CSCI 2824 - CU Boulder, 2019 Summer

Lecture 5: Proof Writing 101

10 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications,
Rosens's Discrete Mathematics and its Applications,
Bettina and Thomas Richmond's A Discrete Transition to Advanced Mathematics, 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

> Mathematical proofs, like diamonds, are hard as well as clear, and will be touched with nothing but strict reasoning.
>
> *John Locke*

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. Since we've already introduced logical inference you have the foundations of proof writing.

We try to prove theorems, statements that can be shown to be true. We do so using arguments as in symbolic logic. We have a thesis statement we wish to prove. Then, we state our premises. These might be axioms, postulates, or previous proven theorems. (We sometimes call building block theorems *lemmas*.) We then build upon these ideas using valid logic with our rules of inference.

2.1 The deception of simplicity

Some conjectures sound very simple but are actually incredibly difficult to prove or disprove. Consider the following:

Theorem 2.1. *Every even integer greater than 2 can be expressed as the sum of two primes.*

This conjecture, called the strong Goldbach conjecture, was proposed in the margin of letters between Leonhard Euler and Christian Goldbach in 1742. It has gone unproven since then! It has been verified for all integers less than 4×10^{18} but despite its simple language there is no proof for it. It seems likely true but in mathematics we require absolute certainty.

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 $\forall a, b \in \mathbb{R}\,(a^2 = b^2) \to (a = b)$. 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 $\forall x \in D, P(x) \to Q(x)$ 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.

Consider $5 = 2 \times 2 + 1$. Then, $m = 2$ and $n = 1$ where only n is odd. This is a counterexample to the statement.

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 $\forall x \in D$, $P(x) \to Q(x)$, 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.

Exercise
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.)

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.

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.

4.3 Proof by Mathematical Induction

This is actually a method of deduction instead of inductive reasoning. We are certain of the result, but we will often call it *proof by induction*. We use this when we have a common structure that we can exploit by using a base case and that if an arbitrary step is true we can get to the next step.

Exercise
Show that $n! > 3^n$ for every integer $n \geq 7$.

We proceed with mathematical induction. Let S_n be the statement that $n! > 3^n$. The base case is S_7, i.e. $7! > 3^7$ which is true since $7! = 5040$ and $3^7 = 2187$. Next, suppose that S_k holds where k is an arbitrary integer greater than or equal to 7. We will show that S_{k+1} holds, i.e. $(k+1)! > 3^{k+1}$.

$$\begin{aligned}
(k+1)! &= k!(k+1) && \text{definition of factorial} \\
&> 3^k(k+1) && \text{inductive step} \\
&> 3^k(3) && \text{since } k \geq 7, \text{ we have } k+1 > 3 \\
&= 3^{k+!}
\end{aligned}$$

Thus, if $k \geq 7$ and S_k holds then S_{k+1} holds. By the principle of mathematical induction, it follows that S_n holds for every integer $n \geq 7$.

This is a tricky idea to wrap your head around, so we will return to it in the coming few days. Think of a concrete example though. An animal shelter has room for at least one dog. If we know that the animal shelter always has room for one more dog then we can conclude that the animal shelter has room for n dogs (in fact any number of dogs).

4.4 Proof by Contraposition

Remember that $p \to q$ is equivalent to the contrapositive $\neg q \to \neg p$. Sometimes the second statement is easier to prove!

Exercise
Given some integer x, if x^2 is even, then x is even.

Suppose x is not even. Then, x is odd. The product of two odd numbers is odd, hence $x^2 = x \times x$ is odd. Thus, x^2 is not even. Thus, if x^2 is even, the supposition must be false, so x has to be even.

It's not always clear when you need to use contraposition. Just try the direct method and if it's failing and you realize you can go the other direction, try that.

4.5 Proof by Contradiction

Consider $p \to q$. What if I assume $\neg p$ and something impossible happens? Then, I know that p must've been the case. For example, "If I went to the ice cream stand, I am happy." Let's assume that I won't go to the ice cream stand some day. If that's the case, I show, using solid logical inference, that unicorns will run all over my room. That's an absurd conclusion that is impossible. Therefore, I must go to the have gone to the ice cream stand because the universe would be broken otherwise. Maybe a more mathematical example will help:

Exercise
Prove that $\sqrt{2}$ is irrational.

