A Quick Guide to Proof Writing

COMP 221/361 — Suhas Arehalli

January 2025

A quirk of the standard Computer Science curriculum is that at a certain point, students somehow realize that the field of Computer Science is distinct from that of, say, Software Engineering or just programming. Instead, CS turns out to be a discipline that overlaps greatly (if not entirely) with Mathematics! That is, we use formal mathematical tools (like, say, proofs and formal logic) to study the abstract concept of *computation*, whether it be analyzing the runtime or correctness of an algorithm or proving that only having a stack as memory will get you into trouble.

Either way, you'll be asked to write a proof. This will probably happen at first in a proper math course (Macalester's Discrete Math!), but moving from proving purely mathematical statements to writing things about algorithms can make things a little more complicated. Unfortunately, on top of building up a mathematical argument, you have to learn to actually *write* a proof on paper (or, rather, in a LaTeX document). You will likely get docked points at some point for writing a proof that is technically correct, but written poorly! **This document's goal is to help introduce you to the proper *style* for mathematical proofs**. However, you should note that this is guidance that is based on **my courses** — most folks with some mathematical training can identify particularly **bad** proofs, but some finer matters of style come down to taste, and in the interest of giving you firm guidance and helping you develop some of that taste, I will be asking you to abide by my stylistic preferences for my courses. Of course, another instructor may tell you to format differently in their courses — this is normal and expected! Embrace the variety as you find your voice!

1 A brief review of proofs

A proof is simply a formal mathematical argument. It's goal is to rigorously argue for the truth of the statement. Because we need to be rigorous, we need to write them in such a way that the underlying logic is clear and undeniable.

However, the primary goal of a proof is to be *convincing*, which requires not just correctness, but *clarity*. Just like any writing, proof writing requires you to write in a manner that is understandable to a human reader (specifically, one

trained in some mathematics). This disallows you from giving me proofs that look like formal logic — wrong class!

To find a happy medium between logically sound and human readable, we will often adopt a *proof technique* to aid us in forming our argument. Sometimes, we'll be able to write a few sentences that logically follow from each other and give us the result we want (i.e., By definition, even numbers can be written in the form $2k$, so 6 is even because it can be written as $3(2)$.), but this will often be limited to very simple results. In other cases, we'll need to employ more complex tools whose logical foundations are well known.

For example, a **proof by contradiction** allows you to assume the statement is false, and show that that leads to an impossible conclusion. Logically, we know that if a statement's falsity is impossible, that statement must be true. A **proof by construction** proves a claim that something exists by presenting that thing. A **proof by counterexample** is a variation of this where a universal claim is proven false by providing a case where it does not hold.

Most important to us is a trickier kind of proof called a **proof by induction**, where we prove a statement that something holds for a (countably) infinite number of cases. We prove this in the same way we knock down (potentially countably infinite) dominos: we set up one case that we can knock down easily, and then arrange the dominos in a way where knocking down any domino knocks down the one after. That is, we construct a **base case** that we can prove easily, and then argue for the **inductive step**: If case n is true (what we call the **inductive hypothesis**), then case $n+1$ is true. With these, we know that this is true for all cases after the base case!

In fact, many proofs will require you to break your argument into **cases**: perhaps it's easy to prove a statement for all odd numbers and all even numbers, but you're asked to prove it for all integers — it turns out every integer is either even or odd, so by proving each half you've solved the whole thing!

2 Tips for Proof Writing

- **Be as precise and explicit as possible.** When introducing a new variable, let the reader know what kind of variable it is (i.e., instead of writing *"for any x or y"* write *"for any pair of integers x and y"* or, better yet, write *"for $x, y \in \mathbb{Z}$"*). When proving a statement, make sure you've written out the statement right at the beginning. The same goes for loop invariants, inductive hypotheses, and other statements used in more sophisticated proof techniques that we'll see! Indicate why steps in the proof are justified (are you using a theorem or definition? Is it just an algebraic reduction or is there something more? Are there other cases you need to handle that are trivial?).

- **Adopt common proof phrasing**. When you read proofs from the textbook, additional readings, or course notes, you'll see a handful of phrases repeated. Proofs are not the place for originality — copy them! i.e., things

like *"Assume for contradiction that..."*, or things like *"by definition, ..."* or *"by our inductive hypothesis"* or *"Proceed by cases:"*.

