A Guide for Making Proofs

This document is loosely based on MIT OpenCourseWare

Abstract. 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.

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.

Euclids axiom-and-proof approach, now called the axiomatic method, is the foundation for mathematics today.

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 $x = \frac{(-b \pm \sqrt{b^2 - 4ac})}{2a}$.
- (Goldbachs 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.

This methode is equivalent to Fitch rule for the introduction of implication:

1	P	
2	$\vdots$	
3	Q	
4	$P \to Q$	($\to$ intro 1,3)

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 scratch-work 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:

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

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. Lets 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 scratch-work while you're trying to figure out the logical steps of a proof. Your scratch-work can be as disorganized as you like – full of dead-ends, strange diagrams, obscene words, whatever. But keep your scratch-work 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.

In propositional logic, this method relies on the fact that $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ is a tautology.

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. □

2.3 Necessary and sufficient

If $P \to Q$ holds, we say that Q is a necessary condition for P. This means that P can never be true without Q being the case as well. If $Q \to P$ holds, we say that Q is a sufficient condition for P. This means that whenever Q is valid, P will also be true. If a condition is both necessary and sufficient, the condition is equivalent, denoted by $P \leftrightarrow Q$. Proving equivalence is discussed in the next section.

3 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 $1+(p-1)\times(p-2)\times\ldots\times3\times2\times1$ is a multiple of p.

3.1 Method #1: Prove Each Statement Implies the Other

The statement "P if and only if Q" ($P \leftrightarrow Q$) 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 $z \in Y$. So set equivalence proofs often have an "if and only if" structure.

Theorem 3. *(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 $z \in A \cap (B \cup C)$. □

3.2 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 statement 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 $x_1, x_2, ..., x_n$ is defined to be:

$$\sqrt{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \ldots + (x_n - \mu)^2}$$

where μ is the average of the values:

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

Theorem 4. *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:

$$\sqrt{(x_1 - \mu)^2 + (x_2 - \mu)^2 + ... + (x_n - \mu)^2} = 0$$

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

$$(x_1 - \mu)^2 + (x_2 - \mu)^2 + \ldots + (x_n - \mu)^2 = 0$$

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. □

3.3 Method #3: Prove a Cycle of Implications

Sometimes you need to prove the equivalence of three or more statements. In that case, it is a good idea to prove a cycle of implications. For example, if you need to prove that P, Q, and R are all equivalent, it suffices to show that $P \to Q$, $Q \to R$, and $R \to P$.

4 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.

4.1 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."

The equivalent structure in a Fitch proof is as follows:

1	$\neg P$	(hypothesis)
2	⋮	
3	Q	
4	$\neg Q$	
5	$\neg\neg P$	($\neg$-intro, 1,3,4)
6	P	($\neg$-elim, 5)

Example

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

Theorem 5. *$\sqrt{2}$ 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. □

4.2 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. Lets look at an example.

Definition 1. *A function f is strictly increasing if $f(x) > f(y)$ for all real x and y such that $x > y$.*

Theorem 6. *If f and g are strictly increasing functions, then $f + g$ is a strictly increasing function.*

Lets first look at a simple, direct proof.

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

$$f(x) > f(y) \quad \text{(since } f \text{ is strictly increasing)}$$
$$g(x) > g(y) \quad \text{(since } g \text{ is strictly increasing)}$$

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. □

5 Case Analysis

The proof of a statement can sometimes be broken down into several cases, which then can be tackled individually.

5.1 The Method

In order to prove a proposition P using case analysis:

1. Write, "We use case analysis."
2. Identify a sequence of conditions, at least one of which must hold. (If this is not obvious, you must prove it.)
3. For each condition:
   (a) State the condition.
   (b) Prove P assuming that the condition holds.

In a Fitch-style proof, this approach is equivalent to using the rule for the elimination of the $\vee$:

1	$A \vee B$	
2	$\vdots$	
3	$\quad A$	(hypothesis)
4	$\quad \vdots$	
5	$\quad P$	
6	$\vdots$	
7	$\quad B$	(hypothesis)
8	$\quad \vdots$	
9	$\quad P$	
10	P	($\vee$-elim, 1, 3-5, 7-9)

Often case analysis arguments extend to several levels. The most difficult challenge in a case analysis argument is try to decide how to break up the problem. The most common error is failing to construct a complete set of cases.

Example

Theorem 7. *There exist irrational numbers p and q such that p raised to the power q is rational.*

This is an ingenious proof, not the sort of thing one would think up in a few minutes.

Proof. We use case analysis. Let $v = \sqrt{2}^{\sqrt{2}}$. There are two cases:

Case 1: v is rational. Let $p = q = \sqrt{2}$. Then $p^q = v$ is rational, so the claim holds.
Case 2: v is irrational. Let $p = v$ and $q = \sqrt{2}$. Then:

$$p^q = v^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Since 2 is rational, the claim holds.

□

6 Proof by Induction

Mathematical statements often assert that a property holds for all positive integers. *Mathematical induction* can be used to prove asertions of this type. Mathematical induction is based on the rule of inference that if $P(1)$ and $\forall k(P(k) \rightarrow P(k+1)$ are true for the domain of positive integers then $\forall n P(n)$ is true. Proofs by induction play a fundamental role throughout discrete mathematics and computer science.

6.1 The Method

To prove by induction that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

Basic step: We verify that $P(1)$ is true.
Inductive step: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

Example

Theorem 8. *If n is a positive integer then*

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

Proof. Let $P(n)$ be the proposition that the sum of the first n positive integers is $n(n+1)/2$. We prove by induction:

Basic step: $P(1)$ is true because $1 = 1(1+1)/2$.
Induction step: For the inductive hypothesis we assume that $P(k)$ holds for an arbitrary positive integer k. That is, we asume that

$$1 + 2 + \ldots + k = \frac{k(k+1)}{2}$$

Under this assumption, it must be shown that $P(k+1)$ is also true, namely that

$$1+2+\ldots+k+(k+1)=\frac{(k+1)((k+1)+1)}{2}=\frac{(k+1)(k+2)}{2}$$

is also true. When we add $k+1$ to both sides of the equation in $P(k)$ we obtain

$$\begin{aligned}1+2+\ldots+k+(k+1) &= \frac{k(k+1)}{2}+k+1\\ &= \frac{k(k+1)+2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

This last equation shows that $P(k+1)$ is true under the asumption that $P(k)$ is true, this completes the inductive step.

By mathematical induction, we have proven that $1+2+\ldots+n=\frac{n(n+1)}{2}$ for all positive integers n. □

7 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.

Dont 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. Dont 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 handwaving 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!