

Lecture 1: The Art and Technique of Argument

1 What is a Proof?

Every major field of study in academia, roughly speaking, has a way of “showing” that something is true. In English/critical literature studies, if you wanted to argue that the concept of whiteness in Melville’s *Moby Dick* was intrinsically tied up with mortality, you would write an essay that quoted Melville’s epic story alongside some of his other writings and perhaps some contemporary literature, and logically argue (using these quotations as “evidence”) that your claim holds. Similarly, if you were a physicist and you wanted to demonstrate **Bell’s inequality**, which roughly states that **local realism** and quantum mechanics are incompatible theories, you’d create an experiment under which these two theories necessarily predict different outcomes.

In mathematics, a **proof** is what we call an argument for showing that something is true. To define the concept of mathematical proof, then, it suffices to understand the words “something,” “argument” and “true.” This may sound pedantic and perhaps silly, but consider the following cautionary examples of “failed” proofs:

Theorem. I am a salmon.

Proof. First, recall the following two facts:

- All UCSB professors are salmon.
- Paddy is a professor at UCSB.

Because I am a UCSB professor and all UCSB professors are salmon, we can logically conclude that I am a salmon. \square

The flaw here, obviously, is that one of the two things we claimed at the start of this proof — that all UCSB professors are salmon — is clearly false. Whenever we’re making a proof, if we want to insure that we get something true at the end, we need to insure somehow that we never do something like the above; i.e. that we never accidentally assume false statements during the course of our proof. But this gets us back to one of the words we’re trying to define: what does it mean for something to be true or false? Mathematically, we define these concepts recursively as follows:

Definition. A mathematical statement is **true** if and only if we have a mathematical proof for that statement.

But wait, you may protest: that’s circular logic!¹ If the only things we can use in mathematical proofs are true statements, and the only way we know if something is true is by finding a mathematical proof for it, we would seem to have no way of actually showing anything is true. To avoid this, we also introduce the concept of axioms:

Definition. We also have a small collection of statements, called **axioms**, which we assume to be true without proof.

For example, in the mathematical field of **set theory**, we have the **ZFC axioms of set theory**, a collection of roughly ten rules that we can use to prove most of the major results in that branch of mathematics.

Typically, when we’re proving a mathematical statement, we won’t worry so much about whether the axioms we’re working from are “naturally true” or not (what would this mean, anyways?); rather, we will often just state at the start of our proof what we’re assuming to be true, and logically proceed from there. For example, the proof above **was** a completely logical proof of the claim “If all UCSB professors are salmon, then I am a salmon:” if that first claim **was** true, then I would indeed be a salmon.

In Math 8, a course you’ll run into later, you’ll deal with these concepts of axioms and “truth” in a much more rigorous and in-depth setting. For now, however, we’re going to mostly assume that common-sense things are “true:” i.e. we know that $1 + 1$ is 2, that $1 < 3$, that there are infinitely many natural numbers, and many other such things (such as the theorems we discuss in class.)

This gives us a notion of “truth.” Before we go much further, we should use this idea of truth to give us an idea of what **statements** are:

Definition. A **statement** (or proposition, or claim) is just some claim that is either true or false. For example, the following are statements:

- P = “Every even number greater than 2 can be expressed as the sum of six primes” is a statement; this one happens to be true (a result in number theory, proven in 1995 by the French mathematician **Olivier Ramaré**.)
- Q = “Every even number can be expressed as the sum of two primes” is another statement; this one is false, as the number 2 cannot be expressed as the sum of two other primes (as there are no prime numbers smaller than 2.)
- R = “Every even number greater than 2 can be expressed as the sum of two primes” is a third statement; this is Goldbach’s conjecture, a famous open problem in number theory. It is either true or false, but mathematicians have not yet discovered which.

Often, we will work with mathematical statements that depend on a variable. For example, we can write

$$P(n) = \text{“A } n \times n \text{ checkerboard can be covered by nonoverlapping } 2 \times 1 \text{ dominoes;”}$$

this statement will be false for odd values of n , and true for even values of n (if you don’t immediately see why, prove this!)

¹See footnote 2 for a definition of circular logic.

