1. Elementary Notions and Notations

1.1 A Proof Primer

For our purposes an *informal proof* is a demonstration that some statement is true. We normally communicate an informal proof in an English-like language that mixes everyday English with symbols that appear in the statement to be proved. In the next few paragraphs we'll discuss some basic techniques for doing informal proofs. These techniques will come in handy in trying to understand someone's proof or in trying to construct a proof of your own, so keep them in your mental tool kit.

We'll start off with a short refresher on logical statements followed by a short discussion about numbers. This will give us something to talk about when we look at examples of informal proof techniques.

1.1.1 Logical Statements

For this primer we'll consider only statements that are either true or false. We'll start by discussing some familiar ways to structure logical statements.

Negation

If S represents some statement, then the *negation* of S is the statement "not S," whose truth value is opposite that of S. We can represent this relationship with a *truth table* in which each row gives a value for S and the corresponding value for not S:

S	not S
true	false
false	true

We often paraphrase the negation of a statement to make it more understandable. For example, to negate the statement "Earth is a star," we normally say, "Earth is not a star," or "It is not the case that Earth is a star," rather than "Not Earth is a star."

We should also observe that negation relates statements about *every* case with statements about *some* case. For example, the statement "Not every planet has a moon" has the same meaning as "Some planet does not have a moon." Similarly, the statement "It is not the case that some planet is a star" has the same meaning as "Every planet is not a star."

A	*B*	*A* and *B*	*A* or *B*
true	true	true	true
true	false	false	true
false	true	false	true
false	false	false	false

Figure 1.1 Truth tables.

Conjunction and Disjunction

The *conjunction* of A and B is the statement "A and B," which is true when both A and B are true. The *disjunction* of A and B is the statement "A or B," which is true if either or both of A and B are true. The truth tables for conjunction and disjunction are given in Figure 1.1.

Sometimes we paraphrase conjunctions and disjunctions. For example, instead of "Earth is a planet and Mars is a planet," we might write "Earth and Mars are planets." Instead of "x is positive or y is positive," we might write "Either x or y is positive."

Conditional Statements

Many statements are written in the general form "If A then B," where A and B are also logical statements. Such a statement is called a *conditional statement* in which A is the *hypothesis* and B is the *conclusion*. We can read "If A then B" in several other ways: "A is a sufficient condition for B," or "B is a necessary condition for A," or simply "A implies B." The truth table for a conditional statement is contained in Figure 1.2.

Let's make a few comments about this table. Notice that the conditional is false only when the hypothesis is true and the conclusion is false. It's true in the other three cases. The conditional truth table gives some people fits because they interpret "If A then B" to mean "B can be proved from A," which assumes that A and B are related in some way. But we've all heard statements like "If the moon is made of green cheese, then $1 = 2$." We nod our heads and agree that the statement is true, even though there is no relationship between the hypothesis and conclusion. Similarly, we shake our heads and don't agree with a statement like "If $1 = 1$, then the moon is made of green cheese."

A	*B*	*if A*, then *B*
true	true	true
true	false	false
false	true	true
false	false	true

Figure 1.2 Truth table.

When the hypothesis of a conditional is false, we say that the conditional is *vacuously* true. For example, the statement "If $1 = 2$, then $39 = 12$" is vacuously true because the hypothesis is false. If the conclusion is true, we say that the conditional is *trivially* true. For example, the statement "If $1 = 2$, then $2 + 2 = 4$" is trivially true because the conclusion is true. We leave it to the reader to convince at least one person that the conditional truth table is defined properly.

The *converse* of "If A, then B" is "If B, then A." The converse does not always have the same truth value. For example, we know that the following statement about numbers is true.

$$\text{If } x > 0 \text{ and } y > 0, \text{ then } x + y > 0.$$

The converse of this statement is

$$\text{If } x + y > 0, \text{ then } x > 0 \text{ and } y > 0.$$

This converse is false. For example, let $x = 3$ and $y = -2$. Then the statement becomes "If $3 + (-2) > 0$, then $3 > 0$ and $-2 > 0$," which is false.

