

chapter 3



LOGIC

GOALS

In this chapter, we will introduce some of the basic concepts of mathematical logic. In order to fully understand some of the later concepts in this book, you must be able to recognize valid logical arguments. Although these arguments will usually be applied to mathematics, they employ the same techniques that are used by a lawyer in a courtroom or a physician examining a patient. An added reason for the importance of this chapter is that the circuits that make up digital computers are designed using the same algebra of propositions that we will be discussing.

3.1 Propositions and Logical Operators

PROPOSITIONS

Definition: Proposition. A proposition is a sentence to which one and only one of the terms true or false can be meaningfully applied.

Example 3.1.1. "Four is even," " $4 \in \{1, 3, 5\}$," and " $43 > 21$ " are propositions.

In traditional logic, a declarative statement with a definite truth value is considered a proposition. Although our ultimate aim is to discuss mathematical logic, we won't separate ourselves completely from the traditional setting. This is natural because the basic assumptions, or postulates, of mathematical logic are modeled after the logic we use in everyday speech. Since compound sentences are frequently used in everyday speech, we expect that logical propositions contain connectives like the word and. The statement "Europa supports life or Mars supports life" is a proposition and, hence, must have a definite truth value. Whatever that truth value is, it should be the same as the truth value of "Mars supports life or Europa supports life."

LOGICAL OPERATORS

There are several ways in which we commonly combine simple statements into compound ones. The words/phrases *and*, *or*, *not*, *if... then*, and *if and only if* can be added to one or more propositions to create a new proposition. To avoid any confusion, we will precisely define each one's meaning and introduce its standard symbol. With the exception of negation (not), all of the operators act on pairs of propositions. Since each proposition has two possible truth values, there are four ways that truth can be assigned to two propositions. In defining the effect that a logical operator has on two propositions, the result must be specified for all four cases. The most convenient way of doing this is with a truth table, which we will illustrate by defining the word *and*.

Conjunction

Definition: Conjunction (And). If p and q are propositions, their conjunction, p and q (denoted $p \wedge q$), is defined by the truth table in Table 3.1.1.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Table 3.1.1. Truth Table for And

Notes:

- (a) To read this truth table, you must realize that any one line represents a case: one possible set of values for p and q .
- (b) The numbers 0 and 1 are used to denote false and true, respectively. This is consistent with the way that many programming languages treat logical, or Boolean, variables since a single bit, 0 or 1, can represent a truth value. Although *Mathematica*'s logical expressions have a value of True or False, there is a built in function called `Boole` which converts the value to 1 or 0, if desired.

`{Boole[False], Boole[True]}`

`{0, 1}`

- (c) For each case, the symbol under p represents the truth value of p . The same is true for q . The symbol under $p \wedge q$ represents the truth value of $p \wedge q$ for that case. For example, the second row of the truth table represents the case in which p is false, q is true, and the resulting truth value for $p \wedge q$ is false. As in everyday speech, $p \wedge q$ is true only when both propositions are true.
- (d) Just as the letters x , y , and z are frequently used in algebra to represent numeric variables, p , q , and r seem to be the most commonly used symbols for logical variables. When we say that p is a logical variable, we mean that any proposition can take the place of p .
- (e) One final comment: The order in which we list the cases in a truth table is standardized in this book. If the truth table involves two simple propositions, the numbers under the simple propositions can be interpreted as the two-digit binary integers in increasing order, 00, 01, 10, and 11, for 0, 1, 2, and 3.

Disjunction

Definition: Disjunction (Or). If p and q are propositions, their disjunction is p or q , denoted $p \vee q$, and is defined by the truth table in Table 3.1.2.

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Table 3.1.2. Truth Table for Or

Chapter 3 - Logic

Note; The only case in which disjunction is false is when both propositions are false. This interpretation of the word or is called the nonexclusive *or*. The exclusive or will be discussed when we consider logical design in Chapter 13.

Negation

Definition: Negation (Not). If p is a proposition, its negation, not p , is denoted $\neg p$ and is defined by the truth table in Table 3.1.3.

p	$\neg p$
0	1
1	0

Table 3.1.3 Truth Table for *Not*

Note: Negation is the only standard operator that acts on a single proposition; hence only two cases are needed.

The Conditional Operator (*If . . . then*).

Consider the following propositions from everyday speech:

- (a) I'm going to quit if I don't get a raise.
- (b) If I pass the final, then I'll graduate.
- (c) I'll be going to the movies provided that my car starts.

All three propositions are conditional, they can all be restated to fit into the form if *Condition*, then *Conclusion*. For example, statement (a) can be rewritten as "If I don't get a raise, then I'm going to quit."

A conditional statement is meant to be interpreted as a guarantee; if the condition is true, then the conclusion is expected to be true. It says no more and no less.

Definition: Conditional Operator. The conditional statement if p then q , denoted $p \rightarrow q$, is defined by the truth table in Table 3.1.4.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Table 3.1.4 Truth Table for *If... then*

Example 3.1.2. Assume your instructor told you "If you receive a grade of 95 or better in the final examination, then you will receive an A in this course." Your instructor has made a promise to you (placed a condition with you). If you fulfill his condition you expect the conclusion (getting an A) to be forthcoming. Your graded final has been returned to you. Has your instructor told the truth (kept the promise) or is your instructor guilty of a falsehood?

Case I: Your final exam score was less than 95 (the condition is false) and you did not receive an A (the conclusion is false). The instructor told the truth.

Case II: Your final exam score was less than 95, yet you received an A for the course. The instructor told the truth. (Perhaps your overall course average was excellent.)

Case III: Your final exam score was greater than 95, but you did not receive an A. The instructor lied.

Case IV: Your final exam score was greater than 95, and you received an A. The instructor told the truth.

To sum up, the only case in which a conditional proposition is false is when the condition is true and the conclusion is false.

The order of the condition and conclusion in a conditional proposition is important. If the condition and conclusion are exchanged, a different proposition is produced.

Definition: Converse. The converse of the proposition $p \rightarrow q$ is the proposition $q \rightarrow p$.

The converse of "If you receive a grade of 95 or better in the final exam, then you will receive an A in this course," is "If you receive an A in this course, then you received a grade of 95 or better in the final exam." It should be clear that these two statements say different things.

Definition: Biconditional Operator (...if and only if...). If p and q are propositions, the biconditional statement " p if and only if q ," denoted $p \leftrightarrow q$, is defined by the truth table in Table 3.1.5.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Table 3.1.5 Truth table for "... if and only if..."

Note that $p \leftrightarrow q$ is true when p and q have the same truth values. It is common to abbreviate "if and only if" to "iff."

Chapter 3 - Logic

Although "if . . . then" and "if and only if" are frequently used in everyday speech, there are several alternate forms that you should be aware of. They are summarized in the following list:

Conditional

If p then q .

p implies q .

q follows from p .

p , only if q .

q , if p .

p is sufficient for q .

q is necessary for p .

Biconditional

p if and only if q .

p is necessary and sufficient for q .

p is equivalent to q .

If p , then q , and if q , then p .

If p , then q and conversely.

EXERCISES FOR SECTION 3.1

A Exercises

1. Let d = "I like discrete structures" c = "I will pass this course" s = "I will do my assignments" Express each of the following propositions in symbolic form:

- (a) I like discrete structures and I will pass this course.
- (b) I will do my assignments or I will not pass this course.
- (c) It is not true that I like discrete structures and I will do my assignments.
- (d) I will not do my assignment and I will not pass this course.

2. For each of the following propositions, identify simple propositions, express the compound proposition in symbolic form, and determine whether it is true or false:

- (a) The world is flat or zero is an even integer.
- (b) If 432,802 is a multiple of 4, then 432,802 is even.
- (c) 5 is a prime number and 6 is not divisible by 4.
- (d) $3 \in \mathbb{Z}$ and $3 \in \mathbb{Q}$.
- (e) $2/3 \in \mathbb{Z}$ and $2/3 \in \mathbb{Q}$.
- (f) The sum of two even integers is even and the sum of two odd integers is odd.

3. Let p = " $2 < 5$," q = "8 is an even integer," and r = "11 is a prime number." Express the following as a statement in English and determine whether the statement is true or false:

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

4. Rewrite each of the following statements using the other conditional forms:

Chapter 3 - Logic

- (a) If an integer is a multiple of 4, then it is even.
 - (b) The fact that a polygon is a square is a sufficient condition that it is a rectangle.
 - (c) If $x = 5$, then $x^2 = 25$.
 - (d) If $x^2 - 5x + 6 = 0$, then $x = 2$ or $x = 3$.
 - (e) $x^2 = y^2$ is a necessary condition for $x = y$.
5. Write the converse of the propositions in exercise 4. Compare the truth of each proposition and its converse.

3.2 Truth Tables and Propositions Generated by a Set

Consider the compound proposition $c = (p \wedge q) \vee (\neg q \wedge r)$, where p , q , and r are propositions. This is an example of a proposition generated by p , q , and r . We will define this terminology later in the section. Since each of the three simple propositions has two possible truth values, it follows that there are eight different combinations of truth values that determine a value for c . These values can be obtained from a truth table for c . To construct the truth table, we build c from p , q , and r and from the logical operators. The result is Table 3.2.1. Strictly speaking, the first three columns and the last column make up the truth table for c . The other columns are work space needed to build up to c .

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	0	1	0	0
1	0	1	0	1	1	1
1	1	0	1	0	0	1
1	1	1	1	0	0	1

Table 3.2.1 Truth Table for $c = (p \wedge q) \vee (\neg q \wedge r)$

Note that the first three columns of the truth table are an enumeration of the eight three-digit binary integers. This standardizes the order in which the cases are listed. In general, if c is generated by n simple propositions, then the truth table for c will have 2^n rows with the first n columns being an enumeration of the n digit binary integers. In our example, we can see at a glance that for exactly four of the eight cases, c will be true. For example, if p and r are true and q is false (the sixth case), then c is true.

Let S be any set of propositions. We will give two definitions of a proposition generated by S . The first is a bit imprecise, but should be clear. The second definition is called a *recursive definition*. If you find it confusing, use the first definition and return to the second later.

Definition: Proposition Generated by S .

(1) A proposition generated by S is any valid combination of propositions in S with conjunction, disjunction, and negation.

(2) (a) If $p \in S$, then p is a proposition generated by S .

(b) If x and y are propositions generated by S , then so are (x) , $\neg x$, $x \vee y$, and $x \wedge y$.

Note: We have not included the conditional and biconditional in the definition because they can both be obtained from conjunction, disjunction, and negation, as we will see later.

If S is a finite set, then we may use slightly different terminology. For example, if $S = \{p, q, r\}$, we might say that a proposition is generated by p , q , and r instead of $\{p, q, r\}$.

