WRITING PROOFS

Christopher Heil
Georgia Institute of Technology

A "theorem" is just a statement of fact. A "proof" of the theorem is a logical explanation of why the theorem is true.

Many theorems have this form:

Theorem I. *If statement A is true then statement B is true.*

This just means that whenever statement A is valid, then statement B *must* be valid as well. A proof is an explanation of WHY statement B must be true whenever statement A is true.

1. Direct Proofs.

There are several ways to write a proof of the theorem "If statement A is true then statement B is true." We'll discuss several of them in these pages. It may not be obvious at first which variety of proof to use, but a good rule of thumb is to try a *direct proof* first.

A direct proof. Start by assuming that statement A is true. After all, if statement A is false then there's nothing to worry about; it doesn't matter then whether B is true or false. So, suppose that statement A is true—write that down as the first step. This is information that you can use and build on. Now try to proceed logically, one step at a time, building on this information until you have shown that statement B is true.

An important point is that a proof is always written in *English*! There are mathematical symbols in with the words, but you must write clear, complete, English sentences, one after another until you've made your way through to statement B. Finally, write an "end-of-proof" symbol: either Q.E.D. or □ to show that you've finished the proof.

Here is an example of a simple theorem and a simple direct proof.

Theorem 1. *If p is a prime number bigger than 2, then p is odd.*

Proof. Suppose that p is a prime number and $p > 2$. *(That's where we've assumed that statement A is true. Now build on this until you've shown that statement B is true.)* To show that p is odd, we have to show that p is not divisible by 2. Now, because p is a prime number, it is divisible only by 1 and itself. Since $2 \neq 1$ and $2 \neq p$, the number 2 is not one of the numbers that divides p. Therefore p is not divisible by 2, and hence p is an odd number. □

Admittedly, that was a pretty easy theorem and a pretty easy proof, which I've made excessively long just to give you the idea. Most theorems are harder, and you have to sit and think before you get the proof straight.

DON'T BE DISAPPOINTED IF YOU DON'T SEE HOW TO DO THE PROOF RIGHT AWAY! Most of the time, it takes THREE sheets of paper to write a proof:

(1) Scratch paper, where you just try out all kinds of ideas, most of which don't work, until you see something that will work.

(2) Second sheet, where you make your first attempt to write the proof. You try to write the proof neatly, but chances are that when you try to do this you'll realize that your proof isn't *quite* correct. So, you work on it some more, turning this sheet into scratchwork also, until you think you've got it right.

(3) Third sheet, where you do write the proof neatly (in English, in complete sentences!). This time you'll probably get it right.

Remember that what you see in class and read in the book is the THIRD SHEET ONLY! The author doesn't show you his scratchwork! Usually, you can't just sit down and work a problem straight through; it takes thought, a lot of scribbling, and a lot of messed-up scratchwork. Also remember that the goal is to **COMMUNICATE** the proof to the reader, so you must write CLEARLY and COMPLETELY!

2. Contrapositive Proofs.

Here is another approach to writing a proof of Theorem I. Logically, Theorem I is exactly the same as this theorem, which is called the **contrapositive** of Theorem I.

Theorem II. *If statement B is false then statement A is false.*

For example, the contrapositive of the theorem "if it rains then there are clouds in the sky" is the theorem "if there are no clouds in the sky then it is not raining." These are logically the SAME statement. So, if you want to prove Theorem I and don't see how, you can try proving Theorem II instead. That is, start by assuming that statement B is false, and try to build on this until you show that statement A is false.

3. Proofs by Contradiction.

Here is another way to prove Theorem I: by *contradiction*. Assume as before that statement A is true. But now, in addition, assume that statement B is *false*. Build on all this information until you obtain a contradiction. This means that your assumption that statement B is false is impossible. Here is an example.

Theorem 2. *If a positive integer m is evenly divisible by some integer $n > 1$, then $m+1$ is not evenly divisible by n.*

Proof. Suppose m is evenly divisible by n. *(This is where you assume statement A is true.)* This means that $m = kn$ for some integer k. Suppose also that $m+1$ was divisible by n. *(This is where you assume that statement B is false. Now use this information!)* The fact that $m + 1$ is evenly divisible by n means that $m + 1 = jn$ for some integer j. Since we have both $m = kn$ and $m + 1 = jn$, this implies that

$$jn = m + 1 = kn + 1,$$

and therefore $(j - k)n = 1$. But n is an integer greater than 1 and $j - k$ is also an integer, so it is impossible for their product to be 1. *(This is the contradiction.)* Hence $m + 1$ cannot be divisible by n. □

Here is a final example of a proof by contradiction. This theorem was proved by Euclid a LONG time ago. Note that the statement of the theorem is slightly different than what we've discussed: it has the form "statement B is true" without any dependence on some statement A. All the same principles apply, however.

Theorem 3. (Euclid) *There are infinitely many prime numbers.*

Proof. Suppose that only finitely many prime numbers existed. *(Here is where we assume that statement B is false.)* Let's call these finitely many prime numbers $p_1, p_2, \ldots, p_N$. Now consider the number $m = p_1 p_2 \cdots p_N$, the product of all those prime numbers. This number m is evenly divisible by each of $p_1, p_2, \ldots, p_N$. Therefore, by Theorem 2, $m + 1$ is NOT divisible by any of $p_1, p_2, \ldots, p_N$! Thus $m + 1$ is only evenly divisible by 1 and itself. But then $m + 1$ is a NEW prime number, bigger than

any of $p_1, p_2, \ldots, p_N$. This is a contradiction, because we said that $p_1, p_2, \ldots, p_N$ were ALL the prime numbers that there were. Since we have obtained a contradiction, our assumption that there existed only finitely many prime numbers must be incorrect. Hence, there must in fact be infinitely many prime numbers. □

It might surprise you learn that the existence of arbitrarily large prime numbers is of vital importance in cryptography. Governments—and now businesses—are paying huge sums of money to encode data using schemes based on huge prime numbers. A fast factoring algorithm is the holy grail of much computing research!