Equivalent Statements

Sometimes it's convenient to write a statement in a different form but with the same truth value. Two statements are said to be *equivalent* if they have the same truth value for any assignment of truth values to the variables that occur in the statements.

We can combine negation with either conjunction or disjunction to obtain the following pairs of equivalent statements.

"not (A and B)" is equivalent to "(not A) or (not B)."
"not (A or B)" is equivalent to "(not A) and (not B)."

For example, the statement "not ($x > 0$ and $y > 0$)" is equivalent to the statement "$x \leq 0$ or $y \leq 0$." The statement "not ($x > 0$ or $y > 0$)" is equivalent to the statement "$x \leq 0$ and $y \leq 0$."

Conjunctions and disjunctions distribute over each other in the following sense:

"A and (B or C)" is equivalent to "(A and B) or (A and C)."
"A or (B and C)" is equivalent to "(A or B) and (A or C)."

For example, the statement "$0 < x$ and ($x < 4$ or $x < 9$)" is equivalent to the statement "$0 < x < 4$ or $0 < x < 9$." The statement "$x > 0$ or ($x > 2$ and $x > 1$)" is equivalent to "($x > 0$ or $x > 2$) and ($x > 0$ or $x > 1$)."

The *contrapositive* of the conditional statement "If A, then B" is the equivalent statement "If not B, then not A." For example, the statement

$$\text{If } (x > 0 \text{ and } y > 0) \text{ then } x + y > 0$$

is equivalent to the statement

$$\text{If } x + y = 0, \text{ then } (x \leq 0 \text{ or } y \leq 0).$$

We can also express the conditional statement "If A, then B" in terms of the equivalent statement "(not A) or B." For example, the statement

$$\text{If } x > 0 \text{ and } y > 0, \text{ then } x + y > 0.$$

is equivalent to the statement

$$(x \leq 0 \text{ or } y \leq 0) \text{ or } x + y > 0.$$

Since we can express a conditional in terms of negation and disjunction, it follows that the statements "not (If A then B)" and "A and (not B)" are equivalent. For example, the statement

It is not the case that if Earth is a planet, then Earth is a star.

is equivalent to the statement

Earth is a planet and Earth is not a star.

Let's summarize the equivalences that we have discussed. Each row of the following table contains two equivalent statements S and T.

S	(is equivalent to) T
not (A and B)	(not A) or (not B)
not (A or B)	(not A) and (not B)
A and (B or C)	(A and B) or (A and C)
A or (B and C)	(A or B) and (A or C)
if A, then B	if not B, then not A
if A, then B	(not A) or B
not (if A then B)	A and (not B)

1.1.2 Something to Talk About

To discuss proof techniques, we need something to talk about when giving sample proofs. Since numbers are familiar to everyone, that's what we'll talk about. But to make sure that we all start on the same page, we'll review a little terminology.

The numbers that we'll be discussing are called *integers*, and we can list them as follows:

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots .$$

The integers in the following list are called *even* integers:

$$\ldots, -4, -2, 0, 2, 4, \ldots .$$

The integers in the following list are called *odd* integers:

$$\ldots, -3, -1, 1, 3, \ldots .$$

So every integer is either even or odd but not both. In fact, every even integer has the form $2n$ for some integer n. Similarly, every odd integer has the form $2n + 1$ for some integer n.

Divisibility and Prime Numbers

An integer d *divides* an integer n if $d \neq 0$ and there is an integer k such that $n = dk$. For example, 3 divides 18 because we can write $18 = (3)(6)$. But 5 does not divide 18 because there is no integer k such that $18 = 5k$. The following list shows all the divisors of 18.

$$-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18.$$

Some alternative words for d *divides* n are d *is a divisor of* n or n *is divisible by* d. We often denote the fact that d divides n with the following shorthand notation:

$$d|n$$

For example, we have $-9|9$, $-3|9$, $-1|9$, $1|9$, $3|9$, and $9|9$. Here are two properties of divisibility that we'll record for future use.

