Proofs

Intuitively, the concept of proof should already be familiar. We all like to assert things, and few of us like to say things that turn out to be false. A proof provides a means for *guaranteeing* such claims.

Proofs in mathematics and computer science require a precisely stated proposition to be proved. But what exactly is a proof? How do you show that a proposition is true? Recall that there are certain propositions called axioms or postulates, that we accept without proof (we have to start somewhere). A formal proof is a sequence of statements, ending with the proposition being proved, with the property that each statement is either an axiom or its truth follows easily from the fact that the previous statements are true. For example, in high school geometry you may have written two-column proofs where one column lists the statements and the other column lists the justifications for each statement. The justifications invoke certain very simple rules of inference which we trust (such as if P is true and Q is true, then $P \wedge Q$ is true). Every proof has these elements, though it does not have to be written in a tabular format. And most importantly, the fact that each step follows from the previous step is so straightforward, it can be checked by a computer program.

A formal proof for all but the simplest propositions is too cumbersome to be useful. In practice, mathematicians routinely skip steps to give proofs of reasonable length. How do they decide which steps to include in the proof? The answer is sufficiently many steps to convince themselves and the reader that the details can easily be filled in if desired. This of course depends upon the knowledge and skill of the audience. So in practice proofs are socially negotiated.

During the first few weeks of the semester, the proofs we will write will be quite formal. Once you get more comfortable with the notion of a proof, we will relax a bit. We will start emphasizing the main ideas in our proofs and sketching some of the routine steps. This will help increase clarity and understanding and reduce clutter. A proof, for the purposes of this class, is essentially a convincing argument. Convincing to whom? First, to you, the author, second, to your classmates, third, to your professor and your TA.

In this lecture you will see some examples of proofs. The proofs chosen are particularly interesting and elegant, and some are of great historical importance. But the purpose of this lecture is not to teach you about these particular proofs (and certainly not for you to attempt to memorize any of them!). Instead, you should see these as good illustrations of various basic proof techniques. You will notice that sometimes when it is hard to even get started proving a certain proposition using one proof technique, it is easy using a different technique. This will come in handy later in the course when you work on homework problems or try to prove a statement on your own. If you find yourself completely stuck, rather than getting discouraged you might find that using a different proof technique opens doors that were previously closed.

We now begin with a few definitions pertaining to proofs.

A **theorem**, informally speaking, is a true proposition that is guaranteed by a proof. If you believe that a statement is true but can't prove it, call it a **conjecture**, essentially an educated guess.

A concept useful for writing up complicated proofs is that of a **lemma**, which is a little theorem that you use in the proof of a bigger theorem. A lemma is to proofs what a subroutine is to programming.

An **axiom** is a statement we accept without proof.

There are many different types of proofs, as you will see. The basic structure of these different types of proofs is best expressed in terms of propositional logic, as we shall see.

Direct Proof

Let us start with a very simple example:

Theorem: If x is an odd integer, then $x+1$ is even.

The proposition that we are trying to prove is of the form $P \implies Q$. A direct proof of this starts by assuming P and eventually concludes Q through a chain of implications:

Direct Proof of $P \implies Q$.
Assume P.
⋮
Therefore Q.

Let us proceed with a direct proof of the simple example given above:

Proof: Assume x is odd. Then by definition, $x = 2k+1$ for some $k \in \mathbb{Z}$. Adding one to both sides, we get $x+1 = 2k+2 = 2(k+1)$. Therefore, by definition $x+1$ is an even number. ♠

Before turning to our next example, we recall that integer d divides n (denoted $d|n$) iff there exists some integer q such that $n = dq$.

For the following, let n be a postive integer less than 1000.

Theorem: If the sum of the digits of n is divisible by 9, then n is divisible by 9.

Note: The theorem is true for arbitary n. We're just doing the three digit case to keep the notation from getting distracting.

Using notation in the previous lecture, note that this statement is equivalent to

$$(\forall n)(\text{sum of } n\text{'s digits divisible by } 9) \implies (n \text{ divisible by } 9).$$

For each n, this statement is of the form $P \implies Q$. So to prove the theorem, we will assume for a generic value of n that P is true, and will show that Q must also be true. i.e. we start by assuming that the sum of n's digits is divisible by 9. Then we perform a sequence of steps to conclude that n itself is divisible by 9. Here is the proof.