We now understand the idea of truth, and what statements are. This leaves us with one last object to clarify: the idea behind “argument.” Consider the following cautionary example:

Theorem. All odd numbers are prime.

Proof. 3 is prime, 5 is prime, 7 is prime . . . seems to always hold. □

In this example, the issue is not that we introduced false statements: the numbers 3, 5 and 7 are all indeed prime. Rather, the problem is that the logic we used to link these facts to our conclusion — “if a statement holds for the first few examples we look at, it must be true in general” — is false. Discussing what it formally means for a piece of logic to be “valid” in a mathematical proof is a rather complicated thing to rigorously do. If you’re interested, a course in [first-order logic](#) might be worthwhile; similarly, Math 8 will again talk about these issues in more depth.

For our purposes, however, we won’t worry about this too much; specifically, you all already know pretty much what logical leaps are valid and which are not. For example, you know that the following logical constructions make sense:

- If both of the statements A and B are true, then either one of the statements A or B are true: roughly speaking, this is like saying that if you have a dog and a cat, it is also true that you have a dog. In terms of the constructions above, this is saying that if $A \wedge B$ is true, then so is A (and similarly so is B .)
- If the statement A is true, and you know that whenever the statement A is true it forces the statement B to be true (in other words, you know that A implies B , or in symbols $A \Rightarrow B$), then you know that B must be true. Again, roughly speaking, this is like saying that knowing the two facts (it’s raining) + (whenever it rains, it’s wet outside) tells you that it’s wet outside. In terms of the constructions above, this is saying that knowing that $A \Rightarrow B$ is true, along with A being true, tells you that B is true.
- If you know that $A \Rightarrow B$, and also that the statement B is false, then you know that there’s no way that the statement A can also be true: i.e. that A is false as well. Again, to give an example, this is like stating that knowing (If there was not another season of My Little Pony, I would be sad) + (I am not sad) tells you that there will be another season of My Little Pony. In terms of the constructions from earlier, this is like saying that if $A \Rightarrow B$ is true and B is false, then A must also be false.

Conversely, you also know that the following arguments don’t actually work for proving statements:

- Just because a property holds for the first few values you examine, doesn’t mean that it’s always true. A famous example is the [Pólya conjecture](#), which fails only at 906, 150, 206 but holds true for every number up to that value.
- Just because $A \Rightarrow B$, doesn’t mean that $B \Rightarrow A$: a quick example is noting that just because I cheer at my television whenever Messi scores a goal, doesn’t mean that

Messi will score a goal if I cheer at my television. This is a special example of the idea that correlation does not imply causation: just because two events are related to each other doesn't mean that they're necessarily related in the way that we'd like.

(There are many other kinds of valid arguments; these are just a few examples of the kinds of logical connections you can make.)

In this class, we are going to prove lots of things! We are mostly going to introduce you to the concept of proof via immersion; rather than formally study proofs for an entire class (again, like in Math 8!) we will start by studying some concepts in Linear Algebra and proving things as we come across them. When you prove things in this class, don't worry about the formalities of things. Rather, focus on just the concepts we discussed above: proofs consist of

1. A well-stated claim.
2. A selection of statements that we know to be true, that seem to be related to the claim.
3. A number of logical links between these statements, that show that our claim is true.

This definition captures the letter of what it means to be a proof. However, it might not properly capture the **spirit** of what a proof should aspire to be! Consider the following example:

Claim 1.

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

Proof.

$$\begin{aligned}\sqrt{xy} &\leq \frac{x+y}{2} \\ xy &\leq \frac{(x+y)^2}{4} \\ 4xy &\leq (x+y)^2 \\ 4xy &\leq x^2 + 2xy + y^2 \\ 0 &\leq x^2 - 2xy + y^2 \\ 0 &\leq (x-y)^2.\end{aligned}$$

□

This proof is **awful**. Why? Well, first and foremost, it has no words! In fact, we have absolutely no idea what we're even proving, nor any idea what x and y are supposed to be, nor any idea how the equations we've drawn are linked together. So: **never do this!** Whenever you're writing a proof, **use words**. Always tell your reader what you're proving,

how you're going about making said proof, and how you're linking together any of these steps.

