CHAPTER

2 Logic

Prerequisites: Chapter 1

Logic is the discipline that deals with the methods of reasoning. On an elementary level, logic provides rules and techniques for determining whether a given argument is valid. Logical reasoning is used in mathematics to prove theorems, in computer science to verify the correctness of programs and to prove theorems, in the natural and physical sciences to draw conclusions from experiments, in the social sciences, and in our everyday lives to solve a multitude of problems. Indeed, we are constantly using logical reasoning. In this chapter we discuss a few of the basic ideas.

LOOKING BACK

In the 1840s Augustus De Morgan, a British mathematician, set out to extend the logic developed by the early Greeks and others and to correct some of the weaknesses in these ideas. De Morgan (1806–1871) was born in India but was educated in England. He taught at London University for many years and was the first to use the word "induction" for a method of proof that had been used in a rather informal manner and put it on a firm rigorous foundation. In 1847, a few years after De Morgan's work on an extended system of logic had appeared, his countryman George Boole published the book entitled *The Mathematical Analysis of Logic* and followed it up a few years later by the book *An Investigation of the Laws of Thought*. Boole's objective in these books was

> to investigate the fundamental laws of those operations of the mind by which reasoning is performed; to give expression to them in the symbolical language of a Calculus; and upon this foundation to establish the science of Logic and construct its method.*

*Quoted in Victor J. Katz, *A History of Mathematics, An Introduction*, New York: HarperCollins, 1993, p. 619.

LOOKING BACK (Continued)

Boole's work in this area firmly established the point of view that logic should use symbols and that algebraic properties should be studied in logic. George Boole (1815–1864) taught at Queen's College in Ireland for many years. Thus, De Morgan started and Boole completed the task of folding a large part of the study of logic into mathematics. We shall briefly study the work of De Morgan and Boole in logic in this chapter, and in Chapter 8 we shall further examine important applications of the work of Boole to many areas in mathematics and computer science.

Augustus De Morgan

George Boole

2.1 Propositions and Logical Operations

A **statement** or **proposition** is a declarative sentence that is either true or false, but not both.

EXAMPLE 1 Which of the following are statements?

(a) The earth is round.
(b) $2 + 3 = 5$
(c) Do you speak English?
(d) $3 - x = 5$
(e) Take two aspirins.
(f) The temperature on the surface of the planet Venus is 800°F.
(g) The sun will come out tomorrow.

Solution

(a) and **(b)** are statements that happen to be true.
(c) is a question, so it is not a statement.
(d) is a declarative sentence, but not a statement, since it is true or false depending on the value of x.
(e) is not a statement; it is a command.
(f) is a declarative sentence whose truth or falsity we do not know at this time; however, we can in principle determine if it is true or false, so it is a statement.
(g) is a statement since it is either true or false, but not both, although we would have to wait until tomorrow to find out if it is true or false. ■

■ Logical Connectives and Compound Statements

In mathematics, the letters $x, y, z, \ldots$ often denote variables that can be replaced by real numbers, and these variables can be combined with the familiar operations $+, \times, -$, and $\div$. In logic, the letters $p, q, r, \ldots$ denote **propositional variables**; that is, variables that can be replaced by statements. Thus we can write p: The sun is shining today. q: It is cold. Statements or propositional variables can be combined by logical connectives to obtain **compound statements**. For example, we may combine the preceding statements by the connective *and* to form the compound statement *p and q*: The sun is shining today *and* it is cold. The truth value of a compound statement depends only on the truth values of the statements being combined and on the types of connectives being used. We shall look at the most important connectives.

TABLE 2.1

p	$\sim p$
T	F
F	T

If p is a statement, the **negation** of p is the statement *not p*, denoted by $\sim p$. Thus $\sim p$ is the statement "it is not the case that p." From this definition, it follows that if p is true, then $\sim p$ is false, and if p is false, then $\sim p$ is true. The truth value of $\sim p$ relative to p is given in Table 2.1. Such a table, giving the truth values of a compound statement in terms of its component parts, is called a **truth table**. Strictly speaking, *not* is not a connective, since it does not join two statements, and $\sim p$ is not really a compound statement. However, *not* is a unary operation for the collection of statements and $\sim p$ is a statement if p is.

EXAMPLE 2 Give the negation of the following statements:

(a) p: $2 + 3 > 1$ **(b)** q: It is cold.

Solution

(a) $\sim p$: $2 + 3$ is not greater than 1. That is, $\sim p$: $2 + 3 \leq 1$. Since p is true in this case, $\sim p$ is false.

(b) $\sim q$: It is not the case that it is cold. More simply, $\sim q$: It is not cold. ■

TABLE 2.2

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

If p and q are statements, the **conjunction** of p and q is the compound statement "p and q," denoted by $p \wedge q$. The connective *and* is denoted by the symbol $\wedge$. In the language of Section 1.6, *and* is a binary operation on the set of statements. The compound statement $p \wedge q$ is true when both p and q are true; otherwise, it is false. The truth values of $p \wedge q$ in terms of the truth values of p and q are given in the truth table shown in Table 2.2. Observe that in giving the truth table of $p \wedge q$ we need to look at four possible cases. This follows from the fact that each of p and q can be true or false.

EXAMPLE 3 Form the conjunction of p and q for each of the following.

(a) p: It is snowing. q: I am cold.
(b) p: $2 < 3$ q: $-5 > -8$
(c) p: It is snowing. q: $3 < 5$

Solution

(a) $p \wedge q$: It is snowing and I am cold.

(b) $p \wedge q$: $2 < 3$ and $-5 > -8$

(c) $p \wedge q$: It is snowing and $3 < 5$. ■

Example 3(c) shows that in logic, unlike in everyday English, we may join two totally unrelated statements by the connective *and*.

If p and q are statements, the **disjunction** of p and q is the compound statement "p or q," denoted by $p \vee q$. The connective *or* is denoted by the symbol $\vee$. The compound statement $p \vee q$ is true if at least one of p or q is true; it is false when both p and q are false. The truth values of $p \vee q$ are given in the truth table shown in Table 2.3.

EXAMPLE 4 Form the disjunction of p and q for each of the following.

(a) p: 2 is a positive integer q: $\sqrt{2}$ is a rational number.
(b) p: $2 + 3 \neq 5$ q: London is the capital of France.

TABLE 2.3

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

Solution

(a) $p \vee q$: 2 is a positive integer or $\sqrt{2}$ is a rational number. Since p is true, the disjunction $p \vee q$ is true, even though q is false.

(b) $p \vee q$: $2 + 3 \neq 5$ or London is the capital of France. Since both p and q are false, $p \vee q$ is false. ■

Example 4(b) shows that in logic, unlike in ordinary English, we may join two totally unrelated statements by the connective *or*.

The connective *or* is more complicated than the connective *and* because it is used in two different ways in English. Suppose that we say "I left for Spain on Monday or I left for Spain on Friday." In this compound statement we have the disjunction of the statements p: I left for Spain on Monday and q: I left for Spain on Friday. Of course, exactly one of the two possibilities could have occurred. Both could not have occurred, so the connective *or* is being used in an *exclusive* sense. On the other hand, consider the disjunction "I passed mathematics or I failed French." In this case, at least one of the two possibilities occurred. However, both could have occurred, so the connective *or* is being used in an *inclusive* sense. In mathematics and computer science we agree to use the connective *or* always in the inclusive manner.

In general, a compound statement may have many component parts, each of which is itself a statement, represented by some propositional variable. The statement s: $p \vee (q \wedge (p \vee r))$ involves three propositions, p, q, and r, each of which may independently be true or false. There are altogether 2^3 or 8 possible combinations of truth values for p, q, and r, and a truth table for s must give the truth or falsity of s in all these cases. If a compound statement s contains n component statements, there will need to be 2^n rows in the truth table for s. (In Section 3.1 we look at how to count the possibilities in such cases.) Such a truth table may be systematically constructed in the following way.

Step 1: The first n columns of the table are labeled by the component propositional variables. Further columns are included for all intermediate combinations of the variables, culminating in a column for the full statement.

Step 2: Under each of the first n headings, we list the 2^n possible n-tuples of truth values for the n component statements.

Step 3: For each of the remaining columns, we compute, in sequence, the remaining truth values.

EXAMPLE 5 Make a truth table for the statement $(p \wedge q) \vee (\sim p)$.

Solution

Because two propositions are involved, the truth table will have 2^2 or 4 rows. In the first two columns we list all possible pairs of truth values for p and q. The

numbers below the remaining columns show the order in which the columns were filled.

p	q	$p \wedge q$	$\vee$	$\sim p$
T	T	T	T	F
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T
		(1)	(3)	(2)

■

■ Quantifiers

In Section 1.1, we defined sets by specifying a property $P(x)$ that elements of the set have in common. Thus, an element of $\{x \mid P(x)\}$ is an object t for which the statement $P(t)$ is true. Such a sentence $P(x)$ is called a **predicate**, because in English the property is grammatically a predicate. $P(x)$ is also called a **propositional function**, because each choice of x produces a proposition $P(x)$ that is either true or false. Another use of predicates is in programming. Two common constructions are "if $P(x)$, then execute certain steps" and "while $Q(x)$, do specified actions." The predicates $P(x)$ and $Q(x)$ are called the **guards** for the block of programming code. Often the guard for a block is a conjunction or disjunction.

EXAMPLE 6

Let $A = \{x \mid x \text{ is an integer less than } 8\}$. Here $P(x)$ is the sentence "x is an integer less than 8." The common property is "is an integer less than 8." Since $P(1)$ is true, $1 \in A$. ■

The **universal quantification** of a predicate $P(x)$ is the statement "For all values of x, $P(x)$ is true." We assume here that only values of x that make sense in $P(x)$ are considered. The universal quantification of $P(x)$ is denoted $\forall x\ P(x)$. The symbol $\forall$ is called the universal quantifier.

EXAMPLE 7

(a) The sentence $P(x)$: $-(-x) = x$ is a predicate that makes sense for real numbers x. The universal quantification of $P(x)$, $\forall x\ P(x)$, is a true statement, because for all real numbers, $-(-x) = x$.

(b) Let $Q(x)$: $x + 1 < 4$. Then $\forall x\ Q(x)$ is a false statement, because $Q(5)$ is not true. ■

Universal quantification can also be stated in English as "for every x," "every x," or "for any x."

A predicate may contain several variables. Universal quantification may be applied to each of the variables. For example, a commutative property can be expressed as $\forall x\ \forall y\ x \square y = y \square x$. The order in which the universal quantifiers are considered does not change the truth value. Often mathematical statements contain implied universal quantifications (for example in Theorem 1, Section 1.2).

