record of the relation.

**DEFINITION 3** The *projection* $P_{i_1 i_2, \ldots, i_m}$ where $i_1 < i_2 < \cdots < i_m$, maps the $n$-tuple $(a_1, a_2, \ldots, a_n)$ to the $m$-tuple $(a_{i_1}, a_{i_2}, \ldots, a_{i_m})$, where $m \leq n$.

In other words, the projection $P_{i_1, i_2, \ldots, i_m}$ deletes $n - m$ of the components of an $n$-tuple, leaving the $i_1$th, $i_2$th, $\ldots$, and $i_m$th components.

**TABLE 2** GPAs.

| *Student_name* | *GPA* |
|---|---|
| Ackermann | 3.88 |
| Adams | 3.45 |
| Chou | 3.49 |
| Goodfriend | 3.45 |
| Rao | 3.90 |
| Stevens | 2.99 |

**TABLE 3** Enrollments.

| *Student* | *Major* | *Course* |
|---|---|---|
| Glauser | Biology | BI 290 |
| Glauser | Biology | MS 475 |
| Glauser | Biology | PY 410 |
| Marcus | Mathematics | MS 511 |
| Marcus | Mathematics | MS 603 |
| Marcus | Mathematics | CS 322 |
| Miller | Computer Science | MS 575 |
| Miller | Computer Science | CS 455 |

**TABLE 4** Majors.

| *Student* | *Major* |
|---|---|
| Glauser | Biology |
| Marcus | Mathematics |
| Miller | Computer Science |

**EXAMPLE 8** What results when the projection $P_{1,3}$ is applied to the 4-tuples $(2, 3, 0, 4)$, (Jane Doe, 234111001, Geography, 3.14), and $(a_1, a_2, a_3, a_4)$?

*Solution:* The projection $P_{1,3}$ sends these 4-tuples to $(2, 0)$, (Jane Doe, Geography), and $(a_1, a_3)$, respectively. ◀

Example 9 illustrates how new relations are produced using projections.

**EXAMPLE 9** What relation results when the projection $P_{1,4}$ is applied to the relation in Table 1?

*Solution:* When the projection $P_{1,4}$ is used, the second and third columns of the table are deleted, and pairs representing student names and grade point averages are obtained. Table 2 displays the results of this projection. ◀

Fewer rows may result when a projection is applied to the table for a relation. This happens when some of the $n$-tuples in the relation have identical values in each of the $m$ components of the projection, and only disagree in components deleted by the projection. For instance, consider the following example.

**EXAMPLE 10** What is the table obtained when the projection $P_{1,2}$ is applied to the relation in Table 3?

*Solution:* Table 4 displays the relation obtained when $P_{1,2}$ is applied to Table 3. Note that there are fewer rows after this projection is applied. ◀

The **join** operation is used to combine two tables into one when these tables share some identical fields. For instance, a table containing fields for airline, flight number, and gate, and another table containing fields for flight number, gate, and departure time can be combined into a table containing fields for airline, flight number, gate, and departure time.

**DEFINITION 4** Let $R$ be a relation of degree $m$ and $S$ a relation of degree $n$. The *join* $J_p(R, S)$, where $p \leq m$ and $p \leq n$, is a relation of degree $m + n - p$ that consists of all $(m + n - p)$-tuples $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-p})$, where the $m$-tuple $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p)$ belongs to $R$ and the $n$-tuple $(c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-p})$ belongs to $S$.

In other words, the join operator $J_p$ produces a new relation from two relations by combining all $m$-tuples of the first relation with all $n$-tuples of the second relation, where the last $p$ components of the $m$-tuples agree with the first $p$ components of the $n$-tuples.

**TABLE 5** Teaching_assignments.

| *Professor* | *Department* | *Course_ number* |
|---|---|---|
| Cruz | Zoology | 335 |
| Cruz | Zoology | 412 |
| Farber | Psychology | 501 |
| Farber | Psychology | 617 |
| Grammer | Physics | 544 |
| Grammer | Physics | 551 |
| Rosen | Computer Science | 518 |
| Rosen | Mathematics | 575 |

**TABLE 6** Class_schedule.

| *Department* | *Course_ number* | *Room* | *Time* |
|---|---|---|---|
| Computer Science | 518 | N521 | 2:00 P.M. |
| Mathematics | 575 | N502 | 3:00 P.M. |
| Mathematics | 611 | N521 | 4:00 P.M. |
| Physics | 544 | B505 | 4:00 P.M. |
| Psychology | 501 | A100 | 3:00 P.M. |
| Psychology | 617 | A110 | 11:00 A.M. |
| Zoology | 335 | A100 | 9:00 A.M. |
| Zoology | 412 | A100 | 8:00 A.M. |

**EXAMPLE 11** What relation results when the join operator $J_2$ is used to combine the relation displayed in Tables 5 and 6?

*Solution:* The join $J_2$ produces the relation shown in Table 7. ◀

There are other operators besides projections and joins that produce new relations from existing relations. A description of these operations can be found in books on database theory.

## SQL

Links

The database query language SQL (short for Structured Query Language) can be used to carry out the operations we have described in this section. Example 12 illustrates how SQL commands are related to operations on $n$-ary relations.

**EXAMPLE 12** We will illustrate how SQL is used to express queries by showing how SQL can be employed to make a query about airline flights using Table 8. The SQL statement

```
SELECT Departure_time
FROM Flights
WHERE Destination='Detroit'
```

is used to find the projection $P_5$ (on the Departure_time attribute) of the selection of 5-tuples in the Flights database that satisfy the condition: Destination = 'Detroit'. The output would be a list containing the times of flights that have Detroit as their destination, namely, 08:10, 08:47,

**TABLE 7** Teaching_schedule.

| *Professor* | *Department* | *Course_number* | *Room* | *Time* |
|---|---|---|---|---|
| Cruz | Zoology | 335 | A100 | 9:00 A.M. |
| Cruz | Zoology | 412 | A100 | 8:00 A.M. |
| Farber | Psychology | 501 | A100 | 3:00 P.M. |
| Farber | Psychology | 617 | A110 | 11:00 A.M. |
| Grammer | Physics | 544 | B505 | 4:00 P.M. |
| Rosen | Computer Science | 518 | N521 | 2:00 P.M. |
| Rosen | Mathematics | 575 | N502 | 3:00 P.M. |

**TABLE 8** **Flights.**

| *Airline* | *Flight_number* | *Gate* | *Destination* | *Departure_time* |
|---|---|---|---|---|
| Nadir | 122 | 34 | Detroit | 08:10 |
| Acme | 221 | 22 | Denver | 08:17 |
| Acme | 122 | 33 | Anchorage | 08:22 |
| Acme | 323 | 34 | Honolulu | 08:30 |
| Nadir | 199 | 13 | Detroit | 08:47 |
| Acme | 222 | 22 | Denver | 09:10 |
| Nadir | 322 | 34 | Detroit | 09:44 |

and 09:44. SQL uses the FROM clause to identify the $n$-ary relation the query is applied to, the WHERE clause to specify the condition of the selection operation, and the SELECT clause to specify the projection operation that is to be applied. (*Beware:* SQL uses SELECT to represent a projection, rather than a selection operation. This is an unfortunate example of conflicting terminology.) ◀

Example 13 shows how SQL queries can be made involving more than one table.

**EXAMPLE 13** The SQL statement

```
SELECT Professor, Time
FROM Teaching_assignments, Class_schedule
WHERE Department='Mathematics'
```

is used to find the projection $P_{1,5}$ of the 5-tuples in the database (shown in Table 7), which is the join $J_2$ of the Teaching_assignments and Class_schedule databases in Tables 5 and 6, respectively, which satisfy the condition: Department = Mathematics. The output would consist of the single 2-tuple (Rosen, 3:00 P.M.). The SQL FROM clause is used here to find the join of two different databases. ◀

We have only touched on the basic concepts of relational databases in this section. More information can be found in [AhUl95].

## Exercises

**1.** List the triples in the relation $\{(a, b, c) \mid a, b, \text{ and } c \text{ are integers with } 0 < a < b < c < 5\}$.

**2.** Which 4-tuples are in the relation $\{(a, b, c, d) \mid a, b, c, \text{ and } d \text{ are positive integers with } abcd = 6\}$?

**3.** List the 5-tuples in the relation in Table 8.

**4.** Assuming that no new $n$-tuples are added, find all the primary keys for the relations displayed in

**a)** Table 3. **b)** Table 5.

**c)** Table 6. **d)** Table 8.

**5.** Assuming that no new $n$-tuples are added, find a composite key with two fields containing the *Airline* field for the database in Table 8.

**6.** Assuming that no new $n$-tuples are added, find a composite key with two fields containing the Professor field for the database in Table 7.

**7.** The 3-tuples in a 3-ary relation represent the following attributes of a student database: student ID number, name, phone number.

**a)** Is student ID number likely to be a primary key?

**b)** Is name likely to be a primary key?

**c)** Is phone number likely to be a primary key?

**8.** The 4-tuples in a 4-ary relation represent these attributes of published books: title, ISBN, publication date, number of pages.

**a)** What is a likely primary key for this relation?

**b)** Under what conditions would (title, publication date) be a composite key?

**c)** Under what conditions would (title, number of pages) be a composite key?

**9.** The 5-tuples in a 5-ary relation represent these attributes of all people in the United States: name, Social Security number, street address, city, state.
   **a)** Determine a primary key for this relation.
   **b)** Under what conditions would (name, street address) be a composite key?
   **c)** Under what conditions would (name, street address, city) be a composite key?

**10.** What do you obtain when you apply the selection operator $s_C$, where $C$ is the condition Room = A100, to the database in Table 7?

**11.** What do you obtain when you apply the selection operator $s_C$, where $C$ is the condition Destination = Detroit, to the database in Table 8?

**12.** What do you obtain when you apply the selection operator $s_C$, where $C$ is the condition (Project = 2) $\wedge$ (Quantity $\geq$ 50), to the database in Table 10?

**13.** What do you obtain when you apply the selection operator $s_C$, where $C$ is the condition (Airline = Nadir) $\vee$ (Destination = Denver), to the database in Table 8?

**14.** What do you obtain when you apply the projection $P_{2,3,5}$ to the 5-tuple $(a, b, c, d, e)$?

**15.** Which projection mapping is used to delete the first, second, and fourth components of a 6-tuple?

**16.** Display the table produced by applying the projection $P_{1,2,4}$ to Table 8.

**17.** Display the table produced by applying the projection $P_{1,4}$ to Table 8.

**18.** How many components are there in the $n$-tuples in the table obtained by applying the join operator $J_3$ to two tables with 5-tuples and 8-tuples, respectively?

**19.** Construct the table obtained by applying the join operator $J_2$ to the relations in Tables 9 and 10.

**20.** Show that if $C_1$ and $C_2$ are conditions that elements of the $n$-ary relation $R$ may satisfy, then $s_{C_1 \wedge C_2}(R) = s_{C_1}(s_{C_2}(R))$.

**21.** Show that if $C_1$ and $C_2$ are conditions that elements of the $n$-ary relation $R$ may satisfy, then $s_{C_1}(s_{C_2}(R)) = s_{C_2}(s_{C_1}(R))$.

**22.** Show that if $C$ is a condition that elements of the $n$-ary relations $R$ and $S$ may satisfy, then $s_C(R \cup S) = s_C(R) \cup s_C(S)$.

**23.** Show that if $C$ is a condition that elements of the $n$-ary relations $R$ and $S$ may satisfy, then $s_C(R \cap S) = s_C(R) \cap s_C(S)$.

**24.** Show that if $C$ is a condition that elements of the $n$-ary relations $R$ and $S$ may satisfy, then $s_C(R - S) = s_C(R) - s_C(S)$.

**25.** Show that if $R$ and $S$ are both $n$-ary relations, then $P_{i_1,i_2,\ldots,i_m}(R \cup S) = P_{i_1,i_2,\ldots,i_m}(R) \cup P_{i_1,i_2,\ldots,i_m}(S)$.

**26.** Give an example to show that if $R$ and $S$ are both $n$-ary relations, then $P_{i_1,i_2,\ldots,i_m}(R \cap S)$ may be different from $P_{i_1,i_2,\ldots,i_m}(R) \cap P_{i_1,i_2,\ldots,i_m}(S)$.

**27.** Give an example to show that if $R$ and $S$ are both $n$-ary relations, then $P_{i_1,i_2,\ldots,i_m}(R - S)$ may be different from $P_{i_1,i_2,\ldots,i_m}(R) - P_{i_1,i_2,\ldots,i_m}(S)$.

**28.** **a)** What are the operations that correspond to the query expressed using this SQL statement?

```
SELECT Supplier
FROM Part_needs
WHERE 1000 ≤ Part_number ≤ 5000
```

   **b)** What is the output of this query given the database in Table 9 as input?

**29.** **a)** What are the operations that correspond to the query expressed using this SQL statement?

```
SELECT Supplier, Project
FROM Part_needs, Parts_inventory
WHERE Quantity ≤ 10
```

   **b)** What is the output of this query given the databases in Tables 9 and 10 as input?

**30.** Determine whether there is a primary key for the relation in Example 2.

**31.** Determine whether there is a primary key for the relation in Example 3.

**32.** Show that an $n$-ary relation with a primary key can be thought of as the graph of a function that maps values of the primary key to $(n - 1)$-tuples formed from values of the other domains.

**TABLE 9** Part_needs.

| *Supplier* | *Part_number* | *Project* |
|---|---|---|
| 23 | 1092 | 1 |
| 23 | 1101 | 3 |
| 23 | 9048 | 4 |
| 31 | 4975 | 3 |
| 31 | 3477 | 2 |
| 32 | 6984 | 4 |
| 32 | 9191 | 2 |
| 33 | 1001 | 1 |

**TABLE 10** Parts_inventory.

| *Part_number* | *Project* | *Quantity* | *Color_code* |
|---|---|---|---|
| 1001 | 1 | 14 | 8 |
| 1092 | 1 | 2 | 2 |
| 1101 | 3 | 1 | 1 |
| 3477 | 2 | 25 | 2 |
| 4975 | 3 | 6 | 2 |
| 6984 | 4 | 10 | 1 |
| 9048 | 4 | 12 | 2 |
| 9191 | 2 | 80 | 4 |

# 9.3 Representing Relations

## Introduction

In this section, and in the remainder of this chapter, all relations we study will be binary relations. Because of this, in this section and in the rest of this chapter, the word relation will always refer to a binary relation. There are many ways to represent a relation between finite sets. As we have seen in Section 9.1, one way is to list its ordered pairs. Another way to represent a relation is to use a table, as we did in Example 3 in Section 9.1. In this section we will discuss two alternative methods for representing relations. One method uses zero–one matrices. The other method uses pictorial representations called directed graphs, which we will discuss later in this section.

Generally, matrices are appropriate for the representation of relations in computer programs. On the other hand, people often find the representation of relations using directed graphs useful for understanding the properties of these relations.

## Representing Relations Using Matrices

A relation between finite sets can be represented using a zero–one matrix. Suppose that $R$ is a relation from $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$. (Here the elements of the sets $A$ and $B$ have been listed in a particular, but arbitrary, order. Furthermore, when $A = B$ we use the same ordering for $A$ and $B$.) The relation $R$ can be represented by the matrix $\mathbf{M}_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 \text{ if } (a_i, b_j) \in R, \\ 0 \text{ if } (a_i, b_j) \notin R. \end{cases}$$

In other words, the zero–one matrix representing $R$ has a 1 as its $(i, j)$ entry when $a_i$ is related to $b_j$, and a 0 in this position if $a_i$ is not related to $b_j$. (Such a representation depends on the orderings used for $A$ and $B$.)

The use of matrices to represent relations is illustrated in Examples 1–6.

**EXAMPLE 1** Suppose that $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Let $R$ be the relation from $A$ to $B$ containing $(a, b)$ if $a \in A$, $b \in B$, and $a > b$. What is the matrix representing $R$ if $a_1 = 1$, $a_2 = 2$, and $a_3 = 3$, and $b_1 = 1$ and $b_2 = 2$?

*Solution:* Because $R = \{(2, 1), (3, 1), (3, 2)\}$, the matrix for $R$ is

$$\mathbf{M}_R = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The 1s in $\mathbf{M}_R$ show that the pairs (2, 1), (3, 1), and (3, 2) belong to $R$. The 0s show that no other pairs belong to $R$. ◀

**EXAMPLE 2** Let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Which ordered pairs are in the relation $R$ represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}?$$

*Solution:* Because $R$ consists of those ordered pairs $(a_i, b_j)$ with $m_{ij} = 1$, it follows that

$$R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}.$$ ◀

The matrix of a relation on a set, which is a square matrix, can be used to determine whether the relation has certain properties. Recall that a relation $R$ on $A$ is reflexive if $(a, a) \in R$ whenever $a \in A$. Thus, $R$ is reflexive if and only if $(a_i, a_i) \in R$ for $i = 1, 2, \ldots, n$. Hence, $R$ is reflexive if and only if $m_{ii} = 1$, for $i = 1, 2, \ldots, n$. In other words, $R$ is reflexive if all the elements on the main diagonal of $\mathbf{M}_R$ are equal to 1, as shown in Figure 1. Note that the elements off the main diagonal can be either 0 or 1.

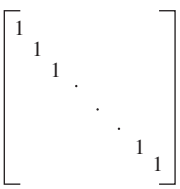


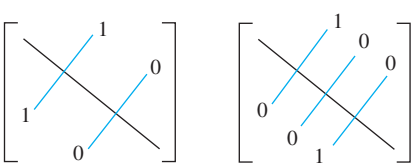
**FIGURE 1 The Zero–One Matrix for a Reflexive Relation. (Off Diagonal Elements Can Be 0 or 1.)**

The relation $R$ is symmetric if $(a, b) \in R$ implies that $(b, a) \in R$. Consequently, the relation $R$ on the set $A = \{a_1, a_2, \ldots, a_n\}$ is symmetric if and only if $(a_j, a_i) \in R$ whenever $(a_i, a_j) \in R$. In terms of the entries of $\mathbf{M}_R$, $R$ is symmetric if and only if $m_{ji} = 1$ whenever $m_{ij} = 1$. This also means $m_{ji} = 0$ whenever $m_{ij} = 0$. Consequently, $R$ is symmetric if and only if $m_{ij} = m_{ji}$, for all pairs of integers $i$ and $j$ with $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$. Recalling the definition of the transpose of a matrix from Section 2.6, we see that $R$ is symmetric if and only if

$$\mathbf{M}_R = (\mathbf{M}_R)^t,$$

that is, if $\mathbf{M}_R$ is a symmetric matrix. The form of the matrix for a symmetric relation is illustrated in Figure 2(a).

The relation $R$ is antisymmetric if and only if $(a, b) \in R$ and $(b, a) \in R$ imply that $a = b$. Consequently, the matrix of an antisymmetric relation has the property that if $m_{ij} = 1$ with $i \neq j$, then $m_{ji} = 0$. Or, in other words, either $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$. The form of the matrix for an antisymmetric relation is illustrated in Figure 2(b).



(a) Symmetric (b) Antisymmetric

**FIGURE 2 The Zero–One Matrices for Symmetric and Antisymmetric Relations.**

**EXAMPLE 3** Suppose that the relation $R$ on a set is represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Is $R$ reflexive, symmetric, and/or antisymmetric?

*Solution:* Because all the diagonal elements of this matrix are equal to 1, $R$ is reflexive. Moreover, because $\mathbf{M}_R$ is symmetric, it follows that $R$ is symmetric. It is also easy to see that $R$ is not antisymmetric. ◀

The Boolean operations join and meet (discussed in Section 2.6) can be used to find the matrices representing the union and the intersection of two relations. Suppose that $R_1$ and $R_2$ are relations on a set $A$ represented by the matrices $\mathbf{M}_{R_1}$ and $\mathbf{M}_{R_2}$, respectively. The matrix

representing the union of these relations has a 1 in the positions where either $\mathbf{M}_{R_1}$ or $\mathbf{M}_{R_2}$ has a 1. The matrix representing the intersection of these relations has a 1 in the positions where both $\mathbf{M}_{R_1}$ and $\mathbf{M}_{R_2}$ have a 1. Thus, the matrices representing the union and intersection of these relations are

$$\mathbf{M}_{R_1 \cup R_2} = \mathbf{M}_{R_1} \vee \mathbf{M}_{R_2} \qquad \text{and} \qquad \mathbf{M}_{R_1 \cap R_2} = \mathbf{M}_{R_1} \wedge \mathbf{M}_{R_2}.$$

**EXAMPLE 4** Suppose that the relations $R_1$ and $R_2$ on a set $A$ are represented by the matrices

$$\mathbf{M}_{R_1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

What are the matrices representing $R_1 \cup R_2$ and $R_1 \cap R_2$?

*Solution:* The matrices of these relations are

$$\mathbf{M}_{R_1 \cup R_2} = \mathbf{M}_{R_1} \vee \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

$$\mathbf{M}_{R_1 \cap R_2} = \mathbf{M}_{R_1} \wedge \mathbf{M}_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

◀

We now turn our attention to determining the matrix for the composite of relations. This matrix can be found using the Boolean product of the matrices (discussed in Section 2.6) for these relations. In particular, suppose that $R$ is a relation from $A$ to $B$ and $S$ is a relation from $B$ to $C$. Suppose that $A$, $B$, and $C$ have $m$, $n$, and $p$ elements, respectively. Let the zero–one matrices for $S \circ R$, $R$, and $S$ be $\mathbf{M}_{S \circ R} = [t_{ij}]$, $\mathbf{M}_R = [r_{ij}]$, and $\mathbf{M}_S = [s_{ij}]$, respectively (these matrices have sizes $m \times p$, $m \times n$, and $n \times p$, respectively). The ordered pair $(a_i, c_j)$ belongs to $S \circ R$ if and only if there is an element $b_k$ such that $(a_i, b_k)$ belongs to $R$ and $(b_k, c_j)$ belongs to $S$. It follows that $t_{ij} = 1$ if and only if $r_{ik} = s_{kj} = 1$ for some $k$. From the definition of the Boolean product, this means that

$$\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S.$$

**EXAMPLE 5** Find the matrix representing the relations $S \circ R$, where the matrices representing $R$ and $S$ are

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad \mathbf{M}_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

*Solution:* The matrix for $S \circ R$ is

$$\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

◀

The matrix representing the composite of two relations can be used to find the matrix for $\mathbf{M}_{R^n}$. In particular,

$$\mathbf{M}_{R^n} = \mathbf{M}_R^{[n]},$$

from the definition of Boolean powers. Exercise 35 asks for a proof of this formula.

**EXAMPLE 6** Find the matrix representing the relation $R^2$, where the matrix representing $R$ is

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

*Solution:* The matrix for $R^2$ is

$$\mathbf{M}_{R^2} = \mathbf{M}_R^{[2]} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

◀

## Representing Relations Using Digraphs

We have shown that a relation can be represented by listing all of its ordered pairs or by using a zero–one matrix. There is another important way of representing a relation using a pictorial representation. Each element of the set is represented by a point, and each ordered pair is represented using an arc with its direction indicated by an arrow. We use such pictorial representations when we think of relations on a finite set as **directed graphs**, or **digraphs**.

**DEFINITION 1** A *directed graph*, or *digraph*, consists of a set $V$ of *vertices* (or *nodes*) together with a set $E$ of ordered pairs of elements of $V$ called *edges* (or *arcs*). The vertex $a$ is called the *initial vertex* of the edge $(a, b)$, and the vertex $b$ is called the *terminal vertex* of this edge.

An edge of the form $(a, a)$ is represented using an arc from the vertex $a$ back to itself. Such an edge is called a **loop**.

**EXAMPLE 7** The directed graph with vertices $a$, $b$, $c$, and $d$, and edges $(a, b)$, $(a, d)$, $(b, b)$, $(b, d)$, $(c, a)$, $(c, b)$, and $(d, b)$ is displayed in Figure 3. ◀

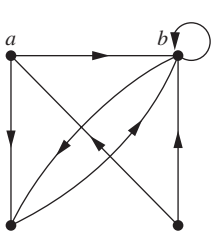



**FIGURE 3**
**A Directed Graph.**

The relation $R$ on a set $A$ is represented by the directed graph that has the elements of $A$ as its vertices and the ordered pairs $(a, b)$, where $(a, b) \in R$, as edges. This assignment sets up a one-to-one correspondence between the relations on a set $A$ and the directed graphs with $A$ as their set of vertices. Thus, every statement about relations corresponds to a statement about directed graphs, and vice versa. Directed graphs give a visual display of information about relations. As such, they are often used to study relations and their properties. (Note that relations from a set $A$ to a set $B$ can be represented by a directed graph where there is a vertex for each element of $A$ and a vertex for each element of $B$, as shown in Section 9.1. However, when $A = B$, such representation provides much less insight than the digraph representations described here.) The use of directed graphs to represent relations on a set is illustrated in Examples 8–10.

