Discrete Mathematics
What is a proof?

Saad Mneimneh

1 The pigeonhole principle

The pigeonhole principle is a basic counting technique. It is illustrated in its simplest form as follows: We have $n+1$ pigeons and n holes. We put all the pigeons in holes (in any way we want). The principle tells us that there must be at least one hole with at least two pigeons in it. Why is that true? Try to visualize the example of $n = 2$; therefore, we have 3 pigeons and 2 holes. Let's try to avoid the consequence stated by the principle. If all pigeons must be placed in holes, the first one must be placed in some hole. This hole can no longer be used. Now the second pigeon must occupy a different hole. The third pigeon must share a hole with another pigeon. It is obvious that this argument/proof can be generalized to any n. However, it is very mechanical. