Guide to Proofs

Thanks to Michael Kim for writing some of the proofs used in this handout.

What makes a proof a "good proof?" It's hard to answer this question directly – it's like asking what makes an essay a "good essay." There are many traits that good essays have in common, and there are many traits that bad essays have in common, but no hard and fast rules governing how to write essays.

In this handout, we've compiled several different proofs that are similar to the proofs that have been submitted in past quarters. We've annotated each of them with our feedback about what we like about them and ways in which they could be improved. Our hope is that by giving you various examples of good proofs, you'll have a better sense for what we're looking for.

If you'd like some additional resources on good proofwriting, we suggest checking out Chapter 2.4 of the online course reader (which has some general style and design tips for proofs), or looking at these links, which have useful information about how to write proofs:

- ***Mathematical Writing*** by Knuth, Larrabee, and Roberts (available online at http://jmlr.org/reviewing-papers/knuth_mathematical_writing.pdf). This is a set of course notes for a class that Prof. Donald Knuth taught at Stanford back in 1987. The "Minicourse in Technical Writing" has great advice about how to write mathematically.
- ***Some Remarks on Writing Mathematical Proofs*** by John M. Lee (available online at http://www.math.washington.edu/~lee/Writing/writing-proofs.pdf). I often refer to these notes myself when trying to write mathematical proofs, as they're accessible, clearly-written, and well-motivated.

Example: Pythagorean Triples

On Problem Set One, we've asked you to prove this result about Pythagorean triples (recall that a Pythagorean triple is a triple (a, b, c) where a, b and c are positive integers and $a^2 + b^2 = c^2$):

> If (a, b, c) is a Pythagorean triple, then $(a + 1, b + 1, c + 1)$ is not a Pythagorean triple.

Let's consider the following, related result:

> There are no positive integers a and b for which (a, a, b) is a Pythagorean triple.

Here is one sample proof of this result:

Proof: If (a, a, b) is a Pythagorean triple, $2a^2 = b^2 \Rightarrow b / a = \sqrt{2}$, which is impossible. ■

This proof is definitely on the short side, but even so it's possible to follow the reasoning. Starting with the assumption that (a, a, b) is a Pythagorean triple, we get that $2a^2 = b^2$ (though you might have to pause for a second to see why). This in turn implies that $b / a = \sqrt{2}$, which can't happen because $\sqrt{2}$ is irrational.

That said, this proof is terse to a fault. Although the reasoning is correct, this proof requires a lot of work from the reader to rehydrate. In particular, let's look at three steps:

If (a, a, b) is a Pythagorean triple, $2a^2 = b^2$
$b / a = \sqrt{2}$
Which is impossible.

Each of these steps, in the context of the preceding steps, is correct. However, unless you already know *why* they're valid, it's difficult to determine it from the proof itself. Proofs exist to convey a line of reasoning to a reader who does not know why the result is true (or that it's even true in the first place). Consequently, when writing proofs, it is important to include details that would let a mathematically educated reader understand why your result is true.

Here is an alternative version of the above proof, in which we've added additional details to clarify the reasoning:

Proof: By contradiction; assume there exists some positive integers a and b for which (a, a, b) is a Pythagorean triple. Since (a, a, b) is a Pythagorean triple, we have $a^2 + a^2 = b^2$, so $2a^2 = b^2$. Because (a, a, b) is a Pythagorean triple, we have $a > 0$, so a is nonzero. Because $2a^2 = b^2$, we can divide both sides by a^2 to get $2 = b^2 / a^2$. Taking the square root of both sides gives us that $b / a = \sqrt{2}$. This means we can write $\sqrt{2} = b / a$ for integers b and a, where $a \neq 0$. Thus $\sqrt{2}$ is rational. However, as proven earlier, $\sqrt{2}$ is irrational. We have reached a contradiction, so our assumption must have been wrong. Thus (a, a, b) cannot be a Pythagorean triple. ■

There are several important differences between this proof and the original:

- *The proof gives guideposts to its overall structure*. The original proof starts off with the assumption that (a, a, b) is a Pythagorean triple without actually explaining why it's doing so. This might confuse the reader – if you're trying to prove that (a, a, b) can't possibly be a Pythagorean triple, why are you assuming it? Additionally, it concludes by explaining that the contradiction that has been reached implies the main result to be proved, which helps explain the arc of the proof.
- *The proof explains how the steps follow from one another*. With some simple arithmetic, it's easy to see why if (a, a, b) is a Pythagorean triple, then $2a^2 = b^2$. The initial proof omits the steps necessary to show this, which forces the reader to stop reading the proof, grab a sheet of paper, and work through the math. This disrupts the narrative flow of the proof, and, in the event that the reader can't determine how the first part implies the second, the reader won't fully understand the proof's logic.
- *The proof justifies its contradiction*. The initial proof concludes by noting $b / a = \sqrt{2}$ is impossible. However, it doesn't explain *why* this is impossible. Calling back to the definition of a rational number helps the reader better understand what is going on.
- *The proof has better narrative flow*. Remember: **treat proofs as essays**. The purpose of a proof is to convey a valid line of reasoning, not to describe a calculation. Therefore, a proof should function as a piece of writing that, while using mathematical symbols, can still be read with ease. A good test for whether a proof is clear and elegant is whether you can read it aloud; the original proof fails this test. Try reading the phrase "If (a, a, b) is a Pythagorean triple, $2a^2 = b^2 \Rightarrow b / a = \sqrt{2}$" aloud; you'll probably get stuck at the comma after "triple" (does the comma indicate "then" or a continuation of what's being assumed?) and at the ⇒ symbol (which cannot easily be articulated.)