Hierarchy of Logical Operations

It is customary to use the following hierarchy for interpreting propositions, with parentheses overriding this order:

First: Negation

Second: Conjunction

Third: Disjunction

Within any level of the hierarchy, work from left to right. Using these rules, $p \wedge q \vee r$ is taken to mean $(p \wedge q) \vee r$. These precedence rules are universal, and are exactly those used by computer languages to interpret logical expressions.

Example 3.2.1. A few shortened expressions and their fully parenthesized versions:

(a) $p \wedge q \wedge r$ is $(p \wedge q) \wedge r$.

(b) $\neg p \vee \neg r$ is $(\neg p) \vee (\neg r)$.

(c) $\neg \neg p$ is $\neg(\neg p)$.

A proposition generated by a set S need not include each element of S in its expression. For example, $\neg q \wedge r$ is a proposition generated by p , q , and r .

EXERCISES FOR SECTION 3.2

A Exercises

1. Construct the truth tables of:

(a) $p \vee p$

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

(c) $p \vee (\neg p)$

Chapter 3 - Logic

(d) $p \wedge p$

2. Construct the truth tables of:

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

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

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

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

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

(f) $p \vee q \vee r \vee s$

3. Rewrite the following with as few extraneous parentheses as possible:

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

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

4. In what order are the operations in the following propositions performed?

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

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

5. Determine the number of rows in the truth table of a proposition containing four variables p , q , r , and s .

6. If there are 45 lines on a sheet of paper, and you want to reserve one line for each line in a truth table, how large could $|S|$ be if you can write truth tables of propositions generated by S on a sheet of paper?

3.3 Equivalence and Implication

Tautologies & Contradictions

Consider two propositions generated by p and q : $\neg(p \wedge q)$ and $\neg p \vee \neg q$. At first glance, they are different propositions. In form, they are different, but they have the same meaning. One way to see this is to substitute actual propositions for p and q ; such as:

p : I've been to Toronto; and q : I've been to Chicago.

Then $\neg(p \wedge q)$ translates to "I haven't been to both Toronto and Chicago," while $\neg p \vee \neg q$ is "I haven't been to Toronto or I haven't been to Chicago." Determine the truth values of these propositions. Naturally, they will be true for some people and false for others. What is important is that no matter what truth values they have, $\neg(p \wedge q)$ and $\neg p \vee \neg q$ will have the same truth value. The easiest way to see this is by examining the truth tables of these propositions ().

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

Table 3.3.1 Truth tables of $\neg(p \wedge q)$ and $\neg p \vee \neg q$.

In all four cases, $\neg(p \wedge q)$ and $\neg p \vee \neg q$ have the same truth value. Then when the biconditional operator is applied to them, the result is a value of true in all cases.

Definition: Tautology. An expression involving logical variables that is true in all cases is called a tautology.

Example 3.3.1. All of the following are tautologies because their truth tables consist of a column of 1's.

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

Definition: Contradiction. An expression involving logical variables that is false for all cases is called a contradiction.

Example 3.3.2. $p \wedge \neg p$ and $(p \vee q) \wedge (\neg p) \wedge (\neg q)$ are contradictions.

Equivalence

Definition: Equivalence. Let S be a set of propositions and let r and s be propositions generated by S . r and s are equivalent if and only if $r \leftrightarrow s$ is a tautology. The equivalence of r and s is denoted $r \Leftrightarrow s$.

Example 3.3.3. The following are all equivalences:

- (a) $(p \wedge q) \vee (\neg p \wedge \neg q) \Leftrightarrow q$.
- (b) $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$
- (c) $p \vee q \Leftrightarrow q \vee p$.

All tautologies are equivalent to one another. We will use the number 1 to symbolize a tautology.

Example 3.3.4. $p \vee \neg p \Leftrightarrow 1$.

All contradictions are equivalent to one another. We will use the number 0 to symbolize a contradiction.

Example 3.3.5. $p \wedge \neg p \Leftrightarrow 0$.

Equivalence is to logic what equality is to algebra. Just as there are many ways of writing an algebraic expression, the same logical meaning can be expressed in many different ways.

IMPLICATION

Example 3.3.6. Consider the two propositions:

x : The money is behind Door A; and

y : The money is behind Door A or Door B.

Chapter 3 - Logic

Imagine that you were told that there is a large sum of money behind one of two doors marked A and B, and that one of the two propositions x and y is true and the other is false. Which door would you choose? All that you need to realize is that if x is true, then y will also be true. Since we know that this can't be the case, y must be the true proposition and the money is behind Door B.

This is an example of a situation in which the truth of one proposition leads to the truth of another. Certainly, y can be true when x is false; but x can't be true when y is false. In this case, we say that x implies y .

Look at the truth table of $p \rightarrow q$ in Table 3.1.4 (copied below). If p implies q , then the third case can be ruled out, since it is the case that makes a conditional proposition false.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Definition: Implication. Let S be a set of propositions and let r and s be propositions generated by S . We say that r implies s if $r \rightarrow s$ is a tautology. We write $r \Rightarrow s$ to indicate this implication.

Example 3.3.7. A commonly used implication is that p implies $p \vee q$, which is verified by the truth table in Table 3.3.2.

p	q	$p \vee q$	$p \rightarrow p \vee q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	1	1

Table 3.3.2 Truth Table for $p \rightarrow (p \vee q)$

If we let p represent "The money is behind Door A" and q represent "The money is behind Door B," $p \Rightarrow (p \vee q)$ is a formalized version of the reasoning used in Example 3.3.6. A common name for this implication is disjunctive addition. In the next section we will consider some of the most commonly used implications and equivalences.

When we defined what we mean by a proposition generated by a set in Section 3.2, we didn't include the conditional and biconditional operators. This was because of the two equivalences $p \rightarrow q \Leftrightarrow \neg p \vee q$ and $p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$. Therefore, any proposition that includes the conditional or biconditional operators can be written in an equivalent way using only conjunction, disjunction, and negation. We could even dispense with disjunction since $p \vee q$ is equivalent to a proposition that uses only conjunction and negation.

EXERCISES FOR SECTION 3.3

A Exercises

1. Given the following propositions generated by p , q , and r , which are equivalent to one another?

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

2. (a) Construct the truth table for $x = (p \wedge \neg q) \vee (r \wedge p)$.

(b) Give an example other than x itself of a proposition generated by p , q , and r that is equivalent to x .

(c) Give an example of a proposition other than x that implies x .

(d) Give an example of a proposition other than x that is implied by x .

3. Is an implication equivalent to its converse? Verify your answer using a truth table.

4. Suppose that x is a proposition generated by p , q , and r that is equivalent to $p \vee \neg q$. Write out the truth table for x .

B Exercises

5. How large is the largest set of propositions generated by p and q with the property that no two elements are equivalent?

Chapter 3 - Logic

6. Find a proposition that is equivalent to $p \vee q$ and uses only conjunction and negation.
7. Explain why a contradiction implies any proposition and any proposition implies a tautology.

3.4 The Laws of Logic

In this section, we will list the most basic equivalences and implications of logic. Most of the equivalences listed in Table 3.4.1 should be obvious to the reader. Remember, 0 stands for contradiction, 1 for tautology. Many logical laws are similar to algebraic laws. For example, there is a logical law corresponding to the associative law of addition, $a + (b + c) = (a + b) + c$. In fact, associativity of both conjunction and disjunction are among the laws of logic. Notice that with one exception, the laws are paired in such a way that exchanging the symbols \wedge , \vee , 1 and 0 for \vee , \wedge , 0, and 1, respectively, in any law gives you a second law. For example, $p \vee 0 \Leftrightarrow p$ results in $p \wedge 1 \Leftrightarrow p$. This called a *duality principle*. For now, think of it as a way of remembering two laws for the price of one. We will leave it to the reader to verify a few of these laws with truth tables. However, the reader should be careful in applying duality to the conditional operator and implication since the dual involves taking the converse. For example, the dual of $p \wedge q \Rightarrow p$ is $p \vee q \Leftarrow p$, which is usually written $p \Rightarrow p \vee q$.

Example 3.4.1. The identity law:

p	1	$p \wedge 1$	$(p \wedge 1) \Leftrightarrow p$
0	1	0	1
1	1	1	1

therefore, $(p \wedge 1) \Leftrightarrow p$.

Some of the logical laws in Table 3.4.2 might be less obvious to you. For any that you are not comfortable with, substitute actual propositions for the logical variables. For example, if p is "John owns a pet store" and q is "John likes pets," the detachment law should make sense.

TABLE 3.4.1 Basic Logical Laws

Commutative Laws	
$p \vee q \Leftrightarrow q \vee p$	$p \wedge q \Leftrightarrow q \wedge p$
Associative Laws	
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
Distributive Laws	
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Identity Laws	
$p \vee 0 \Leftrightarrow p$	$p \wedge 1 \Leftrightarrow p$
Negation Laws	
$p \wedge \neg p \Leftrightarrow 0$	$p \vee \neg p \Leftrightarrow 1$
Idempotent Laws	
$p \vee p \Leftrightarrow p$	$p \wedge p \Leftrightarrow p$
Null Laws	
$p \wedge 0 \Leftrightarrow 0$	$p \vee 1 \Leftrightarrow 1$
Absorption Laws	
$p \wedge (p \vee q) \Leftrightarrow p$	$p \vee (p \wedge q) \Leftrightarrow p$
DeMorgan's Laws	
$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$	$\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$
Involution Law	
$\neg(\neg p) \Leftrightarrow p$	

Chapter 3 - Logic

TABLE 3.4.2 Common Implications and Equivalences

Detachment
$(p \rightarrow q) \wedge p \Rightarrow q$
Indirect Reasoning
$(p \rightarrow q) \wedge \neg q \Rightarrow \neg p$
Disjunctive Addition
$p \Rightarrow (p \vee q)$
Conjunctive Simplification
$(p \wedge q) \Rightarrow p$ and $(p \wedge q) \Rightarrow q$
Disjunctive Simplification
$(p \vee q) \wedge \neg p \Rightarrow q$ and $(p \vee q) \wedge \neg q \Rightarrow p$
Chain Rule
$(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$
Conditional Equivalence
$p \rightarrow q \Leftrightarrow \neg p \vee q$
Biconditional Equivalences
$(p \leftrightarrow q) \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$
Contrapositive
$(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$

EXERCISES FOR SECTION 3.4

A Exercises

1. Write the following in symbolic notation and determine whether it is a tautology: "If I study then I will learn. I will not learn. Therefore, I do not study."
2. Show that the common fallacy $(p \rightarrow q) \wedge \neg p \Rightarrow \neg q$ is not a law of logic.
3. Describe in general how duality can be applied to implications if we introduce the symbol \Leftarrow , read "is implied by."
4. Write the dual of the following statements:
 - (a) $(p \wedge q) \Rightarrow p$
 - (b) $(p \vee q) \wedge \neg q \Rightarrow p$

3.5 Mathematical Systems

In this section, we present an overview of what a mathematical system is and how logic plays an important role in one. The axiomatic method that we will use here will not be duplicated with as much formality anywhere else in the book, but we hope an emphasis on how mathematical facts are developed and organized will help to unify the concepts we will present. The system of propositions and logical operators we have developed will serve as a model for our discussion. Roughly, a mathematical system can be defined as follows:

Definition: Mathematical System. A mathematical system consists of:

- (1) A set or universe, U .
- (2) Definitions — sentences that explain the meaning of concepts that relate to the universe. Any term used in describing the universe itself is said to be undefined. All definitions are given in terms of these undefined concepts of objects.
- (3) Axioms — assertions about the properties of the universe and rules for creating and justifying more assertions. These rules always include the system of logic that we have developed to this point.
- (4) Theorems — the additional assertions mentioned above.