Proof:

Suppose we have n such that the sum of the digits of n is divisible by 9. Let a be the hundred's digit of n, b the ten's digit, and c the one's digit. Then $n = 100a+10b+c$. Now suppose that the sum of the digits of n is divisible by 9. Then,

$$a+b+c = 9k, k \in \mathbb{Z}.$$

Adding $99a+9b$ to both sides of the equation, we get

$$100a+10b+c = n = 9k+99a+9b = 9(k+11a+b)$$

So n is divisible by 9. ♠

In this case the converse of the theorem is also true: If n is divisible by 9, the sum of its digits is divisible by 9, too. In other words, the sum of the digits of n is divisible by 9 if and only if n is divisible by 9. In general, to prove $P \iff Q$, you have to do two proofs: You must show that $P \implies Q$ and then, separately, you must also show that $Q \implies P$. In this particular case, however, one proof just reverses the steps of the other so it's possible to prove both directions at once:

Theorem: n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.

Proof:

n is divisible by 9
$\iff n = 9l, l \in \mathbb{Z}$
$\iff 100a + 10b + c = 9l, l \in \mathbb{Z}$
$\iff 99a + 9b + (a + b + c) = 9l, l \in \mathbb{Z}$
$\iff a + b + c = 9l - 99a - 9b, l \in \mathbb{Z}$
$\iff a + b + c = 9(l - 11a - b), l \in \mathbb{Z}$
$\iff a + b + c = 9k, k \in \mathbb{Z}\ (k = l - 11a - b)$
$\iff a + b + c$ is divisible by 9 ♠

Be *very careful* when proving a biconditional statement in this manner. For the proof to be legitimate, the steps have to make just as much sense backwards as forwards. Go back and read the proof backwards, starting with the last line and ending with the first, and check for yourself that it works.

Proof by Contrapostion

In the last lecture, we learned that a statement of the form $P \implies Q$ is logically equivalent to its contrapositive: $\neg Q \implies \neg P$. This means that proving an implication is equivalent to proving the contrapositive. A proof by contraposition of $P \implies Q$ is just a direct proof of its contrapositive $\neg Q \implies \neg P$:

Proof by Contraposition of $P \Longrightarrow Q$.
Assume $\neg Q$.
⋮
Therefore $\neg P$.
So $\neg Q \Longrightarrow \neg P \equiv P \Longrightarrow Q$.

Sometimes proving the contrapositive of a statement is easier than proving the statement directly. Here is an illustrative example.

Let n be an integer and let d divide n.

Theorem: If n is odd then d is odd.

Proving this directly would be difficult. We would assume n is odd but what then? Proving the contrapositive of the statement, however, is very straightforward. The contrapositive is: If d is even then n is even.

Proof: Suppose d is even, then (by definition) $d = 2k$ for some $k \in \mathbb{Z}$.
Because $d|n$, $n = dl$, for some $l \in \mathbb{Z}$.
Combining these two statements, we have $n = dl = (2k)l = 2(kl)$.
So n is even. So if d is even then n is even. Therefore if n is odd then d is odd. ♠

Proof by contraposition is a very common technique. When proving implications ($P \implies Q$) the contrapositive gives us a second option for how to approach the problem. As a warning, do not confuse the contrapositive with the converse. To give some intuition using English, consider the statement "If it is sunny, then it is daytime." The contrapositive is that "If it is nighttime, then it is not sunny," and the converse is that "If it is daytime, then it is sunny." We know the original statement is true, and its contrapositive is also true. However the converse is simply false (it could be foggy at daytime).

Proof by Contradiction

Proof by contradiction is also called *reductio ad absurdum* (reduction to an absurd thing). The idea is to assume the opposite of what one is trying to prove and then show that this leads to something that is clearly nonsensical: a contradiction.

> Proof by Contradiction of P.
> Assume $\neg P$.
> $\vdots$
> R
> $\vdots$
> $\neg R$
> Contradiction
> Therefore P.