In some situations we only require that there be at least one value for which the predicate is true. The **existential quantification** of a predicate $P(x)$ is the statement "There exists a value of x for which $P(x)$ is true." The existential quantification of $P(x)$ is denoted $\exists x\ P(x)$. The symbol $\exists$ is called the existential quantifier.

EXAMPLE 8

(a) Let $Q(x)$: $x + 1 < 4$. The existential quantification of $Q(x)$, $\exists x\ Q(x)$, is a true statement, because $Q(2)$ is a true statement.

(b) The statement $\exists y\ y + 2 = y$ is false. There is no value of y for which the propositional function $y + 2 = y$ produces a true statement. ■

In English $\exists x$ can also be read "there is an x," "there is some x," "there exists an x," or "there is at least one x."

Existential quantification may be applied to several variables in a predicate and the order in which the quantifications are considered does not affect the truth value. For a predicate with several variables we may apply both universal and existential quantification. In this case the order does matter.

EXAMPLE 9

Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices.

(a) The statement $\forall \mathbf{A}\, \exists \mathbf{B}\ \mathbf{A} + \mathbf{B} = \mathbf{I}_n$ is read "for every $\mathbf{A}$ there is a $\mathbf{B}$ such that $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$." For a given $\mathbf{A} = [\,a_{ij}\,]$, define $\mathbf{B} = [\,b_{ij}\,]$ as follows: $b_{ii} = 1 - a_{ii}$, $1 \le i \le n$ and $b_{ij} = -a_{ij}$, $i \ne j$, $1 \le i \le n$, $1 \le j \le n$. Then $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$ and we have shown that $\forall \mathbf{A}\, \exists \mathbf{B}\ \mathbf{A} + \mathbf{B} = \mathbf{I}_n$ is a true statement.

(b) $\exists \mathbf{B}\, \forall \mathbf{A}\ \mathbf{A} + \mathbf{B} = \mathbf{I}_n$ is the statement "there is a $\mathbf{B}$ such that for all $\mathbf{A}$ $\mathbf{A} + \mathbf{B} = \mathbf{I}_n$." This statement is false; no single $\mathbf{B}$ has this property for all $\mathbf{A}$'s.

(c) $\exists \mathbf{B}\, \forall \mathbf{A}\ \mathbf{A} + \mathbf{B} = \mathbf{A}$ is true. What is the value for $\mathbf{B}$ that makes the statement true? ■

Let p: $\forall x\ P(x)$. The negation of p is false when p is true, and true when p is false. For p to be false there must be at least one value of x for which $P(x)$ is false. Thus, p is false if $\exists x \sim P(x)$ is true. On the other hand, if $\exists x \sim P(x)$ is false, then for every x, $\sim P(x)$ is false; that is, $\forall x\ P(x)$ is true.

EXAMPLE 10

(a) Let p: For all positive integers n, $n^2 + 41n + 41$ is a prime number. Then $\sim p$ is There is at least one positive integer n for which $n^2 + 41n + 41$ is not prime.

(b) Let q: There is some integer k for which $12 = 3k$. Then $\sim q$: For all integers k, $12 \ne 3k$. ■

2.1 Exercises

1. Which of the following are statements?
   - **(a)** Is 2 a positive number?
   - **(b)** $x^2 + x + 1 = 0$
   - **(c)** Study logic.
   - **(d)** There will be snow in January.
   - **(e)** If stock prices fall, then I will lose money.
2. Give the negation of each of the following statements.
   - **(a)** $2 + 7 \le 11$
   - **(b)** 2 is an even integer and 8 is an odd integer.
3. Give the negation of each of the following statements.
   - **(a)** It will rain tomorrow or it will snow tomorrow.
   - **(b)** If you drive, then I will walk.
4. In each of the following, form the conjunction and the disjunction of p and q.
   - **(a)** p: $3 + 1 < 5$ $\quad q$: $7 = 3 \times 6$
   - **(b)** p: I am rich. $\quad q$: I am happy.
5. In each of the following, form the conjunction and the disjunction of p and q.
   - **(a)** p: I will drive my car. $\quad q$: I will be late.
   - **(b)** p: NUM > 10 $\quad q$: NUM $\le$ 15
6. Determine the truth or falsity of each of the following statements.
   - **(a)** $2 < 3$ and 3 is a positive integer.
   - **(b)** $2 \ge 3$ and 3 is a positive integer.
   - **(c)** $2 < 3$ and 3 is not a positive integer.
   - **(d)** $2 \ge 3$ and 3 is not a positive integer.
7. Determine the truth or falsity of each of the following statements.
   - **(a)** $2 < 3$ or 3 is a positive integer.
   - **(b)** $2 \ge 3$ or 3 is a positive integer.
   - **(c)** $2 < 3$ or 3 is not a positive integer.
   - **(d)** $2 \ge 3$ or 3 is not a positive integer.

In Exercises 8 and 9, find the truth value of each proposition if p and r are true and q is false.

8. **(a)** $\sim p \wedge \sim q$ **(b)** $(\sim p \vee q) \wedge r$
   (c) $p \vee q \vee r$ **(d)** $\sim(p \vee q) \wedge r$
9. **(a)** $\sim p \wedge (q \vee r)$ **(b)** $p \wedge (\sim(q \vee \sim r))$
   (c) $(r \wedge \sim q) \vee (p \vee r)$ **(d)** $(q \wedge r) \wedge (p \vee \sim r)$
10. Which of the following statements is the negation of the statement "2 is even and -3 is negative"?
    (a) 2 is even and -3 is not negative.
    (b) 2 is odd and -3 is not negative.
    (c) 2 is even or -3 is not negative.
    (d) 2 is odd or -3 is not negative.
11. Which of the following statements is the negation of the statement "2 is even or -3 is negative"?
    (a) 2 is even or -3 is not negative.
    (b) 2 is odd or -3 is not negative.
    (c) 2 is even and -3 is not negative.
    (d) 2 is odd and -3 is not negative.

In Exercises 12 and 13, use p: Today is Monday; q: The grass is wet; and r: The dish ran away with the spoon.

12. Write each of the following in terms of p, q, r, and logical connectives.
    (a) Today is Monday and the dish did not run away with the spoon.
    (b) Either the grass is wet or today is Monday.
    (c) Today is not Monday and the grass is dry.
    (d) The dish ran away with the spoon, but the grass is wet.
13. Write an English sentence that corresponds to each of the following.
    (a) $\sim r \wedge q$ **(b)** $\sim q \vee r$
    (c) $\sim(p \vee q)$ **(d)** $p \vee \sim r$

In Exercises 14 through 19, use $P(x)$: x is even; $Q(x)$: x is a prime number; $R(x, y)$: $x + y$ is even. The variables x and y represent integers.

14. Write an English sentence corresponding to each of the following.
    (a) $\forall x\, P(x)$ **(b)** $\exists x\, Q(x)$
15. Write an English sentence corresponding to each of the following.
    (a) $\forall x \exists y\, R(x, y)$ **(b)** $\exists x \forall y\, R(x, y)$
16. Write an English sentence corresponding to each of the following.
    (a) $\forall x\, (\sim Q(x))$ **(b)** $\exists y\, (\sim P(y))$
17. Write an English sentence corresponding to each of the following.
    (a) $\sim(\exists x\, P(x))$ **(b)** $\sim(\forall x\, Q(x))$
18. Write each of the following in terms of $P(x)$, $Q(x)$, $R(x, y)$, logical connectives, and quantifiers.
    (a) Every integer is an odd integer.
    (b) The sum of any two integers is an even number.
    (c) There are no even prime numbers.
    (d) Every integer is even or a prime.
19. Determine the truth value of each statement given in Exercises 14 through 18.
20. Give a symbolic statement of the commutative property for addition of real numbers using appropriate quantifiers.
21. Give a symbolic statement of De Morgan's laws for sets using appropriate quantifiers.
22. Give a symbolic statement of the multiplicative inverse property for real numbers using appropriate quantifiers.

In Exercises 23 through 26, make a truth table for the statement.

23. $(\sim p \wedge q) \vee p$ 24. $(p \vee q) \vee \sim q$
25. $(p \vee q) \wedge r$ 26. $(\sim p \vee q) \wedge \sim r$

For Exercises 27 through 29, define $p \downarrow q$ to be a true statement if neither p nor q is true.

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

27. Make a truth table for $(p \downarrow q) \downarrow r$.
28. Make a truth table for $(p \downarrow q) \wedge (p \downarrow r)$.
29. Make a truth table for $(p \downarrow q) \downarrow (p \downarrow r)$.

For Exercises 30 through 32, define $p \triangle q$ to be true if either p or q, but not both, is true. Make a truth table for the statement.

30. **(a)** $p \triangle q$ **(b)** $p \triangle \sim p$
31. $(p \wedge q) \triangle p$
32. $(p \triangle q) \triangle (q \triangle r)$

In Exercises 33 through 36, revision of the given programming block is needed. Replace the guard $P(x)$ with $\sim P(x)$.

33. IF ($x \neq max$ and $y > 4$) THEN take action
34. WHILE (key = "open" or $t <$ limit) take action
35. WHILE (item $\neq$ sought and index < 101) take action
36. IF (cell > 0 or found) THEN take action

2.2 Conditional Statements

If p and q are statements, the compound statement "if p then q," denoted $p \Rightarrow q$, is called a **conditional statement**, or **implication**. The statement p is called the **antecedent** or **hypothesis**, and the statement q is called the **consequent** or **conclusion**. The connective *if ... then* is denoted by the symbol $\Rightarrow$.

Write the implication $p \Rightarrow q$ for each of the following.

(a) p: I am hungry. q: I will eat.
(b) p: It is snowing. q: $3 + 5 = 8$.

Solution

(a) If I am hungry, then I will eat.
(b) If it is snowing, then $3 + 5 = 8$. ■

Example 1(b) shows that in logic we use conditional statements in a more general sense than is customary. Thus in English, when we say "if p then q," we are tacitly assuming there is a cause-and-effect relationship between p and q. That is, we would never use the statement in Example 1(b) in ordinary English, since there is no way statement p can have any effect on statement q.