Example 3.5.1. In Euclidean geometry the universe consists of points and lines (two undefined terms). Among the definitions is a definition of parallel lines and among the axioms is the axiom that two distinct parallel lines never meet.

Example 3.5.2. Propositional calculus is a formal name for the logical system that we've been discussing. The universe consists of propositions. The axioms are the truth tables for the logical operators and the key definitions are those of equivalence and implication. We use propositions to describe any other mathematical system; therefore, this is the minimum amount of structure that a mathematical system can have.

Definition: Theorem. A true proposition derived from axioms of mathematical system is called a theorem.

Theorems are normally expressed in terms of a finite number of propositions, p_1, p_2, \dots, p_n , called the *premises*, and a proposition, C , called the *conclusion*. These theorems take the form

$$p_1 \wedge p_2 \wedge \dots \wedge p_n \Rightarrow C$$

or more informally,

$$p_1, p_2, \dots, \text{ and } p_n \text{ imply } C$$

For a theorem of this type, we say that the premises imply the conclusion. When a theorem is stated, it is assumed that the axioms of the system are true. In addition, any previously proven theorem can be considered an extension of the axioms and can be used in demonstrating that the new theorem is true. When the proof is complete, the new theorem can be used to prove subsequent theorems. A mathematical system can be visualized as an inverted pyramid with the axioms at the base and the theorems expanding out in various directions (Figure 3.5.1).



FIGURE 3.5.1 The body of knowledge in a mathematical system

PROOF

Definition: Proof. A proof of a theorem is a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply the conclusion.

Exactly what constitutes a proof is not always clear. For example, a research mathematician might require only a few steps to prove a theorem to a colleague, but might take an hour to give an effective proof to a class of students. Therefore, what constitutes a proof often depends on the audience. But the audience is not the only factor. One of the most famous theorems in graph theory, The Four Color Theorem, was finally proven in 1976, after over a century of effort by many mathematicians. Part of the proof consisted of having a computer check many different graphs for a certain property. Without the aid of the computer, this checking would have taken years. In the eyes of some mathematicians, this proof was considered questionable. Shorter proofs have been developed since 1976 and there is no controversy associated with The Four Color Theorem at this time. (The theorem is stated in Chapter 9.)

PROOFS IN PROPOSITIONAL CALCULUS

Theoretically, you can prove anything in propositional calculus with truth tables. In fact, the laws of logic stated in Section 5.4 are all theorems. Propositional calculus is one of the few mathematical systems for which any valid sentence can be determined true or false by mechanical means. A program to write truth tables is not too difficult to write; however, what can be done theoretically is not always practical. For example,

$$a, a \rightarrow b, b \rightarrow c, \dots, y \rightarrow z \Rightarrow z$$

is a theorem in propositional calculus. However, suppose that you wrote such a program and you had it write the truth table for

$$(a \wedge (a \rightarrow b) \wedge (b \rightarrow c) \wedge \dots \wedge (y \rightarrow z)) \rightarrow z$$

Chapter 3 - Logic

The truth table will have 2^{26} cases. At one million cases per second, it would take approximately one minute to verify the theorem. Now if you decided to check a similar theorem,

$$p_1, p_1 \rightarrow p_2, \dots, p_{99} \rightarrow p_{100} \Rightarrow p_{100},$$

you would really have time trouble. There would be $2^{100} \approx 1.26765 \times 10^{30}$ cases to check in the truth table. At one million cases per second it would take approximately 1.46719×10^{19} days to check all cases. For most of the remainder of this section, we will discuss an alternate method for proving theorems in propositional calculus. It is the same method that we will use in a less formal way for proofs in other systems. Formal axiomatic methods would be too unwieldy to actually use in later sections. However, none of the theorems in later chapters would be stated if they couldn't be proven by the axiomatic method.

We will introduce two types of proof here, direct and indirect.

DIRECT PROOFS

A **direct proof** is a proof in which the truth of the premises of a theorem are shown to directly imply the truth of the theorem's conclusion.

Example 3.5.3. Theorem: $p \rightarrow r, q \rightarrow s, p \vee q \Rightarrow s \vee r$. A direct proof of this theorem is:

Step	Proposition	Justification
(1)	$p \vee q$	Premise
(2)	$\neg p \rightarrow q$	(1), conditional rule
(3)	$q \rightarrow s$	Premise
(4)	$\neg p \rightarrow s$	(2), (3), chain rule
(5)	$\neg s \rightarrow p$	(4), contrapositive
(6)	$p \rightarrow r$	Premise
(7)	$\neg s \rightarrow r$	(5), (6), chain rule
(8)	$s \vee r$	(7), conditional rule ■

Note that ■ marks the end of a proof.

Rules for Formal Proofs. Example 3.5.3 illustrates the usual method of formal proof in a formal mathematical system. The rules governing these proofs are:

- (1) A proof must end in a finite number of steps.
- (2) Each step must be either a premise or a proposition that is implied from previous steps using any valid equivalence or implication.
- (3) For a direct proof, the last step must be the conclusion of the theorem. For an indirect proof (see below), the last step must be a contradiction.
- (4) Justification Column. The column labeled "justification" is analogous to the comments that appear in most good computer programs. They simply make the proof more readable.

Example 3.5.4. Here are two direct proofs of $\neg p \vee q, s \vee p, \neg q \Rightarrow s$:

(1)	$\neg p \vee q$	Premise
(2)	$\neg q$	Premise
(3)	$\neg p$	Disjunctive simplification, (1), (2)
(4)	$s \vee p$	Premise
(5)	s	Disjunctive simplification, (3), (4). ■

You are invited to justify the steps in this second proof:

- (1) $\neg p \vee q$
- (2) $\neg q \rightarrow \neg p$
- (3) $s \vee p$
- (4) $p \vee s$
- (5) $\neg p \rightarrow s$
- (6) $\neg q \rightarrow s$
- (7) $\neg q$
- (8) s ■

CONDITIONAL CONCLUSIONS

The conclusion of a theorem is often a conditional proposition. The condition of the conclusion can be included as a premise in the proof of the theorem. The object of the proof is then to prove the consequence of the conclusion. This rule is justified by the logical law

$$p \rightarrow (h \rightarrow c) \Leftrightarrow (p \wedge h) \rightarrow c.$$

Example 3.5.5. The following proof of $p \rightarrow (q \rightarrow s)$, $\neg r \vee p, q \Rightarrow r \rightarrow s$ includes r as a fourth premise. The truth of s concludes the proof.

- | | | |
|-----|-----------------------------------|--------------------------------------|
| (1) | $\neg r \vee p$ | Premise |
| (2) | r | Added premise |
| (3) | p | (1), (2), disjunction simplification |
| (4) | $p \rightarrow (q \rightarrow s)$ | Premise |
| (5) | $q \rightarrow s$ | (3), (4), detachment |
| (6) | q | Premise |
| (7) | s | (5), (6), detachment. ■ |

INDIRECT PROOFS / PROOF BY CONTRADICTION

Consider a theorem $P \Rightarrow C$, where P represents p_1, p_2, \dots , and p_n , the premises. The method of indirect proof is based on the equivalence $P \rightarrow C \Leftrightarrow \neg (P \wedge \neg C)$.

In words, this logical law states that if $P \Rightarrow C$, then $P \wedge \neg C$ is always false; that is, $P \wedge \neg C$ is a contradiction. This means that a valid method of proof is to negate the conclusion of a theorem and add this negation to the premises. If a contradiction can be implied from this set of propositions, the proof is complete. For the proofs in this section, a contradiction will often take the form $t \wedge \neg t$. For proofs involving numbers, a contradiction might be $1 = 0$ or $0 < 0$. Indirect proofs involving sets might conclude with $x \in \emptyset$ or $(x \in A \text{ and } x \in A^c)$. Indirect proofs are often more convenient than direct proofs in certain situations. *Indirect proofs are often called **proofs by contradiction**.*

Example 3.5.6. Here is an example of an indirect proof of the theorem in Example 3.5.3:

- | | | |
|------|----------------------------|---------------------------------|
| (1) | $\neg (s \vee r)$ | Negated conclusion |
| (2) | $\neg s \wedge \neg r$ | DeMorgan's Law, (1) |
| (3) | $\neg s$ | Conjunctive simplification, (2) |
| (4) | $q \rightarrow s$ | Premise |
| (5) | $\neg q$ | Indirect reasoning, (3), (4) |
| (6) | $\neg r$ | Conjunctive simplification, (2) |
| (7) | $p \rightarrow r$ | Premise |
| (8) | $\neg p$ | Indirect reasoning, (6), (7) |
| (9) | $(\neg p) \wedge (\neg q)$ | Conjunctive, (5), (8) |
| (10) | $\neg (p \vee q)$ | DeMorgan's Law, (9) |
| (11) | $p \vee q$ | Premise |
| (12) | 0 | (10), (11) ■ |

PROOF STYLE

The rules allow you to list the premises of a theorem immediately; however, a proof is much easier to follow if the premises are only listed when they are needed.

Example 3.5.7. Here is an indirect proof of $a \rightarrow b, \neg(b \vee c) \Rightarrow \neg a$.

- | | | |
|-----|-------------------|----------------------------|
| (1) | a | Negation of the conclusion |
| (2) | $a \rightarrow b$ | Premise |
| (3) | b | (1), (2), detachment |
| (4) | $b \vee c$ | (3), disjunctive addition |
| (5) | $\neg(b \vee c)$ | Premise |
| (6) | 0 | (4), (5) ■ |

As we mentioned at the outset of this section, we are only presenting an overview of what a mathematical system is. For greater detail on axiomatic theories, see Stoll (1961). An excellent description of how propositional calculus plays a part in artificial intelligence is contained in Hofstadter (1980). If you enjoy the challenge of constructing proofs in propositional calculus, you should enjoy the game WFF'N PROOF (1962), by L.E. Allen.