**EXAMPLE 8** The directed graph of the relation

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

on the set $\{1, 2, 3, 4\}$ is shown in Figure 4. ◀

**EXAMPLE 9** What are the ordered pairs in the relation $R$ represented by the directed graph shown in Figure 5?

*Solution:* The ordered pairs $(x, y)$ in the relation are

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

Each of these pairs corresponds to an edge of the directed graph, with $(2, 2)$ and $(3, 3)$ corresponding to loops. ◀

We will study directed graphs extensively in Chapter 10.

The directed graph representing a relation can be used to determine whether the relation has various properties. For instance, a relation is reflexive if and only if there is a loop at every vertex of the directed graph, so that every ordered pair of the form $(x, x)$ occurs in the relation. A relation is symmetric if and only if for every edge between distinct vertices in its digraph there is an edge in the opposite direction, so that $(y, x)$ is in the relation whenever $(x, y)$ is in the relation. Similarly, a relation is antisymmetric if and only if there are never two edges in opposite directions between distinct vertices. Finally, a relation is transitive if and only if whenever there is an edge from a vertex $x$ to a vertex $y$ and an edge from a vertex $y$ to a vertex $z$, there is an edge from $x$ to $z$ (completing a triangle where each side is a directed edge with the correct direction).

***Remark:*** Note that a symmetric relation can be represented by an undirected graph, which is a graph where edges do not have directions. We will study undirected graphs in Chapter 10.

**EXAMPLE 10** Determine whether the relations for the directed graphs shown in Figure 6 are reflexive, symmetric, antisymmetric, and/or transitive.

*Solution:* Because there are loops at every vertex of the directed graph of $R$, it is reflexive. $R$ is neither symmetric nor antisymmetric because there is an edge from $a$ to $b$ but not one from $b$ to $a$, but there are edges in both directions connecting $b$ and $c$. Finally, $R$ is not transitive because there is an edge from $a$ to $b$ and an edge from $b$ to $c$, but no edge from $a$ to $c$.

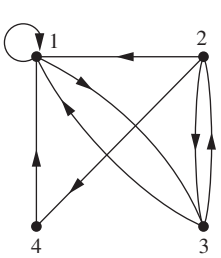



**FIGURE 4 The Directed Graph of the Relation *R*.**

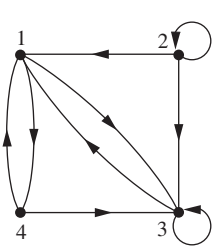
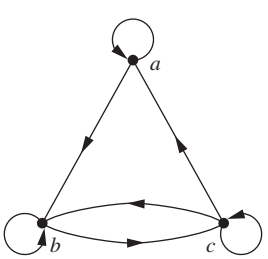
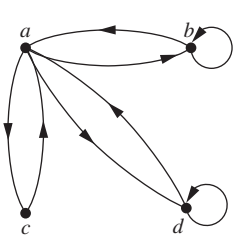



**FIGURE 5 The Directed Graph of the Relation *R*.**




(a) Directed graph of $R$




(b) Directed graph of $S$

**FIGURE 6 The Directed Graphs of the Relations *R* and *S*.**

Because loops are not present at all the vertices of the directed graph of $S$, this relation is not reflexive. It is symmetric and not antisymmetric, because every edge between distinct vertices is accompanied by an edge in the opposite direction. It is also not hard to see from the directed graph that $S$ is not transitive, because $(c, a)$ and $(a, b)$ belong to $S$, but $(c, b)$ does not belong to $S$. ◀

## Exercises

**1.** Represent each of these relations on $\{1, 2, 3\}$ with a matrix (with the elements of this set listed in increasing order).
**a)** $\{(1, 1), (1, 2), (1, 3)\}$
**b)** $\{(1, 2), (2, 1), (2, 2), (3, 3)\}$
**c)** $\{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$
**d)** $\{(1, 3), (3, 1)\}$

**2.** Represent each of these relations on $\{1, 2, 3, 4\}$ with a matrix (with the elements of this set listed in increasing order).
**a)** $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$
**b)** $\{(1, 1), (1, 4), (2, 2), (3, 3), (4, 1)\}$
**c)** $\{(1, 2), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (3, 4), (4, 1), (4, 2), (4, 3)\}$
**d)** $\{(2, 4), (3, 1), (3, 2), (3, 4)\}$

**3.** List the ordered pairs in the relations on $\{1, 2, 3\}$ corresponding to these matrices (where the rows and columns correspond to the integers listed in increasing order).

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

**c)** $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

**4.** List the ordered pairs in the relations on $\{1, 2, 3, 4\}$ corresponding to these matrices (where the rows and columns correspond to the integers listed in increasing order).

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

**c)** $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

**5.** How can the matrix representing a relation $R$ on a set $A$ be used to determine whether the relation is irreflexive?

**6.** How can the matrix representing a relation $R$ on a set $A$ be used to determine whether the relation is asymmetric?

**7.** Determine whether the relations represented by the matrices in Exercise 3 are reflexive, irreflexive, symmetric, antisymmetric, and/or transitive.

**8.** Determine whether the relations represented by the matrices in Exercise 4 are reflexive, irreflexive, symmetric, antisymmetric, and/or transitive.

**9.** How many nonzero entries does the matrix representing the relation $R$ on $A = \{1, 2, 3, \ldots, 100\}$ consisting of the first 100 positive integers have if $R$ is
**a)** $\{(a, b) \mid a > b\}$? **b)** $\{(a, b) \mid a \neq b\}$?
**c)** $\{(a, b) \mid a = b + 1\}$? **d)** $\{(a, b) \mid a = 1\}$?
**e)** $\{(a, b) \mid ab = 1\}$?

**10.** How many nonzero entries does the matrix representing the relation $R$ on $A = \{1, 2, 3, \ldots, 1000\}$ consisting of the first 1000 positive integers have if $R$ is
**a)** $\{(a, b) \mid a \leq b\}$?
**b)** $\{(a, b) \mid a = b \pm 1\}$?
**c)** $\{(a, b) \mid a + b = 1000\}$?
**d)** $\{(a, b) \mid a + b \leq 1001\}$?
**e)** $\{(a, b) \mid a \neq 0\}$?

**11.** How can the matrix for $\overline{R}$, the complement of the relation $R$, be found from the matrix representing $R$, when $R$ is a relation on a finite set $A$?

**12.** How can the matrix for $R^{-1}$, the inverse of the relation $R$, be found from the matrix representing $R$, when $R$ is a relation on a finite set $A$?

**13.** Let $R$ be the relation represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Find the matrix representing
**a)** $R^{-1}$. **b)** $\overline{R}$. **c)** $R^2$.

**14.** Let $R_1$ and $R_2$ be relations on a set $A$ represented by the matrices

$$\mathbf{M}_{R_1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_{R_2} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Find the matrices that represent
**a)** $R_1 \cup R_2$. **b)** $R_1 \cap R_2$. **c)** $R_2 \circ R_1$.
**d)** $R_1 \circ R_1$. **e)** $R_1 \oplus R_2$.

**15.** Let $R$ be the relation represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Find the matrices that represent
**a)** $R^2$. **b)** $R^3$. **c)** $R^4$.

**16.** Let $R$ be a relation on a set $A$ with $n$ elements. If there are $k$ nonzero entries in $\mathbf{M}_R$, the matrix representing $R$, how many nonzero entries are there in $\mathbf{M}_{R^{-1}}$, the matrix representing $R^{-1}$, the inverse of $R$?

**17.** Let $R$ be a relation on a set $A$ with $n$ elements. If there are $k$ nonzero entries in $\mathbf{M}_R$, the matrix representing $R$, how many nonzero entries are there in $\mathbf{M}_{\overline{R}}$, the matrix representing $\overline{R}$, the complement of $R$?

**18.** Draw the directed graphs representing each of the relations from Exercise 1.

**19.** Draw the directed graphs representing each of the relations from Exercise 2.

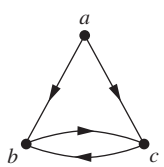
**20.** Draw the directed graph representing each of the relations from Exercise 3.

**21.** Draw the directed graph representing each of the relations from Exercise 4.

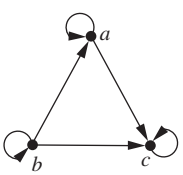
**22.** Draw the directed graph that represents the relation $\{(a, a), (a, b), (b, c), (c, b), (c, d), (d, a), (d, b)\}$.

In Exercises 23–28 list the ordered pairs in the relations represented by the directed graphs.

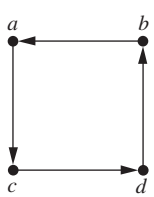
**23.**



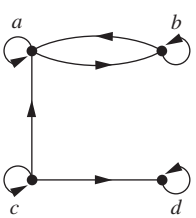

**24.**



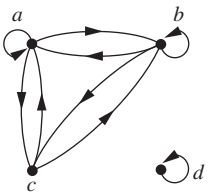

**25.**



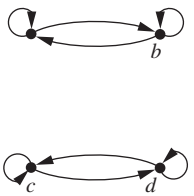

**26.**




**27.**




**28.**




**29.** How can the directed graph of a relation $R$ on a finite set $A$ be used to determine whether a relation is asymmetric?

**30.** How can the directed graph of a relation $R$ on a finite set $A$ be used to determine whether a relation is irreflexive?

**31.** Determine whether the relations represented by the directed graphs shown in Exercises 23–25 are reflexive, irreflexive, symmetric, antisymmetric, and/or transitive.

**32.** Determine whether the relations represented by the directed graphs shown in Exercises 26–28 are reflexive, irreflexive, symmetric, antisymmetric, asymmetric, and/or transitive.

**33.** Let $R$ be a relation on a set $A$. Explain how to use the directed graph representing $R$ to obtain the directed graph representing the inverse relation $R^{-1}$.

**34.** Let $R$ be a relation on a set $A$. Explain how to use the directed graph representing $R$ to obtain the directed graph representing the complementary relation $\overline{R}$.

**35.** Show that if $\mathbf{M}_R$ is the matrix representing the relation $R$, then $\mathbf{M}_R^{[n]}$ is the matrix representing the relation $R^n$.

**36.** Given the directed graphs representing two relations, how can the directed graph of the union, intersection, symmetric difference, difference, and composition of these relations be found?

# 9.4 Closures of Relations

## Introduction

A computer network has data centers in Boston, Chicago, Denver, Detroit, New York, and San Diego. There are direct, one-way telephone lines from Boston to Chicago, from Boston to Detroit, from Chicago to Detroit, from Detroit to Denver, and from New York to San Diego. Let $R$ be the relation containing $(a, b)$ if there is a telephone line from the data center in $a$ to that in $b$. How can we determine if there is some (possibly indirect) link composed of one or more telephone lines from one center to another? Because not all links are direct, such as the link from Boston to Denver that goes through Detroit, $R$ cannot be used directly to answer this. In the language of relations, $R$ is not transitive, so it does not contain all the pairs that can be linked. As we will show in this section, we can find all pairs of data centers that have a link by constructing a transitive relation $S$ containing $R$ such that $S$ is a subset of every transitive relation containing $R$. Here, $S$ is the smallest transitive relation that contains $R$. This relation is called the **transitive closure** of $R$.

In general, let $R$ be a relation on a set $A$. $R$ may or may not have some property **P**, such as reflexivity, symmetry, or transitivity. If there is a relation $S$ with property **P** containing $R$ such that $S$ is a subset of every relation with property **P** containing $R$, then $S$ is called the **closure**

of $R$ with respect to **P**. (Note that the closure of a relation with respect to a property may not exist; see Exercises 15 and 35.) We will show how reflexive, symmetric, and transitive closures of relations can be found.

## Closures

The relation $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$ on the set $A = \{1, 2, 3\}$ is not reflexive. How can we produce a reflexive relation containing $R$ that is as small as possible? This can be done by adding $(2, 2)$ and $(3, 3)$ to $R$, because these are the only pairs of the form $(a, a)$ that are not in $R$. Clearly, this new relation contains $R$. Furthermore, *any* reflexive relation that contains $R$ must also contain $(2, 2)$ and $(3, 3)$. Because this relation contains $R$, is reflexive, and is contained within every reflexive relation that contains $R$, it is called the **reflexive closure** of $R$.

As this example illustrates, given a relation $R$ on a set $A$, the reflexive closure of $R$ can be formed by adding to $R$ all pairs of the form $(a, a)$ with $a \in A$, not already in $R$. The addition of these pairs produces a new relation that is reflexive, contains $R$, and is contained within any reflexive relation containing $R$. We see that the reflexive closure of $R$ equals $R \cup \Delta$, where $\Delta = \{(a, a) \mid a \in A\}$ is the **diagonal relation** on $A$. (The reader should verify this.)

**EXAMPLE 1** What is the reflexive closure of the relation $R = \{(a, b) \mid a < b\}$ on the set of integers?

*Solution:* The reflexive closure of $R$ is

$$R \cup \Delta = \{(a, b) \mid a < b\} \cup \{(a, a) \mid a \in \mathbf{Z}\} = \{(a, b) \mid a \leq b\}.$$ ◀

The relation $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$ on $\{1, 2, 3\}$ is not symmetric. How can we produce a symmetric relation that is as small as possible and contains $R$? To do this, we need only add $(2, 1)$ and $(1, 3)$, because these are the only pairs of the form $(b, a)$ with $(a, b) \in R$ that are not in $R$. This new relation is symmetric and contains $R$. Furthermore, *any* symmetric relation that contains $R$ must contain this new relation, because a symmetric relation that contains $R$ must contain $(2, 1)$ and $(1, 3)$. Consequently, this new relation is called the **symmetric closure** of $R$.

As this example illustrates, the symmetric closure of a relation $R$ can be constructed by adding all ordered pairs of the form $(b, a)$, where $(a, b)$ is in the relation, that are not already present in $R$. Adding these pairs produces a relation that is symmetric, that contains $R$, and that is contained in any symmetric relation that contains $R$. The symmetric closure of a relation can be constructed by taking the union of a relation with its inverse (defined in the preamble of Exercise 26 in Section 9.1); that is, $R \cup R^{-1}$ is the symmetric closure of $R$, where $R^{-1} = \{(b, a) \mid (a, b) \in R\}$. The reader should verify this statement.

**EXAMPLE 2** What is the symmetric closure of the relation $R = \{(a, b) \mid a > b\}$ on the set of positive integers?

Extra Examples

*Solution:* The symmetric closure of $R$ is the relation

$$R \cup R^{-1} = \{(a, b) \mid a > b\} \cup \{(b, a) \mid a > b\} = \{(a, b) \mid a \neq b\}.$$

This last equality follows because $R$ contains all ordered pairs of positive integers where the first element is greater than the second element and $R^{-1}$ contains all ordered pairs of positive integers where the first element is less than the second. ◀

Suppose that a relation $R$ is not transitive. How can we produce a transitive relation that contains $R$ such that this new relation is contained within any transitive relation that contains $R$? Can the transitive closure of a relation $R$ be produced by adding all the pairs of the form $(a, c)$, where $(a, b)$ and $(b, c)$ are already in the relation? Consider the relation

$R = \{(1, 3), (1, 4), (2, 1), (3, 2)\}$ on the set $\{1, 2, 3, 4\}$. This relation is not transitive because it does not contain all pairs of the form $(a, c)$ where $(a, b)$ and $(b, c)$ are in $R$. The pairs of this form not in $R$ are $(1, 2)$, $(2, 3)$, $(2, 4)$, and $(3, 1)$. Adding these pairs does *not* produce a transitive relation, because the resulting relation contains $(3, 1)$ and $(1, 4)$ but does not contain $(3, 4)$. This shows that constructing the transitive closure of a relation is more complicated than constructing either the reflexive or symmetric closure. The rest of this section develops algorithms for constructing transitive closures. As will be shown later in this section, the transitive closure of a relation can be found by adding new ordered pairs that must be present and then repeating this process until no new ordered pairs are needed.

## Paths in Directed Graphs

We will see that representing relations by directed graphs helps in the construction of transitive closures. We now introduce some terminology that we will use for this purpose.

A path in a directed graph is obtained by traversing along edges (in the same direction as indicated by the arrow on the edge).

**DEFINITION 1**

A *path* from $a$ to $b$ in the directed graph $G$ is a sequence of edges $(x_0, x_1)$, $(x_1, x_2)$, $(x_2, x_3), \ldots, (x_{n-1}, x_n)$ in $G$, where $n$ is a nonnegative integer, and $x_0 = a$ and $x_n = b$, that is, a sequence of edges where the terminal vertex of an edge is the same as the initial vertex in the next edge in the path. This path is denoted by $x_0, x_1, x_2, \ldots, x_{n-1}, x_n$ and has *length* $n$. We view the empty set of edges as a path of length zero from $a$ to $a$. A path of length $n \geq 1$ that begins and ends at the same vertex is called a *circuit* or *cycle*.

A path in a directed graph can pass through a vertex more than once. Moreover, an edge in a directed graph can occur more than once in a path.

**EXAMPLE 3** Which of the following are paths in the directed graph shown in Figure 1: $a, b, e, d$; $a, e, c, d, b$; $b, a, c, b, a, a, b$; $d, c$; $c, b, a$; $e, b, a, b, a, b, e$? What are the lengths of those that are paths? Which of the paths in this list are circuits?

*Solution:* Because each of $(a, b)$, $(b, e)$, and $(e, d)$ is an edge, $a, b, e, d$ is a path of length three. Because $(c, d)$ is not an edge, $a, e, c, d, b$ is not a path. Also, $b, a, c, b, a, a, b$ is a path of length six because $(b, a)$, $(a, c)$, $(c, b)$, $(b, a)$, $(a, a)$, and $(a, b)$ are all edges. We see that $d, c$ is a path of length one, because $(d, c)$ is an edge. Also $c, b, a$ is a path of length two, because $(c, b)$ and $(b, a)$ are edges. All of $(e, b)$, $(b, a)$, $(a, b)$, $(b, a)$, $(a, b)$, and $(b, e)$ are edges, so $e, b, a, b, a, b, e$ is a path of length six.

The two paths $b, a, c, b, a, a, b$ and $e, b, a, b, a, b, e$ are circuits because they begin and end at the same vertex. The paths $a, b, e, d$; $c, b, a$; and $d, c$ are not circuits. ◀

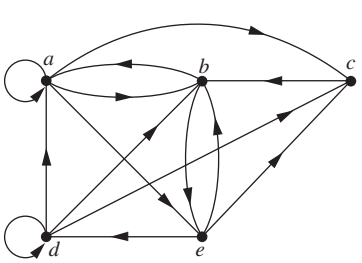



**FIGURE 1** **A Directed Graph.**

The term *path* also applies to relations. Carrying over the definition from directed graphs to relations, there is a **path** from $a$ to $b$ in $R$ if there is a sequence of elements $a, x_1, x_2, \ldots, x_{n-1}, b$ with $(a, x_1) \in R$, $(x_1, x_2) \in R, \ldots,$ and $(x_{n-1}, b) \in R$. Theorem 1 can be obtained from the definition of a path in a relation.

**THEOREM 1**

Let $R$ be a relation on a set $A$. There is a path of length $n$, where $n$ is a positive integer, from $a$ to $b$ if and only if $(a, b) \in R^n$.

*Proof:* We will use mathematical induction. By definition, there is a path from $a$ to $b$ of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Assume that the theorem is true for the positive integer $n$. This is the inductive hypothesis. There is a path of length $n + 1$ from $a$ to $b$ if and only if there is an element $c \in A$ such that there is a path of length one from $a$ to $c$, so $(a, c) \in R$, and a path of length $n$ from $c$ to $b$, that is, $(c, b) \in R^n$. Consequently, by the inductive hypothesis, there is a path of length $n + 1$ from $a$ to $b$ if and only if there is an element $c$ with $(a, c) \in R$ and $(c, b) \in R^n$. But there is such an element if and only if $(a, b) \in R^{n+1}$. Therefore, there is a path of length $n + 1$ from $a$ to $b$ if and only if $(a, b) \in R^{n+1}$. This completes the proof. ◁

## Transitive Closures

We now show that finding the transitive closure of a relation is equivalent to determining which pairs of vertices in the associated directed graph are connected by a path. With this in mind, we define a new relation.

**DEFINITION 2**

Let $R$ be a relation on a set $A$. The *connectivity relation* $R^*$ consists of the pairs $(a, b)$ such that there is a path of length at least one from $a$ to $b$ in $R$.

Because $R^n$ consists of the pairs $(a, b)$ such that there is a path of length $n$ from $a$ to $b$, it follows that $R^*$ is the union of all the sets $R^n$. In other words,

$$R^* = \bigcup_{n=1}^{\infty} R^n.$$

The connectivity relation is useful in many models.

**EXAMPLE 4** Let $R$ be the relation on the set of all people in the world that contains $(a, b)$ if $a$ has met $b$. What is $R^n$, where $n$ is a positive integer greater than one? What is $R^*$?

*Solution:* The relation $R^2$ contains $(a, b)$ if there is a person $c$ such that $(a, c) \in R$ and $(c, b) \in R$, that is, if there is a person $c$ such that $a$ has met $c$ and $c$ has met $b$. Similarly, $R^n$ consists of those pairs $(a, b)$ such that there are people $x_1, x_2, \ldots, x_{n-1}$ such that $a$ has met $x_1$, $x_1$ has met $x_2, \ldots,$ and $x_{n-1}$ has met $b$.

The relation $R^*$ contains $(a, b)$ if there is a sequence of people, starting with $a$ and ending with $b$, such that each person in the sequence has met the next person in the sequence. (There are many interesting conjectures about $R^*$. Do you think that this connectivity relation includes the pair with you as the first element and the president of Mongolia as the second element? We will use graphs to model this application in Chapter 10.) ◀

**EXAMPLE 5** Let $R$ be the relation on the set of all subway stops in New York City that contains $(a, b)$ if it is possible to travel from stop $a$ to stop $b$ without changing trains. What is $R^n$ when $n$ is a positive integer? What is $R^*$?

*Solution:* The relation $R^n$ contains $(a, b)$ if it is possible to travel from stop $a$ to stop $b$ by making at most $n - 1$ changes of trains. The relation $R^*$ consists of the ordered pairs $(a, b)$ where it is possible to travel from stop $a$ to stop $b$ making as many changes of trains as necessary. (The reader should verify these statements.) ◀

**EXAMPLE 6** Let $R$ be the relation on the set of all states in the United States that contains $(a, b)$ if state $a$ and state $b$ have a common border. What is $R^n$, where $n$ is a positive integer? What is $R^*$?

*Solution:* The relation $R^n$ consists of the pairs $(a, b)$, where it is possible to go from state $a$ to state $b$ by crossing exactly $n$ state borders. $R^*$ consists of the ordered pairs $(a, b)$, where it is possible to go from state $a$ to state $b$ crossing as many borders as necessary. (The reader should verify these statements.) The only ordered pairs not in $R^*$ are those containing states that are not connected to the continental United States (i.e., those pairs containing Alaska or Hawaii). ◀

Theorem 2 shows that the transitive closure of a relation and the associated connectivity relation are the same.

**THEOREM 2** The transitive closure of a relation $R$ equals the connectivity relation $R^*$.

***Proof:*** Note that $R^*$ contains $R$ by definition. To show that $R^*$ is the transitive closure of $R$ we must also show that $R^*$ is transitive and that $R^* \subseteq S$ whenever $S$ is a transitive relation that contains $R$.

First, we show that $R^*$ is transitive. If $(a, b) \in R^*$ and $(b, c) \in R^*$, then there are paths from $a$ to $b$ and from $b$ to $c$ in $R$. We obtain a path from $a$ to $c$ by starting with the path from $a$ to $b$ and following it with the path from $b$ to $c$. Hence, $(a, c) \in R^*$. It follows that $R^*$ is transitive.

Now suppose that $S$ is a transitive relation containing $R$. Because $S$ is transitive, $S^n$ also is transitive (the reader should verify this) and $S^n \subseteq S$ (by Theorem 1 of Section 9.1). Furthermore, because

$$S^* = \bigcup_{k=1}^{\infty} S^k$$

and $S^k \subseteq S$, it follows that $S^* \subseteq S$. Now note that if $R \subseteq S$, then $R^* \subseteq S^*$, because any path in $R$ is also a path in $S$. Consequently, $R^* \subseteq S^* \subseteq S$. Thus, any transitive relation that contains $R$ must also contain $R^*$. Therefore, $R^*$ is the transitive closure of $R$. ◁

Now that we know that the transitive closure equals the connectivity relation, we turn our attention to the problem of computing this relation. We do not need to examine arbitrarily long paths to determine whether there is a path between two vertices in a finite directed graph. As Lemma 1 shows, it is sufficient to examine paths containing no more than $n$ edges, where $n$ is the number of elements in the set.

**LEMMA 1** Let $A$ be a set with $n$ elements, and let $R$ be a relation on $A$. If there is a path of length at least one in $R$ from $a$ to $b$, then there is such a path with length not exceeding $n$. Moreover, when $a \neq b$, if there is a path of length at least one in $R$ from $a$ to $b$, then there is such a path with length not exceeding $n - 1$.