In logic, implication is used in a much weaker sense. To say the compound statement $p \Rightarrow q$ is true simply asserts that if p is true, then q will also be found to be true. In other words, $p \Rightarrow q$ says only that we will not have p true and q false at the same time. It does not say that p "caused" q in the usual sense. Table 2.4 describes the truth values of $p \Rightarrow q$ in terms of the truth of p and q. Notice that $p \Rightarrow q$ is considered false only if p is true and q is false. In particular, if p is false, then $p \Rightarrow q$ is true for any q. This fact is sometimes described by the statement "A false hypothesis implies any conclusion." This statement is misleading, since it seems to say that if the hypothesis is false, the conclusion must be true, an obviously silly statement. Similarly, if q is true, then $p \Rightarrow q$ will be true for any statement p. The implication "If $2 + 2 = 5$, then I am the king of England" is true, simply because p: $2 + 2 = 5$ is false, so it is not the case that p is true and q is false simultaneously.

TABLE 2.4

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

In the English language, and in mathematics, each of the following expressions is an equivalent form of the conditional statement $p \Rightarrow q$: p implies q; q, if p; p only if q; p is a sufficient condition for q; q is a necessary condition for p.

If $p \Rightarrow q$ is an implication, then the **converse** of $p \Rightarrow q$ is the implication $q \Rightarrow p$, and the **contrapositive** of $p \Rightarrow q$ is the implication $\sim q \Rightarrow \sim p$.

Give the converse and the contrapositive of the implication "If it is raining, then I get wet."

Solution

We have p: It is raining; and q: I get wet. The converse is $q \Rightarrow p$: If I get wet, then it is raining. The contrapositive is $\sim q \Rightarrow \sim p$: If I do not get wet, then it is not raining. ■

If p and q are statements, the compound statement p if and only if q, denoted by $p \Leftrightarrow q$, is called an **equivalence** or **biconditional**. The connective *if and only if* is denoted by the symbol $\Leftrightarrow$. The truth values of $p \Leftrightarrow q$ are given in Table 2.5. Observe that $p \Leftrightarrow q$ is true only when both p and q are true or when both p and q are false. The equivalence $p \Leftrightarrow q$ can also be stated as p is a necessary and sufficient condition for q.

TABLE 2.5

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

EXAMPLE 3 Is the following equivalence a true statement? $3 > 2$ if and only if $0 < 3 - 2$.

Solution

Let p be the statement $3 > 2$ and let q be the statement $0 < 3 - 2$. Since both p and q are true, we conclude that $p \Leftrightarrow q$ is true. ■

EXAMPLE 4 Compute the truth table of the statement $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$.

Solution

The following table is constructed using steps 1, 2, and 3 as given in Section 2.1. The numbers below the columns show the order in which they were constructed.

p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T
		(1)	(2)	(3)	(4)	(5)

■

A statement that is true for all possible values of its propositional variables is called a **tautology**. A statement that is always false is called a **contradiction** or an **absurdity**, and a statement that can be either true or false, depending on the truth values of its propositional variables, is called a **contingency**.

EXAMPLE 5

(a) The statement in Example 4 is a tautology.
(b) The statement $p \wedge \sim p$ is an absurdity. (Verify this.)
(c) The statement $(p \Rightarrow q) \wedge (p \vee q)$ is a contingency. ■

We have now defined a new mathematical structure with two binary operations and one unary operation, (propositions, $\wedge$, $\vee$, $\sim$). It makes no sense to say two propositions are equal; instead we say p and q are **logically equivalent**, or simply **equivalent**, if $p \Leftrightarrow q$ is a tautology. When an equivalence is shown to be a tautology, this means its two component parts are always either both true or both false, for any values of the propositional variables. Thus the two sides are simply different ways of making the same statement and can be regarded as "equal." We denote that p is equivalent to q by $p \equiv q$. Now we can adapt our properties for operations to say this structure has a property if using equivalent in place of equal gives a true statement.

EXAMPLE 6 The binary operation $\vee$ has the commutative property; that is, $p \vee q \equiv q \vee p$. The truth table for $(p \vee q) \Leftrightarrow (q \vee p)$ shows the statement is a tautology.

p	q	$p \vee q$	$q \vee p$	$(p \vee q) \Leftrightarrow (q \vee p)$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

■

Another way to use a truth table to determine if two statements are equivalent is to construct a column for each statement and compare these to see if they are identical. In Example 6 the third and fourth columns are identical, and this will guarantee that the statements they represent are equivalent.

Forming $p \Rightarrow q$ from p and q is another binary operation for statements, but we can express it in terms of the operations in Section 2.1.

EXAMPLE 7 The conditional statement $p \Rightarrow q$ is equivalent to $(\sim p) \vee q$. Columns 1 and 3 in the following table show that for any truth values of p and q, $p \Rightarrow q$ and $(\sim p) \vee q$ have the same truth values.

p	q	$p \Rightarrow q$	$\sim p$	$\vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T
		(1)	(2)	(3)

■

The structure (propositions, $\wedge$, $\vee$, $\sim$) has many of the same properties as the structure (sets, $\cup$, $\cap$, $^-$).

Theorem 1 The operations for propositions have the following properties.

Commutative Properties

1. $p \vee q \equiv q \vee p$
2. $p \wedge q \equiv q \wedge p$

Associative Properties

3. $p \vee (q \vee r) \equiv (p \vee q) \vee r$
4. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Distributive Properties

5. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
6. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Idempotent Properties

7. $p \vee p \equiv p$
8. $p \wedge p \equiv p$

Properties of Negation

9. $\sim(\sim p) \equiv p$
10. $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$
11. $\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$

Properties 10 and 11 are De Morgan's laws.

Proof

We have proved Property 1 in Example 6. The remaining properties may be proved the same way and are left for the reader as exercises. ■

Truth tables can be used to prove statements about propositions, because in a truth table all possible cases are examined.

The implication operation also has a number of important properties.

Theorem 2

(a) $(p \Rightarrow q) \equiv ((\sim p) \vee q)$
(b) $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$
(c) $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$

(d) $\sim(p \Rightarrow q) \equiv (p \wedge \sim q)$

(e) $\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

Proof

(a) was proved in Example 7 and (b) was proved in Example 4. Notice that (b) says a conditional statement is equivalent to its contrapositive.

(d) gives an alternate version for the negation of a conditional statement. This could be proved using truth tables, but it can also be proved by using previously proven facts. Since $(p \Rightarrow q) \equiv ((\sim p) \vee q)$, the negation of $p \Rightarrow q$ must be equivalent to $\sim((\sim p) \vee q)$. By De Morgan's laws, $\sim((\sim p) \vee q) \equiv (\sim(\sim p)) \wedge (\sim q)$ or $p \wedge (\sim q)$. Thus, $\sim(p \Rightarrow q) \equiv (p \wedge \sim q)$.

The remaining parts of Theorem 2 are left as exercises. ∎

Theorem 3 states two results from Section 2.1, and several other properties for the universal and existential quantifiers.

Theorem 3

(a) $\sim(\forall x\ \mathrm{P}(x)) \equiv \exists x\ \sim\mathrm{P}(x)$

(b) $\sim(\exists x\ \mathrm{P}(x)) \equiv \forall x\ (\sim\mathrm{P}(x))$

(c) $\exists x\ (\mathrm{P}(x) \Rightarrow \mathrm{Q}(x)) \equiv \forall x\ \mathrm{P}(x) \Rightarrow \exists x\ \mathrm{Q}(x)$

(d) $\exists x\ (\mathrm{P}(x) \vee \mathrm{Q}(x)) \equiv \exists x\ \mathrm{P}(x) \vee \exists x\ \mathrm{Q}(x)$

(e) $\forall x\ (\mathrm{P}(x) \wedge \mathrm{Q}(x)) \equiv \forall x\ \mathrm{P}(x) \wedge \forall x\ \mathrm{Q}(x)$

(f) $((\forall x\ \mathrm{P}(x)) \vee (\forall x\ \mathrm{Q}(x))) \Rightarrow \forall x\ (\mathrm{P}(x) \vee \mathrm{Q}(x))$ is a tautology.

(g) $\exists x\ (\mathrm{P}(x) \wedge \mathrm{Q}(x)) \Rightarrow \exists x\ \mathrm{P}(x) \wedge \exists x\ \mathrm{Q}(x)$ is a tautology. ∎

The following theorem gives several important tautologies that are implications. These are used extensively in proving results in mathematics and computer science and we will illustrate them in Section 2.3.

Theorem 4 Each of the following is a tautology.

(a) $(p \wedge q) \Rightarrow p$ **(b)** $(p \wedge q) \Rightarrow q$

(c) $p \Rightarrow (p \vee q)$ **(d)** $q \Rightarrow (p \vee q)$

(e) $\sim p \Rightarrow (p \Rightarrow q)$ **(f)** $\sim(p \Rightarrow q) \Rightarrow p$

(g) $(p \wedge (p \Rightarrow q)) \Rightarrow q$ **(h)** $(\sim p \wedge (p \vee q)) \Rightarrow q$

(i) $(\sim q \wedge (p \Rightarrow q)) \Rightarrow \sim p$ **(j)** $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ ∎

2.2 Exercises

In Exercises 1 and 2, use the following: p: I am awake; q: I work hard; r: I dream of home.

1. Write each of the following statements in terms of p, q, r, and logical connectives.
   (a) I am awake implies that I work hard.
   (b) I dream of home only if I am awake.
   (c) Working hard is sufficient for me to be awake.
   (d) Being awake is necessary for me not to dream of home.
2. Write each of the following statements in terms of p, q, r, and logical connectives.
   (a) I am not awake if and only if I dream of home.
   (b) If I dream of home, then I am awake and I work hard.
   (c) I do not work hard only if I am awake and I do not dream of home.
   (d) Not being awake and dreaming of home is sufficient for me to work hard.
3. State the converse of each of the following implications.
   (a) If $2 + 2 = 4$, then I am not the Queen of England.
   (b) If I am not President of the United Sates, then I will walk to work.
   (c) If I am late, then I did not take the train to work.
   (d) If I have time and I am not too tired, then I will go to the store.
   (e) If I have enough money, then I will buy a car and I will buy a house.
4. State the contrapositive of each implication in Exercise 3.
5. Determine the truth value for each of the following statements.
   (a) If 2 is even, then New York has a large population.
   (b) If 2 is even, then New York has a small population.
   (c) If 2 is odd, then New York has a large population.
   (d) If 2 is odd, then New York has a small population.

In Exercises 6 and 7, let p, q, and r be the following statements: p: I will study discrete structure; q: I will go to a movie; r: I am in a good mood.

6. Write the following statements in terms of p, q, r, and logical connectives.
   (a) If I am not in a good mood, then I will go to a movie.
   (b) I will not go to a movie and I will study discrete structures.
   (c) I will go to a movie only if I will not study discrete structures.
   (d) If I will not study discrete structures, then I am not in a good mood.
7. Write English sentences corresponding to the following statements.
   (a) $((\sim p) \wedge q) \Rightarrow r$ **(b)** $r \Rightarrow (p \vee q)$
   (c) $(\sim r) \Rightarrow ((\sim q \vee p)$ **(d)** $(q \wedge (\sim p)) \Leftrightarrow r$

In Exercises 8 and 9, let p, q, r, and s be the following statements: p: 4 > 1; q: 4 < 5; r: 3 ≤ 3; s: 2 > 2.