Example: Rational and Irrational Numbers

There are infinitely more irrational numbers than rational numbers, though actually showing a particular number is irrational might take some effort. Here's an interesting statement to prove:

$\log_2 3$ is irrational.

Here is one attempted proof of this result:

> *Proof:* Here, we set out to prove that $\log_2 3$ is irrational. Remember that a rational number is a number r where there exists integers p and q such that $p / q = r$. Thus, we need to show that no such p and q exists for $p / q = \log_2 3$. Thus, we will proceed by contradiction and a false statement to prove a true one. If we assume that $\log_2 3 = p / q$ for some integers p and q, then we know by properties of logs that this means $2^{\log_2 3} = 2^{p/q}$. Thus, we have that $3 = 2^{p/q}$. If we raise each side to the qth power we see $2^p = 3^q$, which means we have to find p and q to solve this equation. We see that one such solution is $p = 0$ and $q = 0$ and both sides of the equation are 1. But this is not allowed because we had a q in the denominator, so if $q = 0$, then $\log_2 3$ would be infinite or undefined and wouldn't make sense. Since we know that we can calculate this value, then it can't be that $q = 0$. Thus, we must find another way to prove this fact. To do this, we note the first few powers of 2 and of 3. These are 2, 4, 8, 16, 32, ... and 3, 9, 27, 81, 243, ... As you can see, the powers of 2 are always even and the powers of 3 are always odd. It's now clear that even numbers are closed under exponentiation and so are the odd ones. Thus, we discover that $2^p \neq 3^q$ for any p, q that would be legal to choose. Because we discover this, we know that we have reached a contradiction, so we know it must be false. ■

This is an excellent *first draft* of a proof. It reads as an exploration of the topic at hand – why it's going to use a proof by contradiction, what the first powers of two and powers of three are, why q can't be zero, etc. However, because of this, it's far more verbose than is necessary and contains many pieces that could be significantly condensed or eliminated. Take this part as an example:

> Here, we set out to prove that $\log_2 3$ is irrational. Remember that an irrational number is a number r such that there exists integers p and q such that $p / q = r$. Thus, we need to show that no such p and q exists for $p / q = \log_2 3$. Thus, we will proceed by contradiction and a false statement to prove a true one.

As part of a draft, this is a great line of reasoning to follow. When writing this up as a formal proof, though, it should probably be restructured:

- Since the proof is a proof by contradiction, the proof should probably start off by announcing itself as such.
- The mechanics behind a proof by contradiction – assuming a false statement to prove a true one – are usually not included inside the proof. The reader should already know this.
- The clarification that what needs to be shown is that there aren't any legal choices of p and q such that $p / q = \log_2 3$ is true, but isn't actually used anywhere in the proof. The proof setup works by showing that any choice of p and q satisfying this equation leads to a contradiction, but doesn't try to directly show that no choices of p or q will work.

Here's how we might start the proof off, including the same core ideas but without as much exposition:

> *Proof:* By contradiction; assume that $\log_2 3$ is rational. Then there exists some $p, q \in \mathbb{Z}$ such that $p / q = \log_2 3$ and $q \neq 0$. …

Another example where the proof could be tightened up is here:

> We see that one such solution is $p = 0$ and $q = 0$ and both sides of the equation are 1. But this is not allowed because we had a q in the denominator, so if $q = 0$, then $\log_2 3$ would be infinite or undefined and wouldn't make sense.

Here, the proof is relying on the fact that $p / q = \log_2 3$, so it doesn't make sense for q to be zero. If you look back at the way the original proof is structured, you'll notice that it never asserts that q is nonzero. This means that at this point in the proof, the argument has to "go back in time" and try to patch up a missing step from earlier. In a draft, that's fine, but in a proof submitted for reading (either in a journal or on a problem set) it's expected that the author would clean this up by adopting an approach more along the lines of the one in the updated version.

One last part of the proof that needs some attention is this bit near the end:

> We note the first few powers of 2 and of 3. These are 2, 4, 8, 16, 32, ... and 3, 9, 27, 81, 243, ... As you can see, the powers of 2 are always even and the powers of 3 are always odd. It's now clear that even numbers are closed under exponentiation and so are the odd ones.

