3.3 Inference

Direct Inference (Modus Ponens) and Proofs

We concluded our last section with a proof that the sum of two even numbers is even. That proof contained several crucial ingredients. First, we introduced symbols for members of the universe of integers. In other words, rather than saying "suppose we have two integers," we introduced symbols for the two members of our universe we assumed we had. How did we know to use algebraic symbols? There are many possible answers to this question, but 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 no symbols are in that definition. But they really are there; they are the phrases "even number" and "another number." Since we all know algebra is easier with symbolic variables rather than 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, and, 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 another integer i such that $m = 2i$. We combined this with the assumption that m is even to conclude that in fact there does exist an integer i such that $m = 2i$. This 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 true? In Table 3.5 we take another look at the truth table for implication.

Table 3.5: Another look at implication

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

The only line which has a T in both the p column and the $p \Rightarrow q$ column is the first line. In this line q is true also, and we therefore conclude that if p and $p \Rightarrow q$ hold then q must hold also. While 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 rules (called rules of inference) like the principle of direct inference that people commonly use in proofs without explicitly stating them. Before beginning a formal study of rules of inference, we 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 next 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 number again to say that $m + n$ was even. We then used a rule of inference which says

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. In order to conclude that this statement is true for all integers m and n, we used another rule of inference, one of the 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 x is a member of our universe, then we can conclude the statement is true for every member of our universe.*

Perhaps the reason this rule is hard to put into words is that it is not simply a description of a truth table, but is a principle that we use in order 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 about it, we can agree that a *direct proof* consists of a sequence of statements, each of which is either a hypothesis[5], 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 $p(x) \Rightarrow q(x)$.

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

[5] 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 hypotheses as well.

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 four rules are in effect a description of the truth tables for "and," "or," "implies" and "if and only if." Rule 5 says what we must do in order 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 describes one row of the truth table for $p \Rightarrow q$. Rule 7 is the transitive law, one we could derive by truth table analysis. 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 redundant, they are useful. 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."

This kind of argument could always be used to circumvent the use of Rule 8, so Rule 8 is not required as a rule of inference, but 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 rules of inference above.

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

> Let m be 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 $m^2 = 2h$. Thus if m is even, m^2 is even. Therefore, for all integers m, if m is even, then m^2 is even.

In our first sentence we are setting things up to use Rule 9. In the second sentence we are simply stating an implicit hypothesis. In the next two sentences we use Rule 6, the principle of direct inference. When we said "Therefore, there is an integer $h = 2k^2$ such that $m^2 = 2h$," we were simply stating an algebraic fact. In our next sentence we used Rule 8. Finally, we used 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. Since the columns under $p \Rightarrow q$ and under $\neg q \Rightarrow \neg p$ are exactly the same, we know the two statements are equivalent. This exercise 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.*

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

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

Principle 3.6 (Proof by Contraposition) *The statement $p \Rightarrow q$ and the statement $\neg q \Rightarrow \neg p$ 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 following example demonstrates the utility of the principle 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. (Now we use the rule of algebra for inequalities which says that if $x \leq y$ and $c \geq 0$, then $cx \leq cy$.) Then since $1 \leq n \leq 10$,

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

Thus n^2 is not greater than 100. Therefore, if n is not greater than 10, n^2 is not greater than 100. Then, by the principle of proof by contraposition, if $n^2 > 100$, 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 that 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, the major topic of the remainder of this section, to complete our proof. If you look back at the proof, you will see that we might have been able to shorten it by a sentence by using contrapositive inference.

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, absent-mindedly try to prove the converse of a statement when they mean to prove the statement itself. Try not to join this crowd!

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

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

Proof by contradiction

Proof by contrapositive inference is an example of what we call *indirect proof.* We have actually seen another example indirect proof, the principle of proof by contradiction. In our proof of Corollary 2.6 we introduced the principle of proof by contradiction, Principle 2.1. We were trying to prove the statement

> 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. Then, using the principle of the excluded middle, Principle 3.1 (without saying so), we concluded that if the hypothesis is in fact true, then the only possibility was that the conclusion is true as well.

We used the principle again later in our proof of Euclid's Division Theorem. Recall that in that proof we began by assuming that the theorem was false. We then chose among the pairs of integers (m, n) such that $m \neq qn + r$ with $0 \leq r < n$ a pair with the smallest possible m. We then made some computations by which we proved that in this case there *are* a q and r with $0 \leq r < n$ such that $m = qn + r$. Thus we started out by assuming the theorem was false, and from that assumption we drew drew a contradiction to the assumption. Since 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. For example, we may assume p is true and q is false, and from this 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 $x = 0$. Then $x^2 + x - 2 = 0 + 0 - 2 = -2$. This contradicts $x^2 + x - 2 = 0$. 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 $x^2 + x - 2 = 0$.

On the other hand, we may instead assume p is true and q is false, and derive a contradiction of a known fact, 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 $x = 0$. Then $x^2 + x - 2 = 0 + 0 - 2 = -2$. Thus $0 = -2$, 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 $0 \neq -2$.

Sometimes the statement r that appears in the principle of proof by contradiction is simply a statement that arises naturally as we are trying 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 "$x^2 + x = 2$."

Finally, if proof by contradiction seems to you not to be much different from proof by contraposition, you are right, as the example that follows 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 is called an indirect proof. The last 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 in order to formulate indirect proofs. Instead, we have to ask ourselves whether assuming the opposite of what we are trying to prove gives us insight into why the assumption makes no sense. If it does, we have the basis of an indirect proof, and the way in which we choose to write it 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 $\frac{m}{n}$, where m and n are integers. Squaring both sides of the equation $\frac{m}{n} = \sqrt{5}$, 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, which is a contradiction since 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.* 12 rules of inference appear in this chapter. They are

    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

1. Write down the converse and contrapositive of each of these statements.
   (a) If the hose is 60 feet 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 asks 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 do we really mean when we 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 $m \cdot n$ 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."

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 ok to use the quadratic formula.)

14. Prove that there is no largest prime number.

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