8. Write the following statements in terms of p, q, r, and logical connectives.
   (a) Either $4 > 1$ or $4 < 5$.
   (b) If $3 \leq 3$, then $2 > 2$.
   (c) It is not the case that $2 > 2$ or $4 > 1$.
9. Write English sentences corresponding to the following statements.
   (a) $(p \wedge s) \Rightarrow q$ **(b)** $\sim(r \wedge q)$ **(c)** $(\sim r) \Rightarrow p$

In Exercises 10 through 12, construct truth tables to determine whether the given statement is a tautology, a contingency, or an absurdity.

10. **(a)** $p \wedge \sim p$ **(b)** $q \vee (\sim q \wedge p)$
11. **(a)** $p \Rightarrow (q \Rightarrow p)$ **(b)** $q \Rightarrow (q \Rightarrow p)$
12. **(a)** $(q \wedge p) \vee (q \wedge \sim p)$
    (b) $(p \wedge q) \Rightarrow p$ **(c)** $p \Rightarrow (q \wedge p)$
13. If $p \Rightarrow q$ is false, can you determine the truth value of $(\sim(p \wedge q)) \Rightarrow q$? Explain your answer.
14. If $p \Rightarrow q$ is false, can you determine the truth value of $(\sim p) \vee (p \Leftrightarrow q)$? Explain your answer.
15. If $p \Rightarrow q$ is true, can you determine the truth value of $(p \wedge q) \Rightarrow \sim q$? Explain your answer.
16. If $p \Rightarrow q$ is true, can you determine the truth value of $\sim(p \Rightarrow q) \wedge \sim p$? Explain your answer.

In Exercises 17 and 18, find the truth value of each statement if p and q are true and r, s, and t are false.

17. **(a)** $\sim(p \Rightarrow q)$ **(b)** $(\sim p) \Rightarrow r$
    (c) $(p \Rightarrow s) \wedge (s \Rightarrow t)$ **(d)** $t \Rightarrow \sim q$
18. **(a)** $(\sim q) \Rightarrow (r \Rightarrow (r \Rightarrow (p \vee s)))$
    (b) $p \Rightarrow (r \Rightarrow q)$
    (c) $(q \Rightarrow (r \Rightarrow s)) \wedge ((p \Rightarrow s) \Rightarrow (\sim t))$
    (d) $(r \wedge s \wedge t) \Rightarrow (p \vee q)$
19. Use the definition of $p \downarrow q$ given for Exercise 27 in Section 2.1 and show that $((p \downarrow p) \downarrow (q \downarrow q))$ is equivalent to $p \wedge q$.
20. Write the negation of each of the following in good English.
    (a) The weather is bad and I will not go to work.
    (b) If Carol is not sick, then if she goes to the picnic, she will have a good time.
    (c) I will not win the game or I will not enter the contest.
21. Write the negation of each of the following in good English.
    (a) Jack did not eat fat, but he did eat broccoli.
    (b) Mary lost her lamb or the wolf ate the lamb.
    (c) If Tom stole a pie and ran away, then the three pigs do not have any supper.
22. Consider the following conditional statement:

    p: If the flood destroys my house or the fire destroys my house, then my insurance company will pay me.

    (a) Which of the following is the converse of p?
    (b) Which of the following is the contrapositive of p?
    (i) If my insurance company pays me, then the flood destroys my house or the fire destroys my house.
    (ii) If my insurance company pays me, then the flood destroys my house and the fire destroys my house.
    (iii) If my insurance company does not pay me, then the flood does not destroy my house or the fire does not destroy my house.
    (iv) If my insurance company does not pay me, then the flood does not destroy my house and the fire does not destroy my house.
23. Prove Theorem 1 part 6.
24. Prove Theorem 1 part 11.
25. Prove Theorem 2 part (e).

26. Prove Theorem 3 part (d).
27. Prove Theorem 3 part (e).
28. Prove Theorem 4 part (a).
29. Prove Theorem 4 part (d).
30. Prove Theorem 4 part (g).
31. Prove Theorem 4 part (j).
32. Explain why proving part (e) of Theorem 4 provides a one-line proof of part (f) of Theorem 4.
33. Explain why proving part (a) of Theorem 4 provides a one-line proof of part (b) of Theorem 4.

2.3 Methods of Proof

Some methods of proof we have already used are direct proofs using generic elements, definitions, and previously proven facts, and proofs by cases, such as examining all possible truth value situations in a truth table. Here we look at proofs in more detail.

If an implication $p \Rightarrow q$ is a tautology, where p and q may be compound statements involving any number of propositional variables, we say that q **logically follows** from p. Suppose that an implication of the form $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q$ is a tautology. Then this implication is true regardless of the truth values of any of its components. In this case, we say that q **logically follows** from $p_1, p_2, \ldots, p_n$. When q logically follows from $p_1, p_2, \ldots, p_n$, we write

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ \underline{p_n} \\ \therefore \ q \end{array}$$

where the symbol $\therefore$ means therefore. This means if we know that p_1 is true, p_2 is true, ..., and p_n is true, then we know q is true.

Virtually all mathematical theorems are composed of implications of the type

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q.$$

The p_i's are called the **hypotheses** or **premises**, and q is called the **conclusion**. To "prove the theorem" means to show that the *implication* is a tautology. Note that we are not trying to show that q (the conclusion) is true, but only that q will be true if all the p_i are true. For this reason, mathematical proofs often begin with the statement "suppose that $p_1, p_2, \ldots$, and p_n are true" and conclude with the statement "therefore, q is true." The proof does not show that q is true, but simply shows if the p_i are all true, then q has to be true.

Arguments based on tautologies represent universally correct methods of reasoning. Their validity depends only on the form of the statements involved and not on the truth values of the variables they contain. Such arguments are called **rules of inference**. The various steps in a mathematical proof of a theorem must follow from the use of various rules of inference, and a mathematical proof of a theorem must begin with the hypotheses, proceed through various steps, each justified by some rule of inference, and arrive at the conclusion.

EXAMPLE 1 According to Theorem 4(j) of the last section, $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ is a tautology. Thus the argument

$$\begin{array}{l} p \Rightarrow q \\ \underline{q \Rightarrow r} \\ \therefore \ p \Rightarrow r \end{array}$$

is universally valid, and so is a rule of inference. ■

EXAMPLE 2 Is the following argument valid?

If you invest in the stock market, then you will get rich.
If you get rich, then you will be happy.
$\therefore$ If you invest in the stock market, then you will be happy.

Solution

The argument is of the form given in Example 1, hence the argument is valid, although the conclusion may be false. ■

EXAMPLE 3 The tautology $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$ is Theorem 2(c), Section 2.2. Thus both of the following arguments are valid.

$$\begin{array}{l} p \Leftrightarrow q \\ \therefore \ (p \Rightarrow q) \wedge (q \Rightarrow p) \end{array} \qquad \begin{array}{l} p \Rightarrow q \\ \underline{q \Rightarrow p} \\ \therefore \ p \Leftrightarrow q \end{array}$$

■

Some mathematical theorems are equivalences; that is, they are of the form $p \Leftrightarrow q$. They are usually stated p if and only if q. By Example 3, the proof of such a theorem is logically equivalent with proving both $p \Rightarrow q$ and $q \Rightarrow p$, and this is almost always the way in which equivalences are proved. We first assume that p is true, and show that q must then be true; next we assume that q is true and show that p must then be true.

A very important rule of inference is

$$\begin{array}{l} p \\ \underline{p \Rightarrow q} \\ \therefore \ q. \end{array}$$

That is, p is true, and $p \Rightarrow q$ is true, so q is true. This follows from Theorem 4(g), Section 2.2.

Some rules of inference were given Latin names by classical scholars. Theorem 4(g) is referred to as **modus ponens**, or loosely, the method of asserting.

EXAMPLE 4 Is the following argument valid?

Smoking is healthy.
If smoking is healthy, then cigarettes are prescribed by physicians.
$\therefore$ Cigarettes are prescribed by physicians.

Solution

The argument is valid since it is of the form modus ponens. However, the conclusion is false. Observe that the first premise p: smoking is healthy is false. The second premise $p \Rightarrow q$ is then true and $(p \wedge (p \Rightarrow q))$, the conjunction of the two premises, is false. ■

EXAMPLE 5 Is the following argument valid?

If taxes are lowered, then income rises.
Income rises.
$\therefore$ Taxes are lowered.

Solution

Let p: taxes are lowered and q: income rises. Then the argument is of the form

$$\begin{array}{l} p \Rightarrow q \\ q \\ \hline \therefore\ p. \end{array}$$

Assume that $p \Rightarrow q$ and q are both true. Now $p \Rightarrow q$ may be true with p being false. Then the conclusion p is false. Hence the argument is not valid. Another approach to answering this question is to verify whether the statement $((p \Rightarrow q) \wedge q)$ logically implies the statement p. A truth table shows this is not the case. (Verify this.) ■

An important proof technique, which is an example of an **indirect method** of proof, follows from the tautology $(p \Rightarrow q) \Leftrightarrow ((\sim q) \Rightarrow (\sim p))$. This states, as we previously mentioned, that an implication is equivalent to its contrapositive. Thus to prove $p \Rightarrow q$ indirectly, we assume q is false (the statement $\sim q$) and show that p is then false (the statement $\sim p$).

EXAMPLE 6 Let n be an integer. Prove that if n^2 is odd, then n is odd.

Solution

Let p: n^2 is odd and q: n is odd. We have to prove that $p \Rightarrow q$ is true. Instead, we prove the contrapositive $\sim q \Rightarrow \sim p$. Thus suppose that n is not odd, so that n is even. Then $n = 2k$, where k is an integer. We have $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, so n^2 is even. We thus show that if n is even, then n^2 is even, which is the contrapositive of the given statement. Hence the given statement has been proved. ■

Another important indirect proof technique is **proof by contradiction**. This method is based on the tautology $((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$. Thus the rule of inference

$$\begin{array}{l} p \Rightarrow q \\ \sim q \\ \hline \therefore\ \sim p \end{array}$$

is valid. Informally, this states that if a statement p implies a false statement q, then p must be false. This is often applied to the case where q is an absurdity or contradiction, that is, a statement that is always false. An example is given by taking q as the contradiction $r \wedge (\sim r)$. Thus any statement that implies a contradiction must be false. In order to use proof by contradiction, suppose we wish to show that a statement q logically follows from statements $p_1, p_2, \ldots, p_n$. Assume that $\sim q$ is true (that is, q is false) as an extra hypothesis, and that $p_1, p_2, \ldots, p_n$ are also true. If this enlarged hypothesis $p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge (\sim q)$ implies a contradiction, then at least one of the statements $p_1, p_2, \ldots, p_n, \sim q$ must be false. This means that if all the p_i's are true, then $\sim q$ must be false, so q must be true. Thus q follows from $p_1, p_2, \ldots, p_n$. This is proof by contradiction.