Before proceeding to an example, let us try to understand the logic behind a proof by contradiction. We assume $\neg P$, and then prove both R and $\neg R$. But for any proposition R, $R \wedge \neg R = False$. So we have shown that $\neg P \implies False$. The only way this implication can be true is if $\neg P$ is false. i.e. P is true.

Our first example of a proof by contradiction dates back more than 2000 years – to Euclid. (Note that it is not of the form $P \implies Q$ so contraposition is not an option.)

Theorem: There are infinitely many prime numbers.

Proving this directly would be difficult. How do we construct infinitely many prime numbers? But, as we will see, bad things happen when we assume that this statement is false: that there are only finitely many primes. Before we prove the theorem, we will state a simple lemma that we'll use without proof. We will prove it next week when we learn induction:

Lemma: Every natural number greater than one is either prime or it has a prime divisor.

Now for the proof of the theorem:

Proof:

Suppose toward a contradiction that there are only finitely many primes. Then, we can enumerate them: $p_1, p_2, p_3, \ldots, p_k$.

Consider the number $q = p_1 p_2 p_3 \ldots p_k + 1$, the product of all the primes plus one. Note that q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p (this is the statement R, or more precisely R is the assertion that $p > 1$). Because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p

must be equal to one of them, so p is a divisor of their product.

So we have that p divides $p_1 p_2 p_3 \dots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore $p \leq 1$ (this is $\neg R$). Contradiction. Therefore there are infinitely many primes. ♠.

Note that in the proof, q need not be prime, as tempting as it might be to say so. It's certainly not the case that a product of primes plus one must always be prime (think of $7 \cdot 2 + 1$). When writing a proof, it is important to carefully think through each step, ensuring that it's logically justified. The most important part of learning mathematics is learning a habit of thinking clearly and precisely.

Let's look at another classic proof by contradiction. A **rational number** is a number that can be expressed as the ratio of two integers. For example, $\frac{2}{3}$, $\frac{3}{5}$, and $\frac{9}{16}$ are all rational numbers. In fact, any number with a finite or recurring decimal representation is a rational. (Perhaps you'll prove this on one of your homeworks.) Numbers that cannot be expressed as fractions are called **irrational**.

Theorem: $\sqrt{2}$ is irrational.

Proof: Assume towards a contradiction that $\sqrt{2}$ is rational. By the definition of rational numbers, there are integers a and b with no common factor other than 1, such that $\sqrt{2} = a/b$.

For any numbers x and y, we know that $x = y \implies x^2 = y^2$. Hence $2 = a^2/b^2$.

Multiplying both sides by b^2, we have $a^2 = 2b^2$.

b is an integer, hence b^2 is an integer, hence a^2 is even (by the definition of evenness).

Hence, a is even (by the lemma below).

Therefore, by the definition of evenness, there is an integer c such that $a = 2c$.

Hence $2b^2 = 4c^2$, hence $b^2 = 2c^2$.

Since c is an integer, c^2 is an integer, hence b^2 is even.

Thus, b is even (by the lemma below).

a and b have a common factor 2, contradicting the assertion that a and b have no common factor other than 1. This shows that the original assumption that $\sqrt{2}$ is rational is false, and that $\sqrt{2}$ must be irrational. ♠

Lemma: If a^2 is even, then a is even.

Can you prove this lemma? First try a direct proof? How would you proceed? Now try a proof by contraposition.

Proof by Cases

Sometimes we don't know which of a set of possible cases is true, but we know that at least one of the cases is true. If we can prove our result in each of the cases, then we have a proof. The English phrase "damned if you do and damned if you don't" sums up this proof method. Here's a nice example:

Theorem: For some irrational numbers x and y, x^y is rational.

Proof: Since the theorem is existentially quantified (the phrase 'for some'), we need only prove the existence of at least one example. Consider the case $x = \sqrt{2}$ and $y = \sqrt{2}$. Clearly either

(a) $\sqrt{2}^{\sqrt{2}}$ is rational

or (b) $\sqrt{2}^{\sqrt{2}}$ is irrational.

