Stein et al

3 Reflections on Logic and Proof

In this chapter, we cover some basic principles of logic and describe some methods for constructing proofs. This chapter is not meant to be a complete enumeration of all possible proof techniques. The philosophy of this book is that most people learn more about proofs by reading, watching, and attempting proofs than by an extended study of the logical rules behind proofs. However, now that we have some examples of proofs, reflecting on their structure and discussing what constitutes a proof will help you read and do proofs. We first develop a language that will allow us to talk about proofs, and then we use this language to describe the logical structure of a proof.

3.1 EQUIVALENCE AND IMPLICATION

Equivalence of Statements

Exercise 3.1-1 A group of students is working on a project that involves writing a merge sort program. Joe and Mary have each written an algorithm for a function that takes two sorted lists, `List1` and `List2`, of lengths p and q, respectively, and merges them into a third list, `List3`. Part of Mary's algorithm is as follows:

```
(1)  if ((i+j ≤ p+q) && (i ≤ p)
        && ((j > q)||(List1[i] ≤ List2[j])))
(2)       List3[k] = List1[i]
(3)       i = i+1
(4)  else
(5)       List3[k] = List2[j]
(6)       j = j+1
(7)  k = k+1
```

The corresponding part of Joe's algorithm is

```
(1) if (((i+j ≤ p+q) && (i ≤ p) && (j > q))
       || ((i+j ≤ p+q) && (i ≤ p) && (List1[i] ≤ List2[j])))
(2)       List3[k] = List1[i]
(3)       i = i+1
(4) else
(5)       List3[k] = List2[j]
(6)       j = j+1
(7) k = k+1
```

Do Joe's and Mary's algorithms do the same thing?

Notice that Joe's and Mary's algorithms are exactly the same except for the `if` statement in Line 1 (how convenient; they even used the same local variables!). In Mary's algorithm, we put entry i of `List1` into position k of `List3` if

$$i + j \leq p + q \quad \text{and} \quad i \leq p \quad \text{and} \quad (j > q \quad \text{or} \quad \texttt{List1}[i] \leq \texttt{List2}[j]),$$

whereas in Joe's algorithm, we put entry i of `List1` into position k of `List3` if

$$(i + j \leq p + q \text{ and } i \leq p \text{ and } j > q) \text{ or } (i + j \leq p + q \text{ and } i \leq p \text{ and } \texttt{List1}[i] \leq \texttt{List2}[j]).$$

Joe's and Mary's statements are both built from the same constituent parts (namely, comparison statements), so we can name these constituent parts and rewrite the statements. We use

- s to stand for $i + j \leq p + q$,
- t to stand for $i \leq p$,
- u to stand for $j > q$, and
- v to stand for $\texttt{List1}[i] \leq \texttt{List2}[j]$.

The condition in Mary's `if` statement on Line 1 of her code becomes

$$s \text{ and } t \text{ and } (u \text{ or } v),$$

while Joe's `if` statement on Line 1 of his code becomes

$$(s \text{ and } t \text{ and } u) \text{ or } (s \text{ and } t \text{ and } v).$$

By recasting the statements in this symbolic form, we see that s and t always appear together as "s and t." We can thus simplify the expressions

by substituting w for "s and t." Mary's condition now has the form

$$w \text{ and } (u \text{ or } v),$$

and Joe's has the form

$$(w \text{ and } u) \text{ or } (w \text{ and } v).$$

Although we can argue, based on our knowledge of the structure of the English language, that Joe's statement and Mary's statement are saying the same thing, it will help us understand logic if we formalize the idea of "saying the same thing." If you look closely at Joe's and Mary's statements, you can see that we are saying that the word "and" distributes over the word "or," just as set intersection distributes over set union and multiplication distributes over addition. To analyze when statements mean the same thing, and to explain more precisely what it means to say something like "'and' distributes over 'or,'" logicians have adopted a standard notation for writing symbolic versions of compound statements. We use the symbol $\wedge$ to stand for "and" and $\vee$ to stand for "or." In this notation, Mary's condition becomes

$$w \wedge (u \vee v),$$

and Joe's becomes

$$(w \wedge u) \vee (w \wedge v).$$

We now have a nice notation (which makes our compound statements look a lot like the two sides of the distributive law for intersection of sets over union), but we have not yet explained why two statements with these symbolic forms mean the same thing. We must therefore give a precise definition of "meaning the same thing" and develop a tool for analyzing when two statements satisfy this definition. We are going to consider symbolic compound statements that may be built up from the following notation:

- Symbols (s, t, etc.), which we call *variables*, standing for statements
- The symbol $\wedge$, standing for "and"
- The symbol $\vee$, standing for "or"
- The symbol $\oplus$, standing for "exclusive or"
- The symbol $\neg$, standing for "not"
- Left and right parentheses

Truth Tables

We now develop a theory for deciding when a compound statement is true based on the truth or falsity of its component statements. Using this theory, we can determine for a particular setting of variables, such as s, t, and u, whether a particular compound statement, such as

$$(s \oplus t) \wedge \big(\neg u \vee (s \wedge t)\big) \wedge \neg\big(s \oplus (t \vee u)\big),$$

is true or false. Our technique uses truth tables, which you have probably seen before. We will soon see why truth tables are the proper tool for determining whether two statements are equivalent.

As with arithmetic, the order of operations in a logical statement is important. Our sample compound statement used parentheses to make it clear which operation to do first, with one exception: the use of the symbol $\neg$. The symbol $\neg$ always has the highest priority, which means that $\neg u \vee (s \wedge t)$ means $(\neg u) \vee (s \wedge t)$ rather than $\neg(u \vee (s \wedge t))$. The principle is simple—the symbol $\neg$ applies to either the symbol or the parenthesized expression immediately following it. This is the same principle used with negative numbers in algebraic expressions. With this one exception, we will always use parentheses to make the order in which we are to perform operations clear; you should do the same.

The operators $\wedge$, $\vee$, $\oplus$, and $\neg$ are called **logical connectives**. The truth table for a logical connective tells us, in terms of the possible truth or falsity of the component parts, when the compound statement made by connecting those parts is true and when it is false. The truth tables for the connectives we have mentioned so far are in Figure 3.1.

AND

s	t	$s \wedge t$
T	T	T
T	F	F
F	T	F
F	F	F

OR

s	t	$s \vee t$
T	T	T
T	F	T
F	T	T
F	F	F

XOR

s	t	$s \oplus t$
T	T	F
T	F	T
F	T	T
F	F	F

NOT

s	$\neg s$
T	F
F	T

Figure 3.1: Truth tables for the basic logical connectives

These truth tables define the words "and," "or," "exclusive or" ("xor" for short), and "not" in the context of symbolic compound statements. For

example, the truth table for $\vee$—"or"—tells us that when s and t are both true, then so is "s or t." It tells us that when s is true and t is false, or s is false and t is true, then "s or t" is true. Finally, it tells us that when s and t are both false, then so is "s or t." Is this how we use the word "or" in English? The answer is "sometimes." The word "or" is used ambiguously in English. When a teacher says, "Each question on the test will be short answer or multiple choice," the teacher is presumably not intending that a question could be both. Thus, the word "or" is being used here in the sense of "exclusive or"—the $\oplus$ in Figure 3.1. When someone says, "Let's see, this afternoon I could take a walk or I could shop for some new gloves," he probably does not mean to preclude the possibility of doing both—perhaps even taking a walk downtown and then shopping for new gloves before walking back. Thus, in English, we determine the way in which someone uses the word "or" from context. In mathematics and computer science, because we don't always have context, we agree to say "exclusive or," or "xor" for short, when that is what we mean; otherwise, we mean the "or" whose truth table is given by $\vee$. In the case of "and" and "not," the truth tables are exactly what we would expect.

We have been thinking of s and t as variables that stand for statements. The purpose of a truth table is to define when a compound statement is true or false in terms of when its component statements are true and false. Because we focus on just the truth and falsity of our statements when we are giving truth tables, we can also think of s and t as variables that can take on the values "true" (T) and "false" (F). We refer to these values as the **truth values** of s and t. A truth table, then, gives us the truth values of a compound statement in terms of the truth values of the component parts of the compound statement. The statements $s \wedge t$, $s \vee t$, and $s \oplus t$ each have two component parts, s and t. Notice that there are two values we can assign to s, and for each value we assign to s, there are two values we can assign to t. By the product principle, there are $2 \cdot 2 = 4$ ways to assign truth values to s and t. Thus, we have four rows in our truth table, one for each way of assigning truth values to s and t.

For a more complex compound statement, such as the one in Line 1 in Joe's and Mary's programs, we still want to describe situations in which the statement is true and situations in which the statement is false. We do this by working out a truth table for the compound statement from the truth tables of its symbolic statements and its connectives. We use a variable to represent the truth value of each symbolic statement. The truth table has one column for each of the original variables and one column for each of the pieces we use to build up the compound statement. The truth table has one row for each possible way of assigning truth values to the original variables. Thus, if we have two variables, we have four rows, as

in the "AND," "OR," and "XOR" tables in Figure 3.1. If we have just one variable, then we have just two rows, as in the "NOT" table in Figure 3.1. If we have three variables, then we have $2^3 = 8$ rows, and so on.

Table 3.1 gives the truth table for the symbolic statement derived from Line 1 of Joe's algorithm. The columns to the left of the dark blue line contain the possible truth values of the variables. The columns to the right correspond to various subexpressions whose truth values we need to compute. The truth table has as many columns as we need in order to compute the final result correctly. As a general rule, each column should be easily computed from one or two previous columns.

w	u	v	$u \vee v$	$w \wedge (u \vee v)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	F	F

Table 3.1: *The truth table for Joe's statement*

Table 3.2 gives the truth table for the statement derived from Line 1 of Mary's algorithm.