When exploring why the result is true, it's perfectly reasonable to start listing off powers of two and powers of three and looking for a trend. The trend the proof notes is that powers of two are always even (except for 1, which was accounted for earlier in the proof) and powers of three are always odd, which will cause a problem.

However, the way that this is written could use some work. First, in a mathematical proof, it is usually not sufficient to argue that a result is generally true by listing off examples and saying "as you can see.." or "it's now clear... ." A proof should be a rigorous argument that justifies each of its steps. Here, the proof tries to justify that 2^p is even for integers $p > 1$ and that 3^q is odd for integers $q > 1$. To be more rigorous, the proof might use induction on p and q, or could note that two is a divisor of 2^p for $p > 1$ but is never a divisor of 3^q, etc.

There's actually a small logic hole in this proof. In this discussion, p and q are assumed to be positive, though it's possible that at least one of p and q are negative. Therefore, it's possible that 2^p or 3^q might not actually be an integer, meaning they won't be even or odd. It's worth updating the proof to account for this case.

To summarize our feedback on this proof:

- It's great initially to write out your thoughts, simple examples, basic definitions, etc., but be sure to clean them up in your final draft.
- Adding precision into definitions of variables makes it easier to reason about them later on and can save you a lot of time on what might seem like a difficult digression.
- Avoid phrases like "clearly," "obviously," or "as you can see." Usually, but not always, these phrases indicate that you are skipping a step or failing to justify a statement.

Example: Subsets and Differences

Here's a fact about sets that's often useful when manipulating sets:

For any sets A and B: $A - B = \varnothing$ iff $A \subseteq B$

Here is one possible proof of this fact:

> *Proof:* Let's assume that $A - B = \varnothing$. By definition of set difference, this means that the set of elements in A, but not in B is empty. Thus, there are no elements in A that are not also in B. In other words, for every element, if $x \in A$, then $x \in B$. We know that a set S is a subset of T if and only if for every element $x \in S$, $x \in T$ as well. Thus, by definition, $A - B = \varnothing$ if and only if $A \subseteq B$. ■

Unlike the other proofs in this handout, which are essentially correct but could use some stylistic corrections, this proof actually contains a serious logic error and does not prove what it needs to prove. In particular, look at the statement to prove:

For any sets A and B: $A - B = \varnothing$ iff $A \subseteq B$

Did this proof actually show this? If you look at the very last line, it seems like it might be the case. However, there is something flawed with this reasoning. To prove a biconditional statement like this one, the proof needs to show the following:

If $A - B = \varnothing$, then $A \subseteq B$

If $A \subseteq B$, then $A - B = \varnothing$

Looking at this proof again, you'll notice that it only proves the first of these statements – it starts off by assuming $A - B = \varnothing$, then concludes that $A \subseteq B$. However, it hasn't proven the other direction of implication by starting with the assumption that $A \subseteq B$ and concluding $A - B = \varnothing$.

Example: Odd and Even Numbers

As a final example, consider the following theorem:

For any natural number n, the number $n^2 + n$ is even.

Here's one potential proof:

> *Proof:* By contradiction; assume there is some natural number n where $n^2 + n$ is odd. Consider the parity of n. If n is even, then n^2 is even and n is even, so their sum $n^2 + n$ must be even as well. This contradicts that $n^2 + n$ is odd. Otherwise, n is odd. Then n is odd and n^2 is odd, so their sum $n^2 + n$ must be even. This again contradictions that $n^2 + n$ is odd. In either case we reach a contradiction, so our assumption must have been wrong. Thus for any natural number n, the number $n^2 + n$ is even. ■

This proof is logically sound and stylistically has many nice aspects: it's easy to read and clearly lays out its argument. But while there's nothing *logically* wrong with this proof, but there is something *structurally* amiss. The argument of this proof is, essentially, the following:

1. Assume $n^2 + n$ is odd.
2. If n is even, then $n^2 + n$ is even, which is a contradiction.
3. If n is odd, then $n^2 + n$ is even, which is a contradiction.
4. Both cases reach a contradiction, so the assumption was wrong.
5. Thus $n^2 + n$ is even.

Notice that steps (2) and (3), collectively, form a direct proof that $n^2 + n$ is always even. Instead of structuring it as a proof by contradiction, we could just write it as a direct proof. Compare the above proof to this simpler proof given here, which uses the same basic argument but omits the proof by contradiction:

> *Proof:* If n is even, then n^2 is even and n is even, so their sum $n^2 + n$ must be even as well. Otherwise, if n is odd, then n is odd and n^2 is odd, so their sum $n^2 + n$ must be even. Therefore, the sum $n^2 + n$ must be even. ■

This is much simpler, more compact, and to the point.

Proof by contradiction is often the easiest or simplest way to prove a result. If you want a challenge, try showing that the square root of two is irrational without using a proof by contradiction. However, in many cases proof by contradiction obscures a much simpler line of reasoning that could proceed directly. When writing a proof by contradiction, it's worth double-checking your argument after writing up a draft to see if it's actually necessary. If you can get away with a direct proof, it's often more elegant to do so.