Supose that $\sqrt{2}$ is rational. Then, by definition $\sqrt{2} = \frac{a}{b}$ for some a and b non-zero integers with no common factors. Thus, $b\sqrt{2} = a$. When, we square both sides we get $2b^2 = a^2$. Since 2 divides the left hand side, it must also divide the right hand side. So a^2 is even, which implies a is even. So $a = 2c$ where c is an integer. Substituting we find $2b^2 = (2c)^2 = 4c^2$. Dividing both sides by 2 yields $b^2 = 2c^2$ then by the same argument b must be even. However, if a and b are both even, then have a common factor 2. This contradicts our initial supposition, so $\sqrt{2}$ must be irrational.

4.6 Proof by Construction

As opposed to proof by contradiction, we actually construct an example in proof by construction.

4.7 Proof by Other Techniques

We won't focus on them as much explicitly but there are more proof techniques:

- **Probabilistic proof**: We show using methods of probability theory that an example must exist, even if we cannot state the example.
- **Combinatorial proof**: We show that two expressions are equivalent because they count the same object in different ways.
- **Nonconstructive proofs**: This could be a proof by contradiction. We show that a mathematical object with a certain property exists without explaining how to find it.

- **Statistical proofs**: We show something holds with high probability.
- **Computer assisted-proof**: We use a computer to assist in the process.

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 ... " But, you just stated p was prime. You shouldn't use if since it makes it unclear now what p is.

7 Some practice

Exercise
The product of two odd integers is an odd integer.

Suppose a and b are odd integers. then there exist integers j and k with $a = 2j + 1$ and $b = 2k + 1$. The product ab is

$$\begin{aligned} ab &= (2j + 1)(2k + 1) \\ &= 4jk + 2j + 2k + 1 \\ &= 2(2jk + j + k) + 1 \\ &= 2m + 1 \text{ where } m = 2jk + j + k \in \mathbb{Z} \end{aligned}$$

Thus, ab is odd.

Exercise
Suppose a is a positive real number. If a is irrational, then $\sqrt{a}$ is irrational.

Let a be a positive real number. We prove the contrapositive: $\sqrt{a} \in \mathbb{Q} \rightarrow a \in \mathbb{Q}$. Suppose $\sqrt{a} \in \mathbb{Q}$. Then, $\exists m, n \in \mathbb{Z}$ such that $n \neq 0$ with $\sqrt{a} = \frac{m}{n}$. Then,

$$a = (\sqrt{a})^2 = \frac{m^2}{n^2}$$

where $m^2, n^2 \in \mathbb{Z}$ and $n^2 \neq 0$. Thus, $a \in \mathbb{Q}$ as needed.

Exercise
Consider the game “double-move chess" played exactly like ordinary chess except that each player makes two consecutive moves at each turn. Show that the player to move first (White) can always win or at least draw.

Suppose not. Then no matter how White plays, Black (the second player) can, by playing properly, win. But, White may open by moving a knight out and then moving it back to its original position, effectively giving Black the first move and thus exchanging roles with Black. In particular, White has now assumed the role of the winning player. This contradicts the assumption that Black would win. Thus, White can always win or draw.

Exercise
Prove that there exists a unique multiplicative identity for $\mathbb{R}$ using both a direct and indirect proof. Note that a real number e is a multiplicative identity for $\mathbb{R}$ if $\forall x \in \mathbb{R}\, ex = x$.

First, the direct proof. Because $1x = x \forall x \in \mathbb{R}$, 1 is a multiplicative identity for $\mathbb{R}$. Thus, there exists at least one multiplicative identity for $\mathbb{R}$. To show uniqueness, suppose both e and i are multiplicative identities for $\mathbb{R}$. Then, since forall $x \in \mathbb{R}$ we know $ex = x$ then, $ei = i$ Similarly, $ie = e$. Because multiplication is commutative in $\mathbb{R}$ we have $i = ei = ie = e$. Thus, any two multiplicative identities for $\mathbb{R}$ must be equal and there exist no more than one multiplicative identities for $\mathbb{R}$. Thus, 1 is the unique multiplicative identity for $\mathbb{R}$.

Now, we consider the indirect proof. Suppose there is not a unique multiplicative identity for $\mathbb{R}$. Then either there are no multiplicative identities at all or there are more than one. Because $1x = x$ for all $x \in \mathbb{R}$ there must be more than one multiplicative identity for $\mathbb{R}$. Let e and i be distinct multiplicative identites for $\mathbb{R}$, i.e. $\forall x \in \mathbb{R}$ we know $ex = x$ and $ix = x$ and $e \neq i$. Thus, $ei = i$ and $ie = e$. So, $i = ei = ie = e$ contradicts the uniqueness assumption. Thus, there is a unique multiplicative identity for $\mathbb{R}$.