

## The Art and Technique of Proof

## 1 The Art of Proof

Every field of study has a way of “showing” that some result is true. In English/critical literature studies, if you wanted to prove 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, his other texts, and some of his letters sent to contemporaries. In physics, if you wanted to prove that neutrinos didn’t go faster than the speed of light, you’d write a paper that cited relevant theories (like general relativity) that supported this concept, as well as lots of measurements<sup>1</sup> that supported this idea.

The concept of proof is how mathematicians go about showing that something is true. In structure, a mathematical proof is very similar to a short essay or paper; you start by making a claim, and then go about assembling a series of facts that demonstrate that this claim is true. The only distinction between mathematics and other fields, roughly speaking, is that the only admissible things in a mathematical proof are (1) things we have previously proven to be true, and (2) axioms: i.e. a **small collection of statements** we’ve decided to assume are true. The consequence of this is that once a mathematical statement has been properly proven<sup>2</sup>, it cannot be disproven: unlike in the sciences, where new physical evidence and collected data can simply render a previous result moot, mathematical proofs are immutable. This, in a sense, is the grand bargain mathematics has made: we have gained the ability to deal with absolute truths, in exchange for never being able to make statements about reality (as reality is, for the most part, not admissible in your proofs.)<sup>3</sup>

In this section, 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.

### 1.1 Words and Proofs

We begin by offering a cautionary example of what you should **never** do in proofs:

---

<sup>1</sup>Just not the ones from **Italy**.

<sup>2</sup>It bears noting that mathematicians can make mistakes, and publish false proofs! We try to make that not happen too often, however.

<sup>3</sup> As usual, this is beautifully summed up by a **XKCD** comic.

*Proof.*

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

which is true. □

Why is the above result awful? 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: it's not even a proof of the AM-GM! The failed proof above 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. □

## 1.2 Pictures and Proofs

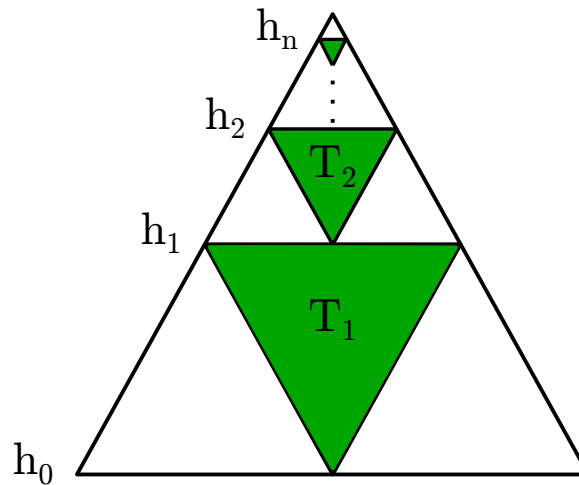
Words and symbols are not the only tool in proofs! In fact, well-chosen and drawn diagrams can often illustrate an idea that would otherwise take pages of text to describe. Pictures alone are rarely proofs: words are almost always necessary to explain what's going on, and you'll have to do some calculations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

**Claim 3.** *For any  $n \in \mathbb{N}$ , we have the following identity:*

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

*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

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

□

### 1.3 Avoiding Overkill in Proofs

One last thing to mention in mathematics (that is particularly applicable to Caltech undergrads) 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. Don’t do this!

There are lots of reasons why we want you to not use any results not proven either by yourself on the HW’s, in class, or in your recitations: one trivial one is that in a modern calculus class, pretty much everything you’ll do will have been proven somewhere or other, and if you could just cite all of mathematics you’d never have to do any work at all! (Well, except for some of the random questions, which are occasionally open problems.) Another reason, which is perhaps more relevant, is the following: proofs that involve this kind of “overkill” are usually **not very illuminating!** For example, consider the following:

**Theorem 4.**  $\sqrt[3]{2}$  is irrational.

*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 hundreds of thousands of hours of labor by scientists throughout the centuries:

*If  $n$  is a natural number  $\geq 3$ , 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. We proceed by contradiction: i.e. assume, for the moment, that  $\sqrt[3]{2}$  was rational. Express it as some ratio  $\frac{p}{q}$ , where  $p, q \in \mathbb{N}$ . Then, if we cube both sides, we have

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

multiplying both sides by  $q^3$  then gives us

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

But Fermat's last theorem says that such a thing cannot exist! Because Fermat's last theorem is true, we have arrived at a contradiction. Therefore,  $\sqrt[3]{2}$  cannot be a rational number, and is thus irrational.  $\square$

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.