EXAMPLE 7 Prove there is no rational number p/q whose square is 2. In other words, show $\sqrt{2}$ is irrational.

Solution

This statement is a good candidate for proof by contradiction, because we could not check all possible rational numbers to demonstrate that none had a square equal to 2. Assume $(p/q)^2 = 2$ for some integers p and q, which have no common factors. If the original choice of p/q is not in lowest terms, we can replace it with its equivalent lowest-term form. Then $p^2 = 2q^2$, so p^2 is even. This implies p is even, since the square of an odd number is odd. Thus, $p = 2n$ for some integer n. We see that $2q^2 = p^2 = (2n)^2 = 4n^2$, so $q^2 = 2n^2$. Thus q^2 is even, and so q is even. We now have that both p and q are even, and therefore have a common factor 2. This is a contradiction to the assumption. Thus the assumption must be false. ■

We have presented several rules of inference and logical equivalences that correspond to valid proof techniques. In order to prove a theorem of the (typical) form $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q$, we begin with the hypothesis $p_1, p_2, \ldots, p_n$ and show that some result r_1 logically follows. Then, using $p_1, p_2, \ldots, p_n, r_1$, we show that some other statement r_2 logically follows. We continue this process, producing intermediate statements $r_1, r_2, \ldots, r_k$, called **steps in the proof**, until we can finally show that the conclusion q logically follows from $p_1, p_2, \ldots, p_n, r_1, r_2, \ldots, r_k$. Each logical step must be justified by some valid proof technique, based on the rules of inference we have developed, or on some other rules that come from tautological implications we have not discussed. At any stage, we can replace a statement that needs to be derived by its contrapositive statement, or any other equivalent form.

In practice, the construction of proofs is an art and must be learned in part from observation and experience. The choice of intermediate steps and methods of deriving them is a creative activity that cannot be precisely described. But a few simple techniques are applicable to a wide variety of settings. We will focus on these techniques throughout the book. The "Tips for Proofs" notes at the end of each chapter highlights the methods most useful for that chapter's material.

EXAMPLE 8 Let m and n be integers. Prove that $n^2 = m^2$ if and only if n is m or n is $-m$.

Solution

Let us analyze the proof as we present it. Suppose p is the statement $n^2 = m^2$, q is the statement n is m, and r is the statement n is $-m$. Then we wish to prove the theorem $p \Leftrightarrow (q \vee r)$. We know from previous discussion that we may instead prove s: $p \Rightarrow (q \vee r)$ and t: $(q \vee r) \Rightarrow p$ are true. First, we assume that either q: n is m or r: n is $-m$ is true. If q is true, then $n^2 = m^2$, and if r is true, then $n^2 = (-m)^2 = m^2$, so in either case p is true. We have therefore shown that the implication t: $(q \vee r) \Rightarrow p$ is true.

Now we must prove that s: $p \Rightarrow (q \vee r)$ is true; that is, we assume p and try to prove either q or r. If p is true, then $n^2 = m^2$, so $n^2 - m^2 = 0$. But $n^2 - m^2 = (n-m)(n+m)$. If r_1 is the intermediate statement $(n-m)(n+m) = 0$, we have shown $p \Rightarrow r_1$ is true. We now show that $r_1 \Rightarrow (q \vee r)$ is true, by showing that the contrapositive $\sim(q \vee r) \Rightarrow (\sim r_1)$ is true. Now $\sim(q \vee r)$ is equivalent to $(\sim q) \wedge (\sim r)$, so we show that $(\sim q) \wedge (\sim r) \Rightarrow (\sim r_1)$. Thus, if $(\sim q)$: n is not m and $(\sim r)$: n is not $-m$ are true, then $(n - m) \neq 0$ and $(n + m) \neq 0$, so $(n - m)(n + m) \neq 0$ and r_1 is false. We have therefore shown that $r_1 \Rightarrow (q \vee r)$ is true. Finally, from the truth of $p \Rightarrow r_1$ and $r_1 \Rightarrow (q \vee r)$, we can conclude that $p \Rightarrow (q \vee r)$ is true, and we are done. ■

We do not usually analyze proofs in this detailed manner. We have done so only to illustrate that proofs are devised by piecing together equivalences and valid steps resulting from rules of inference. The amount of detail given in a proof depends on who the reader is likely to be.

As a final remark, we remind the reader that many mathematical theorems actually mean that the statement is true for all objects of a certain type. Sometimes

this is not evident. Thus the theorem in Example 8 really states that for all integers m and n, $n^2 = m^2$ if and only if n is m or n is $-m$. Similarly, the statement "If x and y are real numbers, and $x \neq y$, then $x < y$ or $y < x$" is a statement about all real numbers x and y. To prove such a theorem, we must make sure that the steps in the proof are valid for every real number. We could not assume, for example, that x is 2, or that y is π or $\sqrt{3}$. This is why proofs often begin by selecting a generic element, denoted by a variable. On the other hand, we know from Section 2.2 that the negation of a statement of the form $\forall x\ \mathrm{P}(x)$ is $\exists x \sim \mathrm{P}(x)$, so we need only find a single example where the statement is false to disprove it.

EXAMPLE 9 Prove or disprove the statement that if x and y are real numbers, $(x^2 = y^2) \Leftrightarrow (x = y)$.

Solution

The statement can be restated in the form $\forall x\ \forall y\ \mathrm{R}(x, y)$. Thus, to prove this result, we would need to provide steps, each of which would be true for all x and y. To disprove the result, we need only find one example for which the implication is false.

Since $(-3)^2 = 3^2$, but $-3 \neq 3$, the result is false. Our example is called a **counterexample**, and any other counterexample would do just as well. ■

In summary, if a statement claims that a property holds for all objects of a certain type, then to prove it, we must use steps that are valid for all objects of that type and that do not make references to any particular object. To disprove such a statement, we need only show one counterexample, that is, one particular object or set of objects for which the claim fails.

2.3 Exercises

In Exercises 1 through 11, state whether the argument given is valid or not. If it is valid, identify the tautology or tautologies on which it is based.

1. If I drive to work, then I will arrive tired.
I am not tired when I arrive at work.
$\therefore$ I do not drive to work.

2. If I drive to work, then I will arrive tired.
I arrive at work tired.
$\therefore$ I drive to work.

3. If I drive to work, then I will arrive tired.
I do not drive to work.
$\therefore$ I will not arrive tired.

4. If I drive to work, then I will arrive tired.
I drive to work.
$\therefore$ I will arrive tired.

5. I will become famous or I will not become a writer.
I will become a writer.
$\therefore$ I will become famous.

6. I will become famous or I will be a writer.
I will not be a writer.
$\therefore$ I will become famous.

7. If I try hard and I have talent, then I will become a musician.
If I become a musician, then I will be happy.
$\therefore$ If I will not be happy, then I did not try hard or I do not have talent.

8. If I graduate this semester, then I will have passed the physics course.
If I do not study physics for 10 hours a week, then I will not pass physics.
If I study physics for 10 hours a week, then I cannot play volleyball.
$\therefore$ If I play volleyball, I will not graduate this semester.

9. If my plumbing plans do not meet the construction code, then I cannot build my house.
If I hire a licensed contractor, then my plumbing plans will meet the construction code.
I hire a licensed contractor.
$\therefore$ I can build my house.

10. (a) $p \vee q$, $\sim q$ $\therefore p$ (b) $p \Rightarrow q$, $\sim p$ $\therefore \sim q$

11. Write each argument in Exercise 10 as a single compound statement.

12. (a) $(p \Rightarrow q) \wedge (q \Rightarrow r)$, $(\sim q) \wedge r$ $\therefore p$ (b) $\sim(p \Rightarrow q)$ $\therefore \sim q$

13. Write each argument in Exercise 12 as a single compound statement.

14. Prove that the sum of two even numbers is even.

15. Prove that the sum of two odd numbers is even.

16. Prove that the structure (even integers, +, *) is closed with respect to *.

17. Prove that the structure (odd integers, +, *) is closed with respect to *.

18. Prove that n^2 is even if and only if n is even.

19. Prove that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

20. Let A and B be subsets of a universal set U. Prove that $A \subseteq B$ if and only if $\overline{B} \subseteq \overline{A}$.

21. Show that
(a) $A \subseteq B$ is a necessary and sufficient condition for $A \cup B = B$.
(b) $A \subseteq B$ is a necessary and sufficient condition for $A \cap B = A$.

22. Show that k is odd is a necessary and sufficient condition for k^3 to be odd.

23. Prove or disprove: $n^2 + 41n + 41$ is a prime number for every integer n.

24. Prove or disprove: The sum of any five consecutive integers is divisible by 5.

25. Prove or disprove that $3 \mid (n^3 - n)$ for every positive integer n.

26. Prove or disprove: $1 + 2^n > 3^n$, for all $n \in Z^+$.

27. Determine if the following is a valid argument. Explain your conclusion.

Prove: $\forall x\ x^3 > x^2$.

Proof: $\forall x\ x^2 > 0$ so $\forall x\ x^2(x - 1) > 0(x - 1)$ and $\forall x\ x^3 - x^2 > 0$. Hence $\forall x\ x^3 > x^2$.

28. Determine if the following is a valid argument. Explain your conclusion.

Prove: If $\mathbf{A}$ and $\mathbf{B}$ are matrices such that $\mathbf{AB} = \mathbf{0}$, then either $\mathbf{A} = \mathbf{0}$ or $\mathbf{B} = \mathbf{0}$.

Proof: There are two cases to consider: $\mathbf{A} = \mathbf{0}$ or $\mathbf{A} \neq \mathbf{0}$. If $\mathbf{A} = \mathbf{0}$, then we are done. If $\mathbf{A} \neq \mathbf{0}$, then $\mathbf{A}^{-1}(\mathbf{AB}) = \mathbf{A}^{-1}\mathbf{0}$ and $(\mathbf{A}^{-1}\mathbf{A})\mathbf{B} = \mathbf{0}$ and $\mathbf{B} = \mathbf{0}$.