Notice that the pattern of T's and F's used to the left of the dark blue line in both Joe's and Mary's truth tables are the same—namely, they are in reverse alphabetical order.[1] Thus, row i of Table 3.1 represents exactly the same assignment of truth values to u, v, and w as row i of Table 3.2. The final columns of Joe's and Mary's truth tables are identical, which means that Joe's symbolic statement and Mary's symbolic statement are true in exactly the same cases. Therefore, the two statements must say the same thing, and Mary's and Joe's program segments return exactly the same values. We say that two symbolic compound statements are **equivalent** if

[1] Alphabetical order is sometimes called *lexicographic order*. Lexicography is the study of the principles and practices used in making dictionaries. Thus, the order we used for the T's and F's is called reverse lexicographic order, or reverse lex order for short.

w	u	v	$w \wedge u$	$w \wedge v$	$(w \wedge u) \vee (w \wedge v)$
T	T	T	T	T	T
T	T	F	T	F	T
T	F	T	F	T	T
T	F	F	F	F	F
F	T	T	F	F	F
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

Table 3.2: *The truth table for Mary's statement*

they are true in exactly the same cases. Alternatively, two statements are equivalent if their truth tables have the same final column (assuming both tables assign truth values to the original symbolic statements in the same pattern).

Tables 3.1 and 3.2 actually prove a **distributive law**:

Lemma 3.1

The statements

$$w \wedge (u \vee v)$$

and

$$(w \wedge u) \vee (w \wedge v)$$

are equivalent.

DeMorgan's Laws

Exercise 3.1-2 **DeMorgan's laws** say that $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$ and that $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$. Use truth tables to demonstrate that DeMorgan's laws are correct.

Exercise 3.1-3 Show that $p \oplus q$ (the exclusive or of p and q) is equivalent to $(p \vee q) \wedge \neg(p \wedge q)$. Apply one of DeMorgan's laws to $\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)$ to find another symbolic statement equivalent to the exclusive or.

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

Table 3.3: *Proving the first DeMorgan's law*

To verify the first DeMorgan's law, we create a "double truth table" by (mentally) condensing two truth tables into one (see Table 3.3). The left sides of the two truth tables we are condensing are identical, so we give just one left side to the left of the first dark blue line. The second dark blue line separates the right sides of the two truth tables we are condensing. In this way, we can still see the computation of the truth values of $\neg(p \vee q)$ and $\neg p \wedge \neg q$. We see that the fourth and the last columns are identical; therefore, the first DeMorgan's law is correct. We can verify the second DeMorgan's law by a similar process.

To show that $p \oplus q$ is equivalent to $(p \vee q) \wedge \neg(p \wedge q)$, we use the double truth table in Table 3.4. Now we deal with the second question in Exercise 3.1-3. Notice first that $\neg(\neg(p \vee q))$ is equivalent to $p \vee q$; t the statement $\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)$ is equivalent to $p \oplus q$. By applying DeMorgan's first law[2] to $\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)$, we see that $p \oplus q$ is also equivalent to $\neg(\neg(p \vee q) \vee (p \wedge q))$. It was easier to use DeMorgan's law to show this equivalence than to use another double truth table.

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

Table 3.4: *An equivalent statement to $p \oplus q$*

[2]Notice that we are applying the law to a statement of the form $\neg s \wedge \neg t$ and getting one of the form $\neg(s \vee t)$.

Implication

Another kind of compound statement occurs frequently in mathematics and computer science. Recall Fermat's Little Theorem (Theorem 2.21):

If p is a prime, then $a^{p-1} \bmod p = 1$ for each nonzero $a \in Z_p$.

Fermat's Little Theorem combines two constituent statements:

- p is a prime, and
- $a^{p-1} \bmod p = 1$ for each nonzero $a \in Z_p$.

We can also restate Fermat's Little Theorem (a bit clumsily) as

- p is a prime only if $a^{p-1} \bmod p = 1$ for each nonzero $a \in Z_p$, or
- p is a prime implies $a^{p-1} \bmod p = 1$ for each nonzero $a \in Z_p$, or
- $a^{p-1} \bmod p = 1$ for each nonzero $a \in Z_p$ if p is prime.

Using s to stand for "p is a prime" and t to stand for "$a^{p-1} \bmod p = 1$ for every nonzero $a \in Z_p$," we can express any of the four statements of Fermat's Little Theorem in symbols as

$$s \Rightarrow t \ ,$$

which most people read as "s implies t." When we translate from symbolic language to English, it is often clearer to say, "If s, then t."

We summarize this discussion in the following definition.

Definition 3.1

The following four English phrases are intended to mean the same thing. In other words, they are defined by the same truth table.

- s implies t.
- If s, then t.
- t if s.
- s only if t.

Observe that the use of "only if" may seem a little different from the normal usage in English. Also observe that there are still other ways of making an "if ... then" statement in English. A number of our lemmas, theorems, and corollaries (for example, Lemma 2.5 and Corollary 2.6) have had two sentences. The first says, "Suppose ...." The second says, "Then

...." The two sentences "Suppose s." and "Then t." are equivalent to the single sentence "$s \Rightarrow t$." When we have a statement equivalent to $s \Rightarrow t$, we call the statement s the **hypothesis** of the implication, and we call the statement t the **conclusion** of the implication.

If and Only If

The word "if" and the phrase "only if" frequently appear together in mathematical statements. For example, Theorem 2.9 stated:

> A number a has a multiplicative inverse in Z_n if and only if there are integers x and y such that $ax + ny = 1$.

Using s to stand for the statement "a number a has a multiplicative inverse in Z_n" and t to stand for the statement "there are integers x and y such that $ax + ny = 1$," we can write this statement symbolically as

$$s \text{ if and only if } t.$$

Referring to Definition 3.1, we parse this as

$$s \text{ if } t, \text{ and } s \text{ only if } t,$$

which by the definition above is the same as

$$t \Rightarrow s \text{ and } s \Rightarrow t.$$

We denote the statement "s if and only if t" by $s \Leftrightarrow t$. Statements of the form $s \Rightarrow t$ and $s \Leftrightarrow t$ are called **conditional statements**, and the connectives $\Rightarrow$ and $\Leftrightarrow$ are called **conditional connectives**.

Exercise 3.1-4 Use truth tables to explain the difference between $s \Rightarrow t$ and $s \Leftrightarrow t$.

To analyze the truth and falsity of statements involving "implies" and "if and only if," we need to understand exactly how they are different. By constructing truth tables for these statements, we see that there is only one case in which they could have different truth values. In particular, if s is true and t is true, then we would say that both $s \Rightarrow t$ and $s \Leftrightarrow t$ are true. If s is true and t is false, we would say that both $s \Rightarrow t$ and $s \Leftrightarrow t$ are false. In the case that both s and t are false, we would say that $s \Leftrightarrow t$ is true. What about $s \Rightarrow t$? Let's try an example. Suppose s is the statement "It is supposed to rain" and t is the statement "I carry an umbrella." If, on a given day, it is not supposed to rain and I do not carry an umbrella, we would

say that the statement "If it is supposed to rain, then I carry an umbrella" is true on that day. This suggests that we also want to say $s \Rightarrow t$ is true if s is false and t is false.[3] Thus, the truth tables are identical in Rows 1, 2, and 4. For "implies" and "if and only if" to mean different things, the truth tables must therefore be different in Row 3. (Row 3 is the case where s is false and t is true.) Clearly, in this case, we would want $s \Leftrightarrow t$ to be false. Therefore either $s \Rightarrow t$ is true or "implies" and "if and only if" are identical, so we need only one of them.

Does it make sense to say that the statement "If it is supposed to rain, then I carry an umbrella" is true if it is not supposed to rain and I carry an umbrella? It depends on how you interpret "if." Mathematicians have found it useful to say that the statement says nothing about what I do on days when it is not supposed to rain. I can choose to carry an umbrella or not to carry an umbrella without contradicting the statement. By this way of thinking, the statement is true even if it is not supposed to rain and I carry an umbrella.

This gives us the truth tables in Figure 3.2.

IMPLIES

s	t	$s \Rightarrow t$
T	T	T
T	F	F
F	T	T
F	F	T

IF AND ONLY IF

s	t	$s \Leftrightarrow t$
T	T	T
T	F	F
F	T	F
F	F	T

Figure 3.2: The truth tables for "implies" and for "if and only if"

Here is another place where English usage is sometimes inconsistent. Suppose a parent says, "I will take the family to McDougall's for dinner if you get an A on this test," and even though the student gets a C, the parent still takes the family to McDougall's for dinner. Although this outcome

[3]Note that we are making this conclusion on the basis of one example. Why can we do so? We are not trying to prove something; rather, we are trying to figure out what the appropriate definition is for the $\Rightarrow$ connective. Because we have said that the truth or falsity of $s \Rightarrow t$ depends only on the truth or falsity of s and t, one example serves to lead us to an appropriate definition. If a different example led us to a different definition, then we would want to define two different kinds of implications, just as we have two different kinds of "ors," $\vee$ and $\oplus$. Fortunately, the only kinds of conditional statements we need for doing mathematics and computer science are "implies" and "if and only if."

is something we didn't expect, was the parent's statement still true? Some people would say "yes"; others would say "no." Those who would say "no" mean, in effect, that in this context, the parent's statement meant the same as, "I will take the family to dinner at McDougall's if and only if you get an A on this test." In other words, to some people and in certain contexts, "if" and "if and only if" mean the same thing. Fortunately, questions of child rearing aren't part of mathematics or computer science (at least not this kind of question!). In mathematics and computer science, we adopt the two truth tables in Figure 3.2 as the meaning of the compound statement $s \Rightarrow t$ (or "if s, then t" or "t if s") and the compound statement $s \Leftrightarrow t$ (or "s if and only if t"). In particular, the truth table for "implies" in Figure 3.2 is the one referred to in Definition 3.1, and thus it defines the mathematical meaning of s implies t or any of the other three statements referred to in that definition.

Some people have difficulty using the truth table for $s \Rightarrow t$ because of this ambiguity in English. The following example can be helpful in resolving this ambiguity: Suppose a classmate holds an ordinary playing card (with its back to you) and says, "If this card is a heart, then it is a queen." In which of the following four circumstances would you say your classmate lie

1. The card is a heart and a queen.
2. The card is a heart and a king.
3. The card is a diamond and a queen.
4. The card is a diamond and a king.

