6.042/18.062J Mathematics for Computer Science February 3, 2005
Srini Devadas and Eric Lehman Lecture Notes

Proofs

Why do you believe that $3 + 3 = 6$?

Is it because your second-grade teacher, Miss Dalrymple, told you so? She might have been lying, you know. Or are you trusting life experience? If you have three coconuts and someone gives you three more coconuts, then you have— aha!— six coconuts. But if *that* is the true basis for your belief, then why do you also believe that

$$3,000,000,000 + 3,000,000,000 = 6,000,000,000?$$

Surely you've never actually counted six billion of anything!

Maybe $3 + 3 = 6$ is just "intuitively obvious", and we shouldn't talk about it anymore.

Hey, here is a game! I secretly put one or more dollar bills into an envelope and then put twice as many dollar bills into a second envelope:

$$\boxed{\$n} \qquad\qquad \boxed{\$2n}$$

I seal both envelopes, mix them up, and present them to you. You can pick one and look inside to see how much money it contains. Then you can either take the money in that envelope *or* take the unknown amount of money in the other envelope. Those are the rules. For example, suppose we play this game and you find $8 in the envelope you initially selected.

$$\boxed{\$8} \qquad\qquad \boxed{?}$$

What is your most profitable course? Keep the $8? Or take the unknown amount in the other envelope? Are both options equally good? This situation is hardly more complicated than having three coconuts and being given three more. Yet now the correct conclusion is far from "intuitively obvious". Seemingly plausible arguments about this problem degenerate to absurdities and contradictions.

So you may want to dismiss $3 + 3 = 6$ and hurry along, but eventually we do have to confront the underlying question: how can we *know anything* in mathematics? When intuition falters as a guide to truth, how can we distinguish valid mathematics from crackpot ravings? These are show-stopper questions. Without clear answers, all the number crunching and variable juggling in mathematics is just so much nonsense.

The Two-Envelopes Game

Here are some "solutions":

- You picked an envelope at random, so you were just as likely to pick the one with more dollars as the one with fewer. Therefore, if you see $8, then the other envelope is equally likely to contain either $4 or $16. On average, the other envelope contains $(4 + 16)/2 = 10$ dollars, which is more than the $8 you see. So you should clearly switch to the unopened envelope.

  However, a similar argument applies no matter what amount you see initially. So you should *always* switch, regardless of the amount in the first envelope. Thus, the best strategy is to pick one envelope and then, without even bothering to look inside, take the amount of money in the other. But that's absurd!

- You were just as likely to pick the envelope with more dollars as with fewer. So, on average, the amount of money in the envelope you picked is the same as the amount in the unopened envelope. So staying or switching makes no difference.

  But what if you saw $1? In that case, you could be certain that the other envelope contained $2. So your strategy *would* make a difference!

- Look at the problem from my perspective. Clearly, I should not put $1 in either envelope; that would give you a big advantage. If you opened the envelope with $1, then you would know to switch. But then if you see $2 in an envelope, you know that the other envelope *must* contain $4 since we just ruled out $1. So you also have a big advantage in this situation. My only choice is to never put $2 in an envelope either. And I can't use $3; if you saw that, you'd know the other envelope held $6. And if you see $4, you know the other envelope must contain $8. Apparently, I can't run the game at all!

  We're revisit this problem later in the term when we study probability.

1 The Axiomatic Method

The standard procedure for establishing truth in mathematics was invented by Euclid, a mathematician working in Alexadria, Egypt around 300 BC. His idea was to begin with five *assumptions* about geometry, which seemed undeniable based on direct experience. (For example, "There is a straight line segment between every pair of points.) Propositions like these that are simply accepted as true are called ***axioms***.

Starting from these axioms, Euclid established the truth of many additional propositions by providing "proofs". A ***proof*** is a sequence of logical deductions from axioms and previously-proved statements that concludes with the proposition in question. You probably wrote many proofs in high school geometry class, and you'll see a lot more in this course.

There are several common terms for a proposition that has been proved. The different terms hint at the role of the proposition within a larger body of work.