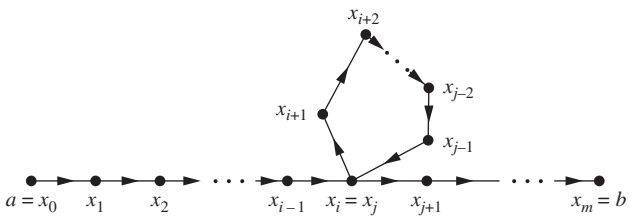



**FIGURE 2** **Producing a Path with Length Not Exceeding *n*.**

*Proof:* Suppose there is a path from $a$ to $b$ in $R$. Let $m$ be the length of the shortest such path. Suppose that $x_0, x_1, x_2, \ldots, x_{m-1}, x_m$, where $x_0 = a$ and $x_m = b$, is such a path.

Suppose that $a = b$ and that $m > n$, so that $m \geq n + 1$. By the pigeonhole principle, because there are $n$ vertices in $A$, among the $m$ vertices $x_0, x_1, \ldots, x_{m-1}$, at least two are equal (see Figure 2).

Suppose that $x_i = x_j$ with $0 \leq i < j \leq m - 1$. Then the path contains a circuit from $x_i$ to itself. This circuit can be deleted from the path from $a$ to $b$, leaving a path, namely, $x_0, x_1, \ldots, x_i, x_{j+1}, \ldots, x_{m-1}, x_m$, from $a$ to $b$ of shorter length. Hence, the path of shortest length must have length less than or equal to $n$.

The case where $a \neq b$ is left as an exercise for the reader. ◁

From Lemma 1, we see that the transitive closure of $R$ is the union of $R$, $R^2$, $R^3, \ldots,$ and $R^n$. This follows because there is a path in $R^*$ between two vertices if and only if there is a path between these vertices in $R^i$, for some positive integer $i$ with $i \leq n$. Because

$$R^* = R \cup R^2 \cup R^3 \cup \cdots \cup R^n$$

and the zero–one matrix representing a union of relations is the join of the zero–one matrices of these relations, the zero–one matrix for the transitive closure is the join of the zero–one matrices of the first $n$ powers of the zero–one matrix of $R$.

**THEOREM 3**

Let $\mathbf{M}_R$ be the zero–one matrix of the relation $R$ on a set with $n$ elements. Then the zero–one matrix of the transitive closure $R^*$ is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \cdots \vee \mathbf{M}_R^{[n]}.$$

**EXAMPLE 7** Find the zero–one matrix of the transitive closure of the relation $R$ where

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

*Solution:* By Theorem 3, it follows that the zero–one matrix of $R^*$ is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]}.$$

Because

$$\mathbf{M}_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

it follows that

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

◀

Links

Theorem 3 can be used as a basis for an algorithm for computing the matrix of the relation $R^*$. To find this matrix, the successive Boolean powers of $\mathbf{M}_R$, up to the $n$th power, are computed. As each power is calculated, its join with the join of all smaller powers is formed. When this is done with the $n$th power, the matrix for $R^*$ has been found. This procedure is displayed as Algorithm 1.

**ALGORITHM 1 A Procedure for Computing the Transitive Closure.**

**procedure** *transitive closure* ($\mathbf{M}_R$ : zero–one $n \times n$ matrix)
$\mathbf{A} := \mathbf{M}_R$
$\mathbf{B} := \mathbf{A}$
**for** $i := 2$ **to** $n$
  $\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$
  $\mathbf{B} := \mathbf{B} \vee \mathbf{A}$
**return** $\mathbf{B}$ {$\mathbf{B}$ is the zero–one matrix for $R^*$}

We can easily find the number of bit operations used by Algorithm 1 to determine the transitive closure of a relation. Computing the Boolean powers $\mathbf{M}_R, \mathbf{M}_R^{[2]}, \ldots, \mathbf{M}_R^{[n]}$ requires that $n-1$ Boolean products of $n \times n$ zero–one matrices be found. Each of these Boolean products can be found using $n^2(2n-1)$ bit operations. Hence, these products can be computed using $n^2(2n-1)(n-1)$ bit operations.

To find $\mathbf{M}_{R^*}$ from the $n$ Boolean powers of $\mathbf{M}_R$, $n-1$ joins of zero–one matrices need to be found. Computing each of these joins uses $n^2$ bit operations. Hence, $(n-1)n^2$ bit operations are used in this part of the computation. Therefore, when Algorithm 1 is used, the matrix of the transitive closure of a relation on a set with $n$ elements can be found using $n^2(2n-1)(n-1) + (n-1)n^2 = 2n^3(n-1)$, which is $O(n^4)$ bit operations. The remainder of this section describes a more efficient algorithm for finding transitive closures.

## Warshall's Algorithm

Links

Warshall's algorithm, named after Stephen Warshall, who described this algorithm in 1960, is an efficient method for computing the transitive closure of a relation. Algorithm 1 can find the transitive closure of a relation on a set with $n$ elements using $2n^3(n-1)$ bit operations. However, the transitive closure can be found by Warshall's algorithm using only $2n^3$ bit operations.

***Remark:*** Warshall's algorithm is sometimes called the Roy–Warshall algorithm, because Bernard Roy described this algorithm in 1959.

Suppose that $R$ is a relation on a set with $n$ elements. Let $v_1, v_2, \ldots, v_n$ be an arbitrary listing of these $n$ elements. The concept of the **interior vertices** of a path is used in Warshall's algorithm. If $a, x_1, x_2, \ldots, x_{m-1}, b$ is a path, its interior vertices are $x_1, x_2, \ldots, x_{m-1}$, that is, all the vertices of the path that occur somewhere other than as the first and last vertices in the path. For instance, the interior vertices of a path $a, c, d, f, g, h, b, j$ in a directed graph

are $c, d, f, g, h$, and $b$. The interior vertices of $a, c, d, a, f, b$ are $c, d, a$, and $f$. (Note that the first vertex in the path is not an interior vertex unless it is visited again by the path, except as the last vertex. Similarly, the last vertex in the path is not an interior vertex unless it was visited previously by the path, except as the first vertex.)

Warshall's algorithm is based on the construction of a sequence of zero–one matrices. These matrices are $\mathbf{W}_0, \mathbf{W}_1, \ldots, \mathbf{W}_n$, where $\mathbf{W}_0 = \mathbf{M}_R$ is the zero–one matrix of this relation, and $\mathbf{W}_k = [w_{ij}^{(k)}]$, where $w_{ij}^{(k)} = 1$ if there is a path from $v_i$ to $v_j$ such that all the interior vertices of this path are in the set $\{v_1, v_2, \ldots, v_k\}$ (the first $k$ vertices in the list) and is 0 otherwise. (The first and last vertices in the path may be outside the set of the first $k$ vertices in the list.) Note that $\mathbf{W}_n = \mathbf{M}_{R^*}$, because the $(i, j)$th entry of $\mathbf{M}_{R^*}$ is 1 if and only if there is a path from $v_i$ to $v_j$, with all interior vertices in the set $\{v_1, v_2, \ldots, v_n\}$ (but these are the only vertices in the directed graph). Example 8 illustrates what the matrix $\mathbf{W}_k$ represents.

**EXAMPLE 8** Let $R$ be the relation with directed graph shown in Figure 3. Let $a, b, c, d$ be a listing of the elements of the set. Find the matrices $\mathbf{W}_0, \mathbf{W}_1, \mathbf{W}_2, \mathbf{W}_3$, and $\mathbf{W}_4$. The matrix $\mathbf{W}_4$ is the transitive closure of $R$.

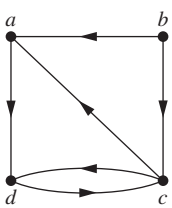



**FIGURE 3 The Directed Graph of the Relation *R*.**

*Solution:* Let $v_1 = a$, $v_2 = b$, $v_3 = c$, and $v_4 = d$. $\mathbf{W}_0$ is the matrix of the relation. Hence,

$$\mathbf{W}_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$\mathbf{W}_1$ has 1 as its $(i, j)$th entry if there is a path from $v_i$ to $v_j$ that has only $v_1 = a$ as an interior vertex. Note that all paths of length one can still be used because they have no interior vertices. Also, there is now an allowable path from $b$ to $d$, namely, $b, a, d$. Hence,

$$\mathbf{W}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$\mathbf{W}_2$ has 1 as its $(i, j)$th entry if there is a path from $v_i$ to $v_j$ that has only $v_1 = a$ and/or $v_2 = b$ as its interior vertices, if any. Because there are no edges that have $b$ as a terminal vertex, no new paths are obtained when we permit $b$ to be an interior vertex. Hence, $\mathbf{W}_2 = \mathbf{W}_1$.

Links

STEPHEN WARSHALL (1935–2006) Stephen Warshall, born in New York City, went to public school in Brooklyn. He attended Harvard University, receiving his degree in mathematics in 1956. He never received an advanced degree, because at that time no programs were available in his areas of interest. However, he took graduate courses at several different universities and contributed to the development of computer science and software engineering.

After graduating from Harvard, Warshall worked at ORO (Operation Research Office), which was set up by Johns Hopkins to do research and development for the U.S. Army. In 1958 he left ORO to take a position at a company called Technical Operations, where he helped build a research and development laboratory for military software projects. In 1961 he left Technical Operations to found Massachusetts Computer Associates. Later, this company became part of Applied Data Research (ADR). After the merger, Warshall sat on the board of directors of ADR and managed a variety of projects and organizations. He retired from ADR in 1982.

During his career Warshall carried out research and development in operating systems, compiler design, language design, and operations research. In the 1971–1972 academic year he presented lectures on software engineering at French universities. There is an interesting anecdote about his proof that the transitive closure algorithm, now known as Warshall's algorithm, is correct. He and a colleague at Technical Operations bet a bottle of rum on who first could determine whether this algorithm always works. Warshall came up with his proof overnight, winning the bet and the rum, which he shared with the loser of the bet. Because Warshall did not like sitting at a desk, he did much of his creative work in unconventional places, such as on a sailboat in the Indian Ocean or in a Greek lemon orchard.

$\mathbf{W}_3$ has 1 as its $(i, j)$th entry if there is a path from $v_i$ to $v_j$ that has only $v_1 = a$, $v_2 = b$, and/or $v_3 = c$ as its interior vertices, if any. We now have paths from $d$ to $a$, namely, $d, c, a$, and from $d$ to $d$, namely, $d, c, d$. Hence,

$$\mathbf{W}_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Finally, $\mathbf{W}_4$ has 1 as its $(i, j)$th entry if there is a path from $v_i$ to $v_j$ that has $v_1 = a$, $v_2 = b$, $v_3 = c$, and/or $v_4 = d$ as interior vertices, if any. Because these are all the vertices of the graph, this entry is 1 if and only if there is a path from $v_i$ to $v_j$. Hence,

$$\mathbf{W}_4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

This last matrix, $\mathbf{W}_4$, is the matrix of the transitive closure. ◀

Warshall's algorithm computes $\mathbf{M}_{R^*}$ by efficiently computing $\mathbf{W}_0 = \mathbf{M}_R$, $\mathbf{W}_1$, $\mathbf{W}_2, \ldots,$ $\mathbf{W}_n = \mathbf{M}_{R^*}$. This observation shows that we can compute $\mathbf{W}_k$ directly from $\mathbf{W}_{k-1}$: There is a path from $v_i$ to $v_j$ with no vertices other than $v_1, v_2, \ldots, v_k$ as interior vertices if and only if either there is a path from $v_i$ to $v_j$ with its interior vertices among the first $k-1$ vertices in the list, or there are paths from $v_i$ to $v_k$ and from $v_k$ to $v_j$ that have interior vertices only among the first $k-1$ vertices in the list. That is, either a path from $v_i$ to $v_j$ already existed before $v_k$ was permitted as an interior vertex, or allowing $v_k$ as an interior vertex produces a path that goes from $v_i$ to $v_k$ and then from $v_k$ to $v_j$. These two cases are shown in Figure 4.

The first type of path exists if and only if $w_{ij}^{[k-1]} = 1$, and the second type of path exists if and only if both $w_{ik}^{[k-1]}$ and $w_{kj}^{[k-1]}$ are 1. Hence, $w_{ij}^{[k]}$ is 1 if and only if either $w_{ij}^{[k-1]}$ is 1 or both $w_{ik}^{[k-1]}$ and $w_{kj}^{[k-1]}$ are 1. This gives us Lemma 2.

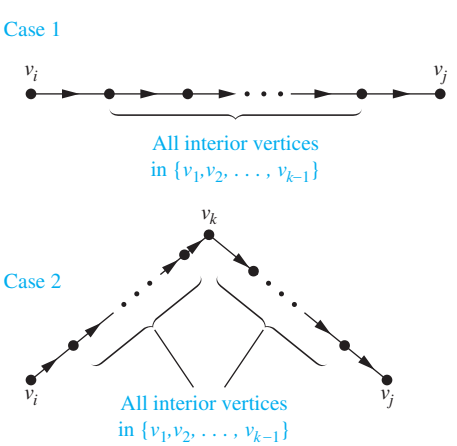



**FIGURE 4 Adding $v_k$ to the Set of Allowable Interior Vertices.**

**LEMMA 2**

Let $\mathbf{W}_k = [w_{ij}^{[k]}]$ be the zero–one matrix that has a 1 in its $(i, j)$th position if and only if there is a path from $v_i$ to $v_j$ with interior vertices from the set $\{v_1, v_2, \ldots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever $i$, $j$, and $k$ are positive integers not exceeding $n$.

Lemma 2 gives us the means to compute efficiently the matrices $\mathbf{W}_k$, $k = 1, 2, \ldots, n$. We display the pseudocode for Warshall's algorithm, using Lemma 2, as Algorithm 2.

**ALGORITHM 2 Warshall Algorithm.**

**procedure** *Warshall* ($\mathbf{M}_R$ : $n \times n$ zero–one matrix)
$\mathbf{W} := \mathbf{M}_R$
**for** $k := 1$ **to** $n$
  **for** $i := 1$ **to** $n$
    **for** $j := 1$ **to** $n$
      $w_{ij} := w_{ij} \vee (w_{ik} \wedge w_{kj})$
**return** $\mathbf{W}\{\mathbf{W} = [w_{ij}]$ is $\mathbf{M}_{R^*}\}$

The computational complexity of Warshall's algorithm can easily be computed in terms of bit operations. To find the entry $w_{ij}^{[k]}$ from the entries $w_{ij}^{[k-1]}$, $w_{ik}^{[k-1]}$, and $w_{kj}^{[k-1]}$ using Lemma 2 requires two bit operations. To find all $n^2$ entries of $\mathbf{W}_k$ from those of $\mathbf{W}_{k-1}$ requires $2n^2$ bit operations. Because Warshall's algorithm begins with $\mathbf{W}_0 = \mathbf{M}_R$ and computes the sequence of $n$ zero–one matrices $\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_n = \mathbf{M}_{R^*}$, the total number of bit operations used is $n \cdot 2n^2 = 2n^3$.

## Exercises

**1.** Let $R$ be the relation on the set $\{0, 1, 2, 3\}$ containing the ordered pairs $(0, 1)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 2)$, and $(3, 0)$. Find the

**a)** reflexive closure of $R$. **b)** symmetric closure of $R$.

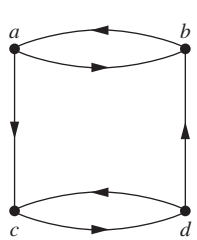
**2.** Let $R$ be the relation $\{(a, b) \mid a \neq b\}$ on the set of integers. What is the reflexive closure of $R$?

**3.** Let $R$ be the relation $\{(a, b) \mid a$ divides $b\}$ on the set of integers. What is the symmetric closure of $R$?

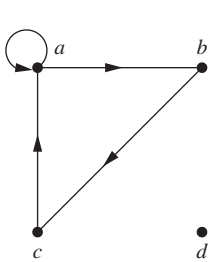
**4.** How can the directed graph representing the reflexive closure of a relation on a finite set be constructed from the directed graph of the relation?

In Exercises 5–7 draw the directed graph of the reflexive closure of the relations with the directed graph shown.

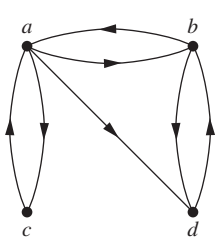
**5.**




**6.**




**7.**




**8.** How can the directed graph representing the symmetric closure of a relation on a finite set be constructed from the directed graph for this relation?

**9.** Find the directed graphs of the symmetric closures of the relations with directed graphs shown in Exercises 5–7.

**10.** Find the smallest relation containing the relation in Example 2 that is both reflexive and symmetric.

**11.** Find the directed graph of the smallest relation that is both reflexive and symmetric that contains each of the relations with directed graphs shown in Exercises 5–7.

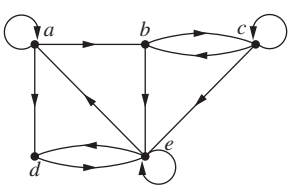
**12.** Suppose that the relation $R$ on the finite set $A$ is represented by the matrix $\mathbf{M}_R$. Show that the matrix that represents the reflexive closure of $R$ is $\mathbf{M}_R \vee \mathbf{I}_n$.

**13.** Suppose that the relation $R$ on the finite set $A$ is represented by the matrix $\mathbf{M}_R$. Show that the matrix that represents the symmetric closure of $R$ is $\mathbf{M}_R \vee \mathbf{M}_R^t$.

**14.** Show that the closure of a relation $R$ with respect to a property **P**, if it exists, is the intersection of all the relations with property **P** that contain $R$.

**15.** When is it possible to define the "irreflexive closure" of a relation $R$, that is, a relation that contains $R$, is irreflexive, and is contained in every irreflexive relation that contains $R$?

**16.** Determine whether these sequences of vertices are paths in this directed graph.




**a)** $a, b, c, e$
**b)** $b, e, c, b, e$
**c)** $a, a, b, e, d, e$
**d)** $b, c, e, d, a, a, b$
**e)** $b, c, c, b, e, d, e, d$
**f)** $a, a, b, b, c, c, b, e, d$

**17.** Find all circuits of length three in the directed graph in Exercise 16.

**18.** Determine whether there is a path in the directed graph in Exercise 16 beginning at the first vertex given and ending at the second vertex given.

**a)** $a, b$ **b)** $b, a$ **c)** $b, b$
**d)** $a, e$ **e)** $b, d$ **f)** $c, d$
**g)** $d, d$ **h)** $e, a$ **i)** $e, c$

**19.** Let $R$ be the relation on the set $\{1, 2, 3, 4, 5\}$ containing the ordered pairs $(1, 3)$, $(2, 4)$, $(3, 1)$, $(3, 5)$, $(4, 3)$, $(5, 1)$, $(5, 2)$, and $(5, 4)$. Find

**a)** $R^2$. **b)** $R^3$. **c)** $R^4$.
**d)** $R^5$. **e)** $R^6$. **f)** $R^*$.

**20.** Let $R$ be the relation that contains the pair $(a, b)$ if $a$ and $b$ are cities such that there is a direct non-stop airline flight from $a$ to $b$. When is $(a, b)$ in

**a)** $R^2$? **b)** $R^3$? **c)** $R^*$?

**21.** Let $R$ be the relation on the set of all students containing the ordered pair $(a, b)$ if $a$ and $b$ are in at least one common class and $a \neq b$. When is $(a, b)$ in

**a)** $R^2$? **b)** $R^3$? **c)** $R^*$?

**22.** Suppose that the relation $R$ is reflexive. Show that $R^*$ is reflexive.

**23.** Suppose that the relation $R$ is symmetric. Show that $R^*$ is symmetric.

**24.** Suppose that the relation $R$ is irreflexive. Is the relation $R^2$ necessarily irreflexive?

**25.** Use Algorithm 1 to find the transitive closures of these relations on $\{1, 2, 3, 4\}$.

**a)** $\{(1, 2), (2, 1), (2, 3), (3, 4), (4, 1)\}$
**b)** $\{(2, 1), (2, 3), (3, 1), (3, 4), (4, 1), (4, 3)\}$
**c)** $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$
**d)** $\{(1, 1), (1, 4), (2, 1), (2, 3), (3, 1), (3, 2), (3, 4), (4, 2)\}$

**26.** Use Algorithm 1 to find the transitive closures of these relations on $\{a, b, c, d, e\}$.

**a)** $\{(a, c), (b, d), (c, a), (d, b), (e, d)\}$
**b)** $\{(b, c), (b, e), (c, e), (d, a), (e, b), (e, c)\}$
**c)** $\{(a, b), (a, c), (a, e), (b, a), (b, c), (c, a), (c, b), (d, a), (e, d)\}$
**d)** $\{(a, e), (b, a), (b, d), (c, d), (d, a), (d, c), (e, a), (e, b), (e, c), (e, e)\}$

**27.** Use Warshall's algorithm to find the transitive closures of the relations in Exercise 25.

**28.** Use Warshall's algorithm to find the transitive closures of the relations in Exercise 26.

**29.** Find the smallest relation containing the relation $\{(1, 2), (1, 4), (3, 3), (4, 1)\}$ that is

**a)** reflexive and transitive.
**b)** symmetric and transitive.
**c)** reflexive, symmetric, and transitive.

**30.** Finish the proof of the case when $a \neq b$ in Lemma 1.

**31.** Algorithms have been devised that use $O(n^{2.8})$ bit operations to compute the Boolean product of two $n \times n$ zero–one matrices. Assuming that these algorithms can be used, give big-$O$ estimates for the number of bit operations using Algorithm 1 and using Warshall's algorithm to find the transitive closure of a relation on a set with $n$ elements.

***32.** Devise an algorithm using the concept of interior vertices in a path to find the length of the shortest path between two vertices in a directed graph, if such a path exists.

**33.** Adapt Algorithm 1 to find the reflexive closure of the transitive closure of a relation on a set with $n$ elements.

**34.** Adapt Warshall's algorithm to find the reflexive closure of the transitive closure of a relation on a set with $n$ elements.

**35.** Show that the closure with respect to the property **P** of the relation $R = \{(0, 0), (0, 1), (1, 1), (2, 2)\}$ on the set $\{0, 1, 2\}$ does not exist if **P** is the property

**a)** "is not reflexive."
**b)** "has an odd number of elements."

# 9.5 Equivalence Relations

## Introduction

In some programming languages the names of variables can contain an unlimited number of characters. However, there is a limit on the number of characters that are checked when a compiler determines whether two variables are equal. For instance, in traditional C, only the first eight characters of a variable name are checked by the compiler. (These characters are

uppercase or lowercase letters, digits, or underscores.) Consequently, the compiler considers strings longer than eight characters that agree in their first eight characters the same. Let $R$ be the relation on the set of strings of characters such that $sRt$, where $s$ and $t$ are two strings, if $s$ and $t$ are at least eight characters long and the first eight characters of $s$ and $t$ agree, or $s = t$. It is easy to see that $R$ is reflexive, symmetric, and transitive. Moreover, $R$ divides the set of all strings into classes, where all strings in a particular class are considered the same by a compiler for traditional C.

The integers $a$ and $b$ are related by the "congruence modulo 4" relation when 4 divides $a - b$. We will show later that this relation is reflexive, symmetric, and transitive. It is not hard to see that $a$ is related to $b$ if and only if $a$ and $b$ have the same remainder when divided by 4. It follows that this relation splits the set of integers into four different classes. When we care only what remainder an integer leaves when it is divided by 4, we need only know which class it is in, not its particular value.

These two relations, $R$ and congruence modulo 4, are examples of equivalence relations, namely, relations that are reflexive, symmetric, and transitive. In this section we will show that such relations split sets into disjoint classes of equivalent elements. Equivalence relations arise whenever we care only whether an element of a set is in a certain class of elements, instead of caring about its particular identity.

## Equivalence Relations


In this section we will study relations with a particular combination of properties that allows them to be used to relate objects that are similar in some way.

**DEFINITION 1**

A relation on a set $A$ is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

Equivalence relations are important in every branch of mathematics!

Equivalence relations are important throughout mathematics and computer science. One reason for this is that in an equivalence relation, when two elements are related it makes sense to say they are equivalent.

**DEFINITION 2**

Two elements $a$ and $b$ that are related by an equivalence relation are called *equivalent*. The notation $a \sim b$ is often used to denote that $a$ and $b$ are equivalent elements with respect to a particular equivalence relation.

For the notion of equivalent elements to make sense, every element should be equivalent to itself, as the reflexive property guarantees for an equivalence relation. It makes sense to say that $a$ and $b$ are related (not just that $a$ is related to $b$) by an equivalence relation, because when $a$ is related to $b$, by the symmetric property, $b$ is related to $a$. Furthermore, because an equivalence relation is transitive, if $a$ and $b$ are equivalent and $b$ and $c$ are equivalent, it follows that $a$ and $c$ are equivalent.

Examples 1–5 illustrate the notion of an equivalence relation.

**EXAMPLE 1** Let $R$ be the relation on the set of integers such that $aRb$ if and only if $a = b$ or $a = -b$. In Section 9.1 we showed that $R$ is reflexive, symmetric, and transitive. It follows that $R$ is an equivalence relation. ◀

**EXAMPLE 2** Let $R$ be the relation on the set of real numbers such that $aRb$ if and only if $a - b$ is an integer. Is $R$ an equivalence relation?

