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.[1]

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

[1] Those interested in exploring this issue in more detail may like to read the influential paper "Social Processes and Proofs of Theorems and Programs" by DeMillo, Lipton and Perlis, *Communications of the ACM* **22** (1979) pages 271–280.

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 as true without proof.

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

Direct Proof

Let us start with a very simple example.

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

Following the notation introduced in the previous Note, the statement of the theorem is equivalent to

$$(\forall x \in \mathbb{Z})(x \text{ is odd} \Longrightarrow x+1 \text{ is even}).$$

(Here $\mathbb{Z}$ denotes the set of all integers.) For each x, the proposition that we are trying to prove is of the form $P(x) \Longrightarrow Q(x)$. A direct proof of this starts by assuming $P(x)$ for a generic value of x and eventually concludes $Q(x)$ through a chain of implications:

Direct Proof of $P \Longrightarrow Q$
Assume P
$\vdots$
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 the integer d divides n (denoted $d|n$) if and only if there exists some integer q such that $n = dq$.

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

Theorem: Let n be a positive integer. If the sum of the digits of n is divisible by 9, then n is divisible by 9.

Comment: The theorem is true for arbitrary n. We're just doing the three digit case here so the notation does not distract from the structure of the argument.

This theorem's statement is equivalent to

$$(\forall n \in \mathbb{Z}^+)(\text{sum of } n\text{'s digits divisible by } 9 \Longrightarrow n \text{ divisible by } 9).$$

(Here $\mathbb{Z}^+$ denotes the set of positive integers, $\{1,2,\ldots\}$.) So once again we start by assuming, for a generic value of n, 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. This amounts to supposing that

$$a+b+c = 9k$$

for some $k \in \mathbb{Z}$. Adding $99a+9b$ to both sides of the equation, we get

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

which is certainly divisible by 9 (since $k+11a+b$ is an integer). And finally, since $n = 100a+10b+c$, we see that n is divisible by 9. □

Exercise: Generalize the above proof so that it works for *any* positive integer n. [HINT: Suppose n has k digits, and write a_i for the ith digit of n, so that $n = \sum_{i=0}^{k-1} a_i \times 10^i$.]

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*[2] 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 $Q \implies P$.

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

Proof: We already proved above that if the sum of the digits of n is divisible by 9 then n is divisible by 9. So we only need to prove the converse. We use the same notation for the digits of n as we used in the previous proof:

n is divisible by 9
$\implies n = 9\ell$, for some $\ell \in \mathbb{Z}$
$\implies 100a+10b+c = 9\ell$
$\implies 99a+9b+(a+b+c) = 9\ell$
$\implies a+b+c = 9\ell-99a-9b$
$\implies a+b+c = 9(\ell-11a-b)$
$\implies a+b+c = 9k$, where $k = \ell-11a-b \in \mathbf{Z}$
$\implies a+b+c$ is divisible by 9. □

Note that, in this simple example, the proof of $Q \implies P$ is essentially the same as the proof of $P \implies Q$ "run backwards." In such a case, it's tempting to try to get away with proving both of the implications at the same time (using the symbol $\iff$ at every step of the proof). However, I do not recommend this approach. Doing so requires *great caution*: for the proof to be legitimate, the steps have to make just as much sense backwards as forwards! (Go back and read the last proof again, starting with the last line and ending with the first, and convince yourself that it also works backwards.) To avoid potential pitfalls, it is recommended that you always prove a statement of the form $P \iff Q$ using two *separate* proofs. This will in any case be necessary in more interesting examples, where the proofs of $P \implies Q$ and of $Q \implies P$ might look very different.

Proof by Contraposition

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 $\neg Q \implies \neg P$:

[2]The phrase "if and only if" is often abbreviated to "iff".

Proof by Contraposition of $P \implies Q$
Assume $\neg Q$
$\vdots$
Therefore $\neg P$
So $\neg Q \implies \neg P$, or equivalently $P \implies Q$

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

Theorem: Let n be an integer and let d divide n. Then, 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 $d|n$, we have $n = dq$ for some $q \in \mathbb{Z}$.
Combining these two statements, we have $n = dq = (2k)q = 2(kq)$.
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 "If it is nighttime, then it is not sunny," and the converse is "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 (for example, a summer afternoon in San Francisco!).