29. Determine if the following is a valid argument. Explain your conclusion.

Let m and n be two relatively prime integers. Prove that if mn is a cube, then m and n are each cubes.

Proof: We first note that in the factorization of any cube into prime factors, each prime must have an exponent that is a multiple of 3. Write m and n each as a product of primes; $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $n = q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$. Suppose m is not a cube. Then at least one a_i is not a multiple of 3. Since each prime factor of mn must have an exponent that is a multiple of 3, n must have a factor $p_i^{b_i}$ such that $b_i \neq 0$ and $a_i + b_i$ is a multiple of 3. But this means that m and n share a factor, p_i. This contradicts the fact that m and n are relatively prime.

30. Determine if the following is a valid argument. Explain your conclusion.

Prove: If x is an irrational number, then $1 - x$ is also an irrational number.

Proof: Suppose $1 - x$ is rational. Then we can write $1 - x$ as $\frac{a}{b}$, with $a, b \in Z$. Now we have $1 - \frac{a}{b} = x$ and $x = \frac{b - a}{b}$, a rational number. This is a contradiction. Hence, if x is irrational, so is $1 - x$.

31. Prove that the sum of two prime numbers, each larger than 2, is not a prime number.

32. Prove that if two lines are each perpendicular to a third line in the plane, then the two lines are parallel.

33. Prove that if x is a rational number and y is an irrational number, then $x + y$ is an irrational number.

34. Prove that if $2y$ is an irrational number, then y is an irrational number.

2.4 Mathematical Induction

Here we discuss another proof technique. Suppose the statement to be proved can be put in the form $\forall n \geq n_0\ \mathrm{P}(n)$, where n_0 is some fixed integer. That is, suppose we wish to show that $\mathrm{P}(n)$ is true for all integers $n \geq n_0$. The following result shows how this can be done. Suppose that (a) $\mathrm{P}(n_0)$ is true and (b) If $\mathrm{P}(k)$ is true for some $k \geq n_0$, then $\mathrm{P}(k + 1)$ must also be true. Then $\mathrm{P}(n)$ is true for all $n \geq n_0$. This result is called the **principle of mathematical induction**. Thus to prove the truth of a statement $\forall n \geq n_0\ \mathrm{P}(n)$, using the principle of mathematical induction, we must begin by proving directly that the first proposition $\mathrm{P}(n_0)$ is true. This is called the **basis step** of the induction and is generally very easy.

Then we must prove that $P(k) \Rightarrow P(k+1)$ is a tautology for any choice of $k \geq n_0$. Since the only case where an implication is false is if the antecedent is true and the consequent is false, this step is usually done by showing that if $P(k)$ were true, then $P(k+1)$ would also have to be true. Note that this is not the same as assuming that $P(k)$ is true for some value of k. This step is called the **induction step**, and some work will usually be required to show that the implication is always true.

EXAMPLE 1 Show, by mathematical induction, that for all $n \geq 1$,

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

Solution

Let $P(n)$ be the predicate $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$. In this example, $n_0 = 1$.

Basis Step

We must first show that $P(1)$ is true. $P(1)$ is the statement

$$1 = \frac{1(1+1)}{2},$$

which is clearly true.

Induction Step

We must now show that for $k \geq 1$, if $P(k)$ is true, then $P(k+1)$ must also be true. We assume that for some fixed $k \geq 1$,

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}. \tag{1}$$

We now wish to show the truth of $P(k+1)$:

$$1+2+3+\cdots+(k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

The left-hand side of $P(k+1)$ can be written as $1+2+3+\cdots+k+(k+1)$ and we have

$$\begin{aligned}
&(1+2+3+\cdots+k)+(k+1) \\
&\quad = \frac{k(k+1)}{2}+(k+1) && \text{using (1) to replace } 1+2+\cdots+k \\
&\quad = (k+1)\left[\frac{k}{2}+1\right] && \text{factoring} \\
&\quad = \frac{(k+1)(k+2)}{2} \\
&\quad = \frac{(k+1)((k+1)+1)}{2} && \text{the right-hand side of } P(k+1)
\end{aligned}$$

Thus, we have shown the left-hand side of $P(k+1)$ equals the right-hand side of $P(k+1)$. By the principle of mathematical induction, it follows that $P(n)$ is true for all $n \geq 1$. ■

EXAMPLE 2 Let $A_1, A_2, A_3, \ldots, A_n$ be any n sets. We show by mathematical induction that

$$\overline{\left(\bigcup_{i=1}^{n} A_i\right)} = \bigcap_{i=1}^{n} \overline{A_i}.$$

(This is an extended version of one of De Morgan's laws.) Let $P(n)$ be the predicate that the equality holds for any n sets. We prove by mathematical induction that for all $n \geq 1$, $P(n)$ is true.

Basis Step

$P(1)$ is the statement $\overline{A_1} = \overline{A_1}$, which is obviously true.

Induction Step

We use $P(k)$ to show $P(k+1)$. The left-hand side of $P(k+1)$ is

$$\begin{aligned}
\overline{\left(\bigcup_{i=1}^{k+1} A_i\right)} &= \overline{A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}} \\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}} && \text{associative property of } \cup \\
&= \overline{(A_1 \cup A_2 \cup \cdots \cup A_k)} \cap \overline{A_{k+1}} && \text{by De Morgan's law for two sets} \\
&= \left(\bigcap_{i=1}^{k} \overline{A_i}\right) \cap \overline{A_{k+1}} && \text{using } P(k) \\
&= \bigcap_{i=1}^{k+1} \overline{A_i} && \text{right-hand side of } P(k+1)
\end{aligned}$$

Thus, the implication $P(k) \Rightarrow P(k+1)$ is a tautology, and by the principle of mathematical induction $P(n)$ is true for all $n \geq 1$. ■

EXAMPLE 3 We show by mathematical induction that any finite, nonempty set is countable; that is, it can be arranged in a list.

Let $P(n)$ be the predicate that if A is any set with $|A| = n \geq 1$, then A is countable. (See Chapter 1 for definitions.)

Basis Step

Here n_0 is 1, so we let A be any set with one element, say $A = \{x\}$. In this case x forms a sequence all by itself whose set is A, so $P(1)$ is true.

Induction Step

We want to use the statement $P(k)$ that if A is any set with k elements, then A is countable. Now choose any set B with $k+1$ elements and pick any element x in B. Since $B - \{x\}$ is a set with k elements, the induction hypothesis $P(k)$ tells us there is a sequence $x_1, x_2, \ldots, x_k$ with $B - \{x\}$ as its corresponding set. The sequence $x_1, x_2, \ldots, x_k, x$ then has B as the corresponding set so B is countable. Since B can be any set with $k+1$ elements, $P(k+1)$ is true if $P(k)$ is. Thus, by the principle of mathematical induction, $P(n)$ is true for all $n \geq 1$. ■

In proving results by induction, you should not start by assuming that $P(k+1)$ is true and attempting to manipulate this result until you arrive at a true statement. This common mistake is always an incorrect use of the principle of mathematical induction.

A natural connection exists between recursion and induction, because objects that are recursively defined often use a natural sequence in their definition. Induction is frequently the best, maybe the only, way to prove results about recursively defined objects.

EXAMPLE 4

Consider the following recursive definition of the factorial function: $1! = 1$, $n! = n(n-1)!$, $n > 1$. Suppose we wish to prove for all $n \geq 1$, $n! \geq 2^{n-1}$. We proceed by mathematical induction. Let $P(n)$: $n! \geq 2^{n-1}$. Here n_0 is 1.

Basis Step

$P(1)$ is the statement $1! \geq 2^0$. Since $1!$ is 1, this statement is true.

Induction Step

We want to show $P(k) \Rightarrow P(k+1)$ is a tautology. It will be a tautology if $P(k)$ true guarantees $P(k+1)$ is true. Suppose $k! \geq 2^{k-1}$ for some $k \geq 1$. Then by the recursive definition, the left side of $P(k+1)$ is

$$\begin{aligned}(k+1)! &= (k+1)k! \\ &\geq (k+1)2^{k-1} && \text{using } P(k) \\ &\geq 2 \times 2^{k-1} && k+1 \geq 2, \text{ since } k \geq 1 \\ &= 2^k && \text{right-hand side of } P(k+1)\end{aligned}$$

Thus, $P(k+1)$ is true. By the principle of mathematical induction, it follows that $P(n)$ is true for all $n \geq 1$. ■

The following example shows one way in which induction can be useful in computer programming. The pseudocode used in this and following examples is described in Appendix A.

EXAMPLE 5

Consider the following function given in pseudocode.

```
FUNCTION SQ(A)
1. C ← 0
2. D ← 0
3. WHILE (D ≠ A)
     a. C ← C + A
     b. D ← D + 1
4. RETURN (C)
END OF FUNCTION SQ
```

The name of the function, SQ, suggests that it computes the square of A. Step 3b shows A must be a positive integer if the looping is to end. A few trials with particular values of A will provide evidence that the function does carry out this task. However, suppose we now want to prove that SQ always computes the square of the positive integer A, no matter how large A might be. We shall give a proof by mathematical induction. For each integer $n \geq 0$, let C_n and D_n be the values of the variables C and D, respectively, after passing through the WHILE loop n times. In particular, C_0 and D_0 represent the values of the variables before looping starts. Let $P(n)$ be the predicate $C_n = A \times D_n$. We shall prove by induction that $\forall n \geq 0\ P(n)$ is true. Here n_0 is 0.

Basis Step

$P(0)$ is the statement $C_0 = A \times D_0$, which is true since the value of both C and D is zero "after" zero passes through the WHILE loop.

Induction Step

We must now use

$$P(k):\ C_k = A \times D_k \tag{2}$$

to show that $P(k+1)$: $C_{k+1} = A \times D_{k+1}$. After a pass through the loop, C is increased by A, and D is increased by 1, so $C_{k+1} = C_k + A$ and $D_{k+1} = D_k + 1$.

$$\begin{aligned}\text{left-hand side of } P(k+1)\text{: } C_{k+1} &= C_k + A \\ &= A \times D_k + A && \text{using (2) to replace } C_k \\ &= A \times (D_k + 1) && \text{factoring} \\ &= A \times D_{k+1} && \text{right-hand side of } P(k+1)\end{aligned}$$

By the principle of mathematical induction, it follows that as long as looping occurs, $C_n = A \times D_n$. The loop must terminate. (Why?) When the loop terminates, $D = A$, so $C = A \times A$, or A^2, and this is the value returned by the function SQ. ■

Example 5 illustrates the use of a **loop invariant**, a relationship between variables that persists through all iterations of the loop. This technique for proving that loops and programs do what is claimed they do is an important part of the theory of algorithm verification. In Example 5 it is clear that the looping stops if A is a positive integer, but for more complex cases, this may also be proved by induction.