Extra Examples

*Solution:* Because $a - a = 0$ is an integer for all real numbers $a$, $aRa$ for all real numbers $a$. Hence, $R$ is reflexive. Now suppose that $aRb$. Then $a - b$ is an integer, so $b - a$ is also an integer. Hence, $bRa$. It follows that $R$ is symmetric. If $aRb$ and $bRc$, then $a - b$ and $b - c$ are integers. Therefore, $a - c = (a - b) + (b - c)$ is also an integer. Hence, $aRc$. Thus, $R$ is transitive. Consequently, $R$ is an equivalence relation. ◀

One of the most widely used equivalence relations is congruence modulo $m$, where $m$ is an integer greater than 1.

**EXAMPLE 3** **Congruence Modulo $m$** Let $m$ be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is an equivalence relation on the set of integers.

*Solution:* Recall from Section 4.1 that $a \equiv b \pmod{m}$ if and only if $m$ divides $a - b$. Note that $a - a = 0$ is divisible by $m$, because $0 = 0 \cdot m$. Hence, $a \equiv a \pmod{m}$, so congruence modulo $m$ is reflexive. Now suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by $m$, so $a - b = km$, where $k$ is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Hence, congruence modulo $m$ is symmetric. Next, suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then $m$ divides both $a - b$ and $b - c$. Therefore, there are integers $k$ and $l$ with $a - b = km$ and $b - c = lm$. Adding these two equations shows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Thus, $a \equiv c \pmod{m}$. Therefore, congruence modulo $m$ is transitive. It follows that congruence modulo $m$ is an equivalence relation. ◀

**EXAMPLE 4** Suppose that $R$ is the relation on the set of strings of English letters such that $aRb$ if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string $x$. Is $R$ an equivalence relation?

*Solution:* Because $l(a) = l(a)$, it follows that $aRa$ whenever $a$ is a string, so that $R$ is reflexive. Next, suppose that $aRb$, so that $l(a) = l(b)$. Then $bRa$, because $l(b) = l(a)$. Hence, $R$ is symmetric. Finally, suppose that $aRb$ and $bRc$. Then $l(a) = l(b)$ and $l(b) = l(c)$. Hence, $l(a) = l(c)$, so $aRc$. Consequently, $R$ is transitive. Because $R$ is reflexive, symmetric, and transitive, it is an equivalence relation. ◀

**EXAMPLE 5** Let $n$ be a positive integer and $S$ a set of strings. Suppose that $R_n$ is the relation on $S$ such that $s R_n t$ if and only if $s = t$, or both $s$ and $t$ have at least $n$ characters and the first $n$ characters of $s$ and $t$ are the same. That is, a string of fewer than $n$ characters is related only to itself; a string $s$ with at least $n$ characters is related to a string $t$ if and only if $t$ has at least $n$ characters and $t$ begins with the $n$ characters at the start of $s$. For example, let $n = 3$ and let $S$ be the set of all bit strings. Then $s R_3 t$ either when $s = t$ or both $s$ and $t$ are bit strings of length 3 or more that begin with the same three bits. For instance, $01 R_3 01$ and $00111 R_3 00101$, but $01 \not R_3 010$ and $01011 \not R_3 01110$.

Show that for every set $S$ of strings and every positive integer $n$, $R_n$ is an equivalence relation on $S$.

*Solution:* The relation $R_n$ is reflexive because $s = s$, so that $s R_n s$ whenever $s$ is a string in $S$. If $s R_n t$, then either $s = t$ or $s$ and $t$ are both at least $n$ characters long that begin with the same $n$ characters. This means that $t R_n s$. We conclude that $R_n$ is symmetric.

Now suppose that $s R_n t$ and $t R_n u$. Then either $s = t$ or $s$ and $t$ are at least $n$ characters long and $s$ and $t$ begin with the same $n$ characters, and either $t = u$ or $t$ and $u$ are at least $n$ characters long and $t$ and $u$ begin with the same $n$ characters. From this, we can deduce that either $s = u$ or both $s$ and $u$ are $n$ characters long and $s$ and $u$ begin with the same $n$ characters (because in this case we know that $s$, $t$, and $u$ are all at least $n$ characters long and both $s$ and $u$ begin with the same $n$ characters as $t$ does). Consequently, $R_n$ is transitive. It follows that $R_n$ is an equivalence relation. ◀

In Examples 6 and 7 we look at two relations that are not equivalence relations.

**EXAMPLE 6** Show that the "divides" relation is the set of positive integers in not an equivalence relation.

*Solution:* By Examples 9 and 15 in Section 9.1, we know that the "divides" relation is reflexive and transitive. However, by Example 12 in Section 9.1, we know that this relation is not symmetric (for instance, $2 \mid 4$ but $4 \not\mid 2$). We conclude that the "divides" relation on the set of positive integers is not an equivalence relation. ◀

**EXAMPLE 7** Let $R$ be the relation on the set of real numbers such that $x\,R\,y$ if and only if $x$ and $y$ are real numbers that differ by less than 1, that is $|x - y| < 1$. Show that $R$ is not an equivalence relation.

*Solution:* $R$ is reflexive because $|x - x| = 0 < 1$ whenever $x \in \mathbf{R}$. $R$ is symmetric, for if $x\,R\,y$, where $x$ and $y$ are real numbers, then $|x - y| < 1$, which tells us that $|y - x| = |x - y| < 1$, so that $y\,R\,x$. However, $R$ is not an equivalence relation because it is not transitive. Take $x = 2.8$, $y = 1.9$, and $z = 1.1$, so that $|x - y| = |2.8 - 1.9| = 0.9 < 1$, $|y - z| = |1.9 - 1.1| = 0.8 < 1$, but $|x - z| = |2.8 - 1.1| = 1.7 > 1$. That is, $2.8\,R\,1.9$, $1.9\,R\,1.1$, but $2.8 \not R\, 1.1$. ◀

## Equivalence Classes

Let $A$ be the set of all students in your school who graduated from high school. Consider the relation $R$ on $A$ that consists of all pairs $(x, y)$, where $x$ and $y$ graduated from the same high school. Given a student $x$, we can form the set of all students equivalent to $x$ with respect to $R$. This set consists of all students who graduated from the same high school as $x$ did. This subset of $A$ is called an equivalence class of the relation.

**DEFINITION 3** Let $R$ be an equivalence relation on a set $A$. The set of all elements that are related to an element $a$ of $A$ is called the *equivalence class* of $a$. The equivalence class of $a$ with respect to $R$ is denoted by $[a]_R$. When only one relation is under consideration, we can delete the subscript $R$ and write $[a]$ for this equivalence class.

In other words, if $R$ is an equivalence relation on a set $A$, the equivalence class of the element $a$ is

$$[a]_R = \{s \mid (a, s) \in R\}.$$

If $b \in [a]_R$, then $b$ is called a **representative** of this equivalence class. Any element of a class can be used as a representative of this class. That is, there is nothing special about the particular element chosen as the representative of the class.

**EXAMPLE 8** What is the equivalence class of an integer for the equivalence relation of Example 1?

*Solution:* Because an integer is equivalent to itself and its negative in this equivalence relation, it follows that $[a] = \{-a, a\}$. This set contains two distinct integers unless $a = 0$. For instance, $[7] = \{-7, 7\}$, $[-5] = \{-5, 5\}$, and $[0] = \{0\}$. ◀

**EXAMPLE 9** What are the equivalence classes of 0 and 1 for congruence modulo 4?

*Solution:* The equivalence class of 0 contains all integers $a$ such that $a \equiv 0 \pmod 4$. The integers in this class are those divisible by 4. Hence, the equivalence class of 0 for this relation is

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}.$$

The equivalence class of 1 contains all the integers $a$ such that $a \equiv 1 \pmod 4$. The integers in this class are those that have a remainder of 1 when divided by 4. Hence, the equivalence class of 1 for this relation is

$$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}.$$ ◀

In Example 9 the equivalence classes of 0 and 1 with respect to congruence modulo 4 were found. Example 9 can easily be generalized, replacing 4 with any positive integer $m$. The equivalence classes of the relation congruence modulo $m$ are called the **congruence classes modulo** $m$. The congruence class of an integer $a$ modulo $m$ is denoted by $[a]_m$, so $[a]_m = \{\ldots, a - 2m, a - m, a, a + m, a + 2m, \ldots\}$. For instance, from Example 9 it follows that $[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ and $[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$.

**EXAMPLE 10** What is the equivalence class of the string 0111 with respect to the equivalence relation $R_3$ from Example 5 on the set of all bit strings? (Recall that $s R_3 t$ if and only if $s$ and $t$ are bit strings with $s = t$ or $s$ and $t$ are strings of at least three bits that start with the same three bits.)

*Solution:* The bit strings equivalent to 0111 are the bit strings with at least three bits that begin with 011. These are the bit strings 011, 0110, 0111, 01100, 01101, 01110, 01111, and so on. Consequently,

$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\}.$$ ◀

**EXAMPLE 11** **Identifiers in the C Programming Language** In the C programming language, an **identifier** is the name of a variable, a function, or another type of entity. Each identifier is a nonempty string of characters where each character is a lowercase or an uppercase English letter, a digit, or an underscore, and the first character is a lowercase or an uppercase English letter. Identifiers can be any length. This allows developers to use as many characters as they want to name an entity, such as a variable. However, for compilers for some versions of C, there is a limit on the number of characters checked when two names are compared to see whether they refer to the same thing. For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. Consequently, developers must be careful not to use identifiers with the same initial 31 characters for different things. We see that two identifiers are considered the same when they are related by the relation $R_{31}$ in Example 5. Using Example 5, we know that $R_{31}$, on the set of all identifiers in Standard C, is an equivalence relation.

What are the equivalence classes of each of the identifiers Number_of_tropical_storms, Number_of_named_tropical_storms, and Number_of_named_tropical_storms_in_the_Atlantic_in_2005?

*Solution:* Note that when an identifier is less than 31 characters long, by the definition of $R_{31}$, its equivalence class contains only itself. Because the identifier Number_of_tropical_storms is 25 characters long, its equivalence class contains exactly one element, namely, itself.

The identifier Number_of_named_tropical_storms is exactly 31 characters long. An identifier is equivalent to it when it starts with these same 31 characters. Consequently, every identifier at least 31 characters long that starts with Number_of_named_tropical_storms is equivalent to this identifier. It follows that the equivalence class of Number_of_named_tropical_storms is the set of all identifiers that begin with the 31 characters Number_of_named_tropical_storms.

An identifier is equivalent to the Number_of_named_tropical_storms_in_the_Atlantic_in_2005 if and only if it begins with its first 31 characters. Because these characters are Number_of_named_tropical_storms, we see that an identifier is equivalent to Number_of_named_tropical_storms_in_the_Atlantic_in_2005 if and only if it is equivalent to Number_of_named_tropical_storms. It follows that these last two identifiers have the same equivalence class. ◀

## Equivalence Classes and Partitions

Let $A$ be the set of students at your school who are majoring in exactly one subject, and let $R$ be the relation on $A$ consisting of pairs $(x, y)$, where $x$ and $y$ are students with the same major. Then $R$ is an equivalence relation, as the reader should verify. We can see that $R$ splits all students in $A$ into a collection of disjoint subsets, where each subset contains students with a specified major. For instance, one subset contains all students majoring (just) in computer science, and a second subset contains all students majoring in history. Furthermore, these subsets are equivalence classes of $R$. This example illustrates how the equivalence classes of an equivalence relation partition a set into disjoint, nonempty subsets. We will make these notions more precise in the following discussion.

Let $R$ be a relation on the set $A$. Theorem 1 shows that the equivalence classes of two elements of $A$ are either identical or disjoint.

**THEOREM 1**

Let $R$ be an equivalence relation on a set $A$. These statements for elements $a$ and $b$ of $A$ are equivalent:

$(i)$ $aRb$ $\quad$ $(ii)$ $[a] = [b]$ $\quad$ $(iii)$ $[a] \cap [b] \neq \emptyset$

***Proof:*** We first show that $(i)$ implies $(ii)$. Assume that $aRb$. We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then $aRc$. Because $aRb$ and $R$ is symmetric, we know that $bRa$. Furthermore, because $R$ is transitive and $bRa$ and $aRc$, it follows that $bRc$. Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar; it is left as an exercise for the reader.

Second, we will show that $(ii)$ implies $(iii)$. Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because $R$ is reflexive).

Next, we will show that $(iii)$ implies $(i)$. Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element $c$ with $c \in [a]$ and $c \in [b]$. In other words, $aRc$ and $bRc$. By the symmetric property, $cRb$. Then by transitivity, because $aRc$ and $cRb$, we have $aRb$.

Because $(i)$ implies $(ii)$, $(ii)$ implies $(iii)$, and $(iii)$ implies $(i)$, the three statements, $(i)$, $(ii)$, and $(iii)$, are equivalent. ◁

We are now in a position to show how an equivalence relation *partitions* a set. Let $R$ be an equivalence relation on a set $A$. The union of the equivalence classes of $R$ is all of $A$, because an element $a$ of $A$ is in its own equivalence class, namely, $[a]_R$. In other words,

$$\bigcup_{a \in A} [a]_R = A.$$

In addition, from Theorem 1, it follows that these equivalence classes are either equal or disjoint, so

$$[a]_R \cap [b]_R = \emptyset,$$

when $[a]_R \neq [b]_R$.

Recall that an *index set* is a set whose members label, or index, the elements of a set.

These two observations show that the equivalence classes form a partition of $A$, because they split $A$ into disjoint subsets. More precisely, a **partition** of a set $S$ is a collection of disjoint nonempty subsets of $S$ that have $S$ as their union. In other words, the collection of subsets $A_i$, $i \in I$ (where $I$ is an index set) forms a partition of $S$ if and only if

$$A_i \neq \emptyset \text{ for } i \in I,$$

$$A_i \cap A_j = \emptyset \text{ when } i \neq j,$$

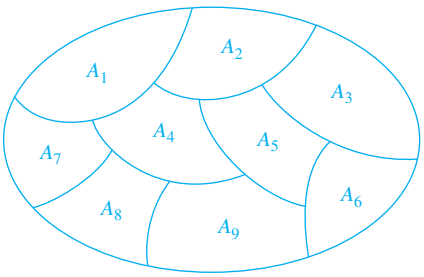



**FIGURE 1** **A Partition of a Set.**

and

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

(Here the notation $\bigcup_{i \in I} A_i$ represents the union of the sets $A_i$ for all $i \in I$.) Figure 1 illustrates the concept of a partition of a set.

**EXAMPLE 12** Suppose that $S = \{1, 2, 3, 4, 5, 6\}$. The collection of sets $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, and $A_3 = \{6\}$ forms a partition of $S$, because these sets are disjoint and their union is $S$. ◀

We have seen that the equivalence classes of an equivalence relation on a set form a partition of the set. The subsets in this partition are the equivalence classes. Conversely, every partition of a set can be used to form an equivalence relation. Two elements are equivalent with respect to this relation if and only if they are in the same subset of the partition.

To see this, assume that $\{A_i \mid i \in I\}$ is a partition on $S$. Let $R$ be the relation on $S$ consisting of the pairs $(x, y)$, where $x$ and $y$ belong to the same subset $A_i$ in the partition. To show that $R$ is an equivalence relation we must show that $R$ is reflexive, symmetric, and transitive.

We see that $(a, a) \in R$ for every $a \in S$, because $a$ is in the same subset as itself. Hence, $R$ is reflexive. If $(a, b) \in R$, then $b$ and $a$ are in the same subset of the partition, so that $(b, a) \in R$ as well. Hence, $R$ is symmetric. If $(a, b) \in R$ and $(b, c) \in R$, then $a$ and $b$ are in the same subset $X$ in the partition, and $b$ and $c$ are in the same subset $Y$ of the partition. Because the subsets of the partition are disjoint and $b$ belongs to $X$ and $Y$, it follows that $X = Y$. Consequently, $a$ and $c$ belong to the same subset of the partition, so $(a, c) \in R$. Thus, $R$ is transitive.

It follows that $R$ is an equivalence relation. The equivalence classes of $R$ consist of subsets of $S$ containing related elements, and by the definition of $R$, these are the subsets of the partition. Theorem 2 summarizes the connections we have established between equivalence relations and partitions.

**THEOREM 2** Let $R$ be an equivalence relation on a set $S$. Then the equivalence classes of $R$ form a partition of $S$. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set $S$, there is an equivalence relation $R$ that has the sets $A_i$, $i \in I$, as its equivalence classes.

Example 13 shows how to construct an equivalence relation from a partition.

**EXAMPLE 13** List the ordered pairs in the equivalence relation $R$ produced by the partition $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, and $A_3 = \{6\}$ of $S = \{1, 2, 3, 4, 5, 6\}$, given in Example 12.

*Solution:* The subsets in the partition are the equivalence classes of $R$. The pair $(a, b) \in R$ if and only if $a$ and $b$ are in the same subset of the partition. The pairs $(1, 1)$, $(1, 2)$, $(1, 3)$, $(2, 1)$, $(2, 2)$, $(2, 3)$, $(3, 1)$, $(3, 2)$, and $(3, 3)$ belong to $R$ because $A_1 = \{1, 2, 3\}$ is an equivalence class; the pairs $(4, 4)$, $(4, 5)$, $(5, 4)$, and $(5, 5)$ belong to $R$ because $A_2 = \{4, 5\}$ is an equivalence class; and finally the pair $(6, 6)$ belongs to $R$ because $\{6\}$ is an equivalence class. No pair other than those listed belongs to $R$. ◀

The congruence classes modulo $m$ provide a useful illustration of Theorem 2. There are $m$ different congruence classes modulo $m$, corresponding to the $m$ different remainders possible when an integer is divided by $m$. These $m$ congruence classes are denoted by $[0]_m, [1]_m, \ldots, [m-1]_m$. They form a partition of the set of integers.

**EXAMPLE 14** What are the sets in the partition of the integers arising from congruence modulo 4?

*Solution:* There are four congruence classes, corresponding to $[0]_4$, $[1]_4$, $[2]_4$, and $[3]_4$. They are the sets

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\},$$
$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\},$$
$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}.$$

These congruence classes are disjoint, and every integer is in exactly one of them. In other words, as Theorem 2 says, these congruence classes form a partition. ◀

We now provide an example of a partition of the set of all strings arising from an equivalence relation on this set.

**EXAMPLE 15** Let $R_3$ be the relation from Example 5. What are the sets in the partition of the set of all bit strings arising from the relation $R_3$ on the set of all bit strings? (Recall that $s R_3 t$, where $s$ and $t$ are bit strings, if $s = t$ or $s$ and $t$ are bit strings with at least three bits that agree in their first three bits.)

*Solution:* Note that every bit string of length less than three is equivalent only to itself. Hence $[\lambda]_{R_3} = \{\lambda\}, [0]_{R_3} = \{0\}, [1]_{R_3} = \{1\}, [00]_{R_3} = \{00\}, [01]_{R_3} = \{01\}, [10]_{R_3} = \{10\}$, and $[11]_{R_3} = \{11\}$. Note that every bit string of length three or more is equivalent to one of the eight bit strings 000, 001, 010, 011, 100, 101, 110, and 111. We have

$$[000]_{R_3} = \{000, 0000, 0001, 00000, 00001, 00010, 00011, \ldots\},$$

$$[001]_{R_3} = \{001, 0010, 0011, 00100, 00101, 00110, 00111, \ldots\},$$

$$[010]_{R_3} = \{010, 0100, 0101, 01000, 01001, 01010, 01011, \ldots\},$$

$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \ldots\},$$

$$[100]_{R_3} = \{100, 1000, 1001, 10000, 10001, 10010, 10011, \ldots\},$$

$$[101]_{R_3} = \{101, 1010, 1011, 10100, 10101, 10110, 10111, \ldots\},$$

$$[110]_{R_3} = \{110, 1100, 1101, 11000, 11001, 11010, 11011, \ldots\},$$

$$[111]_{R_3} = \{111, 1110, 1111, 11100, 11101, 11110, 11111, \ldots\}.$$

These 15 equivalence classes are disjoint and every bit string is in exactly one of them. As Theorem 2 tells us, these equivalence classes partition the set of all bit strings. ◀

## Exercises

**1.** Which of these relations on $\{0, 1, 2, 3\}$ are equivalence relations? Determine the properties of an equivalence relation that the others lack.
**a)** $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$
**b)** $\{(0, 0), (0, 2), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)\}$
**c)** $\{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$
**d)** $\{(0, 0), (1, 1), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$
**e)** $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)\}$

**2.** Which of these relations on the set of all people are equivalence relations? Determine the properties of an equivalence relation that the others lack.
**a)** $\{(a, b) \mid a$ and $b$ are the same age$\}$
**b)** $\{(a, b) \mid a$ and $b$ have the same parents$\}$
**c)** $\{(a, b) \mid a$ and $b$ share a common parent$\}$
**d)** $\{(a, b) \mid a$ and $b$ have met$\}$
**e)** $\{(a, b) \mid a$ and $b$ speak a common language$\}$

**3.** Which of these relations on the set of all functions from $\mathbf{Z}$ to $\mathbf{Z}$ are equivalence relations? Determine the properties of an equivalence relation that the others lack.
**a)** $\{(f, g) \mid f(1) = g(1)\}$
**b)** $\{(f, g) \mid f(0) = g(0)$ or $f(1) = g(1)\}$
**c)** $\{(f, g) \mid f(x) - g(x) = 1$ for all $x \in \mathbf{Z}\}$
**d)** $\{(f, g) \mid$ for some $C \in \mathbf{Z}$, for all $x \in \mathbf{Z}$, $f(x) - g(x) = C\}$
**e)** $\{(f, g) \mid f(0) = g(1)$ and $f(1) = g(0)\}$

**4.** Define three equivalence relations on the set of students in your discrete mathematics class different from the relations discussed in the text. Determine the equivalence classes for each of these equivalence relations.

**5.** Define three equivalence relations on the set of buildings on a college campus. Determine the equivalence classes for each of these equivalence relations.

**6.** Define three equivalence relations on the set of classes offered at your school. Determine the equivalence classes for each of these equivalence relations.

**7.** Show that the relation of logical equivalence on the set of all compound propositions is an equivalence relation. What are the equivalence classes of **F** and of **T**?

**8.** Let $R$ be the relation on the set of all sets of real numbers such that $S\,R\,T$ if and only if $S$ and $T$ have the same cardinality. Show that $R$ is an equivalence relation. What are the equivalence classes of the sets $\{0, 1, 2\}$ and $\mathbf{Z}$?

**9.** Suppose that $A$ is a nonempty set, and $f$ is a function that has $A$ as its domain. Let $R$ be the relation on $A$ consisting of all ordered pairs $(x, y)$ such that $f(x) = f(y)$.
**a)** Show that $R$ is an equivalence relation on $A$.
**b)** What are the equivalence classes of $R$?

**10.** Suppose that $A$ is a nonempty set and $R$ is an equivalence relation on $A$. Show that there is a function $f$ with $A$ as its domain such that $(x, y) \in R$ if and only if $f(x) = f(y)$.

**11.** Show that the relation $R$ consisting of all pairs $(x, y)$ such that $x$ and $y$ are bit strings of length three or more that agree in their first three bits is an equivalence relation on the set of all bit strings of length three or more.

**12.** Show that the relation $R$ consisting of all pairs $(x, y)$ such that $x$ and $y$ are bit strings of length three or more that agree except perhaps in their first three bits is an equivalence relation on the set of all bit strings of length three or more.

**13.** Show that the relation $R$ consisting of all pairs $(x, y)$ such that $x$ and $y$ are bit strings that agree in their first and third bits is an equivalence relation on the set of all bit strings of length three or more.

**14.** Let $R$ be the relation consisting of all pairs $(x, y)$ such that $x$ and $y$ are strings of uppercase and lowercase English letters with the property that for every positive integer $n$, the $n$th characters in $x$ and $y$ are the same letter, either uppercase or lowercase. Show that $R$ is an equivalence relation.

**15.** Let $R$ be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $a + d = b + c$. Show that $R$ is an equivalence relation.

**16.** Let $R$ be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$. Show that $R$ is an equivalence relation.

**17.** (*Requires calculus*)
**a)** Show that the relation $R$ on the set of all differentiable functions from $\mathbf{R}$ to $\mathbf{R}$ consisting of all pairs $(f, g)$ such that $f'(x) = g'(x)$ for all real numbers $x$ is an equivalence relation.
**b)** Which functions are in the same equivalence class as the function $f(x) = x^2$?

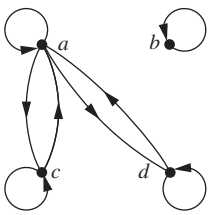
**18.** (*Requires calculus*)
**a)** Let $n$ be a positive integer. Show that the relation $R$ on the set of all polynomials with real-valued coefficients consisting of all pairs $(f, g)$ such that $f^{(n)}(x) = g^{(n)}(x)$ is an equivalence relation. [Here $f^{(n)}(x)$ is the $n$th derivative of $f(x)$.]
**b)** Which functions are in the same equivalence class as the function $f(x) = x^4$, where $n = 3$?