You would certainly say she lied in the case that the card is the king of hearts, and you would certainly say she didn't lie if the card is the queen of hearts. In this example, the inconsistency of the English language should seem out of place to you, and you would not say your classmate is a liar in either of the other cases. Now we apply the **principle of the excluded middle**.

Principle 3.1 (The Principle of the Excluded Middle)

A statement is true exactly when it is not false.

This principle tells us that the statement is true in the three cases where you wouldn't say your classmate lied. We used this principle implicitly when

we introduced proof by contradiction (Principle 2.1). We were explaining Corollary 2.6, which states:

> Suppose there is a b in Z_n such that the equation
>
> $$a \cdot_n x = b$$
>
> does not have a solution. Then a does not have a multiplicative inverse in Z_n.

We had assumed that the hypothesis of the corollary was true so that $a \cdot_n x = b$ does not have a solution. Then we assumed that the conclusion that a does not have a multiplicative inverse was false. We saw that these two assumptions led to a contradiction; thus, it was impossible for both of them to be true. We concluded that whenever the first assumption was true, the second had to be false. Why could we conclude this? Because the principle of the excluded middle says that the second assumption has to be either true or false. We didn't introduce the principle of the excluded middle at that point for two reasons. First, we expected that you would agree with our proof even if we didn't mention the principle, and second, we didn't want to confuse your understanding of proof by contradiction by talking about two principles at once.

Important Concepts, Formulas, and Theorems

1. *Logical statements.* Logical statements may be built up from the following notation:
   - Symbols (s, t, etc.), which we call variables, standing for statements
   - The symbol $\wedge$, standing for "and"
   - The symbol $\vee$, standing for "or"
   - The symbol $\oplus$, standing for "exclusive or"
   - The symbol $\neg$, standing for "not"
   - The symbol $\Rightarrow$, standing for "implies"
   - The symbol $\Leftrightarrow$, standing for "if and only if"
   - Left and right parentheses

   The operators $\wedge$, $\vee$, $\oplus$, $\Rightarrow$, $\Leftrightarrow$, and $\neg$ are called *logical connectives.* The operators $\Rightarrow$ and $\Leftrightarrow$ are called *conditional connectives.*

2. *Truth tables.* The following are truth tables for the basic logical connectives.

AND

s	t	$s \wedge t$
T	T	T
T	F	F
F	T	F
F	F	F

OR

s	t	$s \vee t$
T	T	T
T	F	T
F	T	T
F	F	F

XOR

s	t	$s \oplus t$
T	T	F
T	F	T
F	T	T
F	F	F

NOT

s	$\neg s$
T	F
F	T

3. *Equivalence of logical statements.* We say that two symbolic compound statements are *equivalent* if they are true in exactly the same cases.

4. *Distributive law.* The statements $w \wedge (u \vee v)$ and $(w \wedge u) \vee (w \wedge v)$ are equivalent.

5. *DeMorgan's laws.* DeMorgan's laws say that $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$ and that $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$.

6. *Implication.* The following four English phrases are equivalent:

   - s implies t.
   - If s, then t.
   - t if s.
   - s only if t.

7. *Truth tables for "implies" and "if and only if."*

IMPLIES

s	t	$s \Rightarrow t$
T	T	T
T	F	F
F	T	T
F	F	T

IF AND ONLY IF

s	t	$s \Leftrightarrow t$
T	T	T
T	F	F
F	T	F
F	F	T

8. *Principle of the excluded middle.* A statement is true exactly when it is not false.

Problems

All problems with blue boxes have an answer or hint available at the end of the book.

1. Give truth tables for the following expressions.
   a. $(s \vee t) \wedge (\neg s \vee t) \wedge (s \vee \neg t)$
   b. $(s \Rightarrow t) \wedge (t \Rightarrow u)$
   c. $(s \vee t \vee u) \wedge (s \vee \neg t \vee u)$
2. Find at least two more examples of the use of some word or phrase equivalent to "implies" in lemmas, theorems, or corollaries in Chapters 1 or 2.
3. Find at least two more examples of the use of the phrase "if and only if" in lemmas, theorems, and corollaries in Chapters 1 or 2.
4. Show that the statements $s \Rightarrow t$ and $\neg s \vee t$ are equivalent.
5. Prove the DeMorgan law that states $\neg(p \wedge q) = \neg p \vee \neg q$.
6. Show that $p \oplus q$ is equivalent to $(p \wedge \neg q) \vee (\neg p \wedge q)$.
7. Give a simplified form of each of the following expressions (using T to stand for a statement that is always true and F to stand for a statement that is always false).[4]
   a. $s \vee s$
   b. $s \wedge s$
   c. $s \vee \neg s$
   d. $s \wedge \neg s$
8. Using T to stand for a statement that is always true and F to stand for a statement that is always false, give a simplified form of each of the following statements.
   a. $T \wedge s$
   b. $F \wedge s$
   c. $T \vee s$
   d. $F \vee s$

[4] A statement that is always true is called a *tautology;* a statement that is always false is called a *contradiction.*

9. Use DeMorgan's law, the distributive law, and Problems 7 and/or 8 to show that

$$\neg(s \vee t) \vee \neg(s \vee \neg t)$$

is equivalent to $\neg s$.

10. Give an example in English where "or" seems to mean "exclusive or" (or where you think it would for many people) and an example in English where "or" seems to mean "inclusive or" (or where you think it would for many people).

11. Give an example in English where "if . . . then" seems to mean "if and only if" (or where you think it would to many people) and an example in English where it seems not to mean "if and only if" (or where you think it would not to many people).

12. Find a statement involving only $\wedge$, $\vee$, and $\neg$ (and s and t) equivalent to $s \Leftrightarrow t$. Does your statement have as few symbols as possible? If you think it doesn't, try to find one with fewer symbols.

13. Suppose that for each line of a two-variable truth table, you are told whether the final column in that line should evaluate to true or to false. (For example, you might be told that the final column should contain T, F, F, and T, in that order. Notice that Problem 12 can be interpreted as asking for this pattern.) Explain how to create a logical statement using the symbols s, t, $\wedge$, $\vee$, and $\neg$ that has that pattern as its final column. Can you extend this procedure to an arbitrary number of variables?

14. In Problem 13, your solution may have used $\wedge$, $\vee$, and $\neg$. Is it possible to give a solution using only one of these symbols? Is it possible to give a solution using only two of these symbols?

15. We proved that $\wedge$ distributes over $\vee$ in the sense of giving two equivalent statements that represent the two "sides" of the distributive law. Answer each question that follows, and explain why your answer is correct.

    a. Does $\vee$ distribute over $\wedge$?

    b. Does $\vee$ distribute over $\oplus$?

    c. Does $\wedge$ distribute over $\oplus$?

3.2 VARIABLES AND QUANTIFIERS

Variables and Universes

Statements we use in computer languages to control loops or conditionals are statements about variables. When we declare these variables, we give the computer information about their possible values. For example, in some programming languages, we may declare a variable to be a Boolean or an integer or a real number.[5] In English and in mathematics, we also make statements about variables, but it is not always clear which words are being used as variables and what values these variables may take on. We use the phrase **varies over** to describe the set of values a variable may take on. For example, in English we might say, "If someone's umbrella is up, then it must be raining." In this case, the word "someone" is a variable, and presumably it *varies over* the people who happen to be in a given place at a given time. In mathematics, we might say, "For every pair of positive integers m and n, there are nonnegative integers q and r, with $0 \leq r < n$, such that $m = nq + r$." In this case, m, n, q, and r are clearly variables; our statement itself suggests that two variables range over the positive integers and two range over the nonnegative integers. We call the set of possible values for a variable the **universe** of that variable.

In the statement "m is an even integer," it is clear that m is a variable, but the universe is not given. The universe might be the integers, only the even integers, the rational numbers, or one of many other sets. The choice of the universe is crucial for determining the truth or falsity of a statement. If we choose the set of integers as the universe for m, then the statement is true for some integers and false for others. On the other hand, if we choose integer multiples of 10 as our universe, then the statement is always true. In the same way, when we control a `while` loop with a statement such as "$i < j$," there are some values of i and j for which the statement is true and some for which it is false. In statements like "m is an even integer" and "$i < j$," our variables are not constrained, and so they are called **free variables**. For each possible value of a free variable, we have a new statement, which might be either true or false, determined by substituting the possible value for the variable. The truth value of the statement is determined only after such a substitution.

[5]Note that to declare a variable x as an integer in, say, a C program does not mean the same thing as saying that x is an integer. In a C program, an integer may really be a 32-bit integer, so it is limited to values between $2^{31} - 1$ and -2^{31}. Similarly, a real has some fixed precision; hence, a real variable y may not be able to take on a value of, say, 10^{-985}.

Exercise 3.2-1 For what values of m is the statement $m^2 > m$ a true statement and for what values is it a false statement? Because a universe is not specified, our answer will depend on what universe we choose to use.

For the universe of positive integers, the statement is true for every value of m but 1. For the universe of the real numbers, the statement is true for every value of m except for those in the closed interval $[0, 1]$. There are really two points to make here. First, a statement about a variable can often be interpreted as a statement about more than one universe; so, to make the statement unambiguous, we must clearly state the universe we have in mind. Second, a statement about a variable can be true for some values of a variable and false for others.

Quantifiers

In contrast, the statement

$$\text{For every integer } m,\ m^2 > m. \tag{3.1}$$

is false; we do not need to qualify our answer by saying that it is true some of the time and false at other times. To determine whether Statement 3.1 is true or false, we could substitute various values for m into the simpler statement $m^2 > m$ and decide, for each of these values, whether the statement $m^2 > m$ is true or false. Doing so, we see that the statement $m^2 > m$ is true for values such as $m = -3$ or $m = 9$ but false for $m = 0$ or $m = 1$. Thus, it is not the case that $m^2 > m$ for every integer m. Therefore, Statement 3.1 is false, because it is an assertion that the simpler statement $m^2 > m$ holds for each integer value of m we substitute. A phrase like "for every integer m," which converts a symbolic statement about potentially any member of our universe into a statement about the universe instead, is called a **quantifier**. A quantifier that asserts that a statement about a variable is true for every value of the variable in its universe, for example, "for every integer," is called a **universal quantifier**. This example illustrates a very important point.

