MA 8, WEEK 1: PROOFS AND PROOF TECHNIQUES

1. What is a Proof?

Every field of study has a way of showing that something is "true" in their field. For instance, in English literature, if you wanted to prove that the failed love story in Fitzgerald's *Great Gatsby* is a reflection of the author's disillusionment with the "American Dream," you would write an essay that quoted the story itself, his other texts, biographies, and maybe some of his letters. In physics, if you wanted to prove that neutrinos don't go faster than the speed of light, you'd write a paper that cited relevant theories (like general relativity and quantum mechanics) that support, as well as appropriate measurements.

In the same fashion, mathematical proofs are 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. things we've decided to assume are true. The consequence of this is that once a mathematical statement has been proven, 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 is the deal with the devil that mathematics 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 proofs.)

In fact, if you think about it, it's a miracle in itself that mathematics works to describe the world. Why *should* the laws of physics be written in the language of mathematics? Why does the same calculus that we use to plot trajectories of falling apples also work to describe celestial movements and subatomic phenomena?

This week, we're going to study the **art** of proof. This is a subject that could easily take an entire textbook to develop, but we limit ourselves to a few pages, since the basics are as easy to grasp as any other good game.

Date: October 1, 2013.

1.1. **Words and Proofs.** Here's something you should **never** do in proofs:

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? There are at least three reasons. First and foremost, there are 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 mess 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 result! The failed proof above starts off by **assuming** that the result 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!

Remark 2. Just because you somehow end up with a statement that looks true doesn't mean that the reasoning behind it was valid. 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**. To prove a statement is true, you can't just assume that the statement is true.

OK, so we messed up. What can we do now? Well, instead of starting with the result 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 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. □

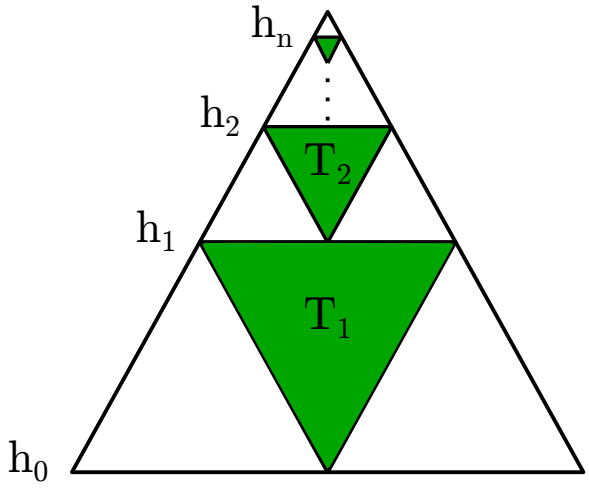
1.2. **Pictures and Proofs.** Words and symbols are not the only tool in proofs! In fact, well-chosen and drawn diagrams can often illustrate an idea that would otherwise take pages of text to describe. Pictures alone are rarely proofs: words are almost always necessary to explain what's going on, and 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:

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

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

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 withinin 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 Techers) 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 classes 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 homeworks, by the professor in class, or by the TAs 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! Another more important reason is that proofs that involve this kind of "overkill" are usually *not very illuminating*! For example, consider the following cute proof.

Theorem 5. $\sqrt[3]{2}$ *is irrational.*

Proof. Recall Fermat's Last Theorem, which says that

$$\textit{If } n \textit{ is a natural number} \geq 3\textit{, the equation}$$
$$a^n + b^n = c^n$$
$$\textit{has no solutions with } a, b, c \in \mathbb{N}.$$

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 $\sqrt[3]{2}$ is rational. We can write it as some ratio $\frac{p}{q}$, where $p, q \in \mathbb{N}$. By cubing both sides, we get

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

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! Since 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. □

This proof works completely! Technically, it is also valid. However, by reading it, we really haven't gained any better insights into what makes a number irrational. Good proofs **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 study four basic methods of proof. In all cases, we want to prove that "$P => Q$".

2.1. **Direct Proofs.** Direct proofs are, as the name suggests, the most obvious way to show that "$P => Q$". Namely,

(1) Assume that P is true.
(2) Use P to show that Q must be true.