**19.** Let $R$ be the relation on the set of all URLs (or Web addresses) such that $x\,R\,y$ if and only if the Web page at $x$ is the same as the Web page at $y$. Show that $R$ is an equivalence relation.

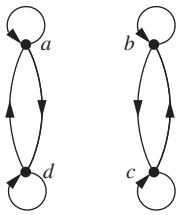
**20.** Let $R$ be the relation on the set of all people who have visited a particular Web page such that $x\,R\,y$ if and only if person $x$ and person $y$ have followed the same set of links starting at this Web page (going from Web page to Web page until they stop using the Web). Show that $R$ is an equivalence relation.

In Exercises 21–23 determine whether the relation with the directed graph shown is an equivalence relation.

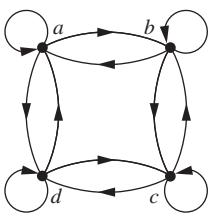
**21.**




**22.**




**23.**




**24.** Determine whether the relations represented by these zero–one matrices are equivalence relations.

**a)** $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ **b)** $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ **c)** $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

**25.** Show that the relation $R$ on the set of all bit strings such that $s\ R\ t$ if and only if $s$ and $t$ contain the same number of 1s is an equivalence relation.

**26.** What are the equivalence classes of the equivalence relations in Exercise 1?

**27.** What are the equivalence classes of the equivalence relations in Exercise 2?

**28.** What are the equivalence classes of the equivalence relations in Exercise 3?

**29.** What is the equivalence class of the bit string 011 for the equivalence relation in Exercise 25?

**30.** What are the equivalence classes of these bit strings for the equivalence relation in Exercise 11?

**a)** 010 **b)** 1011 **c)** 11111 **d)** 01010101

**31.** What are the equivalence classes of the bit strings in Exercise 30 for the equivalence relation from Exercise 12?

**32.** What are the equivalence classes of the bit strings in Exercise 30 for the equivalence relation from Exercise 13?

**33.** What are the equivalence classes of the bit strings in Exercise 30 for the equivalence relation $R_4$ from Example 5 on the set of all bit strings? (Recall that bit strings $s$ and $t$ are equivalent under $R_4$ if and only if they are equal or they are both at least four bits long and agree in their first four bits.)

**34.** What are the equivalence classes of the bit strings in Exercise 30 for the equivalence relation $R_5$ from Example 5 on the set of all bit strings? (Recall that bit strings $s$ and $t$ are equivalent under $R_5$ if and only if they are equal or they are both at least five bits long and agree in their first five bits.)

**35.** What is the congruence class $[n]_5$ (that is, the equivalence class of $n$ with respect to congruence modulo 5) when $n$ is

**a)** 2? **b)** 3? **c)** 6? **d)** $-3$?

**36.** What is the congruence class $[4]_m$ when $m$ is

**a)** 2? **b)** 3? **c)** 6? **d)** 8?

**37.** Give a description of each of the congruence classes modulo 6.

**38.** What is the equivalence class of each of these strings with respect to the equivalence relation in Exercise 14?

**a)** *No* **b)** *Yes* **c)** *Help*

**39. a)** What is the equivalence class of $(1, 2)$ with respect to the equivalence relation in Exercise 15?

**b)** Give an interpretation of the equivalence classes for the equivalence relation $R$ in Exercise 15. [*Hint:* Look at the difference $a - b$ corresponding to $(a, b)$.]

**40. a)** What is the equivalence class of $(1, 2)$ with respect to the equivalence relation in Exercise 16?

**b)** Give an interpretation of the equivalence classes for the equivalence relation $R$ in Exercise 16. [*Hint:* Look at the ratio $a/b$ corresponding to $(a, b)$.]

**41.** Which of these collections of subsets are partitions of $\{1, 2, 3, 4, 5, 6\}$?

**a)** $\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}$ **b)** $\{1\}, \{2, 3, 6\}, \{4\}, \{5\}$
**c)** $\{2, 4, 6\}, \{1, 3, 5\}$ **d)** $\{1, 4, 5\}, \{2, 6\}$

**42.** Which of these collections of subsets are partitions of $\{-3, -2, -1, 0, 1, 2, 3\}$?

**a)** $\{-3, -1, 1, 3\}, \{-2, 0, 2\}$
**b)** $\{-3, -2, -1, 0\}, \{0, 1, 2, 3\}$
**c)** $\{-3, 3\}, \{-2, 2\}, \{-1, 1\}, \{0\}$
**d)** $\{-3, -2, 2, 3\}, \{-1, 1\}$

**43.** Which of these collections of subsets are partitions of the set of bit strings of length 8?

**a)** the set of bit strings that begin with 1, the set of bit strings that begin with 00, and the set of bit strings that begin with 01
**b)** the set of bit strings that contain the string 00, the set of bit strings that contain the string 01, the set of bit strings that contain the string 10, and the set of bit strings that contain the string 11
**c)** the set of bit strings that end with 00, the set of bit strings that end with 01, the set of bit strings that end with 10, and the set of bit strings that end with 11
**d)** the set of bit strings that end with 111, the set of bit strings that end with 011, and the set of bit strings that end with 00
**e)** the set of bit strings that contain $3k$ ones for some nonnegative integer $k$; the set of bit strings that contain $3k + 1$ ones for some nonnegative integer $k$; and the set of bit strings that contain $3k + 2$ ones for some nonnegative integer $k$.

**44.** Which of these collections of subsets are partitions of the set of integers?

**a)** the set of even integers and the set of odd integers
**b)** the set of positive integers and the set of negative integers

**c)** the set of integers divisible by 3, the set of integers leaving a remainder of 1 when divided by 3, and the set of integers leaving a remainder of 2 when divided by 3

**d)** the set of integers less than $-100$, the set of integers with absolute value not exceeding 100, and the set of integers greater than 100

**e)** the set of integers not divisible by 3, the set of even integers, and the set of integers that leave a remainder of 3 when divided by 6

**45.** Which of these are partitions of the set $\mathbf{Z} \times \mathbf{Z}$ of ordered pairs of integers?

**a)** the set of pairs $(x, y)$, where $x$ or $y$ is odd; the set of pairs $(x, y)$, where $x$ is even; and the set of pairs $(x, y)$, where $y$ is even

**b)** the set of pairs $(x, y)$, where both $x$ and $y$ are odd; the set of pairs $(x, y)$, where exactly one of $x$ and $y$ is odd; and the set of pairs $(x, y)$, where both $x$ and $y$ are even

**c)** the set of pairs $(x, y)$, where $x$ is positive; the set of pairs $(x, y)$, where $y$ is positive; and the set of pairs $(x, y)$, where both $x$ and $y$ are negative

**d)** the set of pairs $(x, y)$, where $3 \mid x$ and $3 \mid y$; the set of pairs $(x, y)$, where $3 \mid x$ and $3 \not\mid y$; the set of pairs $(x, y)$, where $3 \not\mid x$ and $3 \mid y$; and the set of pairs $(x, y)$, where $3 \not\mid x$ and $3 \not\mid y$

**e)** the set of pairs $(x, y)$, where $x > 0$ and $y > 0$; the set of pairs $(x, y)$, where $x > 0$ and $y \leq 0$; the set of pairs $(x, y)$, where $x \leq 0$ and $y > 0$; and the set of pairs $(x, y)$, where $x \leq 0$ and $y \leq 0$

**f)** the set of pairs $(x, y)$, where $x \neq 0$ and $y \neq 0$; the set of pairs $(x, y)$, where $x = 0$ and $y \neq 0$; and the set of pairs $(x, y)$, where $x \neq 0$ and $y = 0$

**46.** Which of these are partitions of the set of real numbers?

**a)** the negative real numbers, $\{0\}$, the positive real numbers

**b)** the set of irrational numbers, the set of rational numbers

**c)** the set of intervals $[k, k + 1]$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**d)** the set of intervals $(k, k + 1)$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**e)** the set of intervals $(k, k + 1]$, $k = \ldots, -2, -1, 0, 1, 2, \ldots$

**f)** the sets $\{x + n \mid n \in \mathbf{Z}\}$ for all $x \in [0, 1)$

**47.** List the ordered pairs in the equivalence relations produced by these partitions of $\{0, 1, 2, 3, 4, 5\}$.

**a)** $\{0\}, \{1, 2\}, \{3, 4, 5\}$

**b)** $\{0, 1\}, \{2, 3\}, \{4, 5\}$

**c)** $\{0, 1, 2\}, \{3, 4, 5\}$

**d)** $\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}$

**48.** List the ordered pairs in the equivalence relations produced by these partitions of $\{a, b, c, d, e, f, g\}$.

**a)** $\{a, b\}, \{c, d\}, \{e, f, g\}$

**b)** $\{a\}, \{b\}, \{c, d\}, \{e, f\}, \{g\}$

**c)** $\{a, b, c, d\}, \{e, f, g\}$

**d)** $\{a, c, e, g\}, \{b, d\}, \{f\}$

A partition $P_1$ is called a **refinement** of the partition $P_2$ if every set in $P_1$ is a subset of one of the sets in $P_2$.

**49.** Show that the partition formed from congruence classes modulo 6 is a refinement of the partition formed from congruence classes modulo 3.

**50.** Show that the partition of the set of people living in the United States consisting of subsets of people living in the same county (or parish) and same state is a refinement of the partition consisting of subsets of people living in the same state.

**51.** Show that the partition of the set of bit strings of length 16 formed by equivalence classes of bit strings that agree on the last eight bits is a refinement of the partition formed from the equivalence classes of bit strings that agree on the last four bits.

In Exercises 52 and 53, $R_n$ refers to the family of equivalence relations defined in Example 5. Recall that $s \, R_n \, t$, where $s$ and $t$ are two strings if $s = t$ or $s$ and $t$ are strings with at least $n$ characters that agree in their first $n$ characters.

**52.** Show that the partition of the set of all bit strings formed by equivalence classes of bit strings with respect to the equivalence relation $R_4$ is a refinement of the partition formed by equivalence classes of bit strings with respect to the equivalence relation $R_3$.

**53.** Show that the partition of the set of all identifiers in C formed by the equivalence classes of identifiers with respect to the equivalence relation $R_{31}$ is a refinement of the partition formed by equivalence classes of identifiers with respect to the equivalence relation $R_8$. (Compilers for "old" C consider identifiers the same when their names agree in their first eight characters, while compilers in standard C consider identifiers the same when their names agree in their first 31 characters.)

**54.** Suppose that $R_1$ and $R_2$ are equivalence relations on a set $A$. Let $P_1$ and $P_2$ be the partitions that correspond to $R_1$ and $R_2$, respectively. Show that $R_1 \subseteq R_2$ if and only if $P_1$ is a refinement of $P_2$.

**55.** Find the smallest equivalence relation on the set $\{a, b, c, d, e\}$ containing the relation $\{(a, b), (a, c), (d, e)\}$.

**56.** Suppose that $R_1$ and $R_2$ are equivalence relations on the set $S$. Determine whether each of these combinations of $R_1$ and $R_2$ must be an equivalence relation.

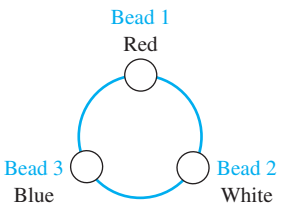
**a)** $R_1 \cup R_2$ **b)** $R_1 \cap R_2$ **c)** $R_1 \oplus R_2$

**57.** Consider the equivalence relation from Example 2, namely, $R = \{(x, y) \mid x - y \text{ is an integer}\}$.

**a)** What is the equivalence class of 1 for this equivalence relation?

**b)** What is the equivalence class of 1/2 for this equivalence relation?

***58.** Each bead on a bracelet with three beads is either red, white, or blue, as illustrated in the figure shown.




Define the relation $R$ between bracelets as: $(B_1, B_2)$, where $B_1$ and $B_2$ are bracelets, belongs to $R$ if and only if $B_2$ can be obtained from $B_1$ by rotating it or rotating it and then reflecting it.

**a)** Show that $R$ is an equivalence relation.

**b)** What are the equivalence classes of $R$?

***59.** Let $R$ be the relation on the set of all colorings of the $2 \times 2$ checkerboard where each of the four squares is colored either red or blue so that $(C_1, C_2)$, where $C_1$ and $C_2$ are $2 \times 2$ checkerboards with each of their four squares colored blue or red, belongs to $R$ if and only if $C_2$ can be obtained from $C_1$ either by rotating the checkerboard or by rotating it and then reflecting it.

**a)** Show that $R$ is an equivalence relation.

**b)** What are the equivalence classes of $R$?

**60. a)** Let $R$ be the relation on the set of functions from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ such that $(f, g)$ belongs to $R$ if and only if $f$ is $\Theta(g)$ (see Section 3.2). Show that $R$ is an equivalence relation.

**b)** Describe the equivalence class containing $f(n) = n^2$ for the equivalence relation of part (a).

**61.** Determine the number of different equivalence relations on a set with three elements by listing them.

**62.** Determine the number of different equivalence relations on a set with four elements by listing them.

***63.** Do we necessarily get an equivalence relation when we form the transitive closure of the symmetric closure of the reflexive closure of a relation?

***64.** Do we necessarily get an equivalence relation when we form the symmetric closure of the reflexive closure of the transitive closure of a relation?

**65.** Suppose we use Theorem 2 to form a partition $P$ from an equivalence relation $R$. What is the equivalence relation $R'$ that results if we use Theorem 2 again to form an equivalence relation from $P$?

**66.** Suppose we use Theorem 2 to form an equivalence relation $R$ from a partition $P$. What is the partition $P'$ that results if we use Theorem 2 again to form a partition from $R$?

**67.** Devise an algorithm to find the smallest equivalence relation containing a given relation.

***68.** Let $p(n)$ denote the number of different equivalence relations on a set with $n$ elements (and by Theorem 2 the number of partitions of a set with $n$ elements). Show that $p(n)$ satisfies the recurrence relation $p(n) = \sum_{j=0}^{n-1} C(n-1, j)p(n-j-1)$ and the initial condition $p(0) = 1$. (*Note:* The numbers $p(n)$ are called **Bell numbers** after the American mathematician E. T. Bell.)

**69.** Use Exercise 68 to find the number of different equivalence relations on a set with $n$ elements, where $n$ is a positive integer not exceeding 10.

# 9.6 Partial Orderings

## Introduction

We often use relations to order some or all of the elements of sets. For instance, we order words using the relation containing pairs of words $(x, y)$, where $x$ comes before $y$ in the dictionary. We schedule projects using the relation consisting of pairs $(x, y)$, where $x$ and $y$ are tasks in a project such that $x$ must be completed before $y$ begins. We order the set of integers using the relation containing the pairs $(x, y)$, where $x$ is less than $y$. When we add all of the pairs of the form $(x, x)$ to these relations, we obtain a relation that is reflexive, antisymmetric, and transitive. These are properties that characterize relations used to order the elements of sets.

Links

**DEFINITION 1** A relation $R$ on a set $S$ is called a *partial ordering* or *partial order* if it is reflexive, antisymmetric, and transitive. A set $S$ together with a partial ordering $R$ is called a *partially ordered set*, or *poset*, and is denoted by $(S, R)$. Members of $S$ are called *elements* of the poset.

We give examples of posets in Examples 1–3.

**EXAMPLE 1** Show that the "greater than or equal" relation $(\geq)$ is a partial ordering on the set of integers.

Extra Examples

*Solution:* Because $a \geq a$ for every integer $a$, $\geq$ is reflexive. If $a \geq b$ and $b \geq a$, then $a = b$. Hence, $\geq$ is antisymmetric. Finally, $\geq$ is transitive because $a \geq b$ and $b \geq c$ imply that $a \geq c$. It follows that $\geq$ is a partial ordering on the set of integers and $(\mathbf{Z}, \geq)$ is a poset. ◀

**EXAMPLE 2** The divisibility relation $|$ is a partial ordering on the set of positive integers, because it is reflexive, antisymmetric, and transitive, as was shown in Section 9.1. We see that $(\mathbf{Z}^+, |)$ is a poset. Recall that ($\mathbf{Z}^+$ denotes the set of positive integers.) ◀

**EXAMPLE 3** Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set $S$.

*Solution:* Because $A \subseteq A$ whenever $A$ is a subset of $S$, $\subseteq$ is reflexive. It is antisymmetric because $A \subseteq B$ and $B \subseteq A$ imply that $A = B$. Finally, $\subseteq$ is transitive, because $A \subseteq B$ and $B \subseteq C$ imply that $A \subseteq C$. Hence, $\subseteq$ is a partial ordering on $P(S)$, and $(P(S), \subseteq)$ is a poset. ◀

Example 4 illustrates a relation that is not a partial ordering.

**EXAMPLE 4** Let $R$ be the relation on the set of people such that $x\,R\,y$ if $x$ and $y$ are people and $x$ is older than $y$. Show that $R$ is not a partial ordering.

Extra Examples

*Solution:* Note that $R$ is antisymmetric because if a person $x$ is older than a person $y$, then $y$ is not older than $x$. That is, if $x\,R\,y$, then $y \not R\, x$. The relation $R$ is transitive because if person $x$ is older than person $y$ and $y$ is older than person $z$, then $x$ is older than $z$. That is, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$. However, $R$ is not reflexive, because no person is older than himself or herself. That is, $x \not R\, x$ for all people $x$. It follows that $R$ is not a partial ordering. ◀

In different posets different symbols such as $\leq$, $\subseteq$, and $|$, are used for a partial ordering. However, we need a symbol that we can use when we discuss the ordering relation in an arbitrary poset. Customarily, the notation $a \preccurlyeq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset $(S, R)$. This notation is used because the "less than or equal to" relation on the set of real numbers is the most familiar example of a partial ordering and the symbol $\preccurlyeq$ is similar to the $\leq$ symbol. (Note that the symbol $\preccurlyeq$ is used to denote the relation in *any* poset, not just the "less than or equals" relation.) The notation $a \prec b$ denotes that $a \preccurlyeq b$, but $a \neq b$. Also, we say "$a$ is less than $b$" or "$b$ is greater than $a$" if $a \prec b$.

When $a$ and $b$ are elements of the poset $(S, \preccurlyeq)$, it is not necessary that either $a \preccurlyeq b$ or $b \preccurlyeq a$. For instance, in $(P(\mathbf{Z}), \subseteq)$, $\{1, 2\}$ is not related to $\{1, 3\}$, and vice versa, because neither set is contained within the other. Similarly, in $(\mathbf{Z}^+, |)$, 2 is not related to 3 and 3 is not related to 2, because $2 \nmid 3$ and $3 \nmid 2$. This leads to Definition 2.

**DEFINITION 2** The elements $a$ and $b$ of a poset $(S, \preccurlyeq)$ are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When $a$ and $b$ are elements of $S$ such that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, $a$ and $b$ are called *incomparable*.

**EXAMPLE 5** In the poset $(\mathbf{Z}^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

*Solution:* The integers 3 and 9 are comparable, because $3 \mid 9$. The integers 5 and 7 are incomparable, because $5 \nmid 7$ and $7 \nmid 5$. ◀

The adjective "partial" is used to describe partial orderings because pairs of elements may be incomparable. When every two elements in the set are comparable, the relation is called a **total ordering**.

**DEFINITION 3** If $(S, \preccurlyeq)$ is a poset and every two elements of $S$ are comparable, $S$ is called a *totally ordered* or *linearly ordered set*, and $\preccurlyeq$ is called a *total order* or a *linear order*. A totally ordered set is also called a *chain*.

**EXAMPLE 6** The poset $(\mathbf{Z}, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever $a$ and $b$ are integers. ◀

**EXAMPLE 7** The poset $(\mathbf{Z}^+, |)$ is not totally ordered because it contains elements that are incomparable, such as 5 and 7. ◀

In Chapter 6 we noted that $(\mathbf{Z}^+, \leq)$ is well-ordered, where $\leq$ is the usual "less than or equal to" relation. We now define well-ordered sets.

**DEFINITION 4** $(S, \preccurlyeq)$ is a *well-ordered set* if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of $S$ has a least element.

**EXAMPLE 8** The set of ordered pairs of positive integers, $\mathbf{Z}^+ \times \mathbf{Z}^+$, with $(a_1, a_2) \preccurlyeq (b_1, b_2)$ if $a_1 < b_1$, or if $a_1 = b_1$ and $a_2 \leq b_2$ (the lexicographic ordering), is a well-ordered set. The verification of this is left as Exercise 53. The set $\mathbf{Z}$, with the usual $\leq$ ordering, is not well-ordered because the set of negative integers, which is a subset of $\mathbf{Z}$, has no least element. ◀

At the end of Section 5.3 we showed how to use the principle of well-ordered induction (there called generalized induction) to prove results about a well-ordered set. We now state and prove that this proof technique is valid.

**THEOREM 1** **THE PRINCIPLE OF WELL-ORDERED INDUCTION** Suppose that $S$ is a well-ordered set. Then $P(x)$ is true for all $x \in S$, if

*INDUCTIVE STEP:* For every $y \in S$, if $P(x)$ is true for all $x \in S$ with $x \prec y$, then $P(y)$ is true.

***Proof:*** Suppose it is not the case that $P(x)$ is true for all $x \in S$. Then there is an element $y \in S$ such that $P(y)$ is false. Consequently, the set $A = \{x \in S \mid P(x) \text{ is false}\}$ is nonempty. Because $S$ is well ordered, $A$ has a least element $a$. By the choice of $a$ as a least element of $A$, we know that $P(x)$ is true for all $x \in S$ with $x \prec a$. This implies by the inductive step $P(a)$ is true. This contradiction shows that $P(x)$ must be true for all $x \in S$. ◁

***Remark:*** We do not need a basis step in a proof using the principle of well-ordered induction because if $x_0$ is the least element of a well ordered set, the inductive step tells us that $P(x_0)$ is true. This follows because there are no elements $x \in S$ with $x \prec x_0$, so we know (using a vacuous proof) that $P(x)$ is true for all $x \in S$ with $x \prec x_0$.

The principle of well-ordered induction is a versatile technique for proving results about well-ordered sets. Even when it is possible to use mathematical induction for the set of positive integers to prove a theorem, it may be simpler to use the principle of well-ordered induction, as we saw in Examples 5 and 6 in Section 6.2, where we proved a result about the well-ordered set $(\mathbf{N} \times \mathbf{N}, \preccurlyeq)$ where $\preccurlyeq$ is lexicographic ordering on $\mathbf{N} \times \mathbf{N}$.

## Lexicographic Order

The words in a dictionary are listed in alphabetic, or lexicographic, order, which is based on the ordering of the letters in the alphabet. This is a special case of an ordering of strings on a set

constructed from a partial ordering on the set. We will show how this construction works in any poset.

First, we will show how to construct a partial ordering on the Cartesian product of two posets, $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$. The **lexicographic ordering** $\preccurlyeq$ on $A_1 \times A_2$ is defined by specifying that one pair is less than a second pair if the first entry of the first pair is less than (in $A_1$) the first entry of the second pair, or if the first entries are equal, but the second entry of this pair is less than (in $A_2$) the second entry of the second pair. In other words, $(a_1, a_2)$ is less than $(b_1, b_2)$, that is,

$$(a_1, a_2) \prec (b_1, b_2),$$

either if $a_1 \prec_1 b_1$ or if both $a_1 = b_1$ and $a_2 \prec_2 b_2$.

We obtain a partial ordering $\preccurlyeq$ by adding equality to the ordering $\prec$ on $A_1 \times A_2$. The verification of this is left as an exercise.

**EXAMPLE 9** Determine whether $(3, 5) \prec (4, 8)$, whether $(3, 8) \prec (4, 5)$, and whether $(4, 9) \prec (4, 11)$ in the poset $(\mathbf{Z} \times \mathbf{Z}, \preccurlyeq)$, where $\preccurlyeq$ is the lexicographic ordering constructed from the usual $\leq$ relation on $\mathbf{Z}$.

*Solution:* Because $3 < 4$, it follows that $(3, 5) \prec (4, 8)$ and that $(3, 8) \prec (4, 5)$. We have $(4, 9) \prec (4, 11)$, because the first entries of $(4, 9)$ and $(4, 11)$ are the same but $9 < 11$. ◀

In Figure 1 the ordered pairs in $\mathbf{Z}^+ \times \mathbf{Z}^+$ that are less than $(3, 4)$ are highlighted. A lexicographic ordering can be defined on the Cartesian product of $n$ posets $(A_1, \preccurlyeq_1)$, $(A_2, \preccurlyeq_2), \ldots, (A_n, \preccurlyeq_n)$. Define the partial ordering $\preccurlyeq$ on $A_1 \times A_2 \times \cdots \times A_n$ by

$$(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n)$$

if $a_1 \prec_1 b_1$, or if there is an integer $i > 0$ such that $a_1 = b_1, \ldots, a_i = b_i$, and $a_{i+1} \prec_{i+1} b_{i+1}$. In other words, one $n$-tuple is less than a second $n$-tuple if the entry of the first $n$-tuple in the first position where the two $n$-tuples disagree is less than the entry in that position in the second $n$-tuple.