> If a statement asserts something for every value of a variable, then to show the statement is false, we need only give one value of the variable for which the assertion is untrue.

Another example of a quantifier is the phrase "There is an integer m" in the sentence "There is an integer m such that $m^2 > m$." This statement is also

about the universe of integers, and as such, it is true—there are plenty of integers m we can substitute into the symbolic statement $m^2 > m$ to make it true. This is an example of an **existential quantifier**, which asserts that a certain element of our universe exists. A second important point similar to the one we made above is as follows:

> To show that a statement with an existential quantifier is true, we need only exhibit one value of the variable being quantified that makes the statement true.

As the more complex statement

> For every pair of positive integers m and n, there are nonnegative integers q and r with $0 \leq r < n$ such that $m = qn + r$

shows, statements of mathematical interest abound with quantifiers. Mathematical statements of theorems, lemmas, and corollaries often have quantifiers. For example, in Lemma 2.5, the phrase "for any" is a quantifier, and in Corollary 2.6, the phrase "there is" is a quantifier. Quantifiers often occur in definitions as well. Recall the following definition of the big O notation, which you have probably used in earlier computer science courses.

Definition 3.2

For a function $f : R \to R$ and a function $g : R \to R$ with nonnegative values, we say that $f(x) = O(g(x))$ if there are positive numbers c and n_0 such that $f(x) \leq cg(x)$ for every $x > n_0$.

Exercise 3.2-2 Quantification is present in our everyday language. The sentences "Every child wants a pony" and "No child wants a toothache" are two different examples of quantified sentences. Give 10 examples of everyday sentences that use quantifiers, but use different words to indicate the quantification.

Exercise 3.2-3 Convert the sentence "No child wants a toothache" into a sentence of the form "It is not the case that...." Find an existential quantifier in your sentence.

Exercise 3.2-4 What would you have to do to show that a statement about one variable with an existential quantifier is false? Correspondingly, what would you have to do to show that a statement about one variable with a universal quantifier is true?

As Exercise 3.2-2 points out, English has many different ways to express quantifiers. For example, the sentences, "All hammers are tools," "Each sandwich is delicious," "No one in their right mind would do that," "Somebody loves me," and "Yes, Virginia, there is a Santa Claus" all contain quantifiers. For Exercise 3.2-3, we can say, "It is not the case that there is a child who wants a toothache." Our quantifier is the phrase "there is."

To show that a statement about one variable with an existential quantifier is false, we have to show that every element of the universe makes the statement (such as $m^2 > m$) false. Thus, to show that the statement "There is an x in $[0, 1]$ with $x^2 > x$" is false, we have to show that every x in the interval makes the statement "$x^2 > x$" false. Similarly, to show that a statement with a universal quantifier is true, we have to show that the statement being quantified is true for every member of our univers Later in this section, we give more details about how to show tha statement about a variable is true or false for every member of our universe.

Standard Notation for Quantification

Each of the many variants of a language that describe quantification describe one of two situations. A quantified statement about a variable x asserts either that

- the statement is true for all x in the universe, or
- there exists an x in the universe that makes the statement true.

All quantified statements have one of these two forms. We use the standard shorthand of $\forall$ for the phrase "for all" and the standard shorthand of $\exists$ for the phrase "there exists." We also adopt the convention of putting parentheses around the expression that is subject to the quantification. For example, using Z to stand for the universe of all integers, we write

$$\forall n \in Z(n^2 \geq n)$$

as a shorthand for the statement "For all integers n, $n^2 \geq n$." It is perhaps more natural to read the notation as "For all n in Z, $n^2 \geq n$," which is how

we recommend reading the symbolism. We similarly use

$$\exists n \in Z(n^2 \not> n)$$

to stand for "There exists an n in Z such that $n^2 \not> n$." Notice that to cast our symbolic form of an existence statement into grammatical English, we have included the supplementary word "an" and the supplementary phrase "such that." People often leave out the "an" as they read an existence statement, but they rarely leave out the "such that." Such supplementary language is not needed with $\forall$.

As another example, we use these symbols to rewrite the definition of the big O notation. We use the letter R to stand for the universe of real numbers and the symbol R^+ to stand for the universe of positive real numbers. We assume implicitly that the function $g : R \to R$ takes nonnegative values.

$f = O(g)$ means that
$\exists c \in R^+(\exists n_0 \in R^+(\forall x \in R(x > n_0 \Rightarrow f(x) \leq cg(x))))$.

We would read this literally as

"f is big O of g" means that there exists a c in R^+ such that there exists an n_0 in R^+ such that for all x in R, if $x > n_0$, then $f(x) \leq cg(x)$.

Clearly, this statement has the same meaning (when we translate it into more idiomatic English) as

"f is big O of g" means that there exist positive real numbers c and n_0 such that for all real numbers $x > n_0$, $f(x) \leq cg(x)$.

This statement is identical to the definition of big O that we gave in Definition 3.2, except it is more precise in describing what c and n_0 actually are.

Exercise 3.2-5 Using the shorthand notation for quantifiers, how would you rewrite the part of Euclid's division theorem (Theorem 2.12), "for every positive integer n and every nonnegative integer m, there are integers q and r, with $0 \leq r < n$, such that $m = qn + r$"? Use Z^+ to stand for the positive integers and N to stand for the nonnegative integers.

We can rewrite Euclid's division theorem as

$$\forall n \in Z^+\Big(\forall m \in N\Big(\exists q \in N\Big(\exists r \in N\big((r < n) \wedge (m = qn + r)\big)\Big)\Big)\Big).$$

Statements about Variables

To discuss a statement about a variable, it is helpful to have a notation for referring to the statement. For example, we can use $p(n)$ to stand for the statement $n^2 > n$. Now we can say that $p(4)$ and $p(-3)$ are true, while $p(1)$ and $p(0.5)$ are false. In effect, we are introducing variables that stand for statements about other variables. We use symbols like $p(n)$, $q(x)$, and so forth to stand for statements about a variable n or x. The statement "For all x in U $p(x)$" can thus be written as $\forall x \in U(p(x))$, and the statement "There exists an n in U such that $q(n)$" can be written as $\exists n \in U(q(n))$. Sometimes we have statements about more than one variable. For example, our definition of big O notation had the form $\exists c(\exists n_0(\forall x(p(c, n_0, x))))$, where $p(c, n_0, x)$ stands for $(x > n_0 \Rightarrow f(x) \leq cg(x))$. (We have left out mention of the universes for our variables to emphasize the form of the statement.)

Exercise 3.2-6 Use the notation for statements about variables to rewrite the part of Euclid's division theorem we gave in Exercise 3.2-5. Leave out the references to universes so that you can see clearly the order in which the quantifiers occur. Use $p(m, n, q, r)$ to stand for "$m = nq + r$ with $0 \leq r < n$."

The form of Euclid's division theorem is $\forall n(\forall m(\exists q(\exists r(p(m, n, q, r)))))$.

Rewriting Statements to Encompass Larger Universes

It is sometimes useful to rewrite a quantified statement so that the universe is larger while the statement itself focuses on a subset of the new universe.

Exercise 3.2-7 Let R stand for the real numbers and R^+ stand for the positive real numbers. Consider the following two statements.

a. $\forall x \in R^+(x > 1)$

b. $\exists x \in R^+(x > 1)$

Rewrite these statements so that the universe is all the real numbers but the statements say the same thing in everyday English that they did before.

For Exercise 3.2-7, there are potentially many ways to rewrite the statements. Two particularly simple ways are $\forall x \in R(x > 0 \Rightarrow x > 1)$ and $\exists x \in R(x > 0 \wedge x > 1)$. Notice that we translated one of these statements with "implies" and one with "and." We can state this rule as a general theorem.

Theorem 3.2 Let U_1 be a universe and let U_2 be another universe, with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement such that

$$U_1 = \{x \mid q(x) \text{ is true}\}. \tag{3.2}$$

Then, if $p(x)$ is a statement about U_2, it may also be interpreted as a statement about U_1, and

a. $\forall x \in U_1\big(p(x)\big)$ is equivalent to $\forall x \in U_2\big(q(x) \Rightarrow p(x)\big)$, and

b. $\exists x \in U_1\big(p(x)\big)$ is equivalent to $\exists x \in U_2\big(q(x) \wedge p(x)\big)$.

Proof By Equation 3.2, the statement $q(x)$ must be true for all $x \in U_1$ and false for all x in U_2 but not U_1. To prove part a, we must show that $\forall x \in U_1(p(x))$ is true in exactly the same cases as the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$. For this purpose, suppose first that $\forall x \in U_1(p(x))$ is true. Then $p(x)$ is true for all x in U_1. Therefore, by the truth table for "implies" and our remark about Equation 3.2, the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is true. Now suppose $\forall x \in U_1(p(x))$ is false. Then there exists an x in U_1 such that $p(x)$ is false. By the truth table for "implies," the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is false. Thus, the statement $\forall x \in U_1(p(x))$ is true if and only if the statement $\forall x \in U_2(q(x) \Rightarrow p(x))$ is true. Therefore, the two statements are true in exactly the same cases. Part a of the theorem follows.

Similarly, for part b, we observe that if $\exists x \in U_1(p(x))$ is true, then $p(x')$ is true for some $x' \in U_1$. For that x', $q(x')$ is also true. Hence, $p(x') \wedge q(x')$ is true so that $\exists x \in U_2(q(x) \wedge p(x))$ is true as well. On the other hand, if $\exists x \in U_1(p(x))$ is false, then no $x \in U_1$ has $p(x)$ true. Therefore, by the truth table for "and," $q(x) \wedge p(x)$ won't be true either. Thus, the two statements in part b are true in exactly the same cases and, so, are equivalent.