- **Re-read your proofs critically!** The goal of a proof is to succinctly present a mathematical argument. When you write a proof, it's easy to overlook missing steps or faulty logic because you have the full argument in your head, so it's good practice to take a break and read your proof back with fresh eyes. When you read, read **critically**: Look for gaps in the logic: Are there hidden assumptions you're making that you haven't stated? Are there missing cases you need to consider? Does the next step follow from the current step? Can you construct a counterexample to a claim you make? Most importantly, can you follow the argument? Clarity matters too!

- **Trim the fat.** While writing a proof, you'll likely want to do a lot of scratch work. For example, if you want to prove that an algorithm is correct, you might want to work through a couple of examples by hand and show that the algorithm works correctly on those particular examples. This will help you build an intuition for how the algorithm works. On the other hand, this is *not* useful for the reader of the proof! You must, instead, provide an argument that the algorithm is *always* right, and an individual example doesn't help do that! Similarly, you might (and hopefully will!) develop deep insights that help you understand *why* the algorithm works, or you realize new ways to reinterpret what the algorithm is doing that make things click for you. These insights are fantastic, but should not be in a formal proof! **Keep proofs rigorous, but terse!**

- **Never get too stuck.** If you don't know how to solve a problem, it's useful to spend some time searching your brain, but it's dangerous to spend too much time not making any progress. My two pieces of advice are to reread the book/your notes, and to just try things. In this course, your job will not be to invent new or novel proof ideas. Instead, it will almost always be to see how a novel looking problem is just a twist on an example we went through in lecture. Jog your memory and see if any seem similar. If one does, see if that technique can apply somewhere. Can you reframe the problem so that it looks like something you've seen before? Worst case, work through some examples! These won't constitute a proof, but they might reveal some ideas that can apply to any example!

3 Sample Proofs, Good and Worse

Of course, these tips are a bit abstract, so here are some sample proofs at different levels of proof-style development. These should give you an idea of the kinds of things I (or a preceptor) might mark you down for in a homework assignment.

First, here's the problem: A classic you may have seen in, say, Discrete Math, along with relevant definitions/corollary.

Sample Problem Prove that $\sqrt{2}$ is *irrational*.

Definition A number $x \in \mathbb{R}$ is **irrational** iff there exist no two integers $a, b \in \mathbb{Z}$ such that $x = \frac{a}{b}$.

Corollary If a number $x \in \mathbb{R}$ is rational, then there exist integers a, b such that $x = \frac{a}{b}$ and a and b share no factors (i.e., x's *simplified form*).

Now lets look at a few proofs. When reading each of these, think about parts of the proof you like and parts of the proof you don't. How would you write out this solution? Do you like reading it? Does it apply the tips I gave you earlier?

After doing this, read my comments about each proof afterwards to get an idea of how I see each proof and adjust your mental model. Again, the goal is not to agree wholeheartedly with my preferences, but to understand what I'm looking for and why *I* prefer the style.

Proof 1: **Lemma:** For $a \in \mathbb{Z}$, if a^2 is even, a is even.
Pf.: We'll proceed by proving the contrapositive: If a is odd, then a^2 is odd. By definition, $a = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} a^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Thus, with $k' = 2k^2 + 2k \in \mathbb{Z}$, $a^2 = 2k' + 1$ and therefore a^2 is odd. □

Statement: $\sqrt{2}$ is irrational.
Pf.: Assume for contradiction that $\sqrt{2}$ is rational. Then, by definition, there exists $a, b \in \mathbb{Z}$ such that $\sqrt{2} = \frac{a}{b}$. By the corollary, we can assume that we choose a and b such that they share no common factors. Thus,

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned}$$

And thus a^2 is even. By the lemma, a must be even, which means there exists $k \in \mathbb{Z}$ such that $a = 2k$, Plugging this back into the above equation, we get

$$\begin{aligned} 2b^2 &= (2k)^2 \\ 2b^2 &= 4k^2 \\ b^2 &= 2k^2 \end{aligned}$$

Thus b^2 is even, and by the lemma b must be even. However, if both a and b are even, they share a common factor of 2, which contracts our assumption that a and b share no common factors. Thus, $\sqrt{2}$ must be irrational. $\square$

Proof 2: $\sqrt{2}$ can't be rational because that would mean it could be written as $\frac{a}{b}$ because then $2 = \frac{a^2}{b^2}$, but then a^2 is even, but because they're squared b^2 is also even, which means a and b are both even, which means that $\frac{a}{b}$ are not in simplest terms. But even if they were in simplest terms, the above argument would still hold, so there must not be any simplest form, which means x is irrational.