## 2 The Technique of Proof

In this section, we get a bit more concrete: we turn our focus from the art of proofs to the techniques involved in proving claims. In specific, we will study three distinct forms of proof in this section: proofs by contradiction, proofs by contrapositive, and proofs by induction, starting with contradiction.

### 2.1 Proofs by Contradiction

What does it mean to prove something by contradiction? Well: consider some proposition  $P$ . By definition,  $P$  is either true or false. Suppose we want to show that  $P$  is true; how could we do this?

One method is to do the following: Take the proposition  $\neg P$ . If we can show that there is some sentence  $Q$  such that  $\neg P$  implies  $Q$  and that  $\neg p$  implies  $\neg Q$ , then we have that whenever  $\neg P$  holds, we have a contradiction! As mathematics is free of contradictions<sup>4</sup>, we have that  $\neg P$  cannot be true! In other words, we must have that  $\neg P$  is false – i.e. that  $P$  is true!

**Theorem 5.** *There are two irrational numbers  $a$  and  $b$  such that  $a^b$  is rational.*

*Proof.* We will prove our theorem with a proof by contradiction, as discussed above. To do this, we first assume that the negation of our theorem holds. In other words, we start off our proof by assuming the following hypothesis:

*There **cannot be** two irrational numbers  $a$  and  $b$  such that  $a^b$  is rational.*

What do we do from here? Well: lacking any better ideas, let's try throwing in numbers we know to be irrational into the above statement! Specifically, let's try setting both  $a$  and  $b$  equal to  $\sqrt{2}$ , because this is pretty much the only number we've even **shown** to be irrational thus far. Our hypothesis then tells us that, in specific,

$$\sqrt{2}^{\sqrt{2}} \text{ is irrational.}$$

---

<sup>4</sup>well, it's hopefully free of contradictions: if you're curious, look up Gödel's incompleteness theorem on Wikipedia (or come talk to me!) for some reasons about why this is a little complicated.

What do we do from here? Well: pretty much the only thing we have is our assumption, our knowledge that  $\sqrt{2}$  is irrational, and our new belief that  $\sqrt{2}^{\sqrt{2}}$  is **also** irrational. The only thing really left to do, then, is to let  $a = \sqrt{2}^{\sqrt{2}}$ ,  $b = \sqrt{2}$ , and apply our hypothesis again. But this is excellent! On one hand, our we have that  $a^b$  is irrational by our hypothesis. On the other hand, we have that  $a^b$  is equal to

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2,$$

which is clearly rational. This is a contradiction! Therefore, we know that our hypothesis must be false: there must be a pair of irrational numbers  $a, b$  such that  $a^b$  is rational.  $\square$

An interesting quirk of the above proof is that it didn't actually give us a pair of irrational numbers  $a, b$  such that  $a^b$  is rational! It simply told us that either

- $\sqrt{2}^{\sqrt{2}}$  is rational, in which case  $a = b = \sqrt{2}$  is an example, or
- $\sqrt{2}^{\sqrt{2}}$  is irrational, in which case  $a = \sqrt{2}^{\sqrt{2}}$ ,  $b = \sqrt{2}$  is an example,

but it never actually tells us which pair satisfies our claim! This is a weird property of proofs by contradiction: they are often **nonconstructive** proofs, in that they will tell you that a statement is true or false without necessarily giving you an example that demonstrates the truth of that statement.

## 2.2 Proofs by Contrapositive

The structure of a proof by contrapositive is remarkably simple: suppose we want to prove some statement of the form  $P \Rightarrow Q$ . Sometimes, this kind of a statement can be rather tricky to prove: perhaps  $P$  is a really tricky condition to start from, and we would prefer to start working from the other end of this implication. How can we do this?