- Important propositions are called ***theorems***.
- A ***lemma*** is a preliminary proposition useful for proving later propositions.
- A ***corollary*** is an afterthought, a proposition that follows in just a few logical steps from a theorem.

The definitions are not precise. In fact, sometimes a good lemma turns out to be far more important than the theorem it was originally used to prove.

Euclid's axiom-and-proof approach, now called the ***axiomatic method***, is the foundation for mathematics today. Amazingly, essentially all mathematics can be derived from just a handful of axioms called ZFC together with a few logical principles. This does not completely settle the question of truth in mathematics, but it greatly focuses the issue. You can still deny a mathematical theorem, but only if you reject one of the elementary ZFC axioms or find a logical error in the proof.

1.1 Our Axioms

For our purposes, the ZFC axioms are *too* primitive— by one reckoning, proving that $2 + 2 = 4$ requires more than 20,000 steps! So instead of starting with ZFC, we're going to take a *huge* set of axioms as our foundation: we'll accept all familiar facts from high school math!

This will give us a quick launch, but you *will* find this imprecise specification of the axioms troubling at times . For example, in the midst of a proof, you may find yourself wondering, "Must I prove this little fact or can I take it as an axiom?" Feel free to ask for guidance, but really there is no absolute answer. Just be upfront about what you're assuming, and don't try to evade homework and exam problems by declaring everything an axiom!

The ZFC Axioms

These are the axioms of Zermelo-Fraenkel set theory with some technicalities omitted. The variables denote distinct sets. Essentially all of mathematics can be derived from these axioms together with a few principles of logic.

Extensionality. Sets are equal if they contain the same elements:

$$\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y$$

Union. The union of a collection of sets is also a set:

$$\exists y \forall z(\exists w(z \in w \wedge w \in x) \Rightarrow z \in y)$$

Infinity. There is an infinite set; specifically, a set contained in the union of its elements.

$$\exists y(\exists x(x \in y) \wedge \forall z(z \in y \Rightarrow \exists w(z \in w \wedge w \in y)))$$

Power Set. All subsets of a set form another set.

$$\exists y \forall z(\forall w(w \in z \Rightarrow w \in x) \Rightarrow z \in y)$$

Replacement. The image of a function is a set.

$$\forall w \exists y \forall z(\phi(w, z) \Rightarrow z = y) \Rightarrow \exists y \forall z(z \in y \Leftrightarrow \exists w(w \in x \wedge \phi(w, z)))$$

Regularity. Every nonempty set contains a set disjoint from itself.

$$\exists y(y \in x) \Rightarrow \exists y(y \in x \wedge \forall z(z \in y \Rightarrow \neg z \in x))$$

Choice. We can pick one element from each set in a collection.

$$\exists y \forall z \forall w((z \in w \wedge w \in x) \Rightarrow \exists v \exists u(\exists t((u \in w \wedge w \in t) \wedge (u \in t \wedge t \in y)) \Leftrightarrow u = v))$$

We're *not* going to be working with the ZFC axioms in this course. We just thought you might like to see them.

1.2 Proofs in Practice

In principle, a proof can be *any* sequence of logical deductions from axioms and previously-proved statements that concludes with the proposition in question. This freedom in constructing a proof can seem overwhelming at first. How do you even *start* a proof?

Here's the good news: many proofs follow one of a handful of standard templates. Proofs all differ in the details, of course, but these templates at least provide you with an outline to fill in. We'll go through several of these standard patterns, pointing out the basic idea and common pitfalls and giving some examples. Many of these templates fit together; one may give you a top-level outline while others help you at the next level of detail. And we'll show you other, more sophisticated proof techniques later on.

The recipes below are very specific at times, telling you exactly which words to write down on your piece of paper. You're certainly free to say things your own way instead; we're just giving you something you *could* say so that you're never at a complete loss.