EXAMPLE 6

Use the technique of Example 5 to prove that the pseudocode program given in Section 1.4 does compute the greatest common divisor of two positive integers.

Solution

Here is the pseudocode given earlier.

```
FUNCTION GCD(X, Y)
1. WHILE (X ≠ Y)
     a. IF (X > Y) THEN
          1. X ← X − Y
     b. ELSE
          1. Y ← Y − X
2. RETURN (X)
END OF FUNCTION GCD
```

We claim that if X and Y are positive integers, then GCD returns $\text{GCD}(X, Y)$. To prove this, let X_n and Y_n be the values of X and Y after $n \geq 0$ passes through the WHILE loop. We claim that $P(n)$: $\text{GCD}(X_n, Y_n) = \text{GCD}(X, Y)$ is true for all $n \geq 0$, and we prove this by mathematical induction. Here n_0 is 0.

Basis Step

$X_0 = X$, $Y_0 = Y$, since these are the values of the variables before looping begins; thus $P(0)$ is the statement $\text{GCD}(X_0, Y_0) = \text{GCD}(X, Y)$, which is true.

Induction Step

Consider the left-hand side of $P(k+1)$, that is, $GCD(X_{k+1}, Y_{k+1})$. After the $k+1$ pass through the loop, either $X_{k+1} = X_k$ and $Y_{k+1} = Y_k - X_k$ or $X_{k+1} = X_k - Y_k$ and $Y_{k+1} = Y_k$. Then if $P(k)$: $GCD(X_k, Y_k) = GCD(X, Y)$ is true, we have, by Theorem 5, Section 1.4, that $GCD(X_{k+1}, Y_{k+1}) = GCD(X_k, Y_k) = GCD(X, Y)$. Thus, by the principle of mathematical induction, $P(n)$ is true for all $n \geq 0$. The exit condition for the loop is $X_n = Y_n$ and we have $GCD(X_n, Y_n) = X_n$. Hence the function always returns the value $GCD(X, Y)$. ■

■ Strong Induction

A slightly different form of mathematical induction is easier to use in some proofs. In the **strong form of mathematical induction**, or strong induction, the induction step is to show that

$$P(n_0) \wedge P(n_0+1) \wedge P(n_0+2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$$

is a tautology. As before, the only case we need to check is that if each $P(j)$, $j = n_0, \ldots, k$, is true, then $P(k+1)$ is true. The strong form of induction is equivalent to the form we first presented so it is a matter of convenience which one we use in a proof.

EXAMPLE 7

Prove that every positive integer $n > 1$ can be written uniquely as $p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where the p_i are primes and $p_1 < p_2 < \cdots < p_s$ (Theorem 3, Section 1.4).

Proof (by strong induction)

Basis Step

Here n_0 is 2. $P(2)$ is clearly true, since 2 is prime.

Induction Step

We use $P(2), P(3), \ldots, P(k)$ to show $P(k+1)$: $k+1$ can be written uniquely as $p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where the p_i are primes and $p_1 < p_2 < \cdots < p_s$. There are two cases to consider. If $k+1$ is a prime, then $P(k+1)$ is true. If $k+1$ is not prime, then $k+1 = lm$, $2 \leq l \leq k$, $2 \leq m \leq k$. Using $P(l)$ and $P(m)$, we have $k = lm = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t} r_1^{c_1} r_2^{c_2} \cdots r_u^{c_u} = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where each $p_i = q_j$ or r_k, $p_1 < p_2 < \cdots < p_s$, and if $q_j = r_k = p_i$, then $a_i = b_j + c_k$, otherwise $p_i = q_j$ and $a_i = b_j$ or $p_i = r_k$ and $a_i = c_k$. Since the factorization of l and m are unique, so is the factorization of $k+1$. ■

2.4 Exercises

In Exercises 1 through 7, prove the statement is true by using mathematical induction.

1. $2 + 4 + 6 + \cdots + 2n = n(n+1)$
2. $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(2n+1)(2n-1)}{3}$
3. $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$
4. $5 + 10 + 15 + \cdots + 5n = \dfrac{5n(n+1)}{2}$
5. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
6. $1 + a + a^2 + \cdots + a^{n-1} = \dfrac{a^n - 1}{a - 1}$
7. $a + ar + ar^2 + \cdots + ar^{n-1} = \dfrac{a(1-r^n)}{1-r}$ for $r \neq 1$
8. Let $P(n)$: $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2 + 4}{4}$.
   (a) Use $P(k)$ to show $P(k+1)$.
   (b) Is $P(n)$ true for all $n \geq 1$?

9. Let $P(n)$: $1 + 5 + 9 + \cdots + (4n-3) = (2n+1)(n-1)$.
   (a) Use $P(k)$ to show $P(k+1)$.
   (b) Is $P(n)$ true for all $n \geq 1$?
10. Prove $1 + 2^n < 3^n$ for $n \geq 2$.
11. Prove $n < 2^n$ for $n > 1$.
12. Prove $1 + 2 + 3 + \cdots + n < \dfrac{(2n+1)^2}{8}$
13. Find the least n for which the statement is true and then prove that $(1 + n^2) < 2^n$.
14. Find the least n for which the statement is true and then prove that $10n < 3^n$.
15. Prove by mathematical induction that if a set A has n elements, then $P(A)$ has 2^n elements.
16. Prove by mathematical induction that $3 \mid (n^3 - n)$ for every positive integer n.
17. Prove by mathematical induction that if $A_1, A_2, \ldots, A_n$ are any n sets, then
$$\overline{\left(\bigcap_{i=1}^{n} A_i\right)} = \bigcup_{i=1}^{n} \overline{A_i}.$$
18. Prove by mathematical induction that if $A_1, A_2, \ldots, A_n$ and B are any $n+1$ sets, then
$$\left(\bigcup_{i=1}^{n} A_i\right) \bigcap B = \bigcup_{i=1}^{n} (A_i \cap B).$$
19. Prove by mathematical induction that if $A_1, A_2, \ldots, A_n$ and B are any $n+1$ sets, then
$$\left(\bigcap_{i=1}^{n} A_i\right) \bigcup B = \bigcap_{i=1}^{n} (A_i \cup B).$$
20. Let $P(n)$ be the statement $2 \mid (2n-1)$.
   (a) Prove that $P(k) \Rightarrow P(k+1)$ is a tautology.
   (b) Show that $P(n)$ is not true for any integer n.
   (c) Do the results in (a) and (b) contradict the principle of mathematical induction? Explain.
21. Let $P(n)$ be the statement $n^2 + n$ is an odd number for $n \in Z^+$.
   (a) Prove that $P(k) \Rightarrow P(k+1)$ is a tautology.
   (b) Is $P(n)$ true for all n? Explain.
22. Explain the flaw in the following "argument."

    For $z \neq 0$, $z^n = 1$, $n \geq 0$.
    Proof: ***Basis Step***: For $n = 0$, P(0): $z^n = 1$ is true by definition.
    Induction Step: $z^{k+1} = \dfrac{z^k}{z^{k-1}} \cdot z^k = \dfrac{1}{1} \cdot 1$ or 1.
23. Explain the flaw in the following "argument."

    All trucks are the same color.
    Proof: Let $P(n)$: Any set of n trucks consists of trucks of the same color.
    Basis Step: Certainly $P(1)$ is true, since there is only one truck in this case.
    Induction Step: We use $P(k)$: Any set of k trucks consists of trucks of the same color to show $P(k+1)$: Any set of $k+1$ trucks consists of trucks of the same color. Choose one truck from the set of $k+1$ trucks and consider the remaining set of k trucks. By $P(k)$ these are all the same color. Now return the chosen truck and set aside another truck. The remaining trucks are all the same color by $P(k)$. But trucks do not change color in this procedure, so all $k+1$ trucks must be the same color.

In Exercises 24 through 26, prove the given statement about matrices. Assume $\mathbf{A}$ *is* $n \times n$.

24. $(\mathbf{A}_1 + \mathbf{A}_2 + \cdots + \mathbf{A}_n)^T = \mathbf{A}_1^T + \mathbf{A}_2^T + \cdots + \mathbf{A}_n^T$
25. $\mathbf{A}^2\mathbf{A}^n = \mathbf{A}^{2+n}$
26. Let $\mathbf{A}$ and $\mathbf{B}$ be square matrices. If $\mathbf{AB} = \mathbf{BA}$, then $(\mathbf{AB})^n = \mathbf{A}^n\mathbf{B}^n$, for $n \geq 1$.
27. Prove that any restaurant bill of $\$n$, $n \geq 5$, can be paid exactly using only \$2 and \$5 bills.
28. Prove that every integer greater than 27 can be written as $5a + 8b$, where $a, b \in Z^+$.
29. Use induction to show that if p is a prime and $p \mid a^n$ for $n > 1$, then $p \mid a$.
30. Prove that if $GCD(a, b) = 1$, then $GCD(a^n, b^n) = 1$ for all $n \geq 1$. (*Hint*: Use Exercise 29.)
31. (a) Find the smallest positive integer n_0 such that $2^{n_0} > n_0^2$.
    (b) Prove $2^n > n^2$ for all $n \geq n_0$.
32. Prove or disprove: $2 + 8 + 18 + \cdots + 2n^2 = n^2 + n$.
33. Prove or disprove: $x - y$ divides $x^n - y^n$ for $n \geq 1$.

In Exercises 34 through 39, show that the given algorithm, correctly used, produces the output stated, by using mathematical induction to prove the relationship indicated is a loop invariant and checking values when the looping stops. All variables represent nonnegative integers.