For example, the thing above is *supposed* to be a proof of the arithmetic-geometric mean inequality, which is the following claim:

Theorem 2. (AM-GM) *For any two nonnegative real numbers x, y , we have that the geometric mean of x and y is less than or equal to the arithmetic mean of x and y : in other words, we have that*

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

With this stated, we can kind of see what we're proving; but it's still hard to see how the equations above actually prove what we want. Again, the solution here is **more words!** When you're writing down your arguments in this class, explain anything that took you more than ten seconds to realize. The goal of your arguments is not to simply verify to yourself that the thing you're proving is true: rather, you're attempting to persuade your **audience** that your claim is true as well! So always use more words.

We present a fixed and fully functional proof here:

Theorem 3. (AM-GM) *For any two nonnegative real numbers x, y , we have that the geometric mean of x and y is less than or equal to the arithmetic mean of x and y : in other words, we have that*

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

Proof. Take any pair of nonnegative real numbers x, y . We know that any squared number is nonnegative: so, in specific, we have that $(x-y)^2$ is nonnegative. If we take the equation $0 \leq (x-y)^2$ and perform some algebraic manipulations, we can deduce that

$$\begin{aligned} 0 &\leq (x-y)^2 \\ \Rightarrow 0 &\leq x^2 - 2xy + y^2 \\ \Rightarrow 4xy &\leq x^2 + 2xy + y^2 \\ \Rightarrow 4xy &\leq (x+y)^2 \\ \Rightarrow xy &\leq \frac{(x+y)^2}{4}. \end{aligned}$$

Because x and y are both nonnegative, we can take square roots of both sides to get

$$\sqrt{xy} \leq \frac{|x+y|}{2}.$$

Again, because both x and y are nonnegative, we can also remove the absolute-value signs on the sum $x+y$, which gives us

$$\sqrt{xy} \leq \frac{x+y}{2},$$

which is what we wanted to prove. □

In terms of the formulas used, this proof is identical to the “awful” proof we had earlier; however, because we added a lot of discussion about precisely “what” we’re trying to prove and why we can justify the steps we’ve made, this proof is a lot more satisfying and persuasive.

1.1 Pictures and Proofs

Words and symbols are not the only tool in proofs! In fact, well-chosen and drawn diagrams can often illustrate an idea that would otherwise take pages of text to describe. Pictures alone are rarely proofs: words are almost always necessary to explain what’s going on, and you’ll have to do some calculations to solve almost any problem. However, a well-placed picture can often be invaluable, as we demonstrate in the following example:

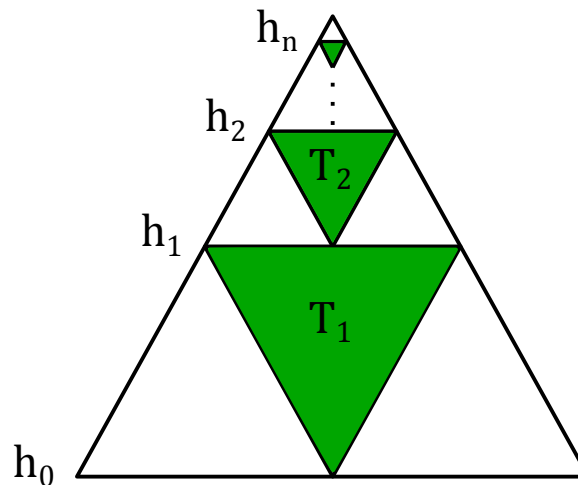
Claim 4. *For any $n \in \mathbb{N}$, we have the following identity:*

$$\sum_{k=1}^n \frac{1}{4^k} = \frac{1 - (1/4)^n}{3}.$$

(The $\sum_{k=1}^n$ -expression above is a shorthand way of writing the sum $\frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \dots + \frac{1}{4^n}$. In general, the \sum symbol is used for this kind of shorthand, where we want to add up a bunch of objects but don’t want to actually completely write out the sum each time.)

Proof. Consider the following construction:

1. Start by taking an equilateral triangle of area 1.
2. By picking out the midpoints of its three sides, inscribe within this triangle a smaller triangle T_1 . Color this triangle green. Also, notice that by symmetry this green triangle has area $\frac{1}{4}$, as drawing it has broken up our original triangle into four identical equilateral triangles.
3. Take the “top” triangle of the three remaining white triangles, and repeat step 2 on this triangle. This creates a new green triangle, T_2 , with area $\frac{1}{4}$ of the white triangle’s area: i.e. $\frac{1}{4} \cdot \frac{1}{4} = \frac{1}{16}$.
4. Keep repeating this process until we have drawn n green triangles, as depicted below:



5. What is the combined area of all of the green triangles? On one hand, we've seen that the area of each T_k is just $(\frac{1}{4})^k$, as T_1 had area $\frac{1}{4}$ and each green triangle after the first had area $\frac{1}{4}$ of the green triangle that came before it. Summing over all of the green triangles, this tells us that

$$\text{Area}(\text{Green}) = \sum_{k=1}^n \frac{1}{4^k}.$$

6. On the other hand, as shown in our picture, we can see that between height h_0 and h_1 , green triangles are taking up precisely a third of the area of our original area-1 triangle. Similarly, green triangles are taking up a third of the area from h_1 to h_2 , h_2 to h_3 , and so on/so forth all the way to h_n , after which there are no more green triangles.

Therefore, the total area of the green triangles is just a third of the area of our original triangle that lies between height h_0 and h_n . Because the area of the last tiny white triangle at the top is (by construction) equal to the area of T_n , i.e. $(\frac{1}{4})^n$, we then have that

$$\text{Area}(\text{Green}) = \frac{1}{3} \cdot \left(1 - \left(\frac{1}{4}\right)^n\right).$$

By combining these two expressions for the total area of the green triangles, we have proven that

$$\sum_{k=1}^n \frac{1}{4^k} = \frac{1 - (1/4)^n}{3}.$$

□

1.2 Avoiding Overkill in Proofs

One last thing to mention in mathematics (that is particularly applicable to CCS students) is the following bit of warning about “overkill” in proofs. Many of you have seen a lot of mathematics before: consequently, when you're going through this course, you're often going to be tempted to use tools you've seen in other math classes to attack problems. Be careful about doing this! While sometimes you can create some absolutely beautiful connections between your different classes by taking results from one and putting them in the other, at other times you may find yourself accidentally making problems trivial that would otherwise be fascinating by using a result that (is much more complex than the result you're studying / actually needs the proof of the problem you're studying in order to prove that result, so you'd be engaging in some circular logic).

For example, consider the following proof:

Theorem 5. $\sqrt[3]{2}$ is irrational: i.e. it cannot be expressed as a fraction in which the numerator and denominator are both integers. Specifically, there is no pair of positive integers p, q , $q \neq 0$, such that $\sqrt[3]{2} = \frac{p}{q}$.

Proof. First, recall **Fermat's Last Theorem**, a result formulated in 1637 by the mathematician Pierre de Fermat and proven in 1995 by the mathematician Andrew Wiles, whose proof was the culmination of centuries of labor by scientists and mathematicians:

If n is a natural number ≥ 3 , the equation

$$a^n + b^n = c^n$$

has no solutions with $a, b, c \in \mathbb{N}$.

We're going to use this to... prove that $\sqrt[3]{2}$ is irrational.

To do this, suppose that we have expressed $\sqrt[3]{2}$ as some ratio $\frac{p}{q}$, where p, q are a pair of positive real numbers. Then, if we cube both sides, we have

$$\frac{p^3}{q^3} = 2;$$

multiplying both sides by q^3 then gives us

$$p^3 = q^3 + q^3.$$

Fermat's last theorem says that such a thing cannot exist, if $p, q \in \mathbb{N}$; therefore, because Fermat's last theorem is true, we know that no matter how we've expressed $\sqrt[3]{2}$ as a ratio $\frac{p}{q}$, we can never have both p and q be positive integers. Therefore, $\sqrt[3]{2}$ must be an irrational number. \square

This proof works completely! – and yet, by reading it, we really haven't gained any better insights into what makes a number irrational. Good proofs are ideally ones that **illuminate** the question at hand: not only do they rigorously show that the statement in question is true, they also shed light on how the concepts involved in the proof work, and how the reader might go about attacking similar problems.