Proof by Contradiction

Proof by contradiction is also called *reductio ad absurdum* (reduction to an absurdity). 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, $R \wedge \neg R \equiv \mathit{False}$. So we have shown that $\neg P \implies \mathit{False}$. 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.

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 about induction.

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

Now for the proof of the theorem.

Proof: Suppose (in order to get a contradiction) that there are only finitely many primes. Then, we can enumerate them: $p_1, p_2, p_3, \ldots, p_k$. (Here k is the total number of primes.)

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 will be our statement R. 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 $p_1 p_2 p_3 \ldots p_k$, and p divides q, but that means p divides their difference, which is 1. Therefore, $p \leq 1$ (this is $\neg R$). Contradiction. If we start with the assumption that there are finitely many primes, we derive a contradiction. The only remaining possibility is that our original assumption (finitely many primes) was wrong. Therefore there are infinitely many primes. □

Note that in the proof, q need not be prime, 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 $7 \times 2 + 1$). Nor is it the case that the product of the first k primes plus one must necessarily be prime (e.g., $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$). 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. [Exercise: Can you prove this?] Numbers that cannot be expressed as fractions are called **irrational**.

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

Proof: Assume (for the sake of contradiction) that $\sqrt{2}$ is rational. By the definition of rational numbers, this means that there exist integers a and b with no common factor other than 1, such that $\sqrt{2} = a/b$. (This will be our assertion R.)

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 $2b^2 = (2c)^2 = 4c^2$, 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).

Thus 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 hence 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 contradiction can seem mysterious. A proof by contradiction of P starts by assuming $\neg P$, and then it explores the consequences of this assumption. But you might wonder: why is it OK to assume $\neg P$ is true? Proofs aren't allowed to make assumptions willy-nilly without justification, so why is it fair game to begin the proof by assuming $\neg P$? The answer: certainly P is either true or false. If P is true, then we're done: we wanted to prove P is true, and it is. So the only thing left to consider is the possibility that P is false (i.e., $\neg P$ is true)—and a proof by contradiction demonstrates that this is in fact impossible, from which it follows that P must be true. Once we conclusively rule out the possibility that P might be false (by deriving a contradiction), we're entitled to conclude that P must be true.

Here is one more proof by contradiction, if you'd like to see another example.

Theorem: $x^5 - x + 1 = 0$ has no solution in the rational numbers.

To prove this theorem, we will first state and prove a useful lemma.

Lemma 1: If x is a real number satisfying $x^5 - x + 1 = 0$, and if $x = a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, then both a and b are even.

Proof: Plugging in $x = a/b$, we have

$$(a/b)^5 - (a/b) + 1 = 0.$$

Multiplying both sides by b^5 yields

$$a^5 - ab^4 + b^5 = 0.$$

Now we perform a case analysis, looking at the parity of a and b:

- Case 0 (a is odd and b is odd): In this case, a^5, ab^4, and b^5 are all odd. Thus the left-hand side (LHS) of the second equation above has the form odd $-$ odd $+$ odd, and so the LHS is odd. However, the right-hand side (RHS) is even, which is impossible.
- Case 1 (a is odd and b is even): In this case, the LHS has the form odd $-$ even $+$ even, so the LHS is odd. As before, this is impossible.
- Case 2 (a is even and b is odd): In this case, the LHS has the form even $-$ even $+$ odd, so the LHS is odd. This too is impossible.

We have eliminated the three cases above as impossible, so the only remaining possibility is that a must be even and b must be even. □

We're now ready to prove the theorem.

Proof: Suppose (for the sake of a contradiction) that there exists some rational number, call it x, such that $x^5 - x + 1 = 0$. Since x is rational, we can find $a, b \in \mathbb{Z}$ such that $x = a/b$ and $b > 0$. Actually, there might be many ways to express x in this way (i.e., many pairs of $a, b \in \mathbb{Z}$ such that $x = a/b$ and $b > 0$); among all of these ways, let a, b be the choice that makes b minimal, i.e., that makes b as small as possible.