EXERCISES FOR SECTION 3.5**A Exercises**

1. Prove with truth tables:

- (a) $p \vee q, \neg q \Rightarrow p$
 (b) $p \rightarrow q, \neg q \Rightarrow \neg p$

2. Prove with truth tables:

- (a) $q, \neg q \Rightarrow p$
 (b) $p \rightarrow q \Rightarrow \neg p \vee q$

B Exercises

3. Give direct and indirect proofs of:

- (a) $a \rightarrow b, c \rightarrow b, d \rightarrow (a \vee c), d \Rightarrow b$.
 (b) $(p \rightarrow q) \wedge (r \rightarrow s), (q \rightarrow t) \wedge (s \rightarrow u), \neg(t \wedge u), p \rightarrow r \Rightarrow \neg p$.
 (c) $p \rightarrow (q \rightarrow s), \neg s \vee p, q \Rightarrow s \rightarrow r$.
 (d) $p \rightarrow q, q \rightarrow r, \neg(p \wedge r), p \vee r \Rightarrow r$.
 (e) $\neg q, p \rightarrow q, p \vee t \Rightarrow t$

4. Give direct and indirect proofs of:

- (a) $p \rightarrow q, \neg r \rightarrow \neg q, \neg r \Rightarrow \neg p$.
 (b) $p \rightarrow \neg q, \neg r \rightarrow q, p \Rightarrow r$.
 (c) $a \vee b, c \wedge d, a \rightarrow \neg c \Rightarrow b$.

5. Are the following arguments valid? If they are valid, construct formal proofs; if they aren't valid, explain why not.

- (a) If wages increase, then there will be inflation. The cost of living will not increase if there is no inflation. Wages will increase. Therefore, the cost of living will increase.
 (b) If the races are fixed or the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed.
 6. Determine the validity of the following argument: For students to do well in a discrete mathematics course, it is necessary that they study hard. Students who do well in courses do not skip classes. Students who study hard do well in courses. Therefore students who do well in a discrete mathematics course do not skip class.

7. Describe how $p_1, p_1 \rightarrow p_2, \dots, p_{99} \rightarrow p_{100} \Rightarrow p_{100}$ could be proven in 199 steps.

3.6 Propositions over a Universe

Example 3.6.1. Consider the sentence "He was a member of the Boston Red Sox." There is no way that we can assign a truth value to this sentence unless "he" is specified. For that reason, we would not consider it a proposition. However, "he" can be considered a variable that holds a place for any name. We might want to restrict the value of "he" to all names in the major-league baseball record books. If that is the case, we say that the sentence is a proposition over the set of major-league baseball players, past and present.

Definition: Proposition over a Universe. Let U be a nonempty set. A proposition over U is a sentence that contains a variable that can take on any value in U and that has a definite truth value as a result of any such substitution.

Example 3.6.2.

- (a) A few propositions over the integers are $4x^2 - 3x = 0$, $0 \leq n \leq 5$, and " k is a multiple of 3."
- (b) A few propositions over the rational numbers are $4x^2 - 3x = 0$, $y^2 = 2$, and $(s - 1)(s + 1) = s^2 - 1$.
- (c) A few propositions over the subsets of \mathbb{P} are $(A = \emptyset) \vee (A = \mathbb{P})$, $3 \in A$, and $A \cap \{1, 2, 3\} \neq \emptyset$.

All of the laws of logic that we listed in Section 3.4 are valid for propositions over a universe. For example, if p and q are propositions over the integers, we can be certain that $p \wedge q \Rightarrow p$, because $(p \wedge q) \rightarrow p$ is a tautology and is true no matter what values the variables in p and q are given. If we specify p and q to be $p(n) : n < 4$ and $q(n) : n < 8$, we can also say that p implies $p \wedge q$. This is not a usual implication, but for the propositions under discussion, it is true. One way of describing this situation in general is with truth sets.

TRUTH SETS

Definition: Truth Set. If p is a proposition over U , the truth set of p is $T_p = \{a \in U \mid p(a) \text{ is true}\}$.

Example 3.6.3. The truth set of the proposition $\{1, 2\} \cap A = \emptyset$ taken as a proposition over the power set of $\{1, 2, 3, 4\}$ is $\{\emptyset, \{3\}, \{4\}, \{3, 4\}\}$.

Example 3.6.4. In the universe \mathbb{Z} (the integers), the truth set of $4x^2 - 3x = 0$ is $\{0\}$. If the universe is expanded to the rational numbers, the truth set becomes $\{0, 3/4\}$. The term solution set is often used for the truth set of an equation such as the one in this example.

Definition: Tautology and Contradiction. A proposition over U is a tautology if its truth set is U . It is a contradiction if its truth set is empty.

Example 3.6.5. $(s - 1)(s + 1) = s^2 - 1$ is a tautology over the rational numbers. $x^2 - 2 = 0$ is a contradiction over the rationals.

The truth sets of compound propositions can be expressed in terms of the truth sets of simple propositions. For example, if $a \in T_{p \wedge q}$, then a makes $p \wedge q$ true. Therefore, a makes both p and q true, which means that $a \in T_p \cap T_q$. This explains why the truth set of the conjunction of two propositions equals the intersection of the truth sets of the two propositions. The following list summarizes the connection between compound and simple truth sets:

$$\begin{aligned} T_{p \wedge q} &= T_p \cap T_q \\ T_{p \vee q} &= T_p \cup T_q \\ T_{\neg p} &= T_p^c \\ T_{p \leftrightarrow q} &= (T_p \cap T_q) \cup (T_p^c \cap T_q^c) \\ T_{p \rightarrow q} &= T_p^c \cup T_q \end{aligned}$$

Definition: Equivalence. Two propositions are equivalent if $p \leftrightarrow q$ is a tautology. In terms of truth sets, this means that p and q are equivalent if $T_p = T_q$.

Example 3.6.6.

- (a) $n + 4 = 9$ and $n = 5$ are equivalent propositions over the integers.
- (b) $A \cap \{4\} \neq \emptyset$ and $4 \in A$ are equivalent propositions over the power set of the natural numbers.

Definition: Implication. If p and q are propositions over U , p implies q if $p \rightarrow q$ is a tautology.

Since the truth set of $p \rightarrow q$ is $T_p^c \cup T_q$, the Venn diagram for $T_{p \rightarrow q}$ in Figure 3.6.1 shows that $p \Rightarrow q$ when $T_p \subseteq T_q$.

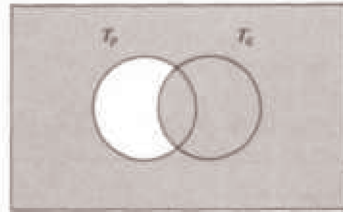


FIGURE 3.6.1 Venn diagram for $T_{p \rightarrow q}$

Example 3.6.7.

- (a) Over the natural numbers: $n < 4 \Rightarrow n < 8$ since $\{0, 1, 2, 3, 4\} \subseteq \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
- (b) Over the power set of the integers: $|A^c| = 1$ implies $A \cap \{0, 1\} \neq \emptyset$.
- (c) $A \subseteq \text{even integers} \Rightarrow A \cap \text{odd integers} = \emptyset$.

EXERCISES FOR SECTION 3.6

A Exercises

1. If $U = \mathcal{P}(\{1, 2, 3, 4\})$, what are the truth sets of the following propositions?

- (a) $A \cap \{2, 4\} = \emptyset$.
- (b) $3 \in A$ and $1 \notin A$.
- (c) $A \cup \{1\} = A$.
- (d) A is a proper subset of $\{2, 3, 4\}$.
- (e) $|A| = |A^c|$.

2. Over the universe of positive integers, define

$p(n) : n$ is prime and $n < 32$.

$q(n) : n$ is a power of 3.

$r(n) : n$ is a divisor of 27.

- (a) What are the truth sets of these propositions?
 - (b) Which of the three propositions implies one of the others?
3. If $U = \{0, 1, 2\}$, how many propositions over U could you list without listing two that are equivalent?
4. Given the propositions over the natural numbers:

$p : n < A$

$q : 2n > 17$

$r : n$ is a divisor of 18

what are the truth sets of:

- (a) q
- (b) $p \wedge q$
- (c) r
- (d) $q \rightarrow r$

5. Suppose that s is a proposition over $\{1, \dots, 8\}$. If $T_s = \{1, 3, 5, 7\}$, give two examples of propositions that are equivalent to s .

6. (a) Determine the truth sets of the following propositions over the positive integers:

$p(n) : n$ is a perfect square and $n < 100$.

Chapter 3 - Logic

$q(n) : n = |\mathcal{P}(A)|$ for some set A

(b) Determine $T_{p \wedge q}$ for p and q above.

7. Let the universe be \mathbb{Z} , the set of integers. Which of the following propositions are equivalent over \mathbb{Z} ?

a : $0 < n^2 < 9$.

b : $0 < n^3 < 27$.

c : $0 < n < 3$.

3.7 Mathematical Induction

In this section, we will examine mathematical induction, a technique for proving propositions over the positive integers. Mathematical (or finite) induction reduces the proof that all of the positive integers belong to a truth set to a finite number of steps.

Mathematical Induction is sometimes called finite induction.

Example 3.7.1. Consider the following proposition over the positive integers, which we will label $p(n)$: The sum of the positive integers from 1 to n is $\frac{n(n+1)}{2}$. This is a well-known formula that is quite simple to verify for a given value of n . For example, $p(5)$ is: The sum of the positive integers from 1 to 5 is $\frac{5(5+1)}{2}$. Indeed, $1 + 2 + 3 + 4 + 5 = 15 = \frac{5(5+1)}{2}$. Unfortunately, this doesn't serve as a proof that $p(n)$ is a tautology. All that we've established is that 5 is in the truth set of p . Since the positive integers are infinite, we certainly can't use this approach to prove the formula.

An Analogy: Mathematical induction is often useful in overcoming a problem such as this one. A proof by mathematical induction is similar to knocking over a row of closely spaced dominos that are standing on end. To

knock over the five dominos in Figure 3.7.1, all you need to do is push Domino 1 to the right. To be assured that they all will be knocked over, some work must be done ahead of time. The dominos must be positioned so that if any domino is pushed to the right, it will push the next domino in the line.



FIGURE 3.7.1 Illustration of example 3.7.1

Now imagine the propositions $p(1)$, $p(2)$, $p(3)$, ... to be an infinite line of dominos. Let's see if these propositions are in the same formation as the dominos were. First, we will focus on one specific point of the line: $p(99)$ and $p(100)$. We are not going to prove that either of these propositions is true, just that the truth of $p(99)$ implies the truth of $p(100)$. In terms of our analogy, if $p(99)$ is knocked over, it will knock over $p(100)$.