Here's an example of a direct proof.

Proposition 1. *If m and n are consecutive natural numbers, then $m + n$ is odd.*

Proof. Since m and n are consecutive natural numbers, we can write $n = m + 1$.Therefore, we have

$$m + n = m + (m + 1) = 2m + 1.$$

Since m is a natural number, $2m + 1 = m + n$ is odd. □

2.2. **Proof by Contradiction (Reductio ad absurdum, if you want to be fancy).** Here we want to prove "$P \Rightarrow Q$" in a slightly funny way.

(1) Assume that P is true.
(2) Assume that $\neg Q$ ("not Q") is true.
(3) Use P and $\neg Q$ to demonstrate a contradiction.

Here's an example of this in action.

Theorem 2. *There are two irrational numbers a and b such that a^b is rational.*

"Proof with inner monologue". We will prove our statement by contradiction. 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 are **no** irrational numbers a and b such that a^b is rational.*

What do we do from here? Well, 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 $\sqrt{2}$, which we know is irrational. Our hypothesis then tells us that

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

OK. What do we do now? Well, the only thing we really 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 we can really do is pick $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$, and apply our hypothesis again. However, this will work! 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. □

Remark 3. 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
- $\sqrt{2}^{\sqrt{2}}$ 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.

2.3. **Proof by Contrapositive.** When do you want to use a proof by contrapositive? Sometimes, proving "$P \Rightarrow Q$" directly is tricky: maybe P is a really subtle 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 $P \implies Q$, 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 logically equivalent to 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 $P \implies Q$, 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.)

In summary, you can apply the technique of proof by contrapositive as follows:

(1) Assume $\neg Q$.
(2) Use $\neg Q$ to show that $\neg P$ holds.

Remark 4. As you can see, proof by contrapositive is a close cousin of the proof by contradiction. Indeed, one way to demonstrate contradiction in Step (3) of the proof by contradiction is to show that both P and $\neg P$ hold, which cannot occur!

To illustrate this, consider the following example:

Theorem 5. *If $n \equiv 2 \mod 3$, 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 $n \equiv 2 \mod 3$ – 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 looks pretty nasty.

Since we are mathematicians, 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. Let's look at the contrapositive of our statement:

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

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

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

This looks much easier! – 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) $k \equiv 0 \mod 3$. 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, $k^2 \equiv 0 \mod 3$.
(2) $k \equiv 1 \mod 3$. 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, $k^2 \equiv 1 \mod 3$.

(3) $k \equiv 2 \mod 3$. 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, $k^2 \equiv 1 \mod 3$.

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

2.4. **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 $n \leq q^n$.
- $P(n) =$ "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 to use mathematical induction.

(1) Prove our statement in the **base case**, that is, show that $P(1)$ is true.
(2) (**Induction step**) *Assume* that $P(k)$ holds, and use this show that $P(k + 1)$ holds.

The intuitive reason why this works is as follows. Since we've established the base case, by applying the induction step over and over again, we see that

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \cdots$$

and so prove our statement for all $n \in \mathbb{N}$. The real reason why this works is that the principle of mathematical induction is rooted in the well-ordering principle, which was briefly discussed in class.

You'll get a lot of practice with this proof technique on the homework, but just so you're not confused, we'll go through a very simple application of proof by induction.

Proposition 6. *For all $n \in \boldsymbol{N}$, we have*

$$S_1(n) = 1 + 2 + \cdots + n = \sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Proof. We will prove our statement by induction on n.

Base case: If $n = 1$, then $S_1(n) = 1$ and $\frac{1(1+1)}{2} = 1$, so our result holds in this case.

Inductive step: Assume that our statement holds for $n = k$. (This called the **induction hypothesis**.) We want to show that our statement holds for $n = k + 1$. By the induction hypothesis,

$$S_1(k) = 1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Adding $k + 1$ to each side, we get

$$\begin{aligned} 1 + 2 + \cdots + k + k + 1 &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k^2 + k + (2k+2)}{2} \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Hence, $S_1(k+1) = \frac{(k+1)(k+2)}{2}$ as desired. By the principle of mathematical induction, our formula holds for all $n \in \mathbb{N}$. $\square$