Via the **contrapositive**! Specifically, if we have a statement of the form  $P \Rightarrow Q$ , the contrapositive of this statement is simply the statement

$$\neg Q \Rightarrow \neg P.$$

The nice thing about the contrapositive of any statement is that it's **exactly the same** as the original statement! For example, if our statement was "all Techers are adorable," the contrapositive of our claim would be the statement "all nonadorable things are not Techers." These two statements clearly express the same meaning – one just starts out by talking about Techers, while the other starts out by talking about nonadorable things. So, if we want to prove a statement  $P \Rightarrow Q$ , we can always just prove the contrapositive  $\neg Q \Rightarrow \neg P$  instead, because they're the same thing! This can allow us to switch from relatively difficult starting points (situations where  $P$  is hard to work with) to easier ones (situations where  $\neg Q$  is easy to work with.)

To illustrate this, consider the following example:

**Theorem 6.** *If  $n \equiv 2 \pmod{3}$ <sup>5</sup>,  $n$  is not a square: in other words, we cannot find any integer  $k$  such that  $k^2 = n$ .*

*Proof.* A direct approach to this problem looks . . . hard. Basically, if we were to prove this problem directly, we would take any  $n \equiv 2 \pmod{3}$  – i.e. any  $n$  of the form  $3m + 2$ , for some integer  $m$  – and try to show that this can never be a square. Basically, we’d be looking at the equation  $k^2 = 3m + 2$  and trying to show that there are no solutions to this equation, which just looks kind of . . . ugly, right?

So: because we are mathematicians, we are **lazy**. In particular, when presented with a tricky-looking problem, our instincts should be to try to make it trivial: in other words, to attempt different proof methods and ideas until one seems to “fit” our question. In this case, as suggested by our section title, let’s attempt to prove our theorem by studying its contrapositive:

*If  $n$  is a square, then  $n \not\equiv 2 \pmod{3}$ .*

Equivalently, because every number is equivalent to either 0, 1, or 2 mod 3, we’re trying to prove the following:

*If  $n$  is a square, then  $n \equiv 0$  or  $1 \pmod{3}$ .*

This is now a much easier claim! – the initial condition is really easy to work with, and the later condition is rather easy to check.

Now that we have some confidence in our ability to prove our theorem, we proceed with the actual work: take any square  $n$ , and express it as  $k^2$ , for some natural number  $k$ . We can break  $k$  into three cases:

1.  $k \equiv 0 \pmod{3}$ . In this case, we have that  $k \equiv 3m$  for some  $m$ , which means that  $k^2 = 9m^2 = 3(3m^2)$  is also a multiple of 3. Thus,  $k^2 \equiv 0 \pmod{3}$ .
2.  $k \equiv 1 \pmod{3}$ . In this case, we have that  $k \equiv 3m + 1$  for some  $m$ , which means that  $k^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$ . Thus,  $k^2 \equiv 1 \pmod{3}$ .
3.  $k \equiv 2 \pmod{3}$ . In this case, we have that  $k \equiv 3m + 2$  for some  $m$ , which means that  $k^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1$ . Thus,  $k^2 \equiv 1 \pmod{3}$ .

Therefore, we’ve shown that  $k^2$  isn’t congruent to 2 mod 3, for any  $k$ . So we’ve proven our claim! □

## 2.3 Proofs by Induction

Sometimes, in mathematics, we will want to prove the truth of some statement  $P(n)$  that depends on some variable  $n$ . For example:

- $P(n) =$  “The sum of the first  $n$  natural numbers is  $\frac{n(n+1)}{2}$ .”
- $P(n) =$  “If  $q \geq 2$ , we have  $n \leq q^n$ .”

---

<sup>5</sup>We write that  $a \equiv b \pmod{c}$  iff  $a - b$  is a multiple of  $c$ : in other words, that  $a$  and  $b$  are the “same” up to some number of copies of  $c$ .



- $P(n)$  = “Every polynomial of degree  $n$  has at most  $n$  roots.”

For any fixed  $n$ , we can usually use our previously-established methods to prove the truth or falsity of the statement. However, sometimes we will want to prove that one of these statements holds for **every** value  $n \in \mathbb{N}$ . How can we do this?