In case (a), we have shown irrational numbers x and y such that x^y is rational.

In case (b), consider the values $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have

$$
\begin{aligned}
x^y &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \\
&= \sqrt{2}^{\sqrt{2}\sqrt{2}} \text{ by the axiom } (x^y)^z = x^{yz} \\
&= \sqrt{2}^2 = 2
\end{aligned}
$$

Hence we have shown irrational numbers x and y such that x^y is rational. ♠

Since one of cases (a) and (b) must be true, it follows that for some irrational numbers x and y, x^y is rational.

Notice that even after the proof, we still don't know which of the two cases is true, so we can't actually exhibit any irrational numbers satisfying the theorem. This is an example of a **nonconstructive** proof, one in which an existential theorem is proved without constructing an example.

Non-proof

Failure to logically structure a proof or note the justification for each step c an lead easily to non-proofs. Consider the following examples.

Theorem: $-2 = 2$.

Proof: Assume $-2 = 2$. Squaring both sides, we get $(-2)^2 = 2^2$, or $4 = 4$ which is true. Therefore, $-2 = 2$. ♠

The theorem is obviously false, so what did we do wrong? Our arithmetic is correct, and it seems like each step follows from the previous step. The problem with this proof does not lie in the arithmetic, but rather the logic. We assumed the very theorem we were trying to prove was true! As you can see, logical soundness and structure are extremely important when proving propositions.

The next proof is incorrect for a different reason.

Theorem: (not!) $1 = -1$

Proof: $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \sqrt{-1}^2 = -1$ ♠

This proof appears to be logically sound, so the error lies elsewhere. Since we have concluded a falsehood, at least one of these steps is false. Indeed, it is simply untrue that $\sqrt{xy} = \sqrt{x}\sqrt{y}$. If you think carefully through each step of your proofs, you can avoid such missteps.

Other classic errors:

- Dividing both sides of an equation by a variable. For example:

  $$ax = bx \text{ hence } a = b$$

  The "axiom" to which this step implicitly appeals is false, because if $x = 0$, the claim $a = b$ is not necessarily true. So in this case, either $x = 0$ or $a = b$ (consider writing the above as $x(a-b) = 0$. Some extra work may be needed to prove $x \neq 0$.

- Dividing both sides of an inequality by a variable. This is even worse! For example:

  $$ax < bx \text{ hence } a < b$$

Here the claim $a < b$ is false if $x < 0$, and unproven if $x = 0$.

- More generally, forgetting about 0. Forgetting to account for the possibility of variables being zero causes lots of headaches (including the above).

Style and substance in proofs

Again, get in the habit of thinking carefully before you write down the next sentence of your proof. If you cannot explain clearly why the step is justified, you are making a leap and you need to go back and think some more. In theory, each step in a proof must be justified by appealing to a definition or general axiom. In practice the depth to which one must do this is a matter of taste. For example, we could break down the step, "Since a is an integer, $(2a^2 + 2a)$ is an integer," into several more steps. [Exercise: what are they?] A justification can be stated without proof only if you are absolutely confident that (1) it is correct and (2) the reader will automatically agree that it is correct.

Notice that in the proof that $\sqrt{2}$ is irrational, we used the result, "For any integer n, if n^2 is even then n is even," twice. This suggests that it may be a useful fact in many proofs. A subsidiary result that is useful in a more complex proof is called a **lemma**. It is often a good idea to break down a long proof into several lemmata. This is similar to the way in which large programming tasks should be divided up into smaller subroutines. Furthermore, make each lemma (like each subroutine) as general as possible so it can be reused elsewhere.

LEMMA

The dividing line between lemmata and theorems is not clear-cut. Usually, when writing a paper, the theorems are those propositions that you want to "export" from the paper to the rest of the world, whereas the lemmata are propositions used in the proofs of your theorems. There are, however, some lemmata (for example, the Pumping Lemma and the Lifting Lemma) that are perhaps more famous and important than the theorems they were used to prove.

Finally, you should remember that the point of this lecture was not the specific statements we proved, but the different proof strategies, and their logical structure. Make sure you understand them clearly; you will be using them when you write your own proofs in homework and exams.