Proving Quantified Statements True or False

Exercise 3.2-8 Let R stand for the real numbers and R^+ stand for the positive real numbers. For each of the following statements, state whether it is true or false and explain why.

a. $\forall x \in R^+(x > 1)$

b. $\exists x \in R^+(x > 1)$

c. $\forall x \in R(\exists y \in R(y > x))$

d. $\forall x \in R(\forall y \in R(y > x))$

e. $\exists x \in R(x \geq 0 \wedge \forall y \in R^+(y > x))$

In Exercise 3.2-8, because $1/2$ is not greater than 1, statement a is false. However, because $2 > 1$, statement b is true. Statement c says that for each real number x, there is a real number y bigger than x, which we know is true. Statement d says that every y in R is larger than every x in R, and so it is false. Statement e says that there is a nonnegative number x such that every positive y is larger than x, which is true because $x = 0$ fills the bill.

We can summarize what we know about the meaning of quantified statements as follows.

Principle 3.2 (The Meaning of Quantified Statements)

- The statement $\exists x \in U(p(x))$ is true if there is at least one value of x in U for which the statement $p(x)$ is true.
- The statement $\exists x \in U(p(x))$ is false if there is no $x \in U$ for which $p(x)$ is true.
- The statement $\forall x \in U(p(x))$ is true if $p(x)$ is true for each value of x in U.
- The statement $\forall x \in U(p(x))$ is false if $p(x)$ is false for at least one value of x in U.

Negation of Quantified Statements

An interesting connection between $\forall$ and $\exists$ arises from the negation of statements.

Exercise 3.2-9 What does the statement "It is not the case that $n^2 > 0$ for all integers n" mean?

From our knowledge of English, we see that the statement[6] $\neg\forall n \in Z(n^2 > 0)$ asserts that it is not the case that we have $n^2 > 0$ for all integers n. Therefore, the statement asserts that there must be some integer n such that $n^2 \not> 0$. In other words, it says there is some integer n such that $n^2 \leq 0$. Thus, the negation of our "for all" statement is a "there exists" statement. We can make this idea more precise by recalling the notion of equivalence of statements. We have said that two symbolic statements are equivalent if they are true in exactly the same cases. By considering the case where $p(x)$ is true for all $x \in U$ (we call this case "always true") and the case where

[6]The convention is that when $\neg$ appears before a quantifier, the entire quantified statement is negated.

$p(x)$ is false for at least one $x \in U$ (we call this case "not always true"), we can analyze the equivalence. The theorem that follows formalizes the example above in which $p(x)$ was the statement $x^2 > 0$. The theorem is proved by dividing all values of the variables into two possibilities: the case where $p(x)$ is always true and the case where it is not always true.

Theorem 3.3 The statements $\neg\forall x \in U(p(x))$ and $\exists x \in U(\neg p(x))$ are equivalent.

Proof Consider the following table (which we have set up much like a truth table, except that the relevant cases are not determined by whether $p(x)$ is true or false, but by whether or not $p(x)$ is true for all x in the universe U).

$p(x)$	$\neg p(x)$	$\forall x \in U(p(x))$	$\neg\forall x \in U(p(x))$	$\exists x \in U(\neg p(x))$
always true	always false	true	false	false
not always true	not always false	false	true	true

Because the last two columns are identical, the theorem holds.

Corollary 3.4 The statements $\neg\exists x \in U(q(x))$ and $\forall x \in U(\neg q(x))$ are equivalent.

Proof Because the two statements in Theorem 3.3 are equivalent, their negations are also equivalent. We then substitute $\neg q(x)$ for $p(x)$ to prove the corollary.

Put another way, when you negate a quantified statement, you switch the quantifier and "push" the negation inside.

To deal with the negation of more complicated statements, we simply take them one quantifier at a time. Recall Definition 3.2, the definition of big O notation:

$$f(x) = O(g(x)) \text{ if } \exists c \in R^+\left(\exists n_0 \in R^+\left(\forall x \in R\left(x > n_0 \Rightarrow f(x) \leq cg(x)\right)\right)\right).$$

What does it mean to say that $f(x)$ is *not* $O(g(x))$? First, we can write

$$f(x) \neq O(g(x)) \text{ if } \neg\exists c \in R^+\left(\exists n_0 \in R^+\left(\forall x \in R\left(x > n_0 \Rightarrow f(x) \leq cg(x)\right)\right)\right).$$

After one application of Corollary 3.4, we get

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+ \left(\neg \exists n_0 \in R^+ \left(\forall x \in R \left(x > n_0 \Rightarrow f(x) \leq cg(x)\right)\right)\right).$$

After another application of Corollary 3.4, we obtain

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+ \left(\forall n_0 \in R^+ \left(\neg \forall x \in R \left(x > n_0 \Rightarrow f(x) \leq cg(x)\right)\right)\right).$$

Now we apply Theorem 3.3 to obtain

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+ \left(\forall n_0 \in R^+ \left(\exists x \in R \left(\neg \left(x > n_0 \Rightarrow f(x) \leq cg(x)\right)\right)\right)\right).$$

Because $\neg(p \Rightarrow q)$ is equivalent to $p \wedge \neg q$, we can write

$$f(x) \neq O(g(x)) \text{ if } \forall c \in R^+ \left(\forall n_0 \in R^+ \left(\exists x \in R \left((x > n_0) \wedge \left(f(x) \not\leq cg(x)\right)\right)\right)\right).$$

Thus, $f(x)$ is *not* $O(g(x))$ if for every c in R^+ and every n_0 in R, there is an x such that $x > n_0$ and $f(x) \not\leq cg(x)$.

In our next exercise, we will use the big Θ notation, defined as follows:

Definition 3.3

$f(x) = \Theta(g(x))$ means that $f(x) = O(g(x))$ and $g(x) = O(f(x))$.

Exercise 3.2-10 Express $\neg(f(x) = \Theta(g(x)))$ in terms similar to those used to describe $f(x) \neq O(g(x))$.

Exercise 3.2-11 Suppose the universe for a statement $p(x)$ is the integers from 1 to 10. Express the statement $\forall x(p(x))$ without any quantifiers. Express the negation in terms of $\neg p$ without any quantifiers. Discuss how negation of "for all" and "there exists" statements corresponds to DeMorgan's law.

By DeMorgan's law, $\neg(f = \Theta(g))$ means $\neg(f = O(g)) \vee \neg(g = O(f))$. Thus, $\neg(f = \Theta(g))$ means either that

- for every c in R^+ and n_0 in R, there is an x in R with $x > n_0$ and $f(x) \not< cg(x)$, or

- for every c in R^+ and n_0 in R, there is an x in R with $x > n_0$ and $g(x) < cf(x)$,

or both. For Exercise 3.2-11, we see that $\forall x(p(x))$ is simply

$$p(1) \wedge p(2) \wedge p(3) \wedge p(4) \wedge p(5) \wedge$$
$$p(6) \wedge p(7) \wedge p(8) \wedge p(9) \wedge p(10).$$

by DeMorgan's law, the negation of this statement is

$$\neg p(1) \vee \neg p(2) \vee \neg p(3) \vee \neg p(4) \vee \neg p(5) \vee \neg p(6)$$
$$\vee \neg p(7) \vee \neg p(8) \vee \neg p(9) \vee \neg p(10).$$

Thus, the relationship that negation gives between "for all" and "there exists" statements is the extension of DeMorgan's law from a finite number of statements to potentially infinitely many statements about a potentially infinite universe.

Implicit Quantification

Exercise 3.2-12 Are there any quantifiers in the statement "The sum of even integers is even"?

An elementary fact about numbers is that the sum of even integers is even. Another way to say this is that if m and n are even, then $m + n$ is even. If $p(n)$ stands for the statement "n is even," then this last sentence translates to $p(m) \wedge p(n) \Rightarrow p(m + n)$. From the logical form of the statement, we see that our variables are free, so we could substitute various integers for m and n to see whether the statement is true. In Exercise 3.2-12, however, we said that we were stating a more general fact about the integers. What we meant to say is that for *every pair of integers* m and n, if m and n are even, then $m + n$ is even. In symbols, using $p(k)$ for "k is even," we have

$$\forall m \in Z\Big(\forall n \in Z\big(p(m) \wedge p(n) \Rightarrow p(m + n)\big)\Big).$$

This way of representing the statement captures the meaning we originally intended. This is one of the reasons that mathematical statements and their proofs sometimes seem confusing—just as in English, sentences in mathematics have to be interpreted in context. Because mathematics has to be written in some natural language, and because context is used to remove ambiguity in natural language, context must be used to remove

ambiguity from mathematical statements made in natural language. In fact, we frequently rely on context when writing mathematical statements with implicit quantifiers, because it makes the statements easier to read. For example, Lemma 2.8 said

> The equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x and y such that $ax + ny = 1$.

In context, it was clear that the a we were talking about was an arbitrary member of Z_n. It would simply have made the statement read more clumsily if we had said

> For every $a \in Z_n$, the equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x and y such that $ax + ny = 1$.

On the other hand, we were making a transition from talking about Z_n to talking about the integers, so it was important for us to include the quantified statement "there exist integers x and y such that $ax + ny = 1$." More recently, in Theorem 3.3, we also did not feel it was necessary to say "for all universes U and for all statements p about U" at the beginning of the theorem. We felt the theorem would be easier to read if we kept those quantifiers implicit and let you infer them from context (not necessarily consciously).