2 Proving an Implication

An enormous number of mathematical claims have the form "If P, then Q" or, equivalently, "P implies Q". Here are some examples:

- (Quadratic Formula) If $ax^2 + bx + c = 0$ and $a \neq 0$, then $x = (-b \pm \sqrt{b^2 - 4ac})/2a$.
- (Goldbach's Conjecture) If n is an even integer greater than 2, then n is a sum of two primes.
- If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$.

There are a couple standard methods for proving an implication.

2.1 Method #1

In order to prove that P implies Q:

1. Write, "Assume P."
2. Show that Q logically follows.

Example

Theorem 1. *If* $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$.

Before we write a proof of this theorem, we have to do some scratchwork to figure out why it is true.

The inequality certainly holds for $x = 0$; then the left side is equal to 1 and $1 > 0$. As x grows, the $4x$ term (which is positive) initially seems to have greater magnitude than $-x^3$ (which is negative). For example, when $x = 1$, we have $4x = 4$, but $-x^3 = -1$ only. In fact, it looks like $-x^3$ doesn't begin to dominate until $x > 2$. So it seems the $-x^3 + 4x$ part should be nonnegative for all x between 0 and 2, which would imply that $-x^3 + 4x + 1$ is positive.

So far, so good. But we still have to replace all those "seems like" phrases with solid, logical arguments. We can get a better handle on the critical $-x^3 + 4x$ part by factoring it, which is not too hard:

$$-x^3 + 4x^2 = x(2 - x)(2 + x)$$

Aha! For x between 0 and 2, all of the terms on the right side are nonnegative. And a product of nonnegative terms is also nonnegative. Let's organize this blizzard of observations into a clean proof.

Proof. Assume $0 \leq x \leq 2$. Then x, $2 - x$, and $2 + x$ are all nonnegative. Therefore, the product of these terms is also nonnegative. Adding 1 to this product gives a positive number, so:

$$x(2 - x)(2 + x) + 1 > 0$$

Multiplying out on the left side proves that

$$-x^3 + 4x + 1 > 0$$

as claimed. □

There are a couple points here that apply to all proofs:

- You'll often need to do some scratchwork while you're trying to figure out the logical steps of aproof. Your scratchwork can be as disorganized as you like— full of dead-ends, strange diagrams, obscene words, whatever. But keep your scratchwork separate from your final proof, which should be clear and concise.

- Proofs typically begin with the word "Proof" and end with some sort of doohickey like □ or "q.e.d". The only purpose for these conventions is to clarify where proofs begin and end.

2.2 Method #2 - Prove the Contrapositive

Remember that an implication ("P implies Q") is logically equivalent to its contrapositive ("not Q implies not P"); proving one is as good as proving the other. And often proving the contrapositive is easier than proving the original statement. If so, then you can proceed as follows:

1. Write, "We prove the contrapositive:" and then state the contrapositive.

2. Proceed as in Method #1.

Example

Theorem 2. *If r is irrational, then $\sqrt{r}$ is also irrational.*

Recall that rational numbers are equal to a ratio of integers and irrational numbers are not. So we must show that if r is *not* a ratio of integers, then $\sqrt{r}$ is also *not* a ratio of integers. That's pretty convoluted! We can eliminate both "not"'s and make the proof straightforward by considering the contrapositive instead.

Proof. We prove the contrapositive: if $\sqrt{r}$ is rational, then r is rational.

Assume that $\sqrt{r}$ is rational. Then there exists integers a and b such that:

$$\sqrt{r} = \frac{a}{b}$$

Squaring both sides gives:

$$r = \frac{a^2}{b^2}$$

Since a^2 and b^2 are integers, r is also rational. □

3 A Bogus Technique: Reasoning Backward

Somewhere out in America there must be dozens of high school teachers whispering into innocent ears that "reasoning backward" in proofs is fine... oh, yes, jusssst fine. Probably they sacrifice little furry animals on moonless nights, too. In any case, *they're wrong.*

Let's use the utterly incorrect, but depressingly popular technique of reasoning backward to "prove" a famous inequality.

