Math/CS 120: Intro. to Math | Professor: Padraic Bartlett

Lecture 1: The Art and Language of Proof

Week 1 | *UCSB 2014*

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 color white 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 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 show that the speed of light is roughly $3.0 \cdot 10^8$ meters per second, you'd set up a series of experiments, collect data, and see if it supports your claim.

In mathematics, a **proof** is an **argument** that mathematicians use to show that something is true. However, the concepts of "argument" and "truth" aren't quite as precise as you might like; certainly, you've had lots of "arguments" with siblings or classmates that haven't proven something is true! Mathematicians mean something slightly different by those words than you may be used to.

We define what a mathematician means by "truth" below:

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

At first glance, this seems like circular[1] logic[2]! 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 need someplace to start: some collection of things that we simply **assert** are true. But we have such a collection — these are simply **definitions**! For example, consider the following notion of "clock arithmetic," from elementary school:

Definition. The set $\mathcal{C}$, of "clock numbers," is defined along with an addition operation $+$ and multiplication operation $\cdot$ as follows:

- Our set is the numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.
- Our addition operation is the operation "addition mod 12," or "clock arithmetic," defined as follows: we say that $a + b \equiv c \mod 12$ if the two integers $a + b$ and c differ by a multiple of 12. Another way of thinking of this is as follows: take a clock, and replace the 12 with a 0. To find out what the quantity $a + b$ is, take your clock, set

[1] See footnote 2 for a definition of circular logic.
[2] See footnote 1 for a definition of circular logic.

the hour hand so that it points at a, and then advance the clock b hours; the result is what we call $a + b$.

For example, $3 + 5 \equiv 8 \mod 12$, and $11 + 3 \equiv 2 \mod 12$. This operation tells us how to add things in our set.

- Similarly, our multiplication operation is the operation "multiplication mod 12," written $a \cdot b \equiv c \mod 12$, and holds whenever $a + b$ and c differ by a multiple of 12. Again, given any pair of numbers a, b, to find the result of this "clock multiplication," look at the integer $a \cdot b$, and add or take away copies of 12 until you get a number between 0 and 11.

  For example, $2 \cdot 3 \equiv 6 \mod 12$, $4 \cdot 4 \equiv 4 \mod 12$, and $6 \cdot 4 \equiv 0 \mod 12$.

We often will denote this object as $\langle \mathbb{Z}/12\mathbb{Z}, +, \cdot \rangle$, instead of as $\mathcal{C}$.

People sometimes generalize this to the concept of "modular arithmetic:"

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ is defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n - 1\}$.
- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \equiv c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

These definitions, in a sense, are the building blocks that we need to start from whenever we prove things! For example: suppose that I wanted to prove the following claim:

Claim. Suppose that n is a **prime**[3] number[4]. Then $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ has the following property:

For any $a, b \in \{0, \ldots n - 1\}$, if $a \cdot b \equiv 0 \mod n$, then at least one of a, b are equal to 0.

We could "prove" this claim from our definitions as follows:

Proof. Take any a, b in $\{0, \ldots n-1\}$. If one of a, b are equal to 0, then we know that $a \cdot b = 0$ in the normal "multiplying integers" world that we've lived in our whole lives. In particular, this means that $a \cdot b \equiv 0 \mod n$ as well.

Now, suppose that neither a nor b are equal to 0. Take both a and b. Recall, from grade school, the concept of **factorization**:

[3] A natural number n is called **prime** if it has the following property: for any pair of natural numbers a, b such that $a \cdot b = n$, exactly one of a, b is equal to 1. In other words, the only factors of n are 1 and itself, if you know what the word factor means. Notice that this means that 1 is not prime!

[4] Number systems! The positive whole numbers, $\{1, 2, 3, \ldots\}$, are called the **natural numbers**, and denoted via the symbol $\mathbb{N}$. Some mathematicians put 0 in their natural numbers; others do not. It's not very consistent. Similarly, the set of all whole numbers $\{\ldots -2, -1, 0, 1, 2, \ldots\}$ is called the **integers**, and is denoted by the symbol $\mathbb{Z}$. (The $\mathbb{Z}$ comes from the German word for "numbers," *zahlen.*)

Observation. Take any nonzero natural number n. We can write n as a product of prime numbers $n_1 \cdot \ldots \cdot n_k$; we think of these prime numbers $n_1, \ldots n_k$ as the "factors" of n. Furthermore, these factors are **unique**, up to the order we write them in: i.e. there is only one way to write n as a product of prime numbers, up to the order in which we write those primes. (For example: while you could say that 60 can be factored as both $2 \cdot 2 \cdot 3 \cdot 5$ and as $3 \cdot 2 \cdot 5 \cdot 2$, those two factorizations are the same if we don't care about the order we write our numbers in.)