Proof of Quantified Statements

We said that "the sum of even integers is even" is an elementary fact about numbers. How do we know it is a fact? One answer is that we know it because our teachers told us so (and presumably they knew it because their teachers told them so). But someone had to figure it out in the first place. So we ask, "How would we prove this statement?" A mathematician asked to give a proof that the sum of even numbers is even might write, "If m and n are even, then $m = 2i$ and $n = 2j$ so that $m + n = 2i + 2j = 2(i + j)$, and thus $m + n$ is even."[7] Because mathematicians think and write in natural language, they often rely on context to remove ambiguities. For example, there are no quantifiers in the mathematician's proof. However, the sentence,

[7] In the context of this book, a mathematician might simply say that this statement follows from Lemma 2.3 since being even is the same as being 0 mod 2. However, our point in proving elementary statements about even and odd numbers is not that we are learning new facts. Instead, we have chosen facts about numbers because they offer a familiar context for illustrating a variety of different aspects of proof. We do not expect any of the facts to be new to you. In fact, we hope that because they are not new, they will help you focus on the actual proof techniques.

though technically incomplete as a proof, captures the essence of why the sum of two even numbers is even. A typical complete (but more formal and wordy than usual) proof might go like the following.

> Let m and n be integers. Suppose m and n are even. If m and n are even, then by definition there are integers i and j such that $m = 2i$ and $n = 2j$. Thus, there are integers i and j such that $m = 2i$ and $n = 2j$. Then
>
> $$m + n = 2i + 2j = 2(i + j) ;$$
>
> so by definition, $m + n$ is an even integer. We have shown that if m and n are even, then $m + n$ is even. Therefore, for every m and n, if m and n are even integers, then so is $m + n$.

We began our proof by assuming that m and n are integers. This assumption gives us symbolic notation for talking about two integers. We then appealed to the definition of an even integer, namely, that an integer h is even if there is an integer k such that $h = 2k$. (Note the use of a quantifier in the definition.) Then we used algebra to show that $m + n$ is also two times another number. Because being two times another integer is the definition of $m + n$ being even, we concluded that $m + n$ is even. This conclusion allowed us to say that if m and n are even, then $m + n$ is even. Finally, we asserted that for every pair of integers m and n, if m and n are even, then $m + n$ is even.

There are a number of principles of proof illustrated here. Section 3.3 is devoted to a discussion of principles used in constructing proofs. For now, let us conclude with a remark about the limitations of logic. How did we know that we wanted to write the symbolic equation

$$m + n = 2i + 2j = 2(i + j) \ ?$$

It was not logic that told us to do this, but intuition and experience.

Important Concepts, Formulas, and Theorems

1. *Varies over.* We use the phrase "varies over" to describe the set of values a variable may take on.
2. *Universe.* We call the set of possible values for a variable the *universe* of that variable.
3. *Free variables.* Variables that are not constrained in any way are called *free variables.*

4. *Quantifier.* A phrase that converts a symbolic statement about potentially any member of our universe into a statement about the universe instead is called a *quantifier*. There are two types of quantifiers:
   - *Universal quantifiers* assert that a statement about a variable is true for every value of the variable in its universe.
   - *Existential quantifiers* assert that a statement about a variable is true for at least one value of the variable in its universe.
5. *Larger universes.* Let U_1 be a universe, and let U_2 be another universe, with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement such that $U_1 = \{x \mid q(x) \text{ is true}\}$. If $p(x)$ is a statement about U_2, it may also be interpreted as a statement about U_1, and
   a. $\forall x \in U_1(p(x))$ is equivalent to $\forall x \in U_2(q(x) \Rightarrow p(x))$, and
   b. $\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \wedge p(x))$.
6. *Proving quantified statements true or false.*
   - The statement $\exists x \in U(p(x))$ is true if there is at least one value of x in U for which the statement $p(x)$ is true.
   - The statement $\exists x \in U(p(x))$ is false if there is no $x \in U$ for which $p(x)$ is true.
   - The statement $\forall x \in U(p(x))$ is true if $p(x)$ is true for each value of x in U.
   - The statement $\forall x \in U(p(x))$ is false if $p(x)$ is false for at least one value of x in U.
7. *Negation of quantified statements.* To negate a quantified statement, you switch the quantifier and push the negation inside.
   - The statements $\neg\forall x \in \mathrm{U}(p(x))$ and $\exists x \in U(\neg p(x))$ are equivalent.
   - The statements $\neg\exists x \in \mathrm{U}(p(x))$ and $\forall x \in U(\neg p(x))$ are equivalent.
8. *Big O.* We say that $f(x) = O(g(x))$ if there are positive numbers c and n_0 such that $f(x) \leq cg(x)$ for every $x > n_0$.
9. *Big Θ.* $f(x) = \Theta(g(x))$ means that $f = O(g(x))$ and $g = O(f(x))$.
10. *Some notation for sets of numbers.* We use R to stand for the real numbers, R^+ to stand for the positive real numbers, Z to stand for the integers (positive, negative, and zero), Z^+ to stand for the positive integers, and N to stand for the nonnegative integers.

Problems

All problems with blue boxes have an answer or hint available at the end of the book.

1. For what positive integers x is the statement $(x-2)^2+1 \leq 2$ true? For what integers is it true? For what real numbers is it true? If you expand the universe for which you are considering a statement about a variable, does this always increase the size of the statement's truth set?

2. Is the statement "There is an integer greater than 2 such that $(x-2)^2+1 \leq 2$" true or false? How do you know?

3. Write the statement "The square of every real number is greater than or equal to 0" as a quantified statement about the universe of real numbers. You may use R to stand for the universe of real numbers.

4. A prime number is defined as an integer greater than 1 whose only positive integer factors are itself and 1. Find two ways to write this definition so that all quantifiers are explicit. (It may be convenient to introduce a variable to stand for the number and perhaps a variable or some variables for its factors.)

5. Write the definition of a greatest common divisor of m and n in such a way that all quantifiers are explicit and expressed explicitly as "for all" or "there exists." Write the part of Euclid's extended greatest common divisor theorem (Theorem 2.14) that relates the greatest common divisor of m and n algebraically to m and n. Again, make sure all quantifiers are explicit and expressed explicitly as "for all" or "there exists."

6. Using $s(x, y, z)$ to be the statement $x = yz$ and $t(x, y)$ to be the statement $x \leq y$, what is the form of the definition of a greatest common divisor d of m and n? (You need not include references to the universes for the variables.)

7. Which of the following statements (in which Z^+ stands for the positive integers and Z stands for all integers) is true and which is false? Explain why.

   a. $\forall z \in Z^+(z^2+6z+10 > 20)$

   b. $\forall z \in Z(z^2 - z \geq 0)$

   c. $\exists z \in Z^+(z - z^2 > 0)$

   d. $\exists z \in Z(z^2 - z = 6)$

8. Are there any (implicit) quantifiers in the statement "The product of odd integers is odd"? If so, what are they?

9. Rewrite the statement "The product of odd integers is odd" with all quantifiers (including any in the definition of odd integers) explicitly stated as "for all" or "there exist."

10. Rewrite the following statement without any negations: "There is no positive integer n such that for all integers $m > n$, all polynomial equations $p(x) = 0$ of degree m have no real numbers for solutions."

11. Consider the following slight modifications of Theorem 3.2. For each part, either prove that it is true or give a counterexample. Let U_1 be a universe, and let U_2 be another universe, with $U_1 \subseteq U_2$. Suppose that $q(x)$ is a statement about U_2 such that $U_1 = \{x \mid q(x) \text{ is true}\}$ and $p(x)$ is a statement about U_2.

   a. $\forall x \in U_1(p(x))$ is equivalent to $\forall x \in U_2(q(x) \wedge p(x))$.

   b. $\exists x \in U_1(p(x))$ is equivalent to $\exists x \in U_2(q(x) \Rightarrow p(x))$.

12. Let $p(x)$ stand for "x is a prime," $q(x)$ for "x is even," and $r(x, y)$ stand for "$x = y$." Use these three symbolic statements and appropriate logical notation to write the statement "There is one and only one even prime." (Use the set Z^+ of positive integers for your universe.)

13. Each of the following expressions represents a statement about the integers. Using $p(x)$ for "x is prime," $q(x, y)$ for "$x = y^2$," $r(x, y)$ for "$x \leq y$," $s(x, y, z)$ for "$z = xy$," and $t(x, y)$ for "$x = y$," determine which expressions represent true statements and which represent false statements.

   a. $\forall x \in Z(\exists y \in Z(q(x, y) \vee p(x)))$

   b. $\forall x \in Z(\forall y \in Z(s(x, x, y) \Leftrightarrow q(x, y)))$

   c. $\forall y \in Z(\exists x \in Z(q(y, x)))$

   d. $\exists z \in Z(\exists x \in Z(\exists y \in Z(p(x) \wedge p(y) \wedge \neg t(x, y))))$

14. Why is $(\exists x \in U(p(x))) \wedge (\exists y \in U(q(y)))$ not equivalent to $\exists z \in U(p(z) \wedge q(z))$? Are the statements $(\exists x \in U(p(x))) \vee (\exists y \in U(q(y)))$ and $\exists z \in U(p(z) \vee q(z))$ equivalent?

15. Give an example (in English) of a statement that has the form $\forall x \in U(\exists y \in V(p(x, y)))$. (The statement can be a mathematical

statement, a statement about everyday life, or whatever you prefer.) Now write (in English) the statement using the same $p(x, y)$ but of the form $\exists y \in V(\forall x \in U(p(x, y)))$. Comment on whether "for all" and "there exist" commute.

3.3 INFERENCE

Direct Inference (Modus Ponens) and Proofs

In this section, we talk about the logical structure of proofs. The examples of proofs we give are chosen to illustrate a concept in a context that we hope will be familiar to you. These examples are not necessarily the only or the best way to prove the results. If you see other ways to do the proofs, that is good, because it means you are putting your prior knowledge to work. It would be useful to try to see how the ideas of this section apply to your alternate proofs.

Section 3.2 concluded with a proof that the sum of two even numbers is even. That proof contained several crucial ingredients. First, it introduced symbols for members of the universe of integers. In other words, rather than saying, "Suppose we have two integers," we used symbols for the two members of our universe by saying, "Let m and n be integers." How did we know to use algebraic symbols? There are many possible answers to this question. In this case, our intuition was probably based on thinking about what an even number is and realizing that the definition itself is essentially symbolic. (You may argue that an even number is just twice another number, and you would be right. Apparently there are no symbols [variables] in that definition. But they really are there in the phrases "even number" and "another number.") Because we all know algebra is easier with symbolic variables than with words, we should recognize that it makes sense to use algebraic notation. Thus, this decision was based on experience, not logic.