Theorem 3 (Arithmetic-Geometric Mean Inequality). *For all nonnegative real numbers a and b:*

$$\frac{a+b}{2} \geq \sqrt{ab}$$

Proof.

$$\begin{aligned}
\frac{a+b}{2} &\overset{?}{\geq} \sqrt{ab} \\
a+b &\overset{?}{\geq} 2\sqrt{ab} \\
a^2+2ab+b^2 &\overset{?}{\geq} 4ab \\
a^2-2ab+b^2 &\overset{?}{\geq} 0 \\
(a-b)^2 &\geq 0
\end{aligned}$$

The last statement is true because the square of a real number (such as $a - b$) is never negative. This proves the claim. ×

In this argument, we started with what we wanted to prove and then reasoned until we reached a statement that is surely true. The little question marks, I guess, are supposed to indicate that we're not quite certain that the inequalities are valid until we get down to the last step. At that point, we know everything checks out, apparently.

3.1 Why Reasoning Backward Is Bad

In reasoning backward, we began with the proposition in question— call it P— and reasoned to a true conclusion. Thus, what we actually proved is:

$$P \Rightarrow \text{ true}$$

But this implication is trivially true, *regardless of whether P is true or false!* Therefore, by reasoning backward we can "prove" not only true statements, but also every false statement! Here's an example:

Claim. $0 = 1$

Proof.

$$\begin{aligned}
0 &\overset{?}{=} 1 \\
0\cdot 0 &\overset{?}{=} 1\cdot 0 \\
0 &= 0
\end{aligned}$$

×

So resist the urge to reason backward. If this keeps happening to you anyway, pound your writing hand with a heavy textbook to make it stop. Shout "WRONG! WRONG!" with each blow.

3.2 Reasoning Backward as Scratchwork

Sometimes you might want to try reasoning backward— *but not in a proof.* In particular, when you're trying to *find* a proof, you'll often do some scratchwork as you explore different approaches and ideas. In this context, reasoning backward is reasonable. You *might* then be able to reverse the order of the steps and get a valid proof.

4 Proving an "If and Only If"

Many mathematical theorems assert that two statements are logically equivalent; that is, one holds if and only if the other does. Here are some examples:

- An integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3.
- Two triangles have the same side lengths if and only if all angles are the same.
- A positive integer $p \geq 2$ is prime if and only if $1 + (p-1) \cdot (p-2) \cdots 3 \cdot 2 \cdot 1$ is a multiple of p.

4.1 Method #1: Prove Each Statement Implies the Other

The statement "P if and only if Q" is equivalent to the two statements "P implies Q" and "Q implies P". So you can prove an "if and only if" by proving *two* implications:

1. Write, "We prove P implies Q and vice-versa."
2. Write, "First, we show P implies Q." Do this by one of the methods in Section 2.
3. Write, "Now, we show Q implies P." Again, do this by one of the methods in Section 2.

Example

Two sets are defined to be equal if they contain the same elements; that is, $X = Y$ means $z \in X$ if and only if $z \in Y$. (This is actually the first of the ZFC axioms.) So set equivalence proofs often have an "if and only if" structure.

Theorem 4 (DeMorgan's Law for Sets). *Let A, B, and C be sets. Then:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Proof. We show $z \in A \cap (B \cup C)$ implies $z \in (A \cap B) \cup (A \cap C)$ and vice-versa.

First, we show $z \in A \cap (B \cup C)$ implies $z \in (A \cap B) \cup (A \cap C)$. Assume $z \in A \cap (B \cup C)$. Then z is in A and z is also in B or C. Thus, z is in either $A \cap B$ or $A \cap C$, which implies $z \in (A \cap B) \cup (A \cap C)$.

Now, we show $z \in (A \cap B) \cup (A \cap C)$ implies $z \in A \cap (B \cup C)$. Assume $z \in (A \cap B) \cup (A \cap C)$. Then z is in both A and B or else z is in both A and C. Thus, z is in A and z is also in B or C. This implies $z \in A \cap (B \cup C)$. □

4.2 Method #2: Construct a Chain of Iffs

In order to prove that P is true if and only if Q is true:

1. Write, "We construct a chain of if-and-only-if implications."
2. Prove P is equivalent to a second statement which is equivalent to a third staement and so forth until you reach Q.