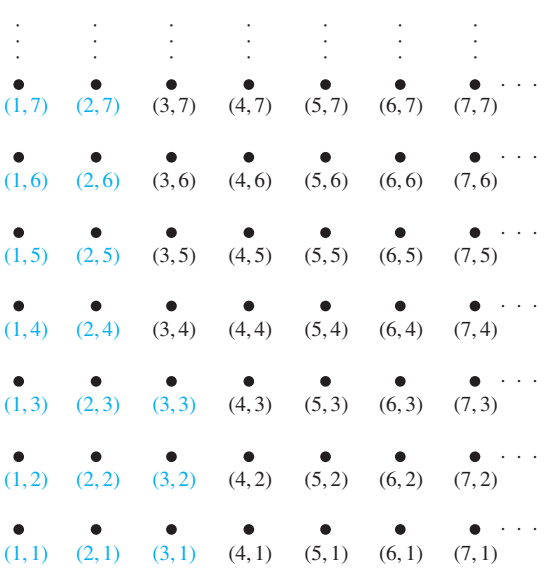



**FIGURE 1** **The Ordered Pairs Less Than (3, 4) in Lexicographic Order.**

**EXAMPLE 10** Note that $(1, 2, 3, 5) \prec (1, 2, 4, 3)$, because the entries in the first two positions of these 4-tuples agree, but in the third position the entry in the first 4-tuple, 3, is less than that in the second 4-tuple, 4. (Here the ordering on 4-tuples is the lexicographic ordering that comes from the usual "less than or equals" relation on the set of integers.) ◀

We can now define lexicographic ordering of strings. Consider the strings $a_1a_2 \dots a_m$ and $b_1b_2 \dots b_n$ on a partially ordered set $S$. Suppose these strings are not equal. Let $t$ be the minimum of $m$ and $n$. The definition of lexicographic ordering is that the string $a_1a_2 \dots a_m$ is less than $b_1b_2 \dots b_n$ if and only if

$$(a_1, a_2, \dots, a_t) \prec (b_1, b_2, \dots, b_t), \text{ or}$$
$$(a_1, a_2, \dots, a_t) = (b_1, b_2, \dots, b_t) \text{ and } m < n,$$

where $\prec$ in this inequality represents the lexicographic ordering of $S^t$. In other words, to determine the ordering of two different strings, the longer string is truncated to the length of the shorter string, namely, to $t = \min(m, n)$ terms. Then the $t$-tuples made up of the first $t$ terms of each string are compared using the lexicographic ordering on $S^t$. One string is less than another string if the $t$-tuple corresponding to the first string is less than the $t$-tuple of the second string, or if these two $t$-tuples are the same, but the second string is longer. The verification that this is a partial ordering is left as Exercise 38 for the reader.

**EXAMPLE 11** Consider the set of strings of lowercase English letters. Using the ordering of letters in the alphabet, a lexicographic ordering on the set of strings can be constructed. A string is less than a second string if the letter in the first string in the first position where the strings differ comes before the letter in the second string in this position, or if the first string and the second string agree in all positions, but the second string has more letters. This ordering is the same as that used in dictionaries. For example,

$$discreet \prec discrete,$$

because these strings differ first in the seventh position, and $e \prec t$. Also,

$$discreet \prec discreetness,$$

because the first eight letters agree, but the second string is longer. Furthermore,

$$discrete \prec discretion,$$

because

$$discrete \prec discreti.$$

◀

## Hasse Diagrams

Many edges in the directed graph for a finite poset do not have to be shown because they must be present. For instance, consider the directed graph for the partial ordering $\{(a, b) \mid a \leq b\}$ on the set $\{1, 2, 3, 4\}$, shown in Figure 2(a). Because this relation is a partial ordering, it is reflexive, and its directed graph has loops at all vertices. Consequently, we do not have to show these loops because they must be present; in Figure 2(b) loops are not shown. Because a partial ordering is transitive, we do not have to show those edges that must be present because of transitivity. For example, in Figure 2(c) the edges $(1, 3)$, $(1, 4)$, and $(2, 4)$ are not shown because they must be present. If we assume that all edges are pointed "upward" (as they are drawn in the figure), we do not have to show the directions of the edges; Figure 2(c) does not show directions.

In general, we can represent a finite poset $(S, \preccurlyeq)$ using this procedure: Start with the directed graph for this relation. Because a partial ordering is reflexive, a loop $(a, a)$ is present at every vertex $a$. Remove these loops. Next, remove all edges that must be in the partial ordering because of the presence of other edges and transitivity. That is, remove all edges $(x, y)$ for which there is an element $z \in S$ such that $x \prec z$ and $z \prec x$. Finally, arrange each edge so that

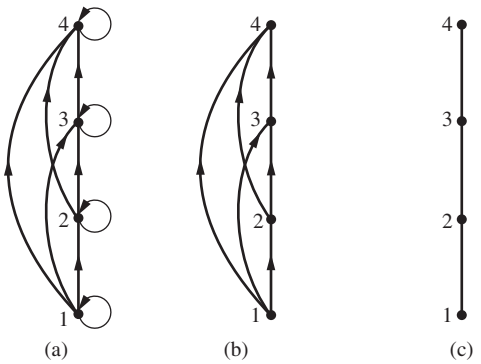



**FIGURE 2** **Constructing the Hasse Diagram for ({1, 2, 3, 4}, ≤).**

its initial vertex is below its terminal vertex (as it is drawn on paper). Remove all the arrows on the directed edges, because all edges point "upward" toward their terminal vertex.

These steps are well defined, and only a finite number of steps need to be carried out for a finite poset. When all the steps have been taken, the resulting diagram contains sufficient information to find the partial ordering, as we will explain later. The resulting diagram is called the **Hasse diagram** of $(S, \preccurlyeq)$, named after the twentieth-century German mathematician Helmut Hasse who made extensive use of them.

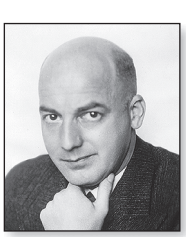
Let $(S, \preccurlyeq)$ be a poset. We say that an element $y \in S$ **covers** an element $x \in S$ if $x \prec y$ and there is no element $z \in S$ such that $x \prec z \prec y$. The set of pairs $(x, y)$ such that $y$ covers $x$ is called the **covering relation** of $(S, \preccurlyeq)$. From the description of the Hasse diagram of a poset, we see that the edges in the Hasse diagram of $(S, \preccurlyeq)$ are upwardly pointing edges corresponding to the pairs in the covering relation of $(S, \preccurlyeq)$. Furthermore, we can recover a poset from its covering relation, because it is the reflexive transitive closure of its covering relation. (Exercise 31 asks for a proof of this fact.) This tells us that we can construct a partial ordering from its Hasse diagram.

**EXAMPLE 12** Draw the Hasse diagram representing the partial ordering $\{(a, b) | a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

*Solution:* Begin with the digraph for this partial order, as shown in Figure 3(a). Remove all loops, as shown in Figure 3(b). Then delete all the edges implied by the transitive property. These are $(1, 4)$, $(1, 6)$, $(1, 8)$, $(1, 12)$, $(2, 8)$, $(2, 12)$, and $(3, 12)$. Arrange all edges to point upward, and delete all arrows to obtain the Hasse diagram. The resulting Hasse diagram is shown in Figure 3(c). ◀

**EXAMPLE 13** Draw the Hasse diagram for the partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set $P(S)$ where $S = \{a, b, c\}$.

Links



HELMUT HASSE (1898–1979) Helmut Hasse was born in Kassel, Germany. He served in the German navy after high school. He began his university studies at Göttingen University in 1918, moving in 1920 to Marburg University to study under the number theorist Kurt Hensel. During this time, Hasse made fundamental contributions to algebraic number theory. He became Hensel's successor at Marburg, later becoming director of the famous mathematical institute at Göttingen in 1934, and took a position at Hamburg University in 1950. Hasse served for 50 years as an editor of *Crelle's Journal*, a famous German mathematics periodical, taking over the job of chief editor in 1936 when the Nazis forced Hensel to resign. During World War II Hasse worked on applied mathematics research for the German navy. He was noted for the clarity and personal style of his lectures and was devoted both to number theory and to his students. (Hasse has been controversial for connections with the Nazi party. Investigations have shown he was a strong German nationalist but not an ardent Nazi.)

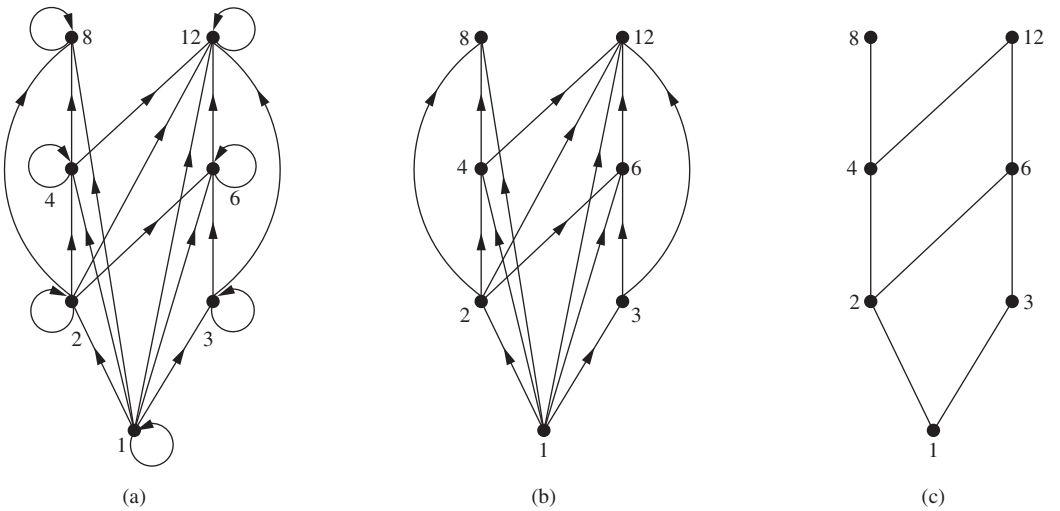



**FIGURE 3** **Constructing the Hasse Diagram of ({1, 2, 3, 4, 6, 8, 12}, |).**

*Solution:* The Hasse diagram for this partial ordering is obtained from the associated digraph by deleting all the loops and all the edges that occur from transitivity, namely, $(\emptyset, \{a, b\})$, $(\emptyset, \{a, c\})$, $(\emptyset, \{b, c\})$, $(\emptyset, \{a, b, c\})$, $(\{a\}, \{a, b, c\})$, $(\{b\}, \{a, b, c\})$, and $(\{c\}, \{a, b, c\})$. Finally all edges point upward, and arrows are deleted. The resulting Hasse diagram is illustrated in Figure 4. ◀

## Maximal and Minimal Elements

Elements of posets that have certain extremal properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset. That is, $a$ is **maximal** in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \prec b$. Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is, $a$ is **minimal** if there is no element $b \in S$ such that $b \prec a$. Maximal and minimal elements are easy to spot using a Hasse diagram. They are the "top" and "bottom" elements in the diagram.

**EXAMPLE 14** Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ are maximal, and which are minimal?

*Solution:* The Hasse diagram in Figure 5 for this poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5. As this example shows, a poset can have more than one maximal element and more than one minimal element. ◀

Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element. That is, $a$ is the **greatest element** of the poset $(S, \preccurlyeq)$

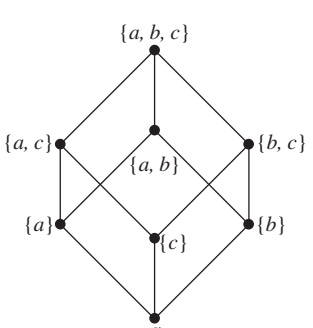



**FIGURE 4** **The Hasse Diagram of $(P(\{a, b, c\}), \subseteq)$.**

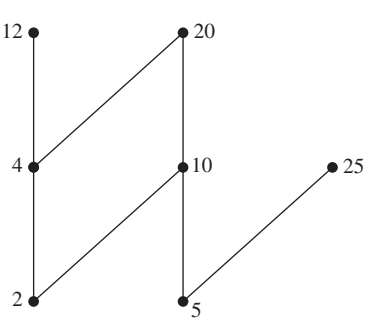



**FIGURE 5** **The Hasse Diagram of a Poset.**

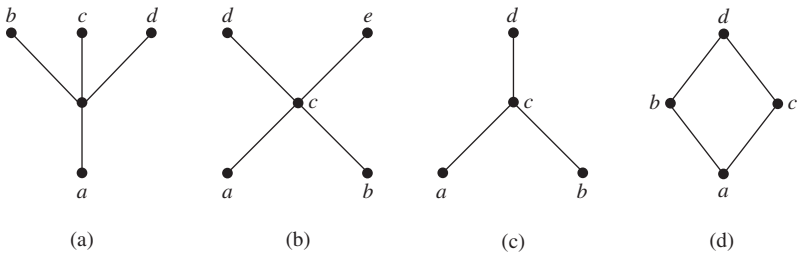



**FIGURE 6** **Hasse Diagrams of Four Posets.**

if $b \preccurlyeq a$ for all $b \in S$. The greatest element is unique when it exists [see Exercise 40(a)]. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is, $a$ is the **least element** of $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$. The least element is unique when it exists [see Exercise 40(b)].

**EXAMPLE 15** Determine whether the posets represented by each of the Hasse diagrams in Figure 6 have a greatest element and a least element.

*Solution:* The least element of the poset with Hasse diagram (a) is $a$. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least nor a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is $d$. The poset with Hasse diagram (d) has least element $a$ and greatest element $d$. ◀

**EXAMPLE 16** Let $S$ be a set. Determine whether there is a greatest element and a least element in the poset $(P(S), \subseteq)$.

*Solution:* The least element is the empty set, because $\emptyset \subseteq T$ for any subset $T$ of $S$. The set $S$ is the greatest element in this poset, because $T \subseteq S$ whenever $T$ is a subset of $S$. ◀

**EXAMPLE 17** Is there a greatest element and a least element in the poset $(\mathbf{Z}^+, |)$?

*Solution:* The integer 1 is the least element because $1|n$ whenever $n$ is a positive integer. Because there is no integer that is divisible by all positive integers, there is no greatest element. ◀

Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset $A$ of a poset $(S, \preccurlyeq)$. If $u$ is an element of $S$ such that $a \preccurlyeq u$ for all elements $a \in A$, then $u$ is called an **upper bound** of $A$. Likewise, there may be an element less than or equal to all the elements in $A$. If $l$ is an element of $S$ such that $l \preccurlyeq a$ for all elements $a \in A$, then $l$ is called a **lower bound** of $A$.

**EXAMPLE 18** Find the lower and upper bounds of the subsets $\{a, b, c\}$, $\{j, h\}$, and $\{a, c, d, f\}$ in the poset with the Hasse diagram shown in Figure 7.

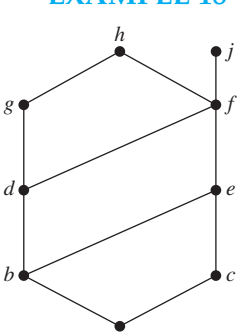



**FIGURE 7** **The Hasse Diagram of a Poset.**

*Solution:* The upper bounds of $\{a, b, c\}$ are $e$, $f$, $j$, and $h$, and its only lower bound is $a$. There are no upper bounds of $\{j, h\}$, and its lower bounds are $a, b, c, d, e$, and $f$. The upper bounds of $\{a, c, d, f\}$ are $f, h$, and $j$, and its lower bound is $a$. ◀

The element $x$ is called the **least upper bound** of the subset $A$ if $x$ is an upper bound that is less than every other upper bound of $A$. Because there is only one such element, if it exists, it makes sense to call this element *the* least upper bound [see Exercise 42(a)]. That is, $x$ is the least upper bound of $A$ if $a \preccurlyeq x$ whenever $a \in A$, and $x \preccurlyeq z$ whenever $z$ is an upper bound of $A$. Similarly, the element $y$ is called the **greatest lower bound** of $A$ if $y$ is a lower bound of $A$ and $z \preccurlyeq y$ whenever $z$ is a lower bound of $A$. The greatest lower bound of $A$ is unique if it exists [see Exercise 42(b)]. The greatest lower bound and least upper bound of a subset $A$ are denoted by $\text{glb}(A)$ and $\text{lub}(A)$, respectively.

**EXAMPLE 19** Find the greatest lower bound and the least upper bound of $\{b, d, g\}$, if they exist, in the poset shown in Figure 7.

*Solution:* The upper bounds of $\{b, d, g\}$ are $g$ and $h$. Because $g \prec h$, $g$ is the least upper bound. The lower bounds of $\{b, d, g\}$ are $a$ and $b$. Because $a \prec b$, $b$ is the greatest lower bound. ◀

**EXAMPLE 20** Find the greatest lower bound and the least upper bound of the sets $\{3, 9, 12\}$ and $\{1, 2, 4, 5, 10\}$, if they exist, in the poset $(\mathbf{Z}^+, |)$.

Extra Examples

*Solution:* An integer is a lower bound of $\{3, 9, 12\}$ if 3, 9, and 12 are divisible by this integer. The only such integers are 1 and 3. Because $1 \mid 3$, 3 is the greatest lower bound of $\{3, 9, 12\}$. The only lower bound for the set $\{1, 2, 4, 5, 10\}$ with respect to $|$ is the element 1. Hence, 1 is the greatest lower bound for $\{1, 2, 4, 5, 10\}$.

An integer is an upper bound for $\{3, 9, 12\}$ if and only if it is divisible by 3, 9, and 12. The integers with this property are those divisible by the least common multiple of 3, 9, and 12, which is 36. Hence, 36 is the least upper bound of $\{3, 9, 12\}$. A positive integer is an upper bound for the set $\{1, 2, 4, 5, 10\}$ if and only if it is divisible by 1, 2, 4, 5, and 10. The integers with this property are those integers divisible by the least common multiple of these integers, which is 20. Hence, 20 is the least upper bound of $\{1, 2, 4, 5, 10\}$. ◀

## Lattices

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**. Lattices have many special properties. Furthermore, lattices are used in many different applications such as models of information flow and play an important role in Boolean algebra.

**EXAMPLE 21** Determine whether the posets represented by each of the Hasse diagrams in Figure 8 are lattices.

*Solution:* The posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound, as the reader should verify. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements $b$ and $c$ have no least upper bound. To see this, note that each of the elements $d$, $e$, and $f$ is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset. ◀

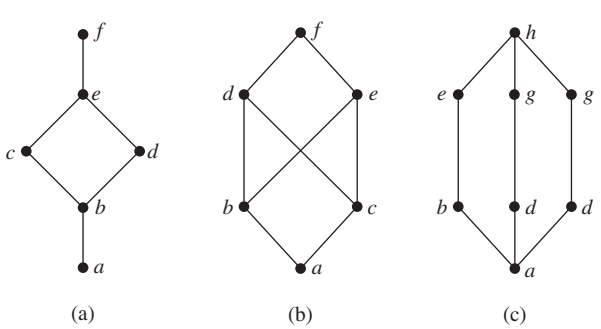



**FIGURE 8** **Hasse Diagrams of Three Posets.**

**EXAMPLE 22** Is the poset $(\mathbf{Z}^+, |)$ a lattice?

*Solution:* Let $a$ and $b$ be two positive integers. The least upper bound and greatest lower bound of these two integers are the least common multiple and the greatest common divisor of these integers, respectively, as the reader should verify. It follows that this poset is a lattice. ◀

**EXAMPLE 23** Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices.

*Solution:* Because 2 and 3 have no upper bounds in $(\{1, 2, 3, 4, 5\}, |)$, they certainly do not have a least upper bound. Hence, the first poset is not a lattice.

Every two elements of the second poset have both a least upper bound and a greatest lower bound. The least upper bound of two elements in this poset is the larger of the elements and the greatest lower bound of two elements is the smaller of the elements, as the reader should verify. Hence, this second poset is a lattice. ◀

**EXAMPLE 24** Determine whether $(P(S), \subseteq)$ is a lattice where $S$ is a set.

*Solution:* Let $A$ and $B$ be two subsets of $S$. The least upper bound and the greatest lower bound of $A$ and $B$ are $A \cup B$ and $A \cap B$, respectively, as the reader can show. Hence, $(P(S), \subseteq)$ is a lattice. ◀

**EXAMPLE 25** **The Lattice Model of Information Flow** In many settings the flow of information from one person or computer program to another is restricted via security clearances. We can use a lattice model to represent different information flow policies. For example, one common information flow policy is the *multilevel security policy* used in government and military systems. Each piece of information is assigned to a security class, and each security class is represented by a pair $(A, C)$ where $A$ is an *authority level* and $C$ is a *category*. People and computer programs are then allowed access to information from a specific restricted set of security classes.


There are billions of pages of classified U.S. government documents.

The typical authority levels used in the U.S. government are unclassified (0), confidential (1), secret (2), and top secret (3). (Information is said to be classified if it is confidential, secret, or top secret.) Categories used in security classes are the subsets of a set of all *compartments* relevant to a particular area of interest. Each compartment represents a particular subject area. For example, if the set of compartments is {*spies, moles, double agents*}, then there are eight different categories, one for each of the eight subsets of the set of compartments, such as {*spies, moles*}.

We can order security classes by specifying that $(A_1, C_1) \preccurlyeq (A_2, C_2)$ if and only if $A_1 \leq A_2$ and $C_1 \subseteq C_2$. Information is permitted to flow from security class $(A_1, C_1)$ into security class $(A_2, C_2)$ if and only if $(A_1, C_1) \preccurlyeq (A_2, C_2)$. For example, information is permitted to flow from the security class (*secret,* {*spies, moles*}) into the security class (*top secret,* {*spies, moles, double agents*}), whereas information is not allowed to flow from the security class (*top secret,* {*spies, moles*}) into either of the security classes (*secret,* {*spies, moles, double agents*}) or (*top secret,* {*spies*}).

We leave it to the reader (see Exercise 48) to show that the set of all security classes with the ordering defined in this example forms a lattice. ◀

## Topological Sorting

Suppose that a project is made up of 20 different tasks. Some tasks can be completed only after others have been finished. How can an order be found for these tasks? To model this problem we set up a partial order on the set of tasks so that $a \prec b$ if and only if $a$ and $b$ are tasks where $b$


cannot be started until $a$ has been completed. To produce a schedule for the project, we need to produce an order for all 20 tasks that is compatible with this partial order. We will show how this can be done.

We begin with a definition. A total ordering $\preccurlyeq$ is said to be **compatible** with the partial ordering $R$ if $a \preccurlyeq b$ whenever $aRb$. Constructing a compatible total ordering from a partial ordering is called **topological sorting**.* We will need to use Lemma 1.

**LEMMA 1** Every finite nonempty poset $(S, \preccurlyeq)$ has at least one minimal element.

***Proof:*** Choose an element $a_0$ of $S$. If $a_0$ is not minimal, then there is an element $a_1$ with $a_1 \prec a_0$. If $a_1$ is not minimal, there is an element $a_2$ with $a_2 \prec a_1$. Continue this process, so that if $a_n$ is not minimal, there is an element $a_{n+1}$ with $a_{n+1} \prec a_n$. Because there are only a finite number of elements in the poset, this process must end with a minimal element $a_n$. ◁

The topological sorting algorithm we will describe works for any finite nonempty poset. To define a total ordering on the poset $(A, \preccurlyeq)$, first choose a minimal element $a_1$; such an element exists by Lemma 1. Next, note that $(A - \{a_1\}, \preccurlyeq)$ is also a poset, as the reader should verify. (Here by $\preccurlyeq$ we mean the restriction of the original relation $\preccurlyeq$ on $A$ to $A - \{a_1\}$.) If it is nonempty, choose a minimal element $a_2$ of this poset. Then remove $a_2$ as well, and if there are additional elements left, choose a minimal element $a_3$ in $A - \{a_1, a_2\}$. Continue this process by choosing $a_{k+1}$ to be a minimal element in $A - \{a_1, a_2, \ldots, a_k\}$, as long as elements remain.

Because $A$ is a finite set, this process must terminate. The end product is a sequence of elements $a_1, a_2, \ldots, a_n$. The desired total ordering $\preccurlyeq_t$ is defined by

$$a_1 \prec_t a_2 \prec_t \cdots \prec_t a_n.$$

This total ordering is compatible with the original partial ordering. To see this, note that if $b \prec c$ in the original partial ordering, $c$ is chosen as the minimal element at a phase of the algorithm where $b$ has already been removed, for otherwise $c$ would not be a minimal element. Pseudocode for this topological sorting algorithm is shown in Algorithm 1.

**ALGORITHM 1 Topological Sorting.**

**procedure** *topological sort* ($(S, \preccurlyeq)$: finite poset)
$k := 1$
**while** $S \neq \emptyset$
    $a_k :=$ a minimal element of $S$ {such an element exists by Lemma 1}
    $S := S - \{a_k\}$
    $k := k + 1$
**return** $a_1, a_2, \ldots, a_n$ {$a_1, a_2, \ldots, a_n$ is a compatible total ordering of $S$}

**EXAMPLE 26** Find a compatible total ordering for the poset $(\{1, 2, 4, 5, 12, 20\}, |)$.

*"Topological sorting" is terminology used by computer scientists; mathematicians use the terminology "linearization of a partial ordering" for the same thing. In mathematics, topology is the branch of geometry dealing with properties of geometric figures that hold for all figures that can be transformed into one another by continuous bijections. In computer science, a topology is any arrangement of objects that can be connected with edges.