One method for proving such claims for every  $n \in \mathbb{N}$  is the method of **mathematical induction!** Proofs by induction are somewhat more complicated than the previous two methods. We sketch their structure below:

- To start, we take our claim  $P(n)$ , that we want to prove holds for every  $n \in \mathbb{N}$ .
- The first step in our proof is the **base step**: in this step, we explicitly prove that the statement  $P(1)$  holds, using normal proof methods.
- With this done, we move to the **induction step** of our proof: here, we prove the statement  $P(n) \implies P(n + 1)$ , for every  $n \in \mathbb{N}$ . This is an implication; we will usually prove it directly by assuming that  $P(n)$  holds and using this to conclude that  $P(n + 1)$  holds.

Once we’ve done these two steps, the principle of induction says that we’ve actually proven our claim for all  $n \in \mathbb{N}$ ! The rigorous reason for this is the **well-ordering principle**, which we discussed in class; however, there are perhaps more intuitive ways to think about induction as well.

The way I usually think of inductive proofs is to think of **toppling dominoes**. Specifically, think of each of your  $P(n)$  propositions as individual dominoes – one labeled  $P(1)$ , one labeled  $P(2)$ , one labeled  $P(3)$ , and so on/so forth. With our inductive step, we are insuring that all of our dominoes are *lined up* – in other words, that if one of them is true, that it will “knock over” whichever one comes after it and force it to be true as well! Then, we can think of the base step as “knocking over” the first domino; once we do that, the inductive step makes it so that all of the later dominoes also have to fall, and therefore that our proposition must be true for all  $n$  (because all the dominoes fell!)

To illustrate how these kinds of proofs go, here’s an example:

**Claim 7.** *For any  $n \in \mathbb{N}$ , take a  $2^n \times 2^n$  grid of unit squares, and remove one square from somewhere in your grid. The resulting grid can be tiled<sup>6</sup> by  - shapes.*

*Proof.* As suggested by the section title, we proceed by induction.

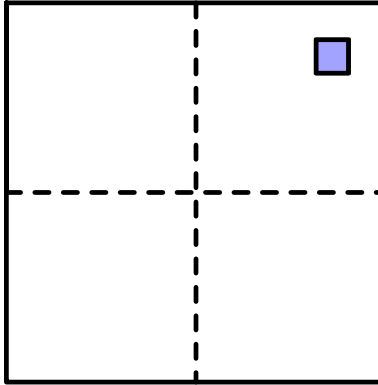
Base case: for  $n = 1$ , we simply have a  $2 \times 2$  grid with one square punched out. As this *is* one of our three-square shapes, we are trivially done here.

Inductive step: Assume that we can do this for a  $2^k \times 2^k$ -grid without a square, for any  $k \leq n$ . We then want to prove that we can do this for a  $2^{n+1} \times 2^{n+1}$  grid minus a square.

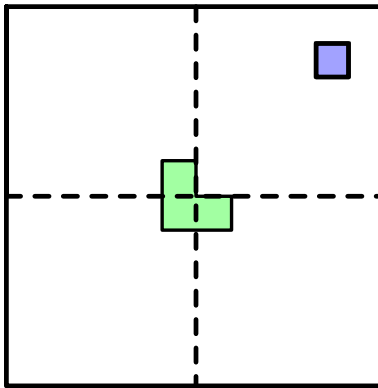
So: take any such grid, and divide it along the dashed indicated lines into four  $2^n \times 2^n$  grids. By rotating our grid, make it so that the one missing square is in the upper-right hand corner, as shown below:

---

<sup>6</sup>Refer to the definition of tiling given in the third random question, if you’ve forgotten!



Take this grid, and carefully place down one three-square shape as depicted in the picture below:



Now, look at each of the four  $2^n \times 2^n$  squares in the above picture. They all are missing exactly one square: the upper-right hand one because of our original setup, and the other three because of our placed three-square-shape. Thus, by our inductive hypothesis, we know that all of these squares can also be tiled! Doing so then gives us a tiling of the whole shape; so we've created a tiling of the  $2^{n+1} \times 2^{n+1}$  grid!

As this completes our inductive step, we are thus done with our proof by induction.  $\square$

The above question – one where you are in some sense “growing” or “extending” a result on smaller values of  $n$  to get to larger values of  $n$  – is precisely the kind of question that induction is set up to solve.