Divisibility Properties (1.1)

a. If $d|a$ and $a|b$, then $d|b$.

b. If $d|a$ and $d|b$, then $d|(ax + by)$ for any integers x and y.

An integer $p > 1$ is called a *prime* number if 1 and p are its only positive divisors. For example, the first eight prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19.$$

Prime numbers have many important properties and they have many applications in computer science. But for now all we need to know is the definiton of a prime.

1.1.3 Proof Techniques

Now that we have something to talk about, we'll discuss some fundamental proof techniques and give some sample proofs for each technique.

Proof by Exhaustive Checking

When a statement asserts that each of a finite number of things has a certain property, then we might be able to prove the statement by checking that each thing has the stated property. For example, suppose someone says, "If n is an integer and $2 \leq n \leq 7$, then $n^2 + 2$ is not divisible by 4." We can prove the statement by *exhaustive checking.* For $2 \leq n \leq 7$, the corresponding values of $n^2 + 2$ are

$$6, 11, 18, 25, 38, 51.$$

We can check that these numbers are not divisible by 4. For another example, suppose someone says, "If n is an integer and $2 \leq n \leq 500$, then $n^2 + 2$ is not divisible by 4." Again, this statement can be proved by exhaustive checking, but perhaps by a computer rather than a person.

Exhaustive checking cannot be used to prove a statement that requires infinitely many things to check. For example, consider the statement, "If n is an integer, then $n^2 + 2$ is not divisible by 4." This statement is true, but there are infinitely many things to check. So another proof technique will be required. We'll get to it after a few more paragraphs.

An example that proves a statement false is often called a *counterexample.* Sometimes counterexamples can be found by exhaustive checking. For example, consider the statement, "Every odd number greater than 1 that is not prime has the form $2 + p$ for some prime p." We can observe that the statement is false because 27 is a counterexample.

Conditional Proof

Many statements that we wish to prove are in conditional form or can be phrased in conditional form (if A then B). The *direct approach* to proving such a statement starts with the assumption that the hypothesis A is true. The next step is to find a statement that is implied by the assumption or known facts. Each step proceeds in this fashion to find a statement that is implied by any of the previous statements or known facts. The *contitional proof* ends when the conclusion B is reached.

example 1.1 A Proof About Sums

We'll prove the following general statement about integers:

The sum of any two odd integers is an even integer.

We can rephrase the statement in the conditional form

If x and y are odd integers, then $x + y$ is an even integer.

Proof: Assume the hypothesis that x and y are odd integers. It follows that x and y can be written in the the form $x = 2k + 1$ and $y = 2m + 1$, where k and m are arbitrary integers. Now substitute for x and y in $x + y$ to obtain

$$x + y = (2k + 1) + (2m + 1) = 2k + 2m + 2 = 2(k + m + 1).$$

Since the expression on the right-hand side contains 2 as a factor, it represents an even integer. QED.

end example

example

1.2 A Divisibility Proof

We'll prove the following statement (1.1a) about divisibility:

$$\text{If } d|a \text{ and } a|b, \text{ then } d|b.$$

Proof: Assume the hypothesis that $d|a$ and $a|b$. It follows from the definition of divisibility that there are integers m and n such that $a = dm$ and $b = an$. Now substitute for a in the first equation.

$$b = an = (dm)n = d(mn).$$

This equation says that $d|b$. QED.

end example

Proving the Contrapositive

Recall that a conditional statement "if A then B" and its contrapositive "if not B then not A" have the same truth table. So a proof of one is also a proof of the other. The *indirect approach* to proving "if A then B" is to *prove the contrapositve*. Start with the assumption that B is false. The next step is to find a statement that is implied by the assumption or known facts. Each step proceeds in this fashion to find a statement that is implied by any of the previous statements or known facts. The proof ends when an implied statement says that A is false.

example

1.3 An Odd Proof

We'll prove the following statement about the integers:

$$\text{If } x^2 \text{ is odd, then } x \text{ is odd.}$$

To prove the statement, we'll prove its contrapositive:

$$\text{If } x \text{ is even, then } x^2 \text{ is even.}$$

Proof: Assume the hypothesis (of the contrapositive) that x is even. It follows that $x = 2k$ for some integer k. Now square x and substitute for x to obtain

$$x^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

The expression on the right side of the equation represents an even number. Therefore, x^2 is even. QED.

end example

Proof by Contradiction

A *contradiction* is a false statement. Another kind of indirect proof is *proof by contradiction*, where we start out by assuming that the statement to be proved is false. Then we argue until we reach a contradiction. Such an argument is often called a *refutation*.

Proof by contradiction is often the method of choice because we can wander wherever the proof takes us to find a contradiction. We'll give two examples to show the wandering that can take place.

example

1.4 A Not-Divisible Proof

We'll prove the following statement about divisibility:

If n is an integer, then $n^2 + 2$ is not divisible by 4.

Proof: Assume the statement is false. Then $4 \mid (n^2 + 2)$ for some intger n. This means that $n^2 + 2 = 4k$ for some integer k. We'll consider the two cases where n even and where n odd. If n is even, then $n = 2m$ for some integer m. Substituting for n we obtain

$$4k = n^2 + 2 = (2m)^2 + 2 = 4m^2 + 2.$$

We can divide both sides of the equations by 2 to obtain

$$2k = 2m^2 + 1.$$

This says that an even number $(2k)$ is equal to an odd number $(2m^2 + 1)$, which is a contradiction. Therefore, n cannot be even. Now assume n is odd. Then $n = 2m + 1$ for some integer m. Substituting for n we obtain

$$4k = n^2 + 2 = (2m + 1)^2 + 2 = 4m^2 + 4m + 3.$$

Isolate 3 on the right side of the equation to obtain

$$4k - 4m^2 - 4m = 3.$$

This is a contradiction because the left side is even and the right side is odd. Therefore, n cannot be odd. QED.

end example

example **1.5 Prime Numbers**

We'll prove the following statement about integers:

Every integer greater than 1 is divisible by a prime.

Proof: Assume the statement is false. Then some integer $n > 1$ is not divisible by a prime. Since a prime divides itself, n cannot be a prime. So there is at least one integer d such that $d|n$ and $1 < d < n$. Assume that d is the smallest divisor of n between 1 and n. Now d is not prime, else it would be a prime divisor of n. So there is an integer a such that $a|d$ and $1 < a < d$. Since $a \mid d$ and $d \mid n$, have $a \mid d$ and $d \mid n$, it follows from Example 2 that $a \mid n$. But now we have $a \mid n$ and $1 < a < d$, which contradicts the assumption that d is the smallest such divisor of n. QED.

end example

If and Only If Proofs

The statement "A if and only if B" is shorthand for the two statements "If A, then B" and "If B, then A." The abbreviation "A *iff* B" is often used for "A if and only if B." Instead of "A iff B," some people write "A is a necessary and sufficient condition for B" or "B is a necessary and sufficient condition for A." Remember that two proofs are required for an iff statement, one for each conditional statement.

example **1.6 An Iff Proof**

We'll prove the following iff statement about integers:

$$x \text{ is odd if and only if } 8 \mid (x^2 - 1).$$

To prove this iff statement, we must prove the following two statements:

a. If x is odd, then $8 \mid (x^2 - 1)$.

b. If $8 \mid (x^2 - 1)$, then x is odd.