Next, we assumed the two integers were even. We then used the definition of even numbers; as our previous parenthetic comment suggests, it was natural to use the definition symbolically. The definition tells us that if m is an even number, then there exists an integer i such that $m = 2i$. We combined this with the assumption that m is even and concluded that, in fact, there does exist an integer i such that $m = 2i$. This argument is an example of using the principle of **direct inference** (called *modus ponens* in Latin).

Principle 3.3 (Direct Inference)

From p and $p \Rightarrow q$, we may conclude q.

This common-sense principle is a cornerstone of logical arguments. But why is it valid? In Table 3.5, we take another look at the truth table for implication.

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

Table 3.5: *Another look at implication*

In Table 3.5, the only line that has a T in both the p column and the $p \Rightarrow q$ column is the first line. In this line, q is also true; thus, we conclude that if p and $p \Rightarrow q$ hold, then q must hold also. Although this may seem like a somewhat inside-out application of the truth table, it is simply a different way of using a truth table.

There are quite a few rules (called "rules of inference"), such as the principle of direct inference, that people commonly use in proofs without explicitly stating them. Before beginning a formal study of rules of inference, however, let's complete our analysis of which rules we used in the proof that the sum of two even integers is even. After concluding that $m = 2i$ and $n = 2j$, we used algebra to show that because $m = 2i$ and $n = 2j$, there exists a k such that $m + n = 2k$ (our k was $i + j$). Next, we used the definition of even numbers again to say that $m + n$ was even. We then used the following rule of inference.

Principle 3.4 (Conditional Proof)

If by assuming p we may prove q, then the statement $p \Rightarrow q$ is true.

Using this principle, we reached the conclusion that if m and n are even integers, then $m + n$ is an even integer. To conclude that this statement is true for all integers m and n, we used another rule of inference, one that is more difficult to describe. We originally introduced the variables m and

n. We used only well-known consequences of the fact that they were in the universe of integers in our proof. Thus, we felt justified in asserting that what we concluded about m and n is true for any pair of integers. We might say that we were treating m and n as generic members of our universe. Thus, our rule of inference says:

Principle 3.5 (Universal Generalization)

If we can prove a statement about x by assuming only that x is a member of our universe, then we can conclude the statement is true for every member of our universe.

Perhaps this rule is hard to put into words because it is not simply a description of a truth table; rather, it is a principle that we use to prove universally quantified statements.

Rules of Inference for Direct Proofs

We have seen the ingredients of a typical proof. What do we mean by a proof in general? A proof of a statement is a convincing argument that the statement is true. To be more precise, we can agree that a **direct proof** consists of a sequence of statements, each of which is either a hypothesis,[8] a generally accepted fact, or the result of one of the following rules of inference for compound statements.

Rules of Inference for Direct Proofs

1. From an example x that does not satisfy $p(x)$, we may conclude $\neg p(x)$.
2. From $p(x)$ and $q(x)$, we may conclude $p(x) \wedge q(x)$.
3. From either $p(x)$ or $q(x)$, we may conclude $p(x) \vee q(x)$.
4. From either $q(x)$ or $\neg p(x)$, we may conclude $p(x) \Rightarrow q(x)$.
5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$, we may conclude $p(x) \Leftrightarrow q(x)$.
6. From $p(x)$ and $p(x) \Rightarrow q(x)$, we may conclude $q(x)$.
7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$, we may conclude $p(x) \Rightarrow r(x)$.
8. If we can derive $q(x)$ from the hypothesis that x satisfies $p(x)$, then we may conclude $p(x) \Rightarrow q(x)$.

[8] If we are proving an implication $s \Rightarrow t$, we call s a hypothesis. If we make assumptions by saying, "Let ...," "Suppose ...," or something similar before we give the statement to be proved, then these assumptions are also hypotheses.

9. If we can derive $p(x)$ from the hypothesis that x is a (generic) member of our universe U, we may conclude $\forall x \in U(p(x))$.
10. From an example of an $x \in U$ satisfying $p(x)$, we may conclude $\exists x \in U(p(x))$.

The first rule is a statement of the principle of the excluded middle as it applies to statements about variables. The next four rules are, in effect, descriptions of the truth tables for "and," "or," "implies," and "if and only if." Rule 5 tells us what we must do to write a proof of an "if and only if" statement. Rule 6, exemplified in our earlier discussion, is the principle of direct inference, and it describes one row of the truth table for $p \Rightarrow q$. Rule 7 is the transitive law, a law that we could derive by analysis of truth tables. Rule 8, the principle of conditional proof, which is also exemplified earlier, may be regarded as yet another description of one row of the truth table of $p \Rightarrow q$. Rule 9 is the principle of universal generalization, discussed and exemplified earlier. Rule 10 specifies what we mean by the truth of an existentially quantified statement according to Principle 3.2.

Although some of our rules of inference are, strictly speaking, redundant, we include them because they allow us to express proofs more concisely. For example, we could have written a portion of our proof that the sum of even numbers is even as follows, without using Rule 8.

> Let m and n be integers. If m is even, then there is a k with $m = 2k$. If n is even, then there is a j with $n = 2j$. Thus, if m is even and n is even, there are a k and j such that $m + n = 2k + 2j = 2(k + j)$. Thus, if m is even and n is even, there is an integer $h = k + j$ such that $m + n = 2h$. Thus, if m is even and n is even, $m + n$ is even.

Because this kind of argument could always be used to circumvent the use of Rule 8, that rule is not required as a rule of inference. However, because it permits us to avoid such unnecessarily complicated "silliness" in our proofs, we choose to include it. Rule 7, the transitive law, has a similar role.

Exercise 3.3-1 Prove that if m is even, then m^2 is even. Explain which steps of the proof use one of the 10 rules of inference.

For Exercise 3.3-1, we can mimic the proof that the sum of even integers is even:

> Let m be an integer. Suppose that m is even. If m is even, then there is a k with $m = 2k$. Thus, there is a k such that $m^2 = 4k^2$.

> Therefore, there is an integer $h = 2k^2$ such that $m^2 = 2h$. This tells us that if m is even, then m^2 is even. Therefore, for all integers m, if m is even, then m^2 is even.

Our first sentence sets us up to use Rule 9. The second sentence simply states an implicit hypothesis. The next two sentences use Rule 6, the principle of direct inference. When we say, "Therefore, there is an integer $h = 2k^2$ such that $m^2 = 2h$," we are simply stating an algebraic fact. The next sentences use Rule 8 and Rule 9. (You might have written the proof in a different way and used different rules of inference.)

Contrapositive Rule of Inference

Exercise 3.3-2 Show that "p implies q" is equivalent to "$\neg q$ implies $\neg p$."

Exercise 3.3-3 Is "p implies q" equivalent to "q implies p"?

To do Exercise 3.3-2, we construct the double truth table in Table 3.6. Because the columns under $p \Rightarrow q$ and under $\neg q \Rightarrow \neg p$ are exactly the same, we know the two statements are equivalent.

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

Table 3.6: *A double truth table for $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$*

Exercise 3.3-2 tells us that if we know that $\neg q \Rightarrow \neg p$, then we can conclude that $p \Rightarrow q$. This is called the principle of **proof by contraposition**.

Principle 3.6 (Proof by Contraposition)

The statements $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are equivalent, and so a proof of one is a proof of the other.

The statement $\neg q \Rightarrow \neg p$ is called the **contrapositive** of the statement $p \Rightarrow q$. The proof of the following lemma demonstrates the utility of proof by contraposition.

Lemma 3.5 If n is a positive integer with $n^2 > 100$, then $n > 10$.

Proof Suppose n is not greater than 10. (We now use the rule of algebra for inequalities that says if $x \leq y$ and $c \geq 0$, then $cx \leq cy$.) Then, because $1 \leq n \leq 10$,

$$n \cdot n \leq n \cdot 10 \leq 10 \cdot 10 = 100.$$

Thus, n^2 is not greater than 100. Therefore, if n is not greater than 10, then n^2 is not greater than 100. By the principle of proof by contraposition, if $n^2 > 100$, then n must be greater than 10.

We adopt Principle 3.6 as a rule of inference called the **contrapositive rule of inference**:

11. From $\neg q(x) \Rightarrow \neg p(x)$, we may conclude $p(x) \Rightarrow q(x)$.

In our proof of the Chinese remainder theorem (Theorem 2.24), we wanted to prove for a certain function f, that if x and y were different integers between 0 and $mn - 1$, then $f(x) \neq f(y)$. To prove this, we assumed that, in fact, $f(x) = f(y)$ and proved that x and y were not different integers between 0 and $mn - 1$. Had we known the principle of contrapositive inference, we could have concluded then and there that f was one-to-one. Instead, we used the more common principle of proof by contradiction, which is the major topic of the remainder of this section, to complete our proof. If you look back at the proof of the Chinese remainder theorem, you will see that we might have been able to use contrapositive inference to shorten it by a sentence.

For Exercise 3.3-3, a quick look at the double truth table for $p \Rightarrow q$ and $q \Rightarrow p$ in Table 3.7 demonstrates that these two statements are *not* equivalent. The statement $q \Rightarrow p$ is called the **converse** of $p \Rightarrow q$. Notice that $p \Leftrightarrow q$ is true exactly when $p \Rightarrow q$ and its converse are true. It is surprising how often people, even professional mathematicians, absentmindedly try to prove the converse of a statement when they mean to prove the statement itself. Try not to join this crowd!

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

Table 3.7: *A double truth table for $p \Rightarrow q$ and $q \Rightarrow p$*

Proof by Contradiction

Proof by contrapositive inference is an example of what we call **indirect proof**. We actually saw another example of indirect proof in the principle of proof by contradiction. We introduced the principle of proof by contradiction (Principle 2.1) in our proof to Corollary 2.6, in which we were trying to prove:

> Suppose there is a b in Z_n such that the equation $a \cdot_n x = b$ does not have a solution. Then a does not have a multiplicative inverse in Z_n.