Now define $\alpha = a/2$ and $\beta = b/2$. By Lemma 1, both a and b must be even, so both α and β must be integers. Also, $x = a/b = (2\alpha/2\beta) = \alpha/\beta$, so $x = \alpha/\beta$. in particular, we have $x = \alpha/\beta$, and also $\alpha, \beta \in \mathbb{Z}$ and $\beta > 0$. In other words, α, β provide another way to express x. But $\beta = b/2$, so $\beta < b$. So b must not have been minimal after all. This is a contradiction. So our assumption must have been wrong—we've proven there does not exist any rational number x satisfying $x^5 - x + 1 = 0$. □

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: There exists some pair of irrational numbers x and y such that x^y is rational.

Comment: This is our first example in this Note of a theorem that is *existentially* quantified ("there exists"). In other words, the statement may be written as

$$(\exists x)(\exists y)(x \text{ is irrational} \wedge y \text{ is irrational} \wedge x^y \text{ is rational}).$$

Thus to prove the theorem we only need to prove the existence of at least one *example* of values x, y that satisfy the claim. (For this reason, proofs of existentially quantified statements are often—but not always—a little easier than proofs of universally quantified ones.)

Proof of the theorem: 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, so we are done.
In case (b), consider the new 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 again shown irrational numbers x and y such that x^y is rational.
Since one of cases (a) and (b) must be true, and since in both cases we have exhibited irrational numbers x and y such that x^y is rational, we can conclude that such numbers must always exist. □

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 explicit example.

Non-proof

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

Theorem: (not!) $-2 = 2$.

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 must be 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, suppose you see the following:

  $ax = bx$ 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, all we can conclude is that either $x = 0$ or $a = b$ (this can also be written 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:

  $ax < bx$ 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).

- "Working backwards." If you ever played with one of those puzzles where you solve a maze on paper, you may have learned the trick of starting at the exit of the maze and working backwards to the entrance. It's tempting to apply the same tricks to proving theorems: start with what you are trying to prove, and manipulate the claim until you get to one of the assumptions. However, this style of reasoning is erroneous; it amounts to a "converse error." You can't start by assuming what you are trying to prove. All reasoning should go "forwards": start with what you are given, and then work out what you can conclude from those givens, and so on.

Style and substance in proofs

We conclude with some general words of advice. First, 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 lemmas. 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.

The dividing line between lemmas 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 lemmas are propositions used locally in the proofs of your theorems. There are, however, some lemmas (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.

Proof Tips

Sometimes you can get some idea of how to structure your proof by looking at the form of the proposition you are trying to prove. Some examples:

- To prove something of the form $P \wedge Q$, first, prove P. Then, prove Q.
- To prove something of the form $P \vee Q$, one possibility is to guess which of P,Q is true and prove just that one. Another possibility is to try proving $(\neg P) \implies Q$ or $(\neg Q) \implies P$.
- To prove something of the form $P \implies Q$, try a direct proof (start by assuming P, work out its consequences, and see if you can derive Q).
- To prove something of the form $(\forall x \in S)P(x)$, try a direct proof: consider a generic x, where you make absolutely no assumptions about the value of x other than that $x \in S$; then see if you can prove that $P(x)$ holds for that value of x. If you proved $P(x)$ without making any assumptions about x, your proof must apply to every possible value of x.

  In the next Note, we will see another technique to prove statements of the form $(\forall n \in \mathbb{N})P(n)$.
- To prove something of the form $(\exists x)P(x)$, try to find a value of x that makes $P(x)$ true, and just list it.
- To prove something of the form P, sometimes it is helpful to split by cases: look for some other proposition Q that allows you to prove both $Q \implies P$ and $(\neg Q) \implies P$. You can then use a proof by cases.
- If the proposition has no quantifiers (no $\forall$ or $\exists$ symbols), you could try a proof by enumeration: draw a truth table and show that the proposition is true in all cases. If you have a compound proposition built up out of $P_1, \ldots, P_k$ atomic propositions, then the truth table will have 2^k rows, so this technique is only feasible if the number of atomic propositions is not too large.

You can combine these techniques. For instance, if you are trying to prove something of the form $(\forall n \in \mathbb{N})(P(n) \implies Q(n))$, you might try a direct proof: consider a generic value of $n \in \mathbb{N}$, where all you are allowed to assume about n is that $P(n)$ is true, and try to derive $Q(n)$.