This method is generally more difficult than the first, but the result can be a short, elegant proof.

Example

The *standard deviation* of a sequence of values $x_1, x_2, \ldots, x_n$ is defined to be:

$$\sqrt{(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2}$$

where μ is the average of the values:

$$\mu = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

Theorem 5. *The standard deviation of a sequence of values $x_1, \ldots, x_n$ is zero if and only if all the values are equal to the mean.*

For example, the standard deviation of test scores is zero if and only if everyone scored exactly the class average.

Proof. We construct a chain of "if and only if" implications. The standard deviation of $x_1, \ldots, x_n$ is zero if and only if:

$$\sqrt{(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2} = 0$$

where μ is the average of $x_1, \ldots, x_n$. This equation holds if and only if

$$(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2 = 0$$

since zero is the only number whose square root is zero. Every term in this equation is nonnegative, so this equation holds if and only every term is actually 0. But this is true if and only if every value x_i is equal to the mean μ. □

5 How to Write *Good* Proofs

The *purpose* of a proof is to provide the reader with definitive evidence of an assertion's truth. To serve this purpose effectively, more is required of a proof than just logical correctness: a good proof must also be clear. These goals are usually complimentary; a well-written proof is more likely to be a correct proof, since mistakes are harder to hide. Here are some tips on writing good proofs:

State your game plan. A good proof begins by explaining the general line of reasoning, e.g. "We use case analysis" or "We argue by contradiction". This creates a rough mental picture into which the reader can fit the subsequent details.

Keep a linear flow. We sometimes see proofs that are like mathematical mosaics, with juicy tidbits of reasoning sprinkled across the page. This is not good. The steps of your argument should follow one another in a sequential order.

A proof is an essay, not a calculation. Many students initially write proofs the way they compute integrals. The result is a long sequence of expressions without explantion. This is bad. A good proof usually looks like an essay with some equations thrown in. Use complete sentences.

Avoid excessive symbolism. Your reader is probably good at understanding words, but much less skilled at reading arcane mathematical symbols. So use words where you reasonably can.

Simplify. Long, complicated proofs take the reader more time and effort to understand and can more easily conceal errors. So a proof with fewer logical steps is a better proof.

Introduce notation thoughtfully. Sometimes an argument can be greatly simplified by introducing a variable, devising a special notation, or defining a new term. But do this sparingly since you're requiring the reader to remember all that new stuff. And remember to actually *define* the meanings of new variables, terms, or notations; don't just start using them!

Structure long proofs. Long programs are usually broken into a heirarchy of smaller procedures. Long proofs are much the same. Facts needed in your proof that are easily stated, but not readily proved are best pulled out and proved in preliminary lemmas. Also, if you are repeating essentially the same argument over and over, try to capture that argument in a general lemma, which you can cite repeatedly instead.

Don't bully. Words such as "clearly" and "obviously" serve no logical function. Rather, they almost always signal an attempt to bully the reader into accepting something which the author is having trouble justifying rigorously. Don't use these words in your own proofs and go on the alert whenever you read one.

Finish. At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the "obvious" conclusion. What is obvious to you as the author is not likely to be obvious to the reader. Instead, tie everything together yourself and explain why the original claim follows.

The analogy between good proofs and good programs extends beyond structure. The same rigorous thinking needed for proofs is essential in the design of critical computer system. When algorithms and protocols only "mostly work" due to reliance on hand-waving arguments, the results can range from problematic to catastrophic. An early example was the Therac 25, a machine that provided radiation therapy to cancer victims, but occasionally killed them with massive overdoses due to a software race condition. More recently, in August 2004, a single faulty command to a computer system used by United and American Airlines grounded the entire fleet of both companies— and all their passengers!

It is a certainty that we'll all one day be at the mercy of critical computer systems designed by you and your classmates. So we really hope that you'll develop the ability to formulate rock-solid logical arguments that a system actually does what you think it does!