In the special case where $n = 1$, we think of this as already factored into the "trivial" product of no prime numbers.

Take a, and write it as a product of prime numbers $a_1 \cdot \ldots \cdot a_k$. Do the same for b, and write it as a product of primes $b_1 \cdot \ldots \cdot b_m$. Notice that because a and b are both numbers that are strictly between 0 and $n-1$, n cannot be one of these prime numbers (because positive multiples of n must be greater than n!)

In particular, this tells us that the number $a \cdot b$ on one hand can be written as the product of primes $a_1 \cdot \ldots \cdot a_k \cdot b_1 \cdot \ldots \cdot b_m$, and on the other hand (because factorizations into primes are unique, up to ordering!) that there is no n in the prime factorization of $a \cdot b$.

Conversely, for any natural number k, the number $k \cdot n$ **must** have a factor of n in its prime factorization. This is because if we factor k into prime numbers $k_1 \cdot \ldots \cdot k_j$, we have $k \cdot n = k_1 \cdot \ldots \cdot k_j \cdot n$, which is a factorization into prime numbers and therefore (up to the order we write our primes) is unique!

In particular, this tells us that for any k, the quantities $a \cdot b$ and $k \cdot n$ are distinct; one of them has a factor of n, and the other does not. Therefore, we have shown that if both a and b are nonzero, then $a \cdot b$ cannot be equal to a multiple of n — in other words, $a \cdot b$ is not congruent to 0 modulo n! Therefore, the only way to pick two $a, b \in \{0, \ldots n-1\}$ such that $a \cdot b$ is congruent to 0 modulo n is if at least one of them is equal to 0, as claimed. □

Notice that in this proof we used both the definitions from modular arithmetic and definitions from other areas of mathematics (like the concepts of prime numbers and factorization!) This is a key thing to point out that you can do in your mathematics classes; you're not always restricted to simply working with the definitions you've seen in that class! Often, you can and will be expected to use your past knowledge of mathematics in attacks on new problems.

Before we go much further, we should pause and describe some of the language we're using in these proofs:

Definition. A **statement** (or proposition, or claim) is just some object 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 at most 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 see why, prove this!)

Definition. Given some statements, we will often want ways to combine them into new statements. The following list contains some of the most common combinations:

1. Given two mathematical statements P and Q, we will often want to form the mathematical statement "P and Q", denoted $P \wedge Q$. This denotes the mathematical statement that is true precisely whenever both of P and Q are true, and is false otherwise.

2. Given two statements P and Q, we can form the mathematical statement "P or Q", denoted $P \vee Q$. This denotes the mathematical statement that is false if and only if both P and Q are false, and is true otherwise.[5]

3. Given a statement P, we can formulate the mathematical statement "not-P," which we denote $\neg P$. This is the mathematical statement that is false whenever P is true, and true whenever P is false.

4. Given two statements P and Q, we can form the mathematical statement "P is equivalent to Q", denoted $P \Leftrightarrow Q$. This denotes the mathematical statement that is true when P and Q are equal (i.e. both true or both false), and false when P and Q are different (i.e. exactly one is true and the other is false.)

5. Given two statements P and Q, we can form the mathematical statement "P implies Q", denoted $P \Rightarrow Q$. This statement is equivalent to the claim that "if P is true, then Q must be true as well." In particular, we say that $P \Rightarrow Q$ is false whenever P is true while Q is false (as this would break the claim "if P is true, then Q must be true as well,") and is true otherwise.

   In particular, notice that if P is false, $P \Rightarrow Q$ will evaluate to true no matter what Q is. This allows us to say that statements like "If I am a purple elephant, then six is an odd number" are true[6]. This is because if the P part is false, it doesn't matter whether the Q part is complete nonsense or not; our implication is automatically true! This is probably one of the harder things to get a grasp on, so take some time to absorb this.