34.
```
SUBROUTINE COMP(X, Y; Z)
1. Z ← X
2. W ← Y
3. WHILE (W > 0)
       a. Z ← Z + Y
       b. W ← W - 1
4. RETURN
END OF SUBROUTINE COMP
COMPUTES: Z = X + Y²
LOOP INVARIANT: (Y × W) + Z = X + Y²
```

35.
```
SUBROUTINE DIFF (X, Y; Z)
1. Z ← X
2. W ← Y
3. WHILE (W > 0)
       a. Z ← Z - 1
       b. W ← W - 1
```

```
    4. RETURN
    END OF SUBROUTINE DIFF
    COMPUTES: Z = X - Y
    LOOP INVARIANT: X - Z + W = Y
```

```
36. SUBROUTINE EXP2 (N,M;R)
    1. R ← 1
    2. K ← 2M
    3. WHILE (K > 0)
           a. R ← R × N
           b. K ← K - 1
    4. RETURN
    END OF SUBROUTINE EXP2
    COMPUTES: R = N^2M
    LOOP INVARIANT: R × N^K = N^2M
```

```
37. SUBROUTINE POWER (X,Y;Z)
    1. Z ← 0
    2. W ← Y
    3. WHILE (W > 0)
           a. Z ← Z + X
           b. W ← W - 1
    4. W ← Y - 1
    5. U ← Z
    6. WHILE (W > 0)
           a. Z ← Z + U
           b. W ← W - 1
    7. RETURN
    END OF SUBROUTINE POWER
    COMPUTES: Z = X × Y^2
    LOOP INVARIANT (first loop):
    X + (X × W) = X × Y
    LOOP INVARIANT (second loop):
    X + (X × Y × W) = X × Y^2
    (Hint: Use the value of Z at the end of the first loop in
    loop 2.)
```

```
38. SUBROUTINE DIV(X,Y)
    1. IF (Y = 0) THEN
           a. PRINT ('error Y = 0')
    2. ELSE
           a. R ← X
           b. K ← 0
           c. WHILE (K ≥ Y)
                  1. R ← R - Y
                  2. K ← K + 1
           d. IF (R = 0) THEN
                  1. PRINT ('true')
           e. ELSE
                  1. PRINT ('false')
    3. RETURN
    END OF SUBROUTINE DIV
    COMPUTES: TRUTH VALUE OF Y | X.
    LOOP INVARIANT: R + K × Y = X
```

```
39. SUBROUTINE SQS(X,Y;Z)
    1. Z ← Y
    2. W ← X
    3. WHILE (W > 0)
           a. Z ← Z + X
           b. W ← W - 1
    4. W ← Y - 1
    5. WHILE (W > 0)
           a. Z ← Z + X
           b. W ← W - 1
    6. RETURN
    END OF SUBROUTINE SQS
    COMPUTES: Z = X^2 × Y^2
    LOOP INVARIANT (first loop):
    Z + (X × W) = Y + X^2
    LOOP INVARIANT (second loop):
    Z + (Y × W) = X^2 + Y^2
```

Tips for Proofs

This chapter provides the formal basis for our proofs, although most proofs are not so formal as the patterns given in Section 2.3. Two new types of proofs are presented: indirect proofs and induction proofs. Indirect proofs are based either on the pattern $(p \Rightarrow q) \wedge \sim q$ (proof by contradiction) or on the fact that $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$ (prove the contrapositive). There are no hard and fast rules about when to use a direct or indirect proof. One strategy is to proceed optimistically with a direct proof. If that does not lead to anything useful, you may be able to identify a counterexample if the statement is in fact false or start a new proof based on one of the indirect models. Where the difficulty occurs in the attempted direct proof can often point the way to go next. Remember that a certain amount of creativity is required for any proof.

Tips for Proofs (Continued)

Statements that are good candidates for proof by induction are ones that involve the counting or whole numbers in some way, either to count something or to describe a pattern. Examples of these are in Section 2.4, Exercises 11 and 15. Notice that for most of the induction proofs in Section 2.4, P(k) is used early and then properties of operations and arithmetic are used, but in proving loop invariants, the "arithmetic" comes first, then the use of P(k).

In proving statements about propositions, try to use the properties of logical operations (see Section 2.2, Theorem 1 for some of these). Building truth tables should be your second-choice strategy.

Key Ideas for Review

- Statement: declarative sentence that is either true or false, but not both
- Propositional variable: letter denoting a statement
- Compound statement: statement obtained by combining two or more statements by a logical connective
- Logical connectives: not ($\sim$), and ($\wedge$), or ($\vee$), if then ($\Rightarrow$), if and only if ($\Leftrightarrow$)
- Conjunction: $p \wedge q$ (p and q)
- Disjunction: $p \vee q$ (p or q)
- Predicate (propositional function): a sentence of the form P(x)
- Universal quantification: $\forall x$ P(x) [For all values of x, P(x) is true.]
- Existential quantification: $\exists x$ P(x) [There exists an x such that P(x) is true.]
- Conditional statement or implication: $p \Rightarrow q$ (if p then q); p is the antecedent or hypothesis and q is the consequent or conclusion
- Converse of $p \Rightarrow q$: $q \Rightarrow p$
- Contrapositive of $p \Rightarrow q$: $\sim q \Rightarrow \sim p$
- Equivalence: $p \Leftrightarrow q$
- Tautology: a statement that is true for all possible values of its propositional variables
- Absurdity: a statement that is false for all possible values of its propositional variables
- Contingency: a statement that may be true or false, depending on the truth values of its propositional variables
- $p \equiv q$ (Logically equivalent statements p and q): $p \Leftrightarrow q$ is a tautology
- Methods of proof:
  - q logically follows from p: see page 62
  - Rules of inference: see page 62
  - Modus ponens: see page 63
  - Indirect method: see page 64
  - Proof by contradiction: see page 64
- Counterexample: single instance that disproves a theorem or proposition
- Principle of mathematical induction: Let n_0 be a fixed integer. Suppose that for each integer $n \geq n_0$ we have a proposition P(n). Suppose that (a) P(n_0) is true and (b) If P(k), then P($k+1$) is a tautology for every $k \geq n_0$. Then the principle of mathematical induction states that P(n) is true for all $n \geq n_0$.
- Loop invariant: a statement that is true before and after every pass through a programming loop
- Strong form of mathematical induction: see page 72

Review Questions

1. Why is it important to recognize the converse and the contrapositive of a conditional statement?
2. How does the strong form of induction differ from basic mathematical induction?
3. What mathematical structure previously studied has the same properties as (logical statements, $\vee$, $\wedge$, $\sim$)?
4. How does an indirect proof technique differ from a direct proof?
5. What is the structure of a proof by contradiction?

Chapter 2 Self-Test

1. Determine the truth value of the given statements if p is true and q is false.
   (a) $\sim p \wedge q$ (b) $\sim p \vee \sim q$
2. Determine the truth value for each of the following statements. Assume $x, y \in Z$.
   (a) $\forall x, y$ $x + y$ is even.

(b) $\exists x \forall y\ x + y$ is even.

3. Make a truth table for $(p \wedge \sim p) \vee (\sim(q \wedge r))$.

For Problems 4 through 6, let p: $1 < -1$, q: $|2| = |-2|$, r: $-3 < -1$, *and* s: $1 < 3$.

4. Write the symbolic version of the converse and of the contrapositive for each of the following propositions.

(a) $p \Rightarrow q$

(b) $(\sim r) \vee (\sim s) \Rightarrow q$

(c) $q \Rightarrow p \vee s$

5. Write the converse and the contrapositive of the propositions in Problem 4 as English sentences.

6. Give the truth value of each proposition in Problem 4.

7. The English word "or" is sometimes used in the exclusive sense meaning that either p or q, but not both, is true. Make a truth table for this exclusive or, *xor*.

8. Let p: An Internet business is cheaper to start, q: I will start an Internet business, and r: An Internet business makes less money. For each of the following write the argument in English sentences and also determine the validity of the argument.

(a)
$$\begin{array}{l} r \Rightarrow (q \Rightarrow p) \\ \sim p \\ \hline \therefore\ (\sim r) \vee (\sim q) \end{array}$$

(b)
$$\begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \\ \hline \therefore\ r \end{array}$$

9. Suppose that m and n are integers such that $n \mid m$ and $m \mid n$. Are these hypotheses sufficient to prove that $m = n$? If so, give a proof. If not, supply a simple additional hypothesis that will guarantee $m = n$ and provide a proof.

10. Prove or disprove by giving a counterexample that the sum of any three consecutive odd integers is divisible by 6.

11. Use mathematical induction to prove that $4^n - 1$ is divisible by 3.

12. Use mathematical induction to prove that

$$1 + 2 + 3 + \cdots + n < \frac{(n+1)^2}{2}.$$

Coding Exercises

For each of the following, write the requested program or subroutine in pseudocode (as described in Appendix A) or in a programming language that you know. Test your code either with a paper-and-pencil trace or with a computer run.

1. Write a program that will print a truth table for $p \wedge \sim q$.

2. Write a program that will print a truth table for $(p \vee q) \Rightarrow r$.

3. Write a program that will print a truth table for any two-variable propositional function.

4. Write a subroutine EQUIVALENT that determines if two logical expressions are equivalent.

5. Write a subroutine that determines if a logical expression is a tautology, a contingency, or an absurdity.

Experiment 2

Many games and puzzles use strategies based on the rules of mathematical logic developed in Chapter 2. We begin here with a simple puzzle situation: Construct an object from beads and wires that satisfies some given conditions. After investigating this object, you will prove that it satisfies certain properties.

Part I. Here are the conditions for the first object.

(a) You must use exactly three beads.

(b) There is exactly one wire between every pair of beads.

(c) Not all beads can be on the same wire.

(d) Any pair of wires has at least one bead in common.

1. Draw a picture of the object.

2. Your object might not be the only one possible, so the following statements are to be proved referring only to the conditions and not to your object.

T1. Any two wires have at most one bead in common.

T2. There are exactly three wires.

T3. No bead is on all the wires.

Part II. Here are the conditions for the second object.

(a) You must use at least one bead.

(b) Every wire has exactly two beads on it.

(c) Every bead is on exactly two wires.

(d) Given a wire, there are exactly three other distinct wires that have no beads in common with the given wire.

1. Draw a picture of the object.

2. Your object might not be the only one possible, so the following statements are to be proved referring only to the conditions and not to your object.

T1. There is at least one wire.

T2. Given a wire, there are exactly two other wires that have a bead in common with the given wire.

T3. There are exactly ____ wires.

T4. There are exactly ____ beads.

Part III. The two objects you created in Parts I and II can be viewed in a number of ways. Instead of beads and wires, consider players and two-person teams, or substitute the words point and line for bead and wire.

1. Translate the statements T1, T2, and T3 in Part I into statements about players and two-person teams.

2. Translate the conditions (a)–(d) given in Part II into statements about points and lines.

3. The type of object created here is often called a finite geometry, because each has a finite number of points and lines. What common geometric concept is described in condition (d) of Part II?

4. The Acian Bolex Tournament will be played soon. Determine the number of players needed and the number of teams that will be formed according to these ancient rules for bolex.

(a) A team must consist of exactly three players.

(b) Two players may be on at most one team in common.

(c) Each player must be on at least three teams.

(d) Not all the players can be on the same team.

(e) At least one team must be formed.

(f) If a player is not on a given team, then the player must be on exactly one team that has no members in common with the given team.