Proof 3: **Statement:** $\sqrt{2}$ is irrational.
Pf.: Suppose x is rational. Then

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned}$$

Then a^2 is even which means a is even. Then

$$\begin{aligned} 2b^2 &= (2k)^2 \\ 2b^2 &= 4k^2 \\ b^2 &= 2k^2 \end{aligned}$$

Then b^2 is even, and thus b is even. $\square$

Proof 4: **Statement:** $\sqrt{2}$ is irrational.
Pf.: There's not a lot to work with for irrational numbers, so we'll use proof by contradiction so we can assume x is rational. Rational numbers can be written as ratios of integers, so we can write x as $\frac{a}{b}$ for integers a, b. Since a rational number can always be expressed in simplest terms, we can assume a and b share no common factors, which means that if we find some c that divides both we've proven our contradiction.

We can then use some algebraic rules to simplify:

$$\sqrt{2} = \frac{a}{b}$$

but then we square both sides

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

and multiply both sides by b^2

$$2b^2 = a^2$$

and since we can let $k = b^2$ then $a^2 = 2k$ and thus a^2 is, by definition, even.

Now if a^2 is even, then for some integer k', $a^2 = 2k'$, and thus the 2 on the right-hand side must be in the a being squared, which means that a must be even too, which means for some k'', $a = 2k''$. For example, if $a^2 = 16$, which is even, then $a = 4$, which is also even.

Thus, we can substitute $2k''$ for a, getting

$$2b^2 = (2k'')^2$$

which reduces to

$$2b^2 = 4k''^2$$

divide by 2 to get

$$b^2 = 2k''^2$$

Which, if we let $k''' = k''^2$, lets us conclude that b^2 is even, and by a similar argument to above, lets us know that b is even.

We assumed at the beginning that a and b shared no common factor, but we found that both a and b are even, which means we found a contradiction. This means that a and b were not in simplified form. One might think that we've just chosen the wrong a and b, but the argument above will work for any a and b that let $x = \frac{a}{b}$, so there can be no simplified form, and thus no form at all. Thus $\sqrt{2}$ must be irrational. $\square$

My comments:

Proof 1: This would be my model solution. Observe how the proof is structured: There is a small part of the proof that is self-contained and not too deeply tied to the main proof, so we silo that off in a lemma beforehand. We are fairly terse (though you can probably be even more brief if you'd like!), and only present enough to show that the result is correct. Every line contributes to the argument, and each line is precise and clear.

Proof 2: This proof is far too threadbare. To me, this proof is hard to follow, with a long series of "which means y" clauses following each other with little justification. The lack of clarity is the worst right at the end, where the corollary is used in a messy way: Much easier and more clear to a reader to present the argument in the way it is in proof 1! Much of the work of proofwriting will be understanding what the right argument is, but don't neglect the work of finding a clear and convincing way to present that argument.

Also note that nothing said here is *wrong*, persay, it's simply that nearly every true statement is *unjustified*. Note that the lemma proved in proof 1 is just assumed implicitly here!

Also note that the proof only implicitly states what you're meant to prove. Write out the statement clearly!

Proof 3: This proof is little more clear than Proof 2 (primarily though better formatting and reliance on mathematical notation), but still lacks the rigor required of a proof at this level. Again, look at how the lemma proven in Proof 1 is just casually assumed!

Also note that the proof leaves out another bit of logic: A reader may wonder why b being even ends the proof! It's tricky to get a feel for how big of a leap of reasoning one should make, but this is certainly to large — observe how the prior proofs presented the tricky logic based on the corollary to go from the fraction being unreduced to showing no such fraction can exist!

Proof 4: This proof is on the other end of things: Way too verbose! The benefit of mathematical notation is that you can save the reader's time by expressing complex things quickly and precisely, but most of the verbiage here is both redundant and *im*precise. For example, all of the text between lines of the algebraic reductions add very little that one couldn't get from reading the equations!

There is also a lot of text that adds nothing to the proof, but adds intuition or recaps the writer's thought process. Remember, a proof is not meant to be autobiographical! These additional lines ("there's not a lot to work with for irrational numbers..." or "One might think that weive just...") might be useful pedagogical tools (in fact, I might pepper them in during my presentation of proofs for that exact reason!), but when you write proofs, keep in mind that you don't have that same goal.

This might be frustrating at times ("I'm doing something the professor is doing, why is it wrong!"), but the key is to do what you should do for all writing: **Consider the audience and the goals of your writing!** Your proofs are not meant to teach, or to show off every bit of information you know, or to demonstrate all of your thought processes. There are other times for that. Your goal is to clearly and concisely present a mathematical argument for the correctness of a statement, Nothing less, but also nothing more!