[5] In mathematics, we almost always assume that our "or" is an inclusive-or: i.e. it is true when either P or Q is true, or even when **both** P and Q are true. In computer science, however, you will sometimes run into "exclusive-or," which is true when **exactly once** of P and Q are true, and is false otherwise. For your CCS classes, you're probably safe to assume that all "or" statements are inclusive-or, unless explicitly stated otherwise.

[6] Provided we are not purple elephants.

Additionally, we will often use the shorthand

- $\forall$ to denote "for all,"
- $\exists$ to denote "there exists,"
- $\in$ to denote "in," and
- $\notin$ to denote "not in,"

because we say these things all the time, and it really simplifies statements.

We now understand the idea of truth, and how to work with and evaluate claims. 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); 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 I was a salmon, I would be sad) + (I am not sad) tells you that I am not a salmon. 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.

1.1 The Art of Proof

With the rest of this talk, we're going to study the **art** of proof. This is a subject that could easily take an entire textbook to develop; we limit ourselves to a few pages, in the interests of time and teaching by example.

In the above section, we came up with a reasonably rigorous definition of what makes up a proof:

1. A well-stated claim (i.e. one that contains all of the things we're assuming to make our claim true.)
2. A selection of statements we've previously proven true, along with perhaps some axioms.
3. A number of logical links between these statements, axioms, and assumptions that concludes that our claim must be true.

This definition indeed captures the letter of what it means to be a proof; however, it does not properly capture the **spirit** of what a proof should aspire to be! Consider the following example:

Claim.

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

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 1. *(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 then see the **second** flaw in the cautionary example above: strictly as written, it's not even a proof of the AM-GM! The failed proof above looks like it starts off by **assuming** that the AM-GM is true, and then deduces a statement that we already know to be true (any squared number is nonnegative.) This does not, **by any means**, prove the statement we are claiming!

For example, if we assume that 1=2, we can easily deduce a true statement by multiplying both sides by 0:

$$\begin{aligned} &1 = 2 \\ \Rightarrow &0 \cdot 1 = 0 \cdot 2 \\ \Rightarrow &0 = 0. \end{aligned}$$

Does this prove 1=2? No! As we stated above, proofs can only take in as admissible evidence **things we already know to be true**. In specific, to prove a statement is true, you can't, um, just assume that the statement is true.

In specific, what does this mean for our proof of the AM-GM? Well, it means that instead of starting with the AM-GM and deducing a true thing, we should start with some true things and then deduce that the AM-GM is a consequence of these true things. We present a fixed and fully functional proof here:

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*

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

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 changed the ordering of these formulas and 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.

1.2 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. 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 $\frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \ldots + \frac{1}{4^n}$. 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.)

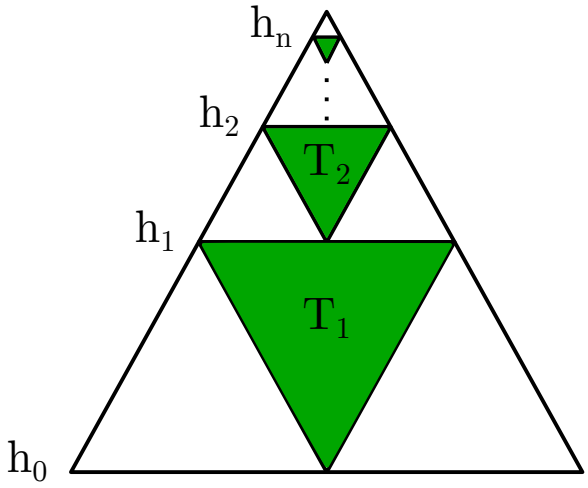
Proof. Consider the following construction:

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 $\left(\frac{1}{4}\right)^k$, 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

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

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. $\left(\frac{1}{4}\right)^n$, we then have that

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

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

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

□

1.3 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 (most notoriously, L'Hôpital's rule) 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 3. *$\sqrt[3]{2}$ is irrational: i.e. there are no pair of positive integers p, q, $q \neq 0$, such that $\sqrt[3]{2}$ can be expressed as the fraction $\frac{p}{q}$.*

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. □

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.