Question: Look carefully at the proof of Euclid's theorem. Does that proof show that if $p_1, p_2, \ldots, p_N$ are prime numbers then $m = p_1 p_2 \cdots p_N + 1$ is also a prime number? Let's check:

$$\begin{aligned} 2 + 1 &= 3 \text{ is prime} \\ 2 \cdot 3 + 1 &= 7 \text{ is prime} \\ 2 \cdot 3 \cdot 5 + 1 &= 31 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311 \text{ is prime} \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 30031 = 59 \cdot 509 \text{ is NOT prime!!} \end{aligned}$$

What went wrong? NOTHING! There's nothing wrong with the proof of Euclid's theorem. Just be careful about what it says. All that the proof says is that IF there were only finitely many prime numbers $p_1, p_2, \ldots, p_N$ THEN $m = p_1 p_2 \cdots p_N + 1$ would be prime. But we showed that there AREN'T finitely many prime numbers, so the statement "IF there were only finitely many prime numbers $p_1, p_2, \ldots, p_N$ THEN $m = p_1 p_2 \cdots p_N + 1$ would be prime" is vacuous, i.e., it simply doesn't apply.

4. If and Only If Theorems.

Here is another typical type of theorem:

Theorem III. *Statement A is true if and only if statement B is true.*

This is logically equivalent to two theorems:

If statement A is true then statement B is true
AND
If statement B is true then statement A is true

Therefore, when you try to write a proof for Theorem III you need to write TWO proofs, one for each "direction." For example, you could write two direct proofs: start by assuming that statement A is true and then proceed until you've shown that statement B is true. Then, start all over: assume statement B is true and work until you've shown that statement A is true. IF YOU ONLY WRITE ONE OF THESE THEN YOU HAVEN'T PROVED THE THEOREM!

Here is an example.

Theorem 4. *Let n be a positive integer. Then n is even if and only if n^2 is even.*

Proof. We have to write TWO PROOFS.

"⇒." *(In this part, we'll use a direct proof to show that if n is even, then n^2 is even.)* Suppose that n is even. This means that $n = 2k$ for some integer k. Therefore $n^2 = 4k^2$. Since $4k^2$ is divisible by 2, we conclude that $n^2 = 4k^2$ is even.

"$\Leftarrow$." *(In this part, we'll use a contrapositive proof to show that if n^2 is even, then n is even. To do this, we must show that if n is not even, then n^2 is not even.)* Suppose that n is odd. That means that $n = 2k+1$ for some integer k. Therefore, $n^2 = 4k^2+4k+1$. But the number $4k^2+4k$ is divisible by 2, so by Theorem 2, the number $4k^2+4k+1$ cannot be divisible by 2. Hence $n^2 = 4k^2+4k+1$ is odd. $\square$

Here is another situation where you have to write two proofs. If X and Y are *sets* (collections of objects) and you want to show that $X = Y$ then you must show two things:

(1) First show that if $x \in X$ then $x \in Y$. This shows that $X \subset Y$.
(2) Next show that if $y \in Y$ then $y \in X$. This shows that $Y \subset X$.

The combination of the two proofs establishes that every object in X is also in Y and vice versa, and therefore that the two sets are the same.

5. Proof by Induction.

Here is a final method of proof that we'll only use rarely. It's used when you have a lot of statements, one for each integer, say, statements A_n for $n = 1, 2, 3, \ldots$, that you need to prove. The theorem looks like this:

Theorem 4. *Statement A_n is true for $n = 1, 2, 3, \ldots$.*

The proof is by a method that should be familiar to anyone in computer science: *recursion!* It's used when you don't see how to prove each statement individually, but you do see how to get from one statement to the next. Here is how to write a proof by induction:

Step 1. Show that the first statement A_1 is true.

Step 2. Prove the following: IF statement A_n is true then statement A_{n+1} is true.

That's all there is: once you've done those two things you've written a complete proof. Why does this show that, say, A_{13} is true? Because of the recursion. We have NOT shown directly that A_{13} is true. What we've shown is that IF A_{12} is true THEN A_{13} is true. Of course, we don't know that A_{12} is true, but we have shown that IF A_{11} is true THEN A_{12} is true, and so forth, down to IF A_1 is true THEN A_2 is true. And we HAVE shown that A_1 is true (that's why you need Step 1), so the recursion works. Follow the links back, and you conclude that A_{13} is true.

Here is an example using induction as the method of proof.

Theorem. *For each integer $n \geq 1$ we have $1 + \cdots + n = \frac{n(n+1)}{2}$.*

Proof.

Step 1. It's true for $n = 1$ because $1 = \frac{1(1+1)}{2}$.

Step 2. We have to show that IF $1 + \cdots + n = \frac{n(n+1)}{2}$ is true for some particular n, then the analogous statement is also true for the number $n+1$. So, ASSUME that $1 + \cdots + n = \frac{n(n+1)}{2}$ is true for some n, and USE this information to show that the formula is also valid for $n+1$. We calculate:

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

We used the formula for n, and what we end up with is the correct formula for $n+1$. Note that we didn't prove the formula for $n+1$ directly! All we did is show that IF it's true for some n THEN it's true for $n+1$. And that's enough to make the recursion work. $\square$