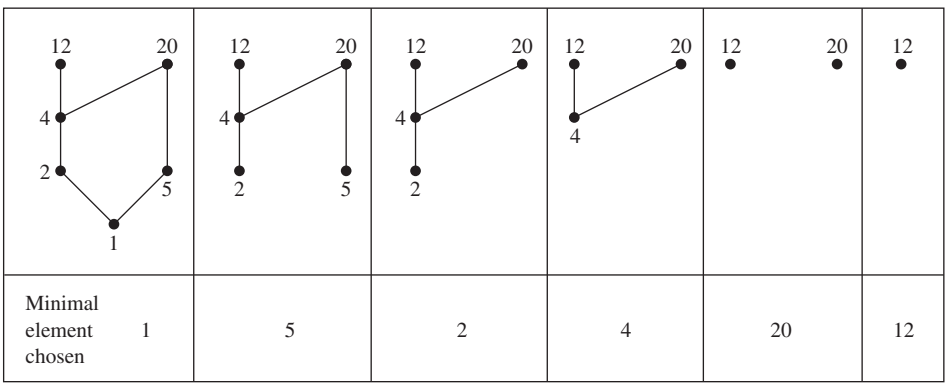



**FIGURE 9** **A Topological Sort of ({1, 2, 4, 5, 12, 20}, |).**

*Solution:* The first step is to choose a minimal element. This must be 1, because it is the only minimal element. Next, select a minimal element of ({2, 4, 5, 12, 20}, |). There are two minimal elements in this poset, namely, 2 and 5. We select 5. The remaining elements are {2, 4, 12, 20}. The only minimal element at this stage is 2. Next, 4 is chosen because it is the only minimal element of ({4, 12, 20}, |). Because both 12 and 20 are minimal elements of ({12, 20}, |), either can be chosen next. We select 20, which leaves 12 as the last element left. This produces the total ordering

$$1 \prec 5 \prec 2 \prec 4 \prec 20 \prec 12.$$

The steps used by this sorting algorithm are displayed in Figure 9. ◀

Topological sorting has an application to the scheduling of projects.

**EXAMPLE 27** A development project at a computer company requires the completion of seven tasks. Some of these tasks can be started only after other tasks are finished. A partial ordering on tasks is set up by considering task $X \prec$ task $Y$ if task $Y$ cannot be started until task $X$ has been completed. The Hasse diagram for the seven tasks, with respect to this partial ordering, is shown in Figure 10. Find an order in which these tasks can be carried out to complete the project.

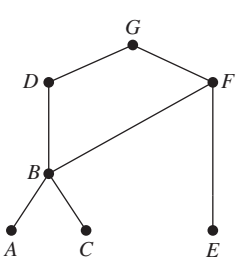



**FIGURE 10** **The Hasse Diagram for Seven Tasks.**

*Solution:* An ordering of the seven tasks can be obtained by performing a topological sort. The steps of a sort are illustrated in Figure 11. The result of this sort, $A \prec C \prec B \prec E \prec F \prec D \prec G$, gives one possible order for the tasks. ◀

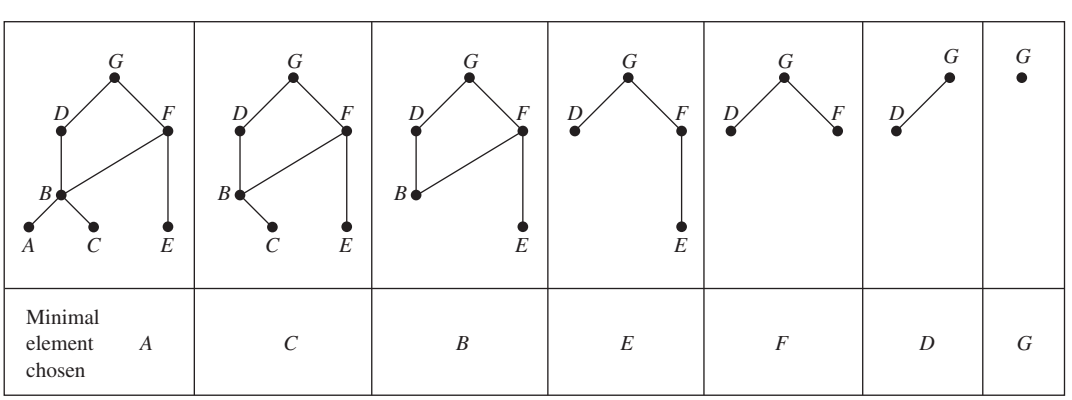



**FIGURE 11** **A Topological Sort of the Tasks.**

## Exercises

**1.** Which of these relations on $\{0, 1, 2, 3\}$ are partial orderings? Determine the properties of a partial ordering that the others lack.

**a)** $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$

**b)** $\{(0, 0), (1, 1), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)\}$

**c)** $\{(0, 0), (1, 1), (1, 2), (2, 2), (3, 3)\}$

**d)** $\{(0, 0), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$

**e)** $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)\}$

**2.** Which of these relations on $\{0, 1, 2, 3\}$ are partial orderings? Determine the properties of a partial ordering that the others lack.

**a)** $\{(0, 0), (2, 2), (3, 3)\}$

**b)** $\{(0, 0), (1, 1), (2, 0), (2, 2), (2, 3), (3, 3)\}$

**c)** $\{(0, 0), (1, 1), (1, 2), (2, 2), (3, 1), (3, 3)\}$

**d)** $\{(0, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 2), (2, 3), (3, 0), (3, 3)\}$

**e)** $\{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 2), (3, 3)\}$

**3.** Is $(S, R)$ a poset if $S$ is the set of all people in the world and $(a, b) \in R$, where $a$ and $b$ are people, if

**a)** $a$ is taller than $b$?

**b)** $a$ is not taller than $b$?

**c)** $a = b$ or $a$ is an ancestor of $b$?

**d)** $a$ and $b$ have a common friend?

**4.** Is $(S, R)$ a poset if $S$ is the set of all people in the world and $(a, b) \in R$, where $a$ and $b$ are people, if

**a)** $a$ is no shorter than $b$?

**b)** $a$ weighs more than $b$?

**c)** $a = b$ or $a$ is a descendant of $b$?

**d)** $a$ and $b$ do not have a common friend?

**5.** Which of these are posets?

**a)** $(\mathbf{Z}, =)$ **b)** $(\mathbf{Z}, \neq)$ **c)** $(\mathbf{Z}, \geq)$ **d)** $(\mathbf{Z}, \not|)$

**6.** Which of these are posets?

**a)** $(\mathbf{R}, =)$ **b)** $(\mathbf{R}, <)$ **c)** $(\mathbf{R}, \leq)$ **d)** $(\mathbf{R}, \neq)$

**7.** Determine whether the relations represented by these zero–one matrices are partial orders.

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

**c)** $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

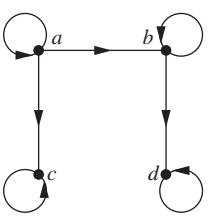
**8.** Determine whether the relations represented by these zero–one matrices are partial orders.

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

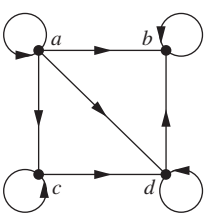
**c)** $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

In Exercises 9–11 determine whether the relation with the directed graph shown is a partial order.

**9.**




**10.**




**11.**


**12.** Let $(S, R)$ be a poset. Show that $(S, R^{-1})$ is also a poset, where $R^{-1}$ is the inverse of $R$. The poset $(S, R^{-1})$ is called the **dual** of $(S, R)$.

**13.** Find the duals of these posets.

**a)** $(\{0, 1, 2\}, \leq)$ **b)** $(\mathbf{Z}, \geq)$

**c)** $(P(\mathbf{Z}), \supseteq)$ **d)** $(\mathbf{Z}^+, |)$

**14.** Which of these pairs of elements are comparable in the poset $(\mathbf{Z}^+, |)$?

**a)** 5, 15 **b)** 6, 9 **c)** 8, 16 **d)** 7, 7

**15.** Find two incomparable elements in these posets.

**a)** $(P(\{0, 1, 2\}), \subseteq)$ **b)** $(\{1, 2, 4, 6, 8\}, |)$

**16.** Let $S = \{1, 2, 3, 4\}$. With respect to the lexicographic order based on the usual "less than" relation,

**a)** find all pairs in $S \times S$ less than $(2, 3)$.

**b)** find all pairs in $S \times S$ greater than $(3, 1)$.

**c)** draw the Hasse diagram of the poset $(S \times S, \preccurlyeq)$.

**17.** Find the lexicographic ordering of these $n$-tuples:

**a)** $(1, 1, 2), (1, 2, 1)$ **b)** $(0, 1, 2, 3), (0, 1, 3, 2)$

**c)** $(1, 0, 1, 0, 1), (0, 1, 1, 1, 0)$

**18.** Find the lexicographic ordering of these strings of lowercase English letters:

**a)** *quack, quick, quicksilver, quicksand, quacking*

**b)** *open, opener, opera, operand, opened*

**c)** *zoo, zero, zoom, zoology, zoological*

**19.** Find the lexicographic ordering of the bit strings 0, 01, 11, 001, 010, 011, 0001, and 0101 based on the ordering $0 < 1$.

**20.** Draw the Hasse diagram for the "greater than or equal to" relation on $\{0, 1, 2, 3, 4, 5\}$.

**21.** Draw the Hasse diagram for the "less than or equal to" relation on $\{0, 2, 5, 10, 11, 15\}$.

**22.** Draw the Hasse diagram for divisibility on the set

**a)** $\{1, 2, 3, 4, 5, 6\}$. **b)** $\{3, 5, 7, 11, 13, 16, 17\}$.

**c)** $\{2, 3, 5, 10, 11, 15, 25\}$. **d)** $\{1, 3, 9, 27, 81, 243\}$.

**23.** Draw the Hasse diagram for divisibility on the set

**a)** $\{1, 2, 3, 4, 5, 6, 7, 8\}$. **b)** $\{1, 2, 3, 5, 7, 11, 13\}$.

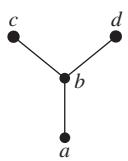
**c)** $\{1, 2, 3, 6, 12, 24, 36, 48\}$.

**d)** $\{1, 2, 4, 8, 16, 32, 64\}$.

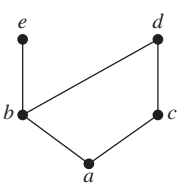
**24.** Draw the Hasse diagram for inclusion on the set $P(S)$, where $S = \{a, b, c, d\}$.

In Exercises 25–27 list all ordered pairs in the partial ordering with the accompanying Hasse diagram.

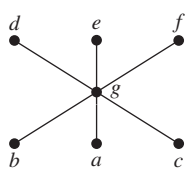
**25.**




**26.**




**27.**



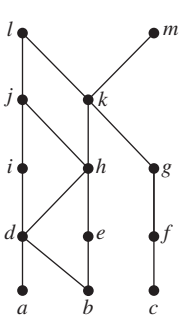

**28.** What is the covering relation of the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 12\}$?

**29.** What is the covering relation of the partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set of $S$, where $S = \{a, b, c\}$?

**30.** What is the covering relation of the partial ordering for the poset of security classes defined in Example 25?

**31.** Show that a finite poset can be reconstructed from its covering relation. [*Hint:* Show that the poset is the reflexive transitive closure of its covering relation.]

**32.** Answer these questions for the partial order represented by this Hasse diagram.




**a)** Find the maximal elements.

**b)** Find the minimal elements.

**c)** Is there a greatest element?

**d)** Is there a least element?

**e)** Find all upper bounds of $\{a, b, c\}$.

**f)** Find the least upper bound of $\{a, b, c\}$, if it exists.

**g)** Find all lower bounds of $\{f, g, h\}$.

**h)** Find the greatest lower bound of $\{f, g, h\}$, if it exists.

**33.** Answer these questions for the poset $(\{3, 5, 9, 15, 24, 45\}, |)$.

**a)** Find the maximal elements.

**b)** Find the minimal elements.

**c)** Is there a greatest element?

**d)** Is there a least element?

**e)** Find all upper bounds of $\{3, 5\}$.

**f)** Find the least upper bound of $\{3, 5\}$, if it exists.

**g)** Find all lower bounds of $\{15, 45\}$.

**h)** Find the greatest lower bound of $\{15, 45\}$, if it exists.

**34.** Answer these questions for the poset $(\{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}, |)$.

**a)** Find the maximal elements.

**b)** Find the minimal elements.

**c)** Is there a greatest element?

**d)** Is there a least element?

**e)** Find all upper bounds of $\{2, 9\}$.

**f)** Find the least upper bound of $\{2, 9\}$, if it exists.

**g)** Find all lower bounds of $\{60, 72\}$.

**h)** Find the greatest lower bound of $\{60, 72\}$, if it exists.

**35.** Answer these questions for the poset $(\{\{1\}, \{2\}, \{4\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}, \subseteq)$.

**a)** Find the maximal elements.

**b)** Find the minimal elements.

**c)** Is there a greatest element?

**d)** Is there a least element?

**e)** Find all upper bounds of $\{\{2\}, \{4\}\}$.

**f)** Find the least upper bound of $\{\{2\}, \{4\}\}$, if it exists.

**g)** Find all lower bounds of $\{\{1, 3, 4\}, \{2, 3, 4\}\}$.

**h)** Find the greatest lower bound of $\{\{1, 3, 4\}, \{2, 3, 4\}\}$, if it exists.

**36.** Give a poset that has

**a)** a minimal element but no maximal element.

**b)** a maximal element but no minimal element.

**c)** neither a maximal nor a minimal element.

**37.** Show that lexicographic order is a partial ordering on the Cartesian product of two posets.

**38.** Show that lexicographic order is a partial ordering on the set of strings from a poset.

**39.** Suppose that $(S, \preccurlyeq_1)$ and $(T, \preccurlyeq_2)$ are posets. Show that $(S \times T, \preccurlyeq)$ is a poset where $(s, t) \preccurlyeq (u, v)$ if and only if $s \preccurlyeq_1 u$ and $t \preccurlyeq_2 v$.

**40.** **a)** Show that there is exactly one greatest element of a poset, if such an element exists.

**b)** Show that there is exactly one least element of a poset, if such an element exists.

**41.** **a)** Show that there is exactly one maximal element in a poset with a greatest element.

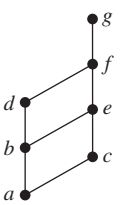
**b)** Show that there is exactly one minimal element in a poset with a least element.

**42.** **a)** Show that the least upper bound of a set in a poset is unique if it exists.

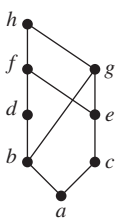
**b)** Show that the greatest lower bound of a set in a poset is unique if it exists.

**43.** Determine whether the posets with these Hasse diagrams are lattices.

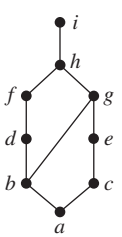
**a)**




**b)**




**c)**




**44.** Determine whether these posets are lattices.

**a)** $(\{1, 3, 6, 9, 12\}, |)$ **b)** $(\{1, 5, 25, 125\}, |)$

**c)** $(\mathbf{Z}, \geq)$

**d)** $(P(S), \supseteq)$, where $P(S)$ is the power set of a set $S$

**45.** Show that every nonempty finite subset of a lattice has a least upper bound and a greatest lower bound.

**46.** Show that if the poset $(S, R)$ is a lattice then the dual poset $(S, R^{-1})$ is also a lattice.

**47.** In a company, the lattice model of information flow is used to control sensitive information with security classes represented by ordered pairs $(A, C)$. Here $A$ is an authority level, which may be nonproprietary (0), proprietary (1), restricted (2), or registered (3). A category $C$ is a subset of the set of all projects {*Cheetah, Impala, Puma*}. (Names of animals are often used as code names for projects in companies.)

**a)** Is information permitted to flow from (*Proprietary*, {*Cheetah, Puma*}) into (*Restricted*, {*Puma*})?

**b)** Is information permitted to flow from (*Restricted*, {*Cheetah*}) into (*Registered*, {*Cheetah, Impala*})?

**c)** Into which classes is information from (*Proprietary*, {*Cheetah*, *Puma*}) permitted to flow?

**d)** From which classes is information permitted to flow into the security class (*Restricted*, {*Impala, Puma*})?

**48.** Show that the set $S$ of security classes $(A, C)$ is a lattice, where $A$ is a positive integer representing an authority class and $C$ is a subset of a finite set of compartments, with $(A_1, C_1) \preccurlyeq (A_2, C_2)$ if and only if $A_1 \leq A_2$ and $C_1 \subseteq C_2$. [*Hint:* First show that $(S, \preccurlyeq)$ is a poset and then show that the least upper bound and greatest lower bound of $(A_1, C_1)$ and $(A_2, C_2)$ are $(\max(A_1, A_2), C_1 \cup C_2)$ and $(\min(A_1, A_2), C_1 \cap C_2)$, respectively.]

***49.** Show that the set of all partitions of a set $S$ with the relation $P_1 \preccurlyeq P_2$ if the partition $P_1$ is a refinement of the partition $P_2$ is a lattice. (See the preamble to Exercise 49 of Section 9.5.)

**50.** Show that every totally ordered set is a lattice.

**51.** Show that every finite lattice has a least element and a greatest element.

**52.** Give an example of an infinite lattice with

**a)** neither a least nor a greatest element.

**b)** a least but not a greatest element.

**c)** a greatest but not a least element.

**d)** both a least and a greatest element.

**53.** Verify that $(\mathbf{Z}^+ \times \mathbf{Z}^+, \preccurlyeq)$ is a well-ordered set, where $\preccurlyeq$ is lexicographic order, as claimed in Example 8.

**54.** Determine whether each of these posets is well-ordered.

**a)** $(S, \leq)$, where $S = \{10, 11, 12, \ldots\}$

**b)** $(\mathbf{Q} \cap [0, 1], \leq)$ (the set of rational numbers between 0 and 1 inclusive)

**c)** $(S, \leq)$, where $S$ is the set of positive rational numbers with denominators not exceeding 3

**d)** $(\mathbf{Z}^-, \geq)$, where $\mathbf{Z}^-$ is the set of negative integers

A poset $(R, \preccurlyeq)$ is **well-founded** if there is no infinite decreasing sequence of elements in the poset, that is, elements $x_1, x_2, \ldots, x_n$ such that $\cdots \prec x_n \prec \cdots \prec x_2 \prec x_1$. A poset $(R, \preccurlyeq)$ is **dense** if for all $x \in S$ and $y \in S$ with $x \prec y$, there is an element $z \in R$ such that $x \prec z \prec y$.

**55.** Show that the poset $(\mathbf{Z}, \preccurlyeq)$, where $x \prec y$ if and only if $|x| < |y|$ is well-founded but is not a totally ordered set.

**56.** Show that a dense poset with at least two elements that are comparable is not well-founded.

**57.** Show that the poset of rational numbers with the usual "less than or equal to" relation, $(\mathbf{Q}, \leq)$, is a dense poset.

***58.** Show that the set of strings of lowercase English letters with lexicographic order is neither well-founded nor dense.

**59.** Show that a poset is well-ordered if and only if it is totally ordered and well-founded.

**60.** Show that a finite nonempty poset has a maximal element.

**61.** Find a compatible total order for the poset with the Hasse diagram shown in Exercise 32.

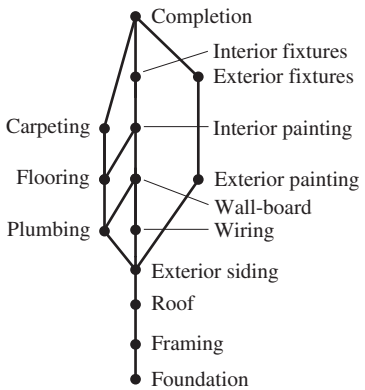
**62.** Find a compatible total order for the divisibility relation on the set {1, 2, 3, 6, 8, 12, 24, 36}.

**63.** Find all compatible total orderings for the poset $(\{1, 2, 4, 5, 12, 20\}, |\}$ from Example 26.

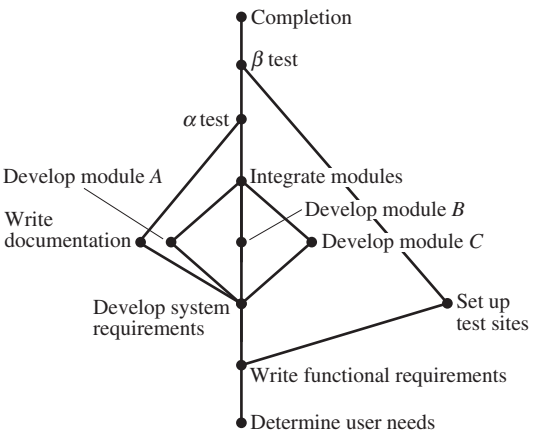
**64.** Find all compatible total orderings for the poset with the Hasse diagram in Exercise 27.

**65.** Find all possible orders for completing the tasks in the development project in Example 27.

**66.** Schedule the tasks needed to build a house, by specifying their order, if the Hasse diagram representing these tasks is as shown in the figure.




**67.** Find an ordering of the tasks of a software project if the Hasse diagram for the tasks of the project is as shown.




## Key Terms and Results

### TERMS

**binary relation from $A$ to $B$:** a subset of $A \times B$

**relation on $A$:** a binary relation from $A$ to itself (i.e., a subset of $A \times A$)

**$S \circ R$:** composite of $R$ and $S$

**$R^{-1}$:** inverse relation of $R$

**$R^n$:** $n$th power of $R$

**reflexive:** a relation $R$ on $A$ is reflexive if $(a, a) \in R$ for all $a \in A$

**symmetric:** a relation $R$ on $A$ is symmetric if $(b, a) \in R$ whenever $(a, b) \in R$

**antisymmetric:** a relation $R$ on $A$ is antisymmetric if $a = b$ whenever $(a, b) \in R$ and $(b, a) \in R$

**transitive:** a relation $R$ on $A$ is transitive if $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$

**$n$-ary relation on $A_1, A_2, \ldots, A_n$:** a subset of $A_1 \times A_2 \times \cdots \times A_n$

**relational data model:** a model for representing databases using $n$-ary relations

**primary key:** a domain of an $n$-ary relation such that an $n$-tuple is uniquely determined by its value for this domain

**composite key:** the Cartesian product of domains of an $n$-ary relation such that an $n$-tuple is uniquely determined by its values in these domains

**selection operator:** a function that selects the $n$-tuples in an $n$-ary relation that satisfy a specified condition

**projection:** a function that produces relations of smaller degree from an $n$-ary relation by deleting fields

**join:** a function that combines $n$-ary relations that agree on certain fields

**directed graph or digraph:** a set of elements called vertices and ordered pairs of these elements, called edges

**loop:** an edge of the form $(a, a)$

**closure of a relation $R$ with respect to a property P:** the relation $S$ (if it exists) that contains $R$, has property **P**, and is contained within any relation that contains $R$ and has property **P**

**path in a digraph:** a sequence of edges $(a, x_1), (x_1, x_2), \ldots, (x_{n-2}, x_{n-1}), (x_{n-1}, b)$ such that the terminal vertex of each edge is the initial vertex of the succeeding edge in the sequence

**circuit (or cycle) in a digraph:** a path that begins and ends at the same vertex

**$R^*$ (connectivity relation):** the relation consisting of those ordered pairs $(a, b)$ such that there is a path from $a$ to $b$

**equivalence relation:** a reflexive, symmetric, and transitive relation

**equivalent:** if $R$ is an equivalence relation, $a$ is equivalent to $b$ if $aRb$

**$[a]_R$ (equivalence class of $a$ with respect to $R$):** the set of all elements of $A$ that are equivalent to $a$

**$[a]_m$ (congruence class modulo $m$):** the set of integers congruent to $a$ modulo $m$

**partition of a set $S$:** a collection of pairwise disjoint nonempty subsets that have $S$ as their union

**partial ordering:** a relation that is reflexive, antisymmetric, and transitive

**poset $(S, R)$:** a set $S$ and a partial ordering $R$ on this set

**comparable:** the elements $a$ and $b$ in the poset $(A, \preccurlyeq)$ are comparable if $a \preccurlyeq b$ or $b \preccurlyeq a$

**incomparable:** elements in a poset that are not comparable

**total (or linear) ordering:** a partial ordering for which every pair of elements are comparable

**totally (or linearly) ordered set:** a poset with a total (or linear) ordering

**well-ordered set:** a poset $(S, \preccurlyeq)$, where $\preccurlyeq$ is a total order and every nonempty subset of $S$ has a least element

**lexicographic order:** a partial ordering of Cartesian products or strings
**Hasse diagram:** a graphical representation of a poset where loops and all edges resulting from the transitive property are not shown, and the direction of the edges is indicated by the position of the vertices
**maximal element:** an element of a poset that is not less than any other element of the poset
**minimal element:** an element of a poset that is not greater than any other element of the poset
**greatest element:** an element of a poset greater than all other elements in this set
**least element:** an element of a poset less than all other elements in this set
**upper bound of a set:** an element in a poset greater than all other elements in the set
**lower bound of a set:** an element in a poset less than all other elements in the set
**least upper bound of a set:** an upper bound of the set that is less than all other upper bounds
**greatest lower bound of a set:** a lower bound of the set that is greater than all other lower bounds
**lattice:** a partially ordered set in which every two elements have a greatest lower bound and a least upper bound
**compatible total ordering for a partial ordering:** a total ordering that contains the given partial ordering
**topological sort:** the construction of a total ordering compatible with a given partial ordering

### RESULTS

The reflexive closure of a relation $R$ on the set $A$ equals $R \cup \Delta$, where $\Delta = \{(a, a) \mid a \in A\}$.
The symmetric closure of a relation $R$ on the set $A$ equals $R \cup R^{-1}$, where $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.
The transitive closure of a relation equals the connectivity relation formed from this relation.
Warshall's algorithm for finding the transitive closure of a relation
Let $R$ be an equivalence relation. Then the following three statements are equivalent: (1) $a\ R\ b$; (2) $[a]_R \cap [b]_R \neq \emptyset$; (3) $[a]_R = [b]_R$.
The equivalence classes of an equivalence relation on a set $A$ form a partition of $A$. Conversely, an equivalence relation can be constructed from any partition so that the equivalence classes are the subsets in the partition.
The principle of well-ordered induction
The topological sorting algorithm

## Review Questions

**1. a)** What is a relation on a set?
**b)** How many relations are there on a set with $n$ elements?

**2. a)** What is a reflexive relation?
**b)** What is a symmetric relation?
**c)** What is an antisymmetric relation?
**d)** What is a transitive relation?