In proving $p(99) \Rightarrow p(100)$, we will use $p(99)$ as our premise. We must prove: The sum of the positive integers from 1 to 100 is $\frac{100(100+1)}{2}$. We start by observing that the sum of the positive integers from 1 to 100 is $(1 + 2 + \dots + 99) + 100$. That is, the sum of the positive integers from 1 to 100 equals the sum of the first ninety-nine plus the final number, 100. We can now apply our premise, $p(99)$, to the sum $1 + 2 + \dots + 99$. After rearranging our numbers, we obtain the desired expression for $1 + 2 + \dots + 100$:

$$\begin{aligned} 1 + 2 + \dots + 99 + 100 &= (1 + 2 + \dots + 99) + 100 \\ &= \frac{99(99+1)}{2} + 100 \\ &= \frac{99 \times 100}{2} + \frac{2 \times 100}{2} \\ &= \frac{100 \times 101}{2} \\ &= \frac{100(100+1)}{2} \end{aligned}$$

What we've just done is analogous to checking two dominos in a line and finding that they are properly positioned. Since we are dealing with an infinite line, we must check all pairs at once. This is accomplished by proving that $p(n) \Rightarrow p(n+1)$ for all $n \geq 1$:

$$\begin{aligned} 1 + 2 + \dots + n + (n+1) &= (1 + 2 + \dots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \quad \text{by } p(n) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

They are all lined up! Now look at $p(1)$: The sum of the positive integers from 1 to 1 is $\frac{1+1}{2}$. Clearly, $p(1)$ is true. This sets off a chain reaction. Since $p(1) \Rightarrow p(2)$, $p(2)$ is true. Since $p(2) \Rightarrow p(3)$, $p(3)$ is true; and so on. ■

The Principle of Mathematical Induction. Let $p(n)$ be a proposition over the positive integers, then $p(n)$ is a tautology if
 (1) $p(1)$ is true, and
 (2) for all $n \geq 1$, $p(n) \Rightarrow p(n+1)$.

Note: The truth of $p(1)$ is called the basis for the induction proof. The premise that $p(n)$ is true in Statement (b) is called the induction hypothesis. The proof that $p(n)$ implies $p(n+1)$ is called the induction step of the proof. Despite our analogy, the basis is usually done first in an induction proof. The order doesn't really matter.

Example 3.7.2. Consider the implication over the positive integers

Chapter 3 - Logic

$$p(n) : q_0 \rightarrow q_1, q_1 \rightarrow q_2, \dots, q_{n-1} \rightarrow q_n, q_0 \Rightarrow q_n$$

A proof that $p(n)$ is a tautology follows.

Basis: $p(1)$ is $q_0 \rightarrow q_1, q_0 \Rightarrow q_1$. This is the logical law of detachment which we know is true. If you haven't done so yet, write out the truth table of $((q_0 \rightarrow q_1) \wedge q_0) \rightarrow q_1$ to verify this step.

Induction: Assume that $p(n)$ is true for some $n \geq 1$. We want to prove that $p(n + 1)$ must be true. That is:

$$q_0 \rightarrow q_1, q_1 \rightarrow q_2, \dots, q_{n-1} \rightarrow q_n, q_n \rightarrow q_{n+1}, q_0 \Rightarrow q_{n+1}$$

Here is a direct proof of $p(n + 1)$:

Steps	Proposition(s)	Justification
(1) - (n + 1)	$q_0 \rightarrow q_1, q_1 \rightarrow q_2, \dots, q_{n-1} \rightarrow q_n, q_0$	Premises
(n + 2)	q_n	(1) - (n + 1), $p(n)$
(n + 3)	$q_n \rightarrow q_{n+1}$	Premise
(n + 4)	q_{n+1}	(n + 2), (n + 3), detachment ■

Example 3.7.3. For all $n \geq 1$, $n^3 + 2n$ is a multiple of 3. An inductive proof follows:

Basis: $1^3 + 2(1) = 3$ is a multiple of 3.

The basis is almost always this easy!

Induction: Assume that $n \geq 1$ and $n^3 + 2n$ is a multiple of 3. Consider $(n + 1)^3 + 2(n + 1)$. Is it a multiple of 3?

$$\begin{aligned} (n + 1)^3 + 2(n + 1) &= (n^3 + 3n^2 + 3n + 1) + (2n + 2) \\ &= n^3 + 2n + 3n^2 + 3n + 3 && \text{Rearrange the terms} \\ &= (n^3 + 2n) + 3(n^2 + n + 1) \end{aligned}$$

Yes, $(n + 1)^3 + 2(n + 1)$ is the sum of two multiples of 3; therefore, it is also a multiple of 3. ■

Variations of Induction

Now we will discuss some of the variations of the principle of mathematical induction. The first simply allows for universes that are similar to \mathbb{P} , like $\{-2, -1, 0, 1, \dots\}$ or $\{5, 6, 7, 8, \dots\}$.

Principle of Mathematical Induction (Generalized). If $p(n)$ is a proposition over $\{k_0, k_0 + 1, k_0 + 2, \dots\}$, where k_0 is any integer, then $p(n)$ is a tautology if

- (1) $p(k_0)$ is true, and
- (2) for all $n \geq k_0$, $p(n) \Rightarrow p(n + 1)$.

Example 3.7.4. In Chapter 2, we stated that the number of different permutations of k elements taken from an n element set, $P(n; k)$, can be computed with the formula $\frac{n!}{(n-k)!}$. We can prove this statement by induction on n . For $n \geq 0$, let $q(n)$ be the proposition

$$P(n; k) = \frac{n!}{(n-k)!} \text{ for all } k \text{ from } 0 \text{ to } n.$$

Basis: $q(0)$ states that

$$\begin{aligned} P(0; 0) &= \text{the number of ways that 0 elements can be} \\ &\quad \text{selected from the empty set and arranged in order} \\ &= 0!/0! = 1. \end{aligned}$$

This is true — a general law in combinatorics is that there is exactly one way of doing nothing.

Induction: Assume that $q(n)$ is true for some natural number n . It is left for us to prove that this assumption implies that $q(n + 1)$ is true. Suppose that we have a set of cardinality $n + 1$ and want to select and arrange k of its elements. There are two cases to consider, the first of which is easy. If $k = 0$, then there is one way of selecting zero elements from the set; hence

$$P(n + 1; 0) = 1 = \frac{(n+1)!}{(n+1+0)!}$$

and the formula works in this case.

The more challenging case is to verify the formula when k is positive and less than or equal to $n + 1$. Here we count the value of $P(n + 1; k)$ by counting the number of ways that the first element in the arrangement can be filled and then counting the number of ways that the remaining $k - 1$ elements can be filled in using the induction hypothesis.

There are $n + 1$ possible choices for the first element. Since that leaves n elements to fill in the remaining $k - 1$ positions, there are $P(n; k - 1)$ ways of completing the arrangement. By the rule of products,

$$\begin{aligned}
 P(n+1; k) &= (n+1) P(n; k-1) \\
 &= (n+1) \frac{n!}{(n-(k-1))!} \\
 &= \frac{(n+1)n!}{(n-k+1)!} \\
 &= \frac{(n+1)!}{((n+1)-k)!} \quad \blacksquare
 \end{aligned}$$

A second variation allows for the expansion of the induction hypothesis. The course-of-values principle includes the previous generalization. It is also sometimes called *strong induction*.

The Course-of-Values Principle of Mathematical Induction. If $p(n)$ is a proposition over $\{k_0, k_0 + 1, k_0 + 2, \dots\}$, where k_0 is any integer, then $p(n)$ is a tautology if

- (1) $p(k_0)$ is true, and
- (2) for all $n \geq k_0$, $p(k_0), p(k_0 + 1), \dots, p(n) \Rightarrow p(n + 1)$.

Example 3.7.5. A prime number is defined as a positive integer that has exactly two positive divisors, 1 and itself. There are an infinite number of primes. The list of primes starts with 2, 3, 5, 7, 11, The proposition over $\{2, 3, 4, \dots\}$ that we will prove here is $p(n) : n$ can be written as the product of one or more primes. In most texts, the assertion that $p(n)$ is a tautology would appear as:

Theorem. Every positive integer greater than or equal to 2 has a prime decomposition.

If you were to encounter this theorem outside the context of a discussion of mathematical induction, it might not be obvious that the proof can be done by induction. Recognizing when an induction proof is appropriate is mostly a matter of experience. Now on to the proof!

Basis: Since 2 is a prime, it is already decomposed into primes (one of them).

Induction: Suppose that for some $k \geq 2$ all of the integers 2, 3, ..., k have a prime decomposition. Notice the course-of-value hypothesis. Consider $k + 1$. Either $k + 1$ is prime or it isn't. If $k + 1$ is prime, it is already decomposed into primes. If not, then $k + 1$ has a divisor, d , other than 1 and $k + 1$. Hence, $k + 1 = cd$ where both c and d are between 2 and k . By the induction hypothesis, c and d have prime decompositions, $c_1 c_2 \dots c_m$ and $d_1 d_2 \dots d_m$, respectively. Therefore, $k + 1$ has the prime decomposition $c_1 c_2 \dots c_m d_1 d_2 \dots d_m$. ■

HISTORICAL NOTE

Mathematical induction originated in the late nineteenth century. Two mathematicians who were prominent in its development were Richard Dedekind and Giuseppe Peano. Dedekind developed a set of axioms that describe the positive integers. Peano refined these axioms and gave a logical interpretation to them. The axioms are usually called the Peano Postulates.

Peano's Postulates. The system of positive integers consists of a nonempty set, \mathbb{P} ; a least element of \mathbb{P} , denoted 1; and a "successor function," s , with the properties

- (1) If $k \in \mathbb{P}$, then there is an element of \mathbb{P} called the successor of k , denoted $s(k)$.
- (2) No two elements of \mathbb{P} have the same successor.
- (3) No element of \mathbb{P} has 1 as its successor.
- (4) If $S \subseteq \mathbb{P}$, $1 \in S$, and $k \in S \Rightarrow s(k) \in S$, then $S = \mathbb{P}$.



Richard Dedekind



Giuseppe Peano

Notes:

- (a) You might recognize $s(k)$ as simply being $k + 1$.
- (b) Axiom 4, mentioned above, is the one that makes mathematical induction possible. In an induction proof, we simply apply that axiom to the truth set of a proposition.

Exercises for Section 3.7

A Exercises

1. Prove that the sum of the first n odd integers equals n^2 .
2. Prove that if $n \geq 1$, then $1(1!) + 2(2!) + \dots + n(n!) = (n+1)! - 1$.