Proof of (a): Assume x is odd. Then we can write x in the form $x = 2k + 1$ for some integer k. Substituting for x in $x^2 - 1$ gives

$$x^2 - 1 = 4k^2 + 4k = 4k(k + 1).$$

Since k and $k + 1$ are consecutive integers, one is odd and the other is even, so the product $k(k + 1)$ is even. So $k(k + 1) = 2m$ for some integer m. Substituting for $k(k + 1)$ gives

$$x^2 - 1 = 4k(k + 1) = 4(2m) = 8m.$$

Therefore, $8 \mid (x^2 - 1)$, so part (a) is proven.

Proof of (b): Assume $8 \mid (x^2 - 1)$. Then $x^2 - 1 = 8k$ for some integer k. Therefore, we have $x^2 = 8k + 1 = 2(4k) + 1$, which has the form of an odd integer. So x^2 is odd and it follows from Example 3 that x is odd, so part (b) is proven. Therefore, the iff statement is proven. QED.

end example

Sometimes we encounter iff statements that can be proven by using statements that are related to each other by iff. Then a proof can be constructed as a sequence of iff statements. For example, to prove A iff B we might be able to find a statement C such that A iff C and C iff B are both true. Then we can conclude that A iff B is true. The proof could then be put in the form A iff C iff B.

example

1.7 Two Proofs in One

We'll prove the following statement about integers:

$$x \text{ is odd if and only if } x^2 + 2x + 1 \text{ is even.}$$

Proof: The following sequence of iff statements connects the left side to the right side. (The reason for each step is given in parentheses.)

x is odd iff	$x = 2k + 1$ for some integer k	(definition)
iff	$x + 1 = 2k + 2$ for some integer k	(algebra)
iff	$x + 1 = 2m$ for some integer m	(algebra)
iff	$x + 1$ is given	(definition)
iff	$(x + 1)^2$ is even	(Exercise 8a)
iff	$x^2 + 2x + 1$ is even	(algebra) QED

end example

On Constructive Existence

If a statement asserts that some object exists, then we can try to prove the statement in either of two ways. One way is to use proof by contradiction, in which we assume that the object does not exist and then come up with some kind of contradiction. The second way is to construct an instance of the object. In either case we know that the object exists, but the second way also gives us an

instance of the object. Computer science leans toward the construction of objects by algorithms. So the *constructive approach* is usually preferred, although it's not always possible.

Important Note

Always try to write out your proofs. Use complete sentences that describe your reasoning. If your proof seems to consist only of a bunch of equations or expressions, you still need to describe how they contribute to the proof. Try to write your proofs the same way you would write a letter to a friend who wants to understand what you have written.

Exercises

1. See whether you can convince yourself, or a friend, that the conditional truth table is correct by making up English sentences of the form "If A, then B."

2. Verify that the truth tables for each of the following pairs of statements are identical.
   a. "not (A and B)" and "(not A) or (not B)."
   b. "not (A or B)" and "(not A) and (not B)."
   c. "if A, then B" and "if (not B), then (not A)."
   d. "if A, then B" and "(not A) or B."
   e. "not (if A then B)" and "A and (not B)."

3. Prove or disprove each of the following statements by exhaustive checking.

   a. There is a prime number between 45 and 54.
   b. The product of any two of the four numbers 2, 3, 4, and 5 is even.
   c. Every odd integer between 2 and 26 is either prime or the product of two primes.
   d. If $d \mid ab$, then $d \mid a$ or $d \mid b$.
   e. If m and n are integers, then $(3m + 2)(3n + 2)$ has the form $(3k + 2)$ for some integer k.

4. Prove each of the following statements about the integers.

   a. If x and y are even, then $x + y$ is even.
   b. If x is even and y is odd, then $x + y$ is odd.
   c. If x and y are odd, then $x - y$ is even.
   d. If $3n$ is even, then n is even.

5. Write down the converse of the following statement about integers:

   If x and y are odd, then $x - y$ is even.

   Is the statement that you wrote down true or false? Prove your answer.