We assumed that the hypothesis that $a \cdot_n x = b$ does not have a solution was true. We also assumed that the conclusion that a does not have a multiplicative inverse was false. We showed that these two assumptions together led to a contradiction. Using the principle of the excluded middle (Principle 3.1), but without saying so, we concluded that if the hypothesis was in fact true, then the only possibility was that the conclusion was also true.

We used the principle of proof by contradiction again in our proof of Euclid's division theorem. Recall that in that proof, we began by assuming that there was an integer m for which there were no integers q and r with $m = qn + r$ and $0 \leq r < n$. We then chose the smallest integer m such that there was not a pair of integers q and r with $m = qn + r$ and $0 \leq r < n$. We then made some computations by which we proved that, in this case, there *are* integers q and r with $0 \leq r < n$ such that $m = qn + r$. In overview, we started out by assuming the theorem was false, and from that assumption, we drew a contradiction (to the assumption itself). Because all our reasoning, except for the assumption that the theorem was false, used accepted rules of inference, the only source of that contradiction was our assumption. Thus, by the principle of the excluded middle, our assumption had to be incorrect. We adopt the principle of proof by contradiction (also called the principle of **reduction to absurdity**) as our last rule of inference.

12. If from assuming $p(x)$ and $\neg q(x)$, we can derive both $r(x)$ and $\neg r(x)$ for some statement $r(x)$, then we may conclude $p(x) \Rightarrow q(x)$.

There can be many variations of proof by contradiction. These variations are all examples of what we call an "indirect proof." Each of the next three indirect proofs of the same statement gets a slightly different contradiction. In each case, p is the statement $x^2 + x - 2 = 0$, and s is the statement $x \neq 0$. In each case, we prove that p implies q.

1. We may assume p is true and q is false; from this, we derive the contradiction that p is false, as in the following example.

   Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Proof Suppose that $x^2 + x - 2 = 0$. Assume that $x = 0$. Substituting 0 for x in the polynomial gives $x^2 + x - 2 = 0 + 0 - 2 = -2$, which contradicts the assumption that $x^2 + x - 2 = 0$. Thus, by the principle of proof by contradiction, if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Here the statement r was identical to p, namely, $x^2 + x - 2 = 0$.

2. We may assume p is true and q is false and derive a contradiction of a known fact. Here is an example.

   Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Proof Suppose that $x^2 + x - 2 = 0$. Assume that $x = 0$. Then $x^2 + x - 2 = 0 + 0 - 2 = -2$. Thus, $0 = -2$, which is a contradiction. Thus, by the principle of proof by contradiction, if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Here the statement r is the known fact that $0 \neq -2$.

3. Sometimes the statement r that appears in the principle of proof by contradiction is simply a statement that arises naturally as we try to construct our proof, as in the following example.

   Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Proof Suppose that $x^2 + x - 2 = 0$. Then $x^2 + x = 2$. Assume that $x = 0$. Then $x^2 + x = 0 + 0 = 0$. But this is a contradiction to our observation that $x^2 + x = 2$. Thus, by the principle of proof by contradiction, if $x^2 + x - 2 = 0$, then $x \neq 0$.

   Here the statement r is $x^2 + x = 2$.

4. Finally, if proof by contradiction seems to you not to be much different from proof by contraposition, you are right, as the following example shows.

Prove that if $x^2 + x - 2 = 0$, then $x \neq 0$.

Proof Assume that $x = 0$. Then $x^2 + x - 2 = 0 + 0 - 2 = -2$, so that $x^2 + x - 2 \neq 0$. Thus, by the principle of proof by contraposition, if $x^2 + x - 2 = 0$, then $x \neq 0$.

Any proof that uses one of the indirect methods of inference, either contradiction or contraposition, is called an **indirect proof**. The previous four examples illustrate the rich possibilities that indirect proof provides us. Of course, they also illustrate why indirect proof can be confusing. There is no set formula that we use in writing a proof by contradiction, so there is no rule we can memorize to formulate indirect proofs. Instead, we have to ask ourselves whether assuming the opposite of what we are trying to prove gives insight into why the assumption makes no sense. If it does, we have the basis of an indirect proof. The way in which we choose to write that proof is a matter of personal choice.

Exercise 3.3-4 Without extracting square roots, prove that if n is a positive integer such that $n^2 < 9$, then $n < 3$. You may use rules of algebra for dealing with inequalities.

Exercise 3.3-5 Prove that $\sqrt{5}$ is not rational.

To prove the statement in Exercise 3.3-4, we assume, for purposes of contradiction, that $n \geq 3$. Squaring both sides of this equation, we obtain

$$n^2 \geq 9,$$

which contradicts our hypothesis that $n^2 < 9$. Therefore, by the principle of proof by contradiction, $n < 3$.

To prove the statement in Exercise 3.3-5, we assume, for the purpose of contradiction, that $\sqrt{5}$ is rational. This means that it can be expressed as the fraction m/n, where m and n are integers. Squaring both sides of the equation $m/n = \sqrt{5}$, we obtain

$$\frac{m^2}{n^2} = 5,$$

or

$$m^2 = 5n^2.$$

Now, m^2 must have an even number of prime factors (counting each prime factor as many times as it occurs), as must n^2. But $5n^2$ has an odd number of prime factors. Thus, a product of an even number of prime factors is equal to a product of an odd number of prime factors. This is a contradiction, because each positive integer may be expressed uniquely as a product of (positive) prime numbers. Thus, by the principle of proof by contradiction, $\sqrt{5}$ is not rational.

Important Concepts, Formulas, and Theorems

1. *Principle of direct inference or modus ponens.* From p and $p \Rightarrow q$, we may conclude q.
2. *Principle of conditional proof.* If by assuming p we may prove q, then the statement $p \Rightarrow q$ is true.
3. *Principle of universal generalization.* If we can prove a statement about x by assuming x is a member of our universe, then we can conclude it is true for every member of our universe.
4. *Rules of inference.* The following 12 rules of inference appear in this chapter.
    1. From an example x that does not satisfy $p(x)$, we may conclude $\neg p(x)$.
    2. From $p(x)$ and $q(x)$, we may conclude $p(x) \wedge q(x)$.
    3. From either $p(x)$ or $q(x)$, we may conclude $p(x) \vee q(x)$.
    4. From either $q(x)$ or $\neg p(x)$, we may conclude $p(x) \Rightarrow q(x)$.
    5. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow p(x)$, we may conclude $p(x) \Leftrightarrow q(x)$.
    6. From $p(x)$ and $p(x) \Rightarrow q(x)$, we may conclude $q(x)$.
    7. From $p(x) \Rightarrow q(x)$ and $q(x) \Rightarrow r(x)$, we may conclude $p(x) \Rightarrow r(x)$.
    8. If we can derive $q(x)$ from the hypothesis that x satisfies $p(x)$, then we may conclude $p(x) \Rightarrow q(x)$.
    9. If we can derive $p(x)$ from the hypothesis that x is a (generic) member of our universe U, we may conclude $\forall x \in U(p(x))$.
    10. From an example of an $x \in U$ satisfying $p(x)$, we may conclude $\exists x \in U(p(x))$.
    11. From $\neg q(x) \Rightarrow \neg p(x)$, we may conclude $p(x) \Rightarrow q(x)$.
    12. If from assuming $p(x)$ and $\neg q(x)$, we can derive both $r(x)$ and $\neg r(x)$ for some statement r, then we may conclude $p(x) \Rightarrow q(x)$.

5. *Contrapositive of $p \Rightarrow q$.* The contrapositive of the statement $p \Rightarrow q$ is the statement $\neg q \Rightarrow \neg p$.
6. *Converse of $p \Rightarrow q$.* The converse of the statement $p \Rightarrow q$ is the statement $q \Rightarrow p$.
7. *Contrapositive rule of inference.* From $\neg q \Rightarrow \neg p$, we may conclude $p \Rightarrow q$.
8. *Principle of proof by contradiction.* If from assuming p and $\neg q$ we can derive both r and $\neg r$ for some statement r, then we may conclude $p \Rightarrow q$.

Problems

All problems with blue boxes have an answer or hint available at the end of the book.

1. Write the converse and contrapositive of each statement.
   a. If the hose is 60 ft long, then the hose will reach the tomatoes.
   b. George goes for a walk only if Mary goes for a walk.
   c. Pamela recites a poem if Andre asked for a poem.
2. Construct a proof that if m is odd, then m^2 is odd.
3. Construct a proof that for all integers m and n, if m is even and n is odd, then $m + n$ is odd.
4. What does it really mean to say, "Prove that if m is odd, and n is odd, then $m + n$ is even"? Prove this more precise statement.
5. Prove that for all integers m and n, if m is odd and n is odd, then mn is odd.
6. Is the statement $p \Rightarrow q$ equivalent to the statement $\neg p \Rightarrow \neg q$?
7. Construct a contrapositive proof that for all real numbers x, if $x^2 - 2x \neq -1$, then $x \neq 1$.
8. Construct a proof by contradiction that for all real numbers x, if $x^2 - 2x \neq -1$, then $x \neq 1$.
9. Prove that if $x^3 > 8$, then $x > 2$.
10. Prove that $\sqrt{3}$ is irrational.
11. Construct a proof that if m is an integer such that m^2 is even, then m is even.

12. Prove or disprove the following statement: "For every positive integer n, if n is prime, then 12 and $n^3 - n^2 + n$ have a common factor greater than 1."

13. Prove or disprove the following statement: "For all integers b, c, and d, if x is a rational number such that $x^2 + bx + c = d$, then x is an integer." (*Hints:* Are all the quantifiers given explicitly? It is okay, but not necessary, to use the quadratic formula.)

14. Prove that there is no largest prime number.

15. Prove that if f, g, and h are functions from R^+ to R^+ such that $f(x) = O(g(x))$ and $g(x) = O(h(x))$, then $f(x) = O(h(x))$.