3. Prove that for $n \geq 1$: $\sum_{k=1}^n k^2 = \frac{1}{6} n(n+1)(2n+1)$.

4. Prove that for $n \geq 1$: $\sum_{k=0}^n 2^k = 2^{n+1} - 1$.

5. Use mathematical induction to show that for $n \geq 1$,

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

6. Prove that if $n \geq 2$, the generalized DeMorgan's Law is true:

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

B Exercises

7. The number of strings of n zeros and ones that contain an even number of ones is 2^{n-1} . Prove this fact by induction for $n \geq 1$.

8. Let $p(n)$ be $8^n - 3^n$ is a multiple of 5. Prove that $p(n)$ is a tautology over \mathbb{N} .

9. Suppose that there are n people in a room, $n \geq 1$, and that they all shake hands with one another. Prove that $\frac{n(n-1)}{2}$ handshakes will have occurred.

10. Prove that it is possible to make up any postage of eight cents or more using only three- and five-cent stamps.

C Exercises

11. Generalized associativity. It is well known that if a_1, a_2 , and a_3 are numbers, then no matter what order the sums in the expression $a_1 + a_2 + a_3$ are taken in, the result is always the same. Call this fact $p(3)$ and assume it is true. Prove using course-of-values induction that if a_1, a_2, \dots , and a_n are numbers, then no matter what order the sums in the expression $a_1 + a_2 + \cdots + a_n$ are taken in, the result is always the same.

12. Let S be the set of all numbers that can be produced by applying any of the rules below in any order a finite number of times.

Rule 1: $\frac{1}{2} \in S$

Rule 2: $1 \in S$

Rule 3: If a and b have been produced by the rules, then $ab \in S$.

Rule 4: If a and b have been produced by the rules, then $\frac{a+b}{2} \in S$.

Prove by course-of-values induction that $a \in S \Rightarrow 0 < a \leq 1$. Hint: The number of times the rules are applied should be the integer that you do the induction on.

13. A recursive definition is similar to an inductive proof. It consists of a basis, usually the simple part of the definition, and the recursion, which defines complex objects in terms of simpler ones. For example, if x is a real number and n is a positive integer, we can define x^n as follows:

Basis: $x^1 = x$.

Recursion: if $n \geq 2$, $x^n = x^{n-1}x$.

For example, $x^3 = x^2x = (x^1x)x = (xx)x$. Proofs involving objects that are defined recursively are often inductive. Prove that if $n, m \in \mathbb{P}$, $x^{m+n} = x^m x^n$. Hint: Let $p(m)$ be the proposition that $x^{m+n} = x^m x^n$ for all $n \geq 1$. There is much more on recursion in Chapter 8.

14. Let S be a finite set and let P_n , be defined recursively by $P_1 = S$ and $P_n = S \times P_{n-1}$ for $n \geq 2$.

(a) List the elements of P_3 for the case $S = \{a, b\}$.

(b) Determine the formula for $|P_n|$, given that $|S| = k$, and prove your formula by induction.

3.8 Quantifiers

As we saw in Section 3.6, if $p(n)$ is a proposition over a universe U , its truth set T_p is equal to a subset of U . In many cases, such as when $p(n)$ is an equation, we are most concerned with whether T_p is empty or not. In other cases, we might be interested in whether $T_p = U$; that is, whether $p(n)$ is a tautology. Since the conditions $T_p \neq \emptyset$ and $T_p = U$ are so often an issue, we have a special system of notation for them.

THE EXISTENTIAL QUANTIFIER

If $p(n)$ is a proposition over U with $T_p \neq \emptyset$, we commonly say "There exists an n in U such that $p(n)$ (is true)." We abbreviate this with the symbols $(\exists n)_U (p(n))$. The symbol \exists is called the existential quantifier. If the context is clear, the mention of U is dropped: $(\exists n) (p(n))$.

Example 3.8.1.

(a) $(\exists k)_\mathbb{Z} (k^2 - k - 12 = 0)$ is another way of saying that there is an integer that solves the equation $k^2 - k - 12 = 0$. The fact that two such integers exist doesn't affect the truth of this proposition in any way.

(b) $(\exists k)_\mathbb{Z} (3k = 102)$ simply states that 102 is a multiple of 3, which is true. On the other hand, $(\exists k)_\mathbb{Z} (3k = 100)$ states that 100 is a multiple of 3, which is false.

(c) $(\exists x)_\mathbb{R} (x^2 + 1 = 0)$ is false since the solution set of the equation $x^2 + 1 = 0$ in the real numbers is empty. It is common to write $(\nexists x)_\mathbb{R} (x^2 + 1 = 0)$ in this case.

There are a wide variety of ways that you can write a proposition with an existential quantifier. Table 3.8.1 contains a list of different variations that could be used for both the existential and universal quantifiers.

THE UNIVERSAL QUANTIFIER

If $p(n)$ is a proposition over U with $T_p = U$, we commonly say "For all n in U , $p(n)$ (is true)." We abbreviate this with the symbols $(\forall n)_U (p(n))$. The symbol \forall is called the universal quantifier. If the context is clear, the mention of U is dropped: $(\forall n) (p(n))$.

Example 3.8.2.

(a) We can say that the square of every real number is non-negative symbolically with a universal quantifier: $(\forall x)_\mathbb{R} (x^2 \geq 0)$.

(b) $(\forall n)_\mathbb{Z} (n + 0 = 0 + n = n)$ says that the sum of zero and any integer n is n . This fact is called the identity property of zero for addition.

Table 3.8.1 Notational Variations for Existential and Universal Quantifiers

Universal Quantifier	Existential Quantifier
$(\forall n)_U (p(n))$	$(\exists n)_U (p(n))$
$(\forall n \in U) (p(n))$	$(\exists n \in U) (p(n))$
$\forall n \in U, p(n)$	$\exists n \in U$ such that $p(n)$
$p(n), \forall n \in U$	$p(n)$ is true for some $n \in U$
$p(n)$ is true for all $n \in U$	

THE NEGATION OF QUANTIFIED PROPOSITIONS

When you negate a quantified proposition, the existential and universal quantifiers complement one another.

Example 3.8.3. Over the universe of animals, define $F(x)$: x is a fish and $W(x)$: x lives in the water. We know that the proposition $W(x) \rightarrow F(x)$ is not always true. In other words, $(\forall x)(W(x) \rightarrow F(x))$ is false. Another way of stating this fact is that there exists an animal that lives in the water and is not a fish; that is,

$$\neg (\forall x) (W(x) \rightarrow F(x)) \Leftrightarrow (\exists x) (\neg (W(x) \rightarrow F(x))) \\ \Leftrightarrow (\exists x) (W(x) \wedge \neg F(x))$$

Note that the negation of a universally quantified proposition is an existentially quantified proposition. In addition, when you negate an existentially quantified proposition, you obtain a universally quantified proposition. Symbolically,

$$\neg ((\forall n)_U (p(n))) \Leftrightarrow (\exists n)_U (\neg p(n)), \text{ and}$$

$$\neg ((\exists n)_U (p(n))) \Leftrightarrow (\forall n)_U (\neg p(n))$$

Example 3.8.4.

(a) The ancient Greeks first discovered that $\sqrt{2}$ is an irrational number; that is, $\sqrt{2}$ is not a rational number. $\neg ((\exists r)_\mathbb{Q} (r^2 = 2))$ and

Chapter 3 - Logic

$(\forall r)_{\mathbb{Q}} (r^2 \neq 2)$ both state this fact symbolically.

(b) $\neg((\forall n)_{\mathbb{P}} (n^2 - n + 41 \text{ is prime}))$ is equivalent to $(\exists n)_{\mathbb{P}} (n^2 - n + 41 \text{ is composite})$. They are both either true or false.

MULTIPLE QUANTIFIERS

If a proposition has more than one variable, then you can quantify it more than once. For example, if $p(x, y) : x^2 - y^2 = (x + y)(x - y)$ is a tautology over the set of all pairs of real numbers because it is true for each pair (x, y) in $\mathbb{R} \times \mathbb{R}$. Another way to look at this proposition is as a proposition with two variables. The assertion that $p(x, y)$ is a tautology could be quantified as $(\forall x)_{\mathbb{R}} ((\forall y)_{\mathbb{R}} (p(x, y)))$ or $(\forall y)_{\mathbb{R}} ((\forall x)_{\mathbb{R}} (p(x, y)))$

In general, multiple universal quantifiers can be arranged in any order without logically changing the meaning of the resulting proposition. The same is true for multiple existential quantifiers. For example, $p(x, y) : x + y = 4$ and $x - y = 2$ is a proposition over $\mathbb{R} \times \mathbb{R}$. $(\exists x)_{\mathbb{R}} ((\exists y)_{\mathbb{R}} (x + y = 4 \text{ and } x - y = 2))$ and $(\exists y)_{\mathbb{R}} ((\exists x)_{\mathbb{R}} (x + y = 4 \text{ and } x - y = 2))$ are equivalent. A proposition with multiple existential quantifiers such as this one says that there are simultaneous values for the quantified variables that make the proposition true. A similar example is $q(x, y) : 2x - y = 2$ and $4x - 2y = 5$, which is always false; and the following are all equivalent

$$\begin{aligned} \neg((\exists x)_{\mathbb{R}} ((\exists y)_{\mathbb{R}} (q(x, y)))) &\Leftrightarrow \neg(\exists y)_{\mathbb{R}} ((\exists x)_{\mathbb{R}} (q(x, y))) \\ &\Leftrightarrow (\forall y)_{\mathbb{R}} (\neg((\exists x)_{\mathbb{R}} (q(x, y)))) \\ &\Leftrightarrow ((\forall y)_{\mathbb{R}} ((\forall x)_{\mathbb{R}} (\neg q(x, y)))) \\ &\Leftrightarrow ((\forall x)_{\mathbb{R}} ((\forall y)_{\mathbb{R}} (\neg q(x, y)))) \end{aligned}$$

When existential and universal quantifiers are mixed, the order cannot be exchanged without possibly changing the meaning of the proposition. For example, let \mathbb{R}^+ be the positive real numbers, $x : (\forall a)_{\mathbb{R}^+} ((\exists b)_{\mathbb{R}^+} (ab = 1))$ and $y : (\exists b)_{\mathbb{R}^+} ((\forall a)_{\mathbb{R}^+} (ab = 1))$ have different meanings; x is true, while y is false.