6 Proof by Contradiction

In a ***proof by contradiction*** or ***indirect proof***, you show that if a proposition were false, then some logical contradiction or absurdity would follow. Thus, the proposition must be true. Proof by contradiction is *always* a viable approach. However, as the name suggests, indirect proofs can be a little convoluted. So direct proofs are generally preferable as a matter of clarity.

6.1 Method

In order to prove a proposition P by contradiction:

1. Write, "We use proof by contradiction."

2. Write, "Suppose P is false."

3. Deduce a logical contradiction.

4. Write, "This is a contradiction. Therefore, P must be true."

Example

Remember that a number is *rational* if it is equal to a ratio of integers. For example, $3.5 = 7/2$ and $0.1111\ldots = 1/9$ are rational numbers. On the other hand, we'll prove by contradiction that $\sqrt{2}$ is irrational.

Theorem 6. *$\sqrt{2}$ is irrational.*

Proof. We use proof by contradiction. Suppose the claim is false; that is, $\sqrt{2}$ is rational. Then we can write $\sqrt{2}$ as a fraction a/b in *lowest terms*.

Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that a is even; that is, a is a multiple of 2. Therefore, a^2 must be a multiple of 4. Because of the equality $2b^2 = a^2$, we know $2b^2$ must also be a multiple of 4. This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms.

This is a contradiction. Therefore, $\sqrt{2}$ must be irrational. □

6.2 Potential Pitfall

Often students use an indirect proof when a direct proof would be simpler. Such proofs aren't wrong; they just aren't excellent. Let's look at an example. A function f is *strictly increasing* if $f(x) > f(y)$ for all real x and y such that $x > y$.

Theorem 7. *If f and g are strictly increasing functions, then $f+g$ is a strictly increasing function.*

Let's first look at a simple, direct proof.

Proof. Let x and y be arbitrary real numbers such that $x > y$. Then:

$$\begin{aligned} f(x) > f(y) &\qquad \text{(since } f \text{ is strictly increasing)} \\ g(x) > g(y) &\qquad \text{(since } g \text{ is strictly increasing)} \end{aligned}$$

Adding these inequalities gives:

$$f(x) + g(x) > f(y) + g(y)$$

Thus, $f + g$ is strictly increasing as well. □

Now we *could* prove the same theorem by contradiction, but this makes the argument needlessly convoluted.

Proof. We use proof by contradiction. Suppose that $f + g$ is not strictly increasing. Then there must exist real numbers x and y such that $x > y$, but

$$f(x) + g(x) \leq f(y) + g(y)$$

This inequality can only hold if either $f(x) \leq f(y)$ or $g(x) \leq g(y)$. Either way, we have a contradiction because both f and g were defined to be strictly increasing. Therefore, $f + g$ must actually be strictly increasing. □

7 Does All This Really Work?

So this is where mainstream mathematics stands today: there is a handfull of axioms from which everything else in mathematics can be logically derived. This sounds like a rosy situation, but there are several dark clouds, suggesting that the essence of truth in mathematics is not completely resolved.

- The ZFC axioms weren't etched in stone by God. Instead, they were mostly made up by some guy named Zermelo. Probably some days he forgot his house keys.
- No one knows whether the ZFC axioms are logically consistent; there is some possibility that one person might prove a proposition P and another might prove the proposition $\neg P$. Then math would be broken. This sounds like a crazy situation, but it has happened before. Around the beginning of the 20th century several mathematicians— most famously Bertrand Russell— discovered that accepted principles of mathematics at that time actually *were* self-contradictory!
- While the ZFC axioms largely generate the mathematics everyone wants— where $3 + 3 = 6$ and other basic facts are true— they also imply some disturbing conclusions. For example, the Banach-Tarski Theorem says that a ball can be cut into six pieces and then the pieces can be rearranged to give *two* balls, each the same size as the original!
- In the 1930's, Gödel proved that the ZFC axioms are not complete; that is, there exist propositions that are true, but do not logically follow from the axioms. There seems to be no way out of this disturbing situation; simply adding more axioms does not eliminate the problem.

These problems will not trouble us in 6.042, but they are interesting to think about!