

Lecture 5: Proof Writing 101

10 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications and Andrew Altomare's notes.

1 Review

We've now covered a unit on logic. We will use these ideas throughout the rest of the course. I will throw some review problems in the quizzes from time to time to keep it fresh in your mind.

2 Proof Introduction

Mathematics, as a science commenced when first someone, probably a Greek, proved propositions about "any" things or about "some" things without specification of definite particular things.

Alfred North Whitehead

Imagine you're having a discussion with an elementary school student who just learned about prime numbers. They insist that 9923 is the largest prime number. Of course, you, having studied math for many more years, know that it isn't. You now have to prove to them that there *exists* a larger number that is prime. Maybe you show them that 10039 is larger and is also prime.

You go away and start thinking later, "what is the largest prime number?" It keeps you awake but eventually you come to the conclusion that there is no largest prime number. For any prime number, you can find an even bigger one! You see that elementary student again and they say, "I don't believe you!" How do you convince them? If you can't, they might triumphantly claim that, "Since you can't then I'm right!" (That's actually a logical fallacy!) If you're worried, we'll discuss how to prove just that in a later lecture in case you ever encounter such a precocious elementary student.

In math, we want to very precisely talk about ideas. We write out proofs that explain our reasoning. It can look very complicated and daunting at first, so we will learn how to break the process down into steps. It is also critical to maintain the growth mentality because you will recognize frustration as an opportunity to learn instead of evidence that you cannot write the proof.

3 Disproof

3.1 Deciding whether it is true

Consider the statement, “For every real number a and b , if $a^2 = b^2$ then $a = b$.” From our unit on logic, you know that we can more concisely write that as $\forall a, b \in \mathbb{R} (a^2 = b^2) \rightarrow (a = b)$. This is a crisp phrase that is either true or false. In every day scenarios, you likely won’t be given such clean formulations but will have to tease them out from whatever problem you are working on. That’s how research works; a large amount of work, maybe most of it, is figuring out what you are trying to prove.

Once, you’ve settled on such a statement, you have to decide whether it is true or false. You have to experiment some and gain intuition. You likely know that this statement is false from your days in algebra. What do you do when you want to disprove a universal statement?

3.2 Disproving universal statements by counterexample

When someone says “all cats are black” you can prove them wrong by finding a white cat. We do the exact same thing in math. To prove that the statement was false, we can consider $a = 1$ and $b = -1$. Then, $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$. So $a^2 = b^2$ but $a \neq b$! We found the white cat in this scenario.

Definition: *Disproof by counterexample*

To disprove a statement of the form $\forall x \in D, P(x) \rightarrow Q(x)$ find a value of $x \in D$ for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a counterexample. This process is disproof by counterexample.

Notice that if the statement had instead been “There exists a pair of real numbers a and b such that if $a^2 = b^2$ then $a = b$ ” this counterexample no longer applies. Disproving existential statements is different from universal statements. To disprove that statement, we have to show that every possible pair of real numbers does not satisfy the conditional. That’s infinitely many options! The relationship between existential and universal statements can be helpful. If you are struggling to prove one, consider a related statement of the other form to think about. Just don’t forget to translate your proof back to the original setting.

Exercise

Disprove $\forall m, n \in \mathbb{Z}$, if $2m + n$ is odd then m and n are both odd.

4 Proving universal statements

There are many methods of proof.

4.1 By exhaustion

The first thing you might think is to consider each possible example individually. For example, I might say that every person in this classroom was born on planet Earth. We could prove that by going person by person and learning where they were born and then confirming that is indeed on Earth. It seems reasonable for a small class. What if I instead say that every US citizen was born on Earth? You now have to go track down every US citizen and do the same inquiry.

Mathematically, we can sometimes do that, but it's often not easy because we are thinking about large collections of things, possibly even infinitely many things!

4.2 Direct proof

Mathematical statements are nice to us though. Often, once we establish the reasoning for a single element, we can write it in an abstract way that will apply to any element. This is called direct proof.

Definition: *Direct proof*

In a direct proof of a statement of the form $\forall x \in D, P(x) \rightarrow Q(x)$, we first consider an arbitrary x where $P(x)$ is true. We then use our definitions, previous proofs, new ideas, and the rules of logical inference to show that $Q(x)$ must hold for this arbitrary x .

The following is an example of a direct proof.

Theorem 4.1. *The sum of any two even integers is even. (We could also state this as $\forall a, b \in \mathbb{Z}$ if a and b are even, then $a + b$ is even.)*

Proof. Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s . Then by substitution $m + n = 2r + 2s$. This factors to $2(r + s)$. Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence $m + n = 2t$ where t is an integer. It follows by the definition of even that $m + n$ is even. \square

Notice how concise and clear this proof is. We do not add extra ideas or superfluous language. Writing such a proof does not happen automatically. You will likely have to first write out your reasoning and then rewrite it into a crisp format. The final proof is not what you write first. See the Epp book for some excellent examples of how we move from ideas to the final proof.

5 What makes a proof great?

Some proofs are better than others in how they're written. Here are a few key details to follow:

1. **The statement of the theorem should be clear.** Don't start proving if your reader has not first understood what you're trying to prove.
2. **Clearly divide the theorem and your proof.** If they blend together, the reader will be confused.

3. **Make your proof self-contained.** Never use a variable without first defining it. Similarly, if you use ideas or other theorems in your proof make sure they are clear by context to the reader.
4. **Use full, complete sentences.** Using only symbols can be hard to follow. Using only incomplete sentences is similarly unclear.
5. **Keep your reader clear how you are progressing in your proof.** Make the idea of the proof crystal clear.
6. **Justify each assertion in your proof.** It's not a proof otherwise. Some later proofs may omit simpler ideas because it is assumed the reader can fill in the small detail. For example, we don't define what an integer is in our proofs because everyone knows it.
7. **Include transition words to make the proof flow.**
8. **Make the equations and math clean and clear.**

6 What makes a proof not so great? Common mistakes.

At first, you might make many common mistakes. Here is some advice to avoid them:

1. **Do not argue from examples.** Just because you can think of many, many examples where your statement is true does not mean that it is universally true.
2. **Do not reuse a variable name.** You can probably imagine how confusing that would be.
3. **Do not jump to conclusions.** Consider the *proof*, "Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s . Then, $m + n = 2r + 2s$. So $m + n$ is even." It is tempting to assume that the reader will see the obvious step, but what is obvious to you is not obvious to every one. Write out all the steps even if it's tedious.
4. **Do not unintentionally assume what you are trying to prove.** It might seem like you'll never do it, but it's very easy to prove a variation of your conclusion without meaning to.
5. **Do not confuse what has been proven and what remains to be proven.**
6. **Do not use *any* where you really mean *some*.** An example would be "Suppose m is a particular but arbitrarily chosen odd integer. By definition of odd, $m = 2a + 1$ for any integer a ." Surely you don't mean any there. You mean some integer, not any integer will work but there is one.
7. **Do not misuse the word *if*.** An example: "Suppose p is a prime number. If p is prime, then $p \dots$ " But, you just stated p was prime. You shouldn't use if since it makes it unclear now what p is.