TIPS ON READING MULTIPLY QUANTIFIED PROPOSITIONS

It is understandable that you would find propositions such as x difficult to read. The trick to deciphering these expressions is to "peel" one quantifier off the proposition just as you would peel off the layers of an onion (but quantifiers shouldn't make you cry). Since the outermost quantifier in x is universal, x says that $z(a) : (\exists b)_{\mathbb{R}^+} (ab = 1)$ is true for each value that a can take on. Now take the time to select a value for a , like 6. For the value that we selected, we get $z(6) : (\exists b)_{\mathbb{R}^+} (6b = 1)$, which is obviously true since $6b = 1$ has a solution in the positive real numbers. We will get that same truth value no matter which positive real number we choose for a ; therefore, $z(a)$ is a tautology over \mathbb{R}^+ and we are justified in saying that x is true. The key to understanding propositions like x on your own is to experiment with actual values for the outermost variables as we did above.

Now consider y . To see that y is false, we peel off the outer quantifier. Since it is an existential quantifier, all that y says is that some positive real number makes $w(b) : (\forall a)_{\mathbb{R}^+} (ab = 1)$ true. Choose a few values of b to see if you can find one that makes $w(b)$ true. For example, if we pick $b = 2$, we get $(\forall a)_{\mathbb{R}^+} (2a = 1)$, which is false, since $2a$ is almost always different from 1. You should be able to convince yourself that no value of b will make $w(b)$ true. Therefore, y is false.

Another way of convincing yourself that y is false is to convince yourself that $\neg y$ is true:

$$\begin{aligned} \neg((\exists b)_{\mathbb{R}^+} ((\forall a)_{\mathbb{R}^+} (ab = 1))) &\Leftrightarrow (\forall b)_{\mathbb{R}^+} \neg((\forall a)_{\mathbb{R}^+} (ab = 1)) \\ &\Leftrightarrow (\forall b)_{\mathbb{R}^+} ((\exists a)_{\mathbb{R}^+} (ab \neq 1)) \end{aligned}$$

In words, for each value of b , a value for a that makes $ab \neq 1$. One such value is $a = \frac{1}{b} + 1$. Therefore, $\neg y$ is true.

EXERCISES FOR SECTION 3.8

A Exercises

1. Let $C(x)$ be " x is cold-blooded," let $F(x)$ be " x is a fish," and let $S(x)$ be " x lives in the sea."

(a) Translate into a formula: Every fish is cold-blooded.

(b) Translate into English: $(\exists x)(S(x) \wedge \neg F(x))$

and $(\forall x)(F(x) \rightarrow S(x))$.

2. Let $M(x)$ be " x is a mammal," let $A(x)$ be " x is an animal," and let $W(x)$ be " x is warm-blooded."

(a) Translate into a formula: Every mammal is warm-blooded.

(b) Translate into English: $(\exists x)(A(x) \wedge (\neg M(x)))$.

3. Over the universe of books, define the propositions $B(x)$: x has a blue cover, $M(x)$: x is a mathematics book, $C(x)$: x is published in the United States, and $R(x, y)$: The bibliography of x includes y . Translate into words:

(a) $(\exists x)(\neg B(x))$.

(b) $(\forall x)(M(x) \wedge U(x) \rightarrow B(x))$.

(c) $(\exists x)(M(x) \wedge \neg B(x))$.

Chapter 3 - Logic

(d) $(\exists y)((\forall x)(M(x) \rightarrow R(x, y)))$.

Express using quantifiers:

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States.

(g) Not all books have bibliographies.

revised

4. Let the universe of discourse, U , be the set of all people, and let $M(x, y)$ be " x is the mother of y ."

(a) Which of the following is a true statement? Translate it into English.

(i) $(\exists x)_U((\forall y)_U(M(x, y)))$

(ii) $(\forall y)_U((\exists x)_U(M(x, y)))$

(b) Translate the following statement into logical notation using quantifiers and the proposition $M(x, y)$ over U : "Everyone has a grandmother,"

5. Translate into your own words and indicate whether it is true or false that $(\exists u)_{\mathbb{Z}}(4u^2 - 9 = 0)$.

6. Use quantifiers to say that $\sqrt{3}$ is an irrational number.

7. What do the following propositions say, where U is the power set of $\{1, 2, \dots, 9\}$? Which of these propositions are true?

(a) $(\forall A)_U(|A| \neq |A^c|)$.

(b) $(\exists A)_U(\exists B)_U(|A| = 5, |B| = 5, \text{ and } A \cap B = \emptyset)$

(c) $(\forall A)_U(\forall B)_U(A - B = B^c - A^c)$

8. Use quantifiers to state that for every positive integer, there is a larger positive integer.

9. Use quantifiers to state that the sum of any two rational numbers is rational.

10. Over the universe of real numbers, use quantifiers to say that the equation $a + x = b$ has a solution for all values of a and b . Hint: You will need three quantifiers.

11. Let n be a positive integer. Describe using quantifiers:

(a) $x \in \bigcup_{k=1}^n A_k$

(b) $x \in \bigcap_{k=1}^n A_k$

12. Prove that $(\exists x)(\forall y)(p(x, y)) \Rightarrow (\forall y)(\exists x)(p(x, y))$, but the converse is not true.

3.9 A Review of Methods of Proof

One of the major goals of this chapter is to acquaint the reader with the key concepts in the nature of proof in logic, which of course carries over into all areas of mathematics and its applications. In this section we will stop, reflect, and "smell the roses," so that these key ideas are not lost in the many concepts covered in logic. In Chapter 4 we will use set theory as a vehicle for further practice and insights into methods of proof.

KEY CONCEPTS IN PROOF

1. All theorems in mathematics can be expressed in "If P then C " ($P \Rightarrow C$) format, or in " C_1 if and only if C_2 " ($P \Leftrightarrow C$) format. The latter is equivalent to "If C_1 then C_2 , and if C_2 then C_1 ." Alternate ways of expressing conditional propositions are found in Section 3.1.
2. In "If P then C ," P is the premise (or hypothesis) and C is the conclusion. It is important to realize that a theorem makes a statement that is dependent on the premise being true.
3. There are two basic methods for proving $P \Rightarrow C$:

(a) **Direct:** Assume P is true and prove C is true; and

(b) **Indirect (proof by contradiction):** Assume P is true and C is false and prove that this leads to a contradiction of some premise, theorem, or basic concept.

4. The method of proof for "If and only if" (iff) theorems is found in the law $(P \leftrightarrow C) \Leftrightarrow ((P \rightarrow C) \wedge (C \rightarrow P))$. Hence to prove an "If and only if" statement one must prove an "if . . . then ..." statement and its converse.

The initial response of most people when confronted with the task of being told they must be able to read and do proofs is:

(a) Why? or,

(b) I cannot do proofs.

To answer the first question, problem solving, even on the most trivial level, involves being able to read statements. First we must understand the problem and know the hypothesis; second, we must realize when we are done and we must understand the conclusion. To apply theorems or algorithms we must be able to read theorems and their proofs intelligently.

To be able to do the actual proofs of theorems we are forced to learn:

(1) the actual meaning of the theorems, and

(2) the basic definitions and concepts of the topic discussed.

For example, when we discuss rational numbers and refer to a number x as being rational, this means we can substitute a fraction $\frac{p}{q}$ in place of x , with the understanding that p and q are integers and $q \neq 0$. Therefore, to prove a theorem about rational numbers it is absolutely necessary that you know what a rational number "looks like."

It's easy to comment on the response, "I cannot do proofs." Have you tried? As elementary school students we were in awe of anyone who could handle algebraic expressions, especially complicated ones. We learned by trying and applying ourselves. Maybe we cannot solve all problems in algebra or calculus, but we are comfortable enough with these subjects to know that we can solve many and can express ourselves intelligently in these areas. The same remarks hold true for proofs.

THE ART OF PROVING $P \Rightarrow C$

First one must completely realize what is given, the hypothesis. The importance of this is usually overlooked by beginners. It makes sense, whenever you begin any task, to spend considerable time thinking about the tools at your disposal. Write down the premise in precise language. Similarly, you have to know when the task is finished. Write down the conclusion in precise language. Then you usually start with P and attempt to show that C follows logically. How do you begin? Basically you attack the proof the same way you solve a complicated equation in elementary algebra. You may not know exactly what each and every step is but you must try something. If we are lucky, C follows naturally; if it doesn't, try something else. Often what is helpful is to work backward from C . Finally, we have all learned, possibly the hard way, that mathematics is a participating sport, not a spectator sport. One learns proofs by doing them, not by watching others do them. We give several illustrations of how to set up the proofs of several examples. Our aim here is not to prove the statements given, but to concentrate on the logical procedure.

Example 3.9.1. We will outline a proof that the sum of any two odd integers is even. Our first step will be to write the theorem in the familiar conditional form: If j and k are odd integers, then $j + k$ is even. The premise and conclusion of this theorem should be clear now. Notice that if j and k are not both odd, then the conclusion may or may not be true. Our only objective is to show that the truth of the premise forces the conclusion to be true. Therefore, we can express the integers j and k in the form that all integers take; that is:

$$n \in \mathbb{Z} \text{ is odd implies } (\exists m \in \mathbb{Z}) (n = 2m + 1).$$

This observation allows us to examine the sum $y + k$ and to verify that it must be even.

Example 3.9.2. Let $n \in \mathbb{Z}$. We will outline a proof that n^2 is even if and only if n is even.

Outline of a proof: Since this is an "If and only if" theorem we must prove two facts (see key concept number 4 above):

Chapter 3 - Logic

I. (\Rightarrow) If n^2 is even, then n is even. To do this directly, assume that n^2 is even and prove that n is even. To do this indirectly, assume n^2 is even and that n is odd, and reach a contradiction. It turns out that the latter of the two approaches is easiest here.

II. (\Leftarrow) If n is even, then n^2 is even. To do this directly, assume that n is even and prove that n^2 is even.

Now that we have broken the theorem down into two parts and know what to prove, we proceed to prove the two implications. The final ingredient that we need is a convenient way of describing even integers. When we refer to an integer n (or m , or k , . . .) as even, we can always replace it with a product of the form $2q$, where q is an integer (more precisely, $(\exists q)_{\mathbb{Z}} (n = 2q)$). In other words, for an integer to be even it must have a factor of two in its prime decomposition.

Example 3.9.3. Our final example will be an outline of the proof that the square root of 2 is irrational (not an element of \mathbb{Q}). This is an example of the theorem that does not appear to be in the standard $P \Rightarrow C$ form. One way to rephrase the theorem is: If x is a rational number, then $x^2 \neq 2$. A direct proof of this theorem would require that we verify that the square of every rational number is not equal to 2. There is no convenient way of doing this, so we must turn to the indirect method of proof. In such a proof, we assume that x is a rational number and that $x^2 = 2$ (i.e., $\sqrt{2}$ is a rational number). This will lead to a contradiction. In order to reach this contradiction, we need to use the following facts:

(a) A rational number is a quotient of two integers.