**3.** Give an example of a relation on the set $\{1, 2, 3, 4\}$ that is
**a)** reflexive, symmetric, and not transitive.
**b)** not reflexive, symmetric, and transitive.
**c)** reflexive, antisymmetric, and not transitive.
**d)** reflexive, symmetric, and transitive.
**e)** reflexive, antisymmetric, and transitive.

**4. a)** How many reflexive relations are there on a set with $n$ elements?
**b)** How many symmetric relations are there on a set with $n$ elements?
**c)** How many antisymmetric relations are there on a set with $n$ elements?

**5. a)** Explain how an $n$-ary relation can be used to represent information about students at a university.
**b)** How can the 5-ary relation containing names of students, their addresses, telephone numbers, majors, and grade point averages be used to form a 3-ary relation containing the names of students, their majors, and their grade point averages?
**c)** How can the 4-ary relation containing names of students, their addresses, telephone numbers, and majors and the 4-ary relation containing names of students, their student numbers, majors, and numbers of credit hours be combined into a single $n$-ary relation?

**6. a)** Explain how to use a zero–one matrix to represent a relation on a finite set.
**b)** Explain how to use the zero–one matrix representing a relation to determine whether the relation is reflexive, symmetric, and/or antisymmetric.

**7. a)** Explain how to use a directed graph to represent a relation on a finite set.
**b)** Explain how to use the directed graph representing a relation to determine whether a relation is reflexive, symmetric, and/or antisymmetric.

**8. a)** Define the reflexive closure and the symmetric closure of a relation.
**b)** How can you construct the reflexive closure of a relation?
**c)** How can you construct the symmetric closure of a relation?
**d)** Find the reflexive closure and the symmetric closure of the relation $\{(1, 2), (2, 3), (2, 4), (3, 1)\}$ on the set $\{1, 2, 3, 4\}$.

**9. a)** Define the transitive closure of a relation.
**b)** Can the transitive closure of a relation be obtained by including all pairs $(a, c)$ such that $(a, b)$ and $(b, c)$ belong to the relation?

**c)** Describe two algorithms for finding the transitive closure of a relation.
**d)** Find the transitive closure of the relation $\{(1,1), (1,3), (2,1), (2,3), (2,4), (3,2), (3,4), (4,1)\}$.

**10. a)** Define an equivalence relation.
**b)** Which relations on the set $\{a, b, c, d\}$ are equivalence relations and contain $(a, b)$ and $(b, d)$?

**11. a)** Show that congruence modulo $m$ is an equivalence relation whenever $m$ is a positive integer.
**b)** Show that the relation $\{(a, b) \mid a \equiv \pm b \pmod 7\}$ is an equivalence relation on the set of integers.

**12. a)** What are the equivalence classes of an equivalence relation?
**b)** What are the equivalence classes of the "congruent modulo 5" relation?
**c)** What are the equivalence classes of the equivalence relation in Question 11(b)?

**13.** Explain the relationship between equivalence relations on a set and partitions of this set.

**14. a)** Define a partial ordering.
**b)** Show that the divisibility relation on the set of positive integers is a partial order.

**15.** Explain how partial orderings on the sets $A_1$ and $A_2$ can be used to define a partial ordering on the set $A_1 \times A_2$.

**16. a)** Explain how to construct the Hasse diagram of a partial order on a finite set.
**b)** Draw the Hasse diagram of the divisibility relation on the set $\{2, 3, 5, 9, 12, 15, 18\}$.

**17. a)** Define a maximal element of a poset and the greatest element of a poset.
**b)** Give an example of a poset that has three maximal elements.
**c)** Give an example of a poset with a greatest element.

**18. a)** Define a lattice.
**b)** Give an example of a poset with five elements that is a lattice and an example of a poset with five elements that is not a lattice.

**19. a)** Show that every finite subset of a lattice has a greatest lower bound and a least upper bound.
**b)** Show that every lattice with a finite number of elements has a least element and a greatest element.

**20. a)** Define a well-ordered set.
**b)** Describe an algorithm for producing a totally ordered set compatible with a given partially ordered set.
**c)** Explain how the algorithm from (b) can be used to order the tasks in a project if tasks are done one at a time and each task can be done only after one or more of the other tasks have been completed.

## Supplementary Exercises

**1.** Let $S$ be the set of all strings of English letters. Determine whether these relations are reflexive, irreflexive, symmetric, antisymmetric, and/or transitive.
**a)** $R_1 = \{(a, b) \mid a$ and $b$ have no letters in common$\}$
**b)** $R_2 = \{(a, b) \mid a$ and $b$ are not the same length$\}$
**c)** $R_3 = \{(a, b) \mid a$ is longer than $b\}$

**2.** Construct a relation on the set $\{a, b, c, d\}$ that is
**a)** reflexive, symmetric, but not transitive.
**b)** irreflexive, symmetric, and transitive.
**c)** irreflexive, antisymmetric, and not transitive.
**d)** reflexive, neither symmetric nor antisymmetric, and transitive.
**e)** neither reflexive, irreflexive, symmetric, antisymmetric, nor transitive.

**3.** Show that the relation $R$ on $\mathbf{Z} \times \mathbf{Z}$ defined by $(a, b)\ R\ (c, d)$ if and only if $a + d = b + c$ is an equivalence relation.

**4.** Show that a subset of an antisymmetric relation is also antisymmetric.

**5.** Let $R$ be a reflexive relation on a set $A$. Show that $R \subseteq R^2$.

**6.** Suppose that $R_1$ and $R_2$ are reflexive relations on a set $A$. Show that $R_1 \oplus R_2$ is irreflexive.

**7.** Suppose that $R_1$ and $R_2$ are reflexive relations on a set $A$. Is $R_1 \cap R_2$ also reflexive? Is $R_1 \cup R_2$ also reflexive?

**8.** Suppose that $R$ is a symmetric relation on a set $A$. Is $\overline{R}$ also symmetric?

**9.** Let $R_1$ and $R_2$ be symmetric relations. Is $R_1 \cap R_2$ also symmetric? Is $R_1 \cup R_2$ also symmetric?

**10.** A relation $R$ is called **circular** if $a\,R\,b$ and $b\,R\,c$ imply that $c\,R\,a$. Show that $R$ is reflexive and circular if and only if it is an equivalence relation.

**11.** Show that a primary key in an $n$-ary relation is a primary key in any projection of this relation that contains this key as one of its fields.

**12.** Is the primary key in an $n$-ary relation also a primary key in a larger relation obtained by taking the join of this relation with a second relation?

**13.** Show that the reflexive closure of the symmetric closure of a relation is the same as the symmetric closure of its reflexive closure.

**14.** Let $R$ be the relation on the set of all mathematicians that contains the ordered pair $(a, b)$ if and only if $a$ and $b$ have written a published mathematical paper together.
**a)** Describe the relation $R^2$.
**b)** Describe the relation $R^*$.
**c)** The **Erdős number** of a mathematician is 1 if this mathematician wrote a paper with the prolific Hungarian mathematician Paul Erdős, it is 2 if this mathematician did not write a joint paper with Erdős but wrote a joint paper with someone who wrote a joint paper with Erdős, and so on (except that the Erdős number of Erdős himself is 0). Give a definition of the Erdős number in terms of paths in $R$.

**15.** **a)** Give an example to show that the transitive closure of the symmetric closure of a relation is not necessarily the same as the symmetric closure of the transitive closure of this relation.

**b)** Show, however, that the transitive closure of the symmetric closure of a relation must contain the symmetric closure of the transitive closure of this relation.

**16.** **a)** Let $S$ be the set of subroutines of a computer program. Define the relation $R$ by $\mathbf{P}\,R\,\mathbf{Q}$ if subroutine $\mathbf{P}$ calls subroutine $\mathbf{Q}$ during its execution. Describe the transitive closure of $R$.

**b)** For which subroutines $\mathbf{P}$ does $(\mathbf{P}, \mathbf{P})$ belong to the transitive closure of $R$?

**c)** Describe the reflexive closure of the transitive closure of $R$.

**17.** Suppose that $R$ and $S$ are relations on a set $A$ with $R \subseteq S$ such that the closures of $R$ and $S$ with respect to a property $\mathbf{P}$ both exist. Show that the closure of $R$ with respect to $\mathbf{P}$ is a subset of the closure of $S$ with respect to $\mathbf{P}$.

**18.** Show that the symmetric closure of the union of two relations is the union of their symmetric closures.

***19.** Devise an algorithm, based on the concept of interior vertices, that finds the length of the longest path between two vertices in a directed graph, or determines that there are arbitrarily long paths between these vertices.

**20.** Which of these are equivalence relations on the set of all people?

**a)** $\{(x, y) \mid x \text{ and } y \text{ have the same sign of the zodiac}\}$

**b)** $\{(x, y) \mid x \text{ and } y \text{ were born in the same year}\}$

**c)** $\{(x, y) \mid x \text{ and } y \text{ have been in the same city}\}$

***21.** How many different equivalence relations with exactly three different equivalence classes are there on a set with five elements?

**22.** Show that $\{(x, y) \mid x - y \in \mathbf{Q}\}$ is an equivalence relation on the set of real numbers, where $\mathbf{Q}$ denotes the set of rational numbers. What are $[1]$, $[\frac{1}{2}]$, and $[\pi]$?

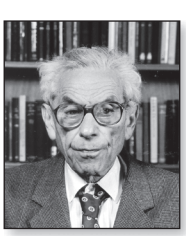
**23.** Suppose that $P_1 = \{A_1, A_2, \ldots, A_m\}$ and $P_2 = \{B_1, B_2, \ldots, B_n\}$ are both partitions of the set $S$. Show that the collection of nonempty subsets of the form $A_i \cap B_j$ is a partition of $S$ that is a refinement of both $P_1$ and $P_2$ (see the preamble to Exercise 49 of Section 9.5).

***24.** Show that the transitive closure of the symmetric closure of the reflexive closure of a relation $R$ is the smallest equivalence relation that contains $R$.

**25.** Let $\mathbf{R}(S)$ be the set of all relations on a set $S$. Define the relation $\preccurlyeq$ on $\mathbf{R}(S)$ by $R_1 \preccurlyeq R_2$ if $R_1 \subseteq R_2$, where $R_1$ and $R_2$ are relations on $S$. Show that $(\mathbf{R}(S), \preccurlyeq)$ is a poset.

**26.** Let $\mathbf{P}(S)$ be the set of all partitions of the set $S$. Define the relation $\preccurlyeq$ on $\mathbf{P}(S)$ by $P_1 \preccurlyeq P_2$ if $P_1$ is a refinement of $P_2$ (see Exercise 49 of Section 9.5). Show that $(\mathbf{P}(S), \preccurlyeq)$ is a poset.

**Links**



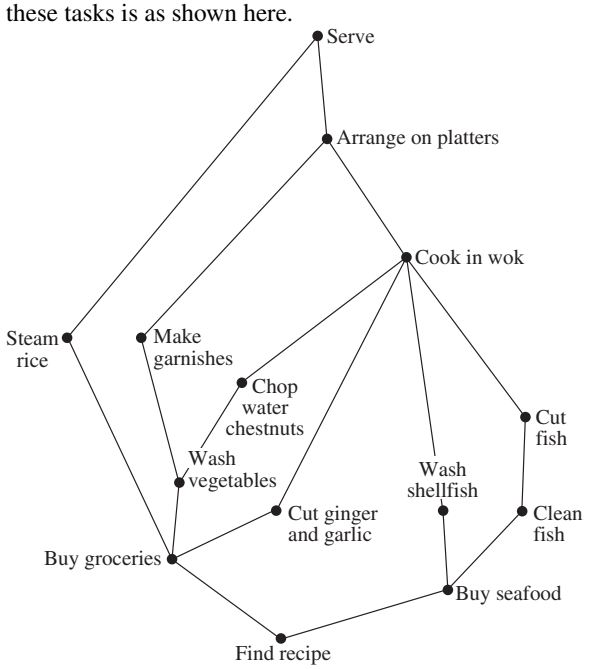
PAUL ERDŐS (1913–1996) Paul Erdős, born in Budapest, Hungary, was the son of two high school mathematics teachers. He was a child prodigy; at age 3 he could multiply three-digit numbers in his head, and at 4 he discovered negative numbers on his own. Because his mother did not want to expose him to contagious diseases, he was mostly home-schooled. At 17 Erdős entered Eötvös University, graduating four years later with a Ph.D. in mathematics. After graduating he spent four years at Manchester, England, on a postdoctoral fellowship. In 1938 he went to the United States because of the difficult political situation in Hungary, especially for Jews. He spent much of his time in the United States, except for 1954 to 1962, when he was banned as part of the paranoia of the McCarthy era. He also spent considerable time in Israel.

Erdős made many significant contributions to combinatorics and to number theory. One of the discoveries of which he was most proud is his elementary proof (in the sense that it does not use any complex analysis) of the prime number theorem, which provides an estimate for the number of primes not exceeding a fixed positive integer. He also participated in the modern development of the Ramsey theory.

Erdős traveled extensively throughout the world to work with other mathematicians, visiting conferences, universities, and research laboratories. He had no permanent home. He devoted himself almost entirely to mathematics, traveling from one mathematician to the next, proclaiming "My brain is open." Erdős was the author or coauthor of more than 1500 papers and had more than 500 coauthors. Copies of his articles are kept by Ron Graham, a famous discrete mathematician with whom he collaborated extensively and who took care of many of his worldly needs.

Erdős offered rewards, ranging from $10 to $10,000, for the solution of problems that he found particularly interesting, with the size of the reward depending on the difficulty of the problem. He paid out close to $4000. Erdős had his own special language, using such terms as "epsilon" (child), "boss" (woman), "slave" (man), "captured" (married), "liberated" (divorced), "Supreme Fascist" (God), "Sam" (United States), and "Joe" (Soviet Union). Although he was curious about many things, he concentrated almost all his energy on mathematical research. He had no hobbies and no full-time job. He never married and apparently remained celibate. Erdős was extremely generous, donating much of the money he collected from prizes, awards, and stipends for scholarships and to worthwhile causes. He traveled extremely lightly and did not like having many material possessions.

**27.** Schedule the tasks needed to cook a Chinese meal by specifying their order, if the Hasse diagram representing these tasks is as shown here.




A subset of a poset such that every two elements of this subset are comparable is called a **chain**. A subset of a poset is called an **antichain** if every two elements of this subset are incomparable.

**28.** Find all chains in the posets with the Hasse diagrams shown in Exercises 25–27 in Section 9.6.

**29.** Find all antichains in the posets with the Hasse diagrams shown in Exercises 25–27 in Section 9.6.

**30.** Find an antichain with the greatest number of elements in the poset with the Hasse diagram of Exercise 32 in Section 9.6.

**31.** Show that every maximal chain in a finite poset $(S, \preccurlyeq)$ contains a minimal element of $S$. (A maximal chain is a chain that is not a subset of a larger chain.)

****32.** Show that every finite poset can be partitioned into $k$ chains, where $k$ is the largest number of elements in an antichain in this poset.

***33.** Show that in any group of $mn + 1$ people there is either a list of $m + 1$ people where a person in the list (except for the first person listed) is a descendant of the previous person on the list, or there are $n + 1$ people such that none of these people is a descendant of any of the other $n$ people. [*Hint:* Use Exercise 32.]

Suppose that $(S, \preccurlyeq)$ is a well-founded partially ordered set. The *principle of well-founded induction* states that $P(x)$ is true for all $x \in S$ if $\forall x(\forall y(y \prec x \rightarrow P(y)) \rightarrow P(x))$.

**34.** Show that no separate basis case is needed for the principle of well-founded induction. That is, $P(u)$ is true for all minimal elements $u$ in $S$ if $\forall x(\forall y(y \prec x \rightarrow P(y)) \rightarrow P(x))$.

***35.** Show that the principle of well-founded induction is valid.

A relation $R$ on a set $A$ is a **quasi-ordering** on $A$ if $R$ is reflexive and transitive.

**36.** Let $R$ be the relation on the set of all functions from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ such that $(f, g)$ belongs to $R$ if and only if $f$ is $O(g)$. Show that $R$ is a quasi-ordering.

**37.** Let $R$ be a quasi-ordering on a set $A$. Show that $R \cap R^{-1}$ is an equivalence relation.

***38.** Let $R$ be a quasi-ordering and let $S$ be the relation on the set of equivalence classes of $R \cap R^{-1}$ such that $(C, D)$ belongs to $S$, where $C$ and $D$ are equivalence classes of $R$, if and only if there are elements $c$ of $C$ and $d$ of $D$ such that $(c, d)$ belongs to $R$. Show that $S$ is a partial ordering.

Let $L$ be a lattice. Define the **meet** ($\wedge$) and **join** ($\vee$) operations by $x \wedge y = \text{glb}(x, y)$ and $x \vee y = \text{lub}(x, y)$.

**39.** Show that the following properties hold for all elements $x$, $y$, and $z$ of a lattice $L$.

**a)** $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ **(commutative laws)**

**b)** $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$ **(associative laws)**

**c)** $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ **(absorption laws)**

**d)** $x \wedge x = x$ and $x \vee x = x$ **(idempotent laws)**

**40.** Show that if $x$ and $y$ are elements of a lattice $L$, then $x \vee y = y$ if and only if $x \wedge y = x$.

A lattice $L$ is **bounded** if it has both an **upper bound**, denoted by 1, such that $x \preccurlyeq 1$ for all $x \in L$ and a **lower bound**, denoted by 0, such that $0 \preccurlyeq x$ for all $x \in L$.

**41.** Show that if $L$ is a bounded lattice with upper bound 1 and lower bound 0 then these properties hold for all elements $x \in L$.

**a)** $x \vee 1 = 1$ **b)** $x \wedge 1 = x$

**c)** $x \vee 0 = x$ **d)** $x \wedge 0 = 0$

**42.** Show that every finite lattice is bounded.

A lattice is called **distributive** if $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for all $x$, $y$, and $z$ in $L$.

***43.** Give an example of a lattice that is not distributive.

**44.** Show that the lattice $(P(S), \subseteq)$ where $P(S)$ is the power set of a finite set $S$ is distributive.

**45.** Is the lattice $(\mathbf{Z}^+, |)$ distributive?

The **complement** of an element $a$ of a bounded lattice $L$ with upper bound 1 and lower bound 0 is an element $b$ such that $a \vee b = 1$ and $a \wedge b = 0$. Such a lattice is **complemented** if every element of the lattice has a complement.

**46.** Give an example of a finite lattice where at least one element has more than one complement and at least one element has no complement.

**47.** Show that the lattice $(P(S), \subseteq)$ where $P(S)$ is the power set of a finite set $S$ is complemented.

***48.** Show that if $L$ is a finite distributive lattice, then an element of $L$ has at most one complement.

The game of Chomp, introduced in Example 12 in Section 1.8, can be generalized for play on any finite partially ordered set $(S, \preceq)$ with a least element $a$. In this game, a move consists of selecting an element $x$ in $S$ and removing $x$ and all elements larger than it from $S$. The loser is the player who is forced to select the least element $a$.

**49.** Show that the game of Chomp with cookies arranged in an $m \times n$ rectangular grid, described in Example 12 in Section 1.8, is the same as the game of Chomp on the poset $(S, |)$, where $S$ is the set of all positive integers that divide $p^{m-1}q^{n-1}$, where $p$ and $q$ are distinct primes.

**50.** Show that if $(S, \preceq)$ has a greatest element $b$, then a winning strategy for Chomp on this poset exists. [*Hint:* Generalize the argument in Example 12 in Section 1.8.]

## Computer Projects

### Write programs with these input and output.

**1.** Given the matrix representing a relation on a finite set, determine whether the relation is reflexive and/or irreflexive.

**2.** Given the matrix representing a relation on a finite set, determine whether the relation is symmetric and/or antisymmetric.

**3.** Given the matrix representing a relation on a finite set, determine whether the relation is transitive.

**4.** Given a positive integer $n$, display all the relations on a set with $n$ elements.

***5.** Given a positive integer $n$, determine the number of transitive relations on a set with $n$ elements.

***6.** Given a positive integer $n$, determine the number of equivalence relations on a set with $n$ elements.

***7.** Given a positive integer $n$, display all the equivalence relations on the set of the $n$ smallest positive integers.

**8.** Given an $n$-ary relation, find the projection of this relation when specified fields are deleted.

**9.** Given an $m$-ary relation and an $n$-ary relation, and a set of common fields, find the join of these relations with respect to these common fields.

**10.** Given the matrix representing a relation on a finite set, find the matrix representing the reflexive closure of this relation.

**11.** Given the matrix representing a relation on a finite set, find the matrix representing the symmetric closure of this relation.

**12.** Given the matrix representing a relation on a finite set, find the matrix representing the transitive closure of this relation by computing the join of the Boolean powers of the matrix representing the relation.

**13.** Given the matrix representing a relation on a finite set, find the matrix representing the transitive closure of this relation using Warshall's algorithm.

**14.** Given the matrix representing a relation on a finite set, find the matrix representing the smallest equivalence relation containing this relation.

**15.** Given a partial ordering on a finite set, find a total ordering compatible with it using topological sorting.

## Computations and Explorations

### Use a computational program or programs you have written to do these exercises.

**1.** Display all the different relations on a set with four elements.

**2.** Display all the different reflexive and symmetric relations on a set with six elements.

**3.** Display all the reflexive and transitive relations on a set with five elements.

***4.** Determine how many transitive relations there are on a set with $n$ elements for all positive integers $n$ with $n \leq 7$.

**5.** Find the transitive closure of a relation of your choice on a set with at least 20 elements. Either use a relation that corresponds to direct links in a particular transportation or communications network or use a randomly generated relation.

**6.** Compute the number of different equivalence relations on a set with $n$ elements for all positive integers $n$ not exceeding 20.

**7.** Display all the equivalence relations on a set with seven elements.

***8.** Display all the partial orders on a set with five elements.

***9.** Display all the lattices on a set with five elements.

## Writing Projects

**Respond to these with essays using outside sources.**

1. Discuss the concept of a fuzzy relation. How are fuzzy relations used?
2. Describe the basic principles of relational databases, going beyond what was covered in Section 9.2. How widely used are relational databases as compared with other types of databases?
3. Look up the original papers by Warshall and by Roy (in French) in which they develop algorithms for finding transitive closures. Discuss their approaches. Why do you suppose that what we call Warshall's algorithm was discovered independently by more than one person?
4. Describe how equivalence classes can be used to define the rational numbers as classes of pairs of integers and how the basic arithmetic operations on rational numbers can be defined following this approach. (See Exercise 40 in Section 9.5.)
5. Explain how Helmut Hasse used what we now call Hasse diagrams.
6. Describe some of the mechanisms used to enforce information flow policies in computer operating systems.
7. Discuss the use of the Program Evaluation and Review Technique (PERT) to schedule the tasks of a large complicated project. How widely is PERT used?
8. Discuss the use of the Critical Path Method (CPM) to find the shortest time for the completion of a project. How widely is CPM used?
9. Discuss the concept of *duality* in a lattice. Explain how duality can be used to establish new results.
10. Explain what is meant by a *modular lattice*. Describe some of the properties of modular lattices and describe how modular lattices arise in the study of projective geometry.