(b) Every fraction can be reduced to lowest terms, so that the numerator and denominator have no common factor greater than 1.

(c) If n is an integer, n^2 is even if and only if n is even.

EXERCISES FOR SECTION 3.9

B Exercises

1. Prove that the sum of two odd positive integers is even.

2. Write out a complete proof that if n is an integer, n^2 is even if and only if n is even.

3. Write out a complete proof that $\sqrt{2}$ is irrational.

4. Prove that $\sqrt[3]{2}$ is an irrational number.

5. Prove that if x and y are real numbers such that $x + y \leq 1$, then either $x \leq \frac{1}{2}$ or $y \leq \frac{1}{2}$.

6. Use the following definition of absolute value to prove the given statements: If x is a real number, then the absolute value of x , $|x|$, is defined by:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

(a) For any real number x , $|x| \geq 0$. Moreover, $|x| = 0$ implies $x = 0$.

(b) For any two real numbers x and y , $|x| \cdot |y| = |xy|$.

(c) For any two real numbers x and y , $|x + y| \leq |x| + |y|$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 3

Section 3.1

1. Construct the truth tables of

- (a) $p \vee p$
- (b) $p \wedge (\neg p)$
- (c) $p \vee (\neg p)$
- (d) $p \wedge p$

2. Express each of the following in symbolic form and determine whether they are true or false:

- (a) If $a, b \in \mathbb{Z}$, and if $a = 0$ or $b = 0$, then $a \cdot b = 0$.
- (b) If $a, b \in \mathbb{Z}$, and if $a \cdot b = 0$, then $a = 0$ or $b = 0$.
- (c) Let $a, b \in \mathbb{Z}$. $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$.
- (d) If $\{5\} \subseteq \mathbb{Z}$, then $2 + 3 = 8$.
- (e) If $2 + 3 = 8$, then the world is flat.
- (f) 5 is an odd integer if and only if 8 is an even integer.

Section 3.2

3. Write the truth table for the expression $p \vee q \wedge \neg p$.

4. Insert parentheses in the following statements to indicate the order in which the operations are performed:

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

Section 3.3

5. Use truth tables to verify that $((p \rightarrow \neg q) \wedge (q \vee r) \wedge (\neg r)) \Rightarrow \neg p$ is a tautology.

6. Is an implication equivalent to its converse? Verify your answer using a truth table.

7. Prove that an implication is always equivalent to its contrapositive.

8. (a) Construct truth tables for the following propositions generated by p, q , and r .

- (i) $r \wedge (p \wedge q)$ (ii) $r \vee (p \vee q)$ (iii) $r \wedge q$

(b) Which of the propositions i, ii, and iii in part (a) imply proposition i? Explain.

9. Suppose that x is a proposition generated by p and q , and x is equivalent to $p \rightarrow p \wedge q$. What is the truth table for x ?

10. The Sheffer Stroke is the logical operator defined by the following truth table:

p	q	$p q$
0	0	1
0	1	1
1	0	1
1	1	0

Truth Table for the Sheffer Stroke

(a) Prove that $p | q$ is equivalent to $\neg(p \wedge q)$.

The significance of the Sheffer Stroke is that it is a "universal" operator. All other operators can be built from it.

(b) Prove that $\neg p \Leftrightarrow p | p$.

(c) Build \wedge using only the Sheffer Stroke.

Chapter 3 - Logic

(d) Build \vee using only the Sheffer Stroke.

Section 3.4

11. Write the negation of each of the following statements:

- (a) 3 is a prime number and it is even.
- (b) 4 is a prime number or it is odd.
- (c) If I can exhibit an example of a statement then I have proven it true.
- (d) If $x^2 - 11x + 12 = 0$, then $x = 3$ or $x = 8$.

12. Prove that all $\bar{\wedge}$ defined by has the same property as the Sheffer Stroke (see problem 10) in that is a "universal" operator.

p	q	$p \bar{\wedge} q$
0	0	0
0	1	1
1	0	1
1	1	1

Truth Table for $p \bar{\wedge} q$

13. The following are frequently used and very important tautologies in logic. Use truth tables to prove them.

- (a) $(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$
- (b) $(p \leftrightarrow q) \Leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

14. Write the following in symbolic notation and prove it is a tautology: "The statement p if and only if q is equivalent to saying if p then q and if q then p ."

15. Write the following in symbolic notation and determine whether it is a valid argument: "If I quit my job, then I will starve. If I don't do my work, then I must quit my job. I did my work, therefore I will eat."

16. Write the dual of each of the following statements:

- (a) $(\neg p \vee 0) \Rightarrow 1$
- (b) $(p \vee q) \wedge (\neg p \vee r) \Rightarrow (r \vee q)$

Section 3.5

17. Write the following in symbolic form and then determine its validity. "If this car is made in England then parts are difficult to obtain. This car is expensive, or it is not difficult to obtain parts. But this car is not expensive. Hence it was not made in England."

18. In order to attach the Mark 13 printer to the Lemon III computer, you must set eight "dip switches" in the computer according to the following rules. The switches are labeled a through h and are set to be either ON or OFF.

- (1) Neither a nor c is set the same as d.
- (2) b and g are different if and only if e and g are in the same positions.
- (3) g is OFF if d is OFF, but g is ON if b is OFF.
- (4) d is ON, unless e is the same as/.
- (5) h is not the same as a if either b or e is OFF.
- (6) g is OFF only if e is not the same as h.
- (7) b, f, and g are not all the same.

How should the switches be set?

19. Consider the following argument:

If person X does not live in France, then X does not speak French.
X does not drive a Chevrolet.
If X lives in France, then he rides a bicycle.
Either X speaks French or he drives a Chevrolet.
Therefore, X rides a bicycle.

Chapter 3 - Logic

Let p = "X lives in France."

q = "X speaks French."

r = "X drives a Chevrolet."

s = "X rides a bicycle."

Translate the argument into logical notation using these propositions, and prove it by any method except a truth table.

20. Determine the validity of the following argument: "I will miss class only if I sleep late. I will not sleep late. Therefore, I will not miss class."

21. Mayoral candidate Ms. Perpetual Candidate made the following promise to the voters: "If I am elected, I will bring industry to the town. If I bring industry to the town, your taxes will decrease. If your taxes decrease, you will be wealthier. Therefore, if I am elected, you will be wealthier." Express this argument in symbolic notation and determine whether the mayoral candidate is telling the truth.

22. Professor Smoothtalker made the following promise to his class. "If you receive an A in this course, you are happy. You will do all your assignments or you are not happy. If you concentrate too hard, you will not do all your assignments. Therefore, if you are happy, do not concentrate too hard." Is Professor Smoothtalker's argument valid?

23. Determine whether the following argument is valid: Taxes will increase or government spending decreases. Government spending increases or more people have jobs. More people do not have jobs or people are rich. Therefore, if taxes decrease, people are rich.

Section 3.6

24. Let $p(n)$ be $n < 2$ and let $q(n)$ be $n^2 < 5$.

(a) Over the universe of integers, \mathbb{Z} , are p and q equivalent? Does one imply the other?

(b) Over the universe of natural numbers, \mathbb{N} , are p and q equivalent? Does one imply the other?

25. Prove that: $T_{p \wedge q} = T_p \cap T_q$.

26. Prove that: $T_{p \rightarrow q} = T_p^c \cup T_q$.

Section 3.7

27. Express 60 and 120 as a product of primes.

28. Prove that for $n \geq 1$

$$\sum_{i=1}^n i^3 = \frac{1}{4} n^2 (n+1)^2 = \left(\frac{1}{2} n (n+1) \right)^2$$

29. (a) Prove that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ for $k > 1$ and $n \geq k + 1$.

(b) Use mathematical induction to prove the binomial theorem:

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

30. Use mathematical induction to prove for all $n \geq 1$ and for all real numbers c , a_i , and b_i , $i = 1, 2, \dots, n$:

$$(a) \quad \sum_{i=1}^n (a_i + b_i) = \sum_{i=1}^n a_i + \sum_{i=1}^n b_i$$

$$(b) \quad \sum_{i=1}^n c a_i = c \sum_{i=1}^n a_i$$

Section 3.8

31. Write the negation of: "Some sailing is dangerous and all fishing is tedious" in graceful English.

32. Prove: $\neg((\exists u)(\forall v)(p)) \Leftrightarrow (\forall u)((\exists v)(\neg p))$

33. Translate the following sentences into expressions using quantifiers:

(a) All fish except sharks are kind to children.

(b) Either every wine-drinker is very communicative, or some pawn broker is honest and doesn't drink wine.

(c) If all clever philosophers are cynics, and only women are clever philosophers, then, if there are any clever philosophers, some women are cynics.

34. First write each of the following in logical notation using quantifiers, then write the negative of each logical expression using symbols and complete English sentences. If possible, determine which of the statements are true.

Chapter 3 - Logic

- (a) All people in this classroom are over six feet tall.
- (b) Some of the people in this classroom are over six feet tall and are bald.
- (c) Let $U = \{2, 3, 4, 5\}$ and let $p(n)$ denote the statement " n is a prime number." Apply the above directions to the statement: Every number in U is a prime number.
- (d) All prime numbers are odd.
- (e) You will all pass the course Discrete Structures or you will all fail.
- (f) You can fool some of the people some of the time.

35. Use quantifiers to state that for every positive integer, there is a larger positive integer.

36. Over the universe of students in your class, let $N(x, y)$ be " x knows y 's name." Interpret in English:

- (a) $(\exists x)((\forall y)(N(x, y)))$
- (b) $(\forall y)((\exists x)(N(x, y) \text{ and } x \neq y))$
- (c) How would you symbolically say that everyone knows everyone's name?
- (d) How would you symbolically say that everyone knows your name?
- (e) How would you symbolically say that someone in the class has amnesia?

Section 3.9

37. For any nonzero real number x ,

$$x^2 = 1 \Leftrightarrow x = 1 \text{ or } x = -1$$

- (a) Outline the logical procedure you would use to prove this statement.
- (b) Fill in the proof.

38. Let $a, b, c \in \mathbb{P}$ and read $a \mid b$ as " a divides evenly into b ." Consider the statements

- (i) $b \mid a$ and $a \mid b$ implies $a = b$.
- (ii) If p is prime and $p \mid a^2$, then $p \mid a$.
- (a) Are these statements true? Explain your answers.
- (b) Is the converse of each of these statements true? Explain your answers.
- (c) Is the contrapositive of each of these statements true? Explain your answers.

39. Let $a, b \in \mathbb{R}$. A necessary and sufficient condition for $a \cdot b = 0$ is that $a = 0$ or $b = 0$.

- (a) Is this statement true? Explain your answer.
- (b) Outline the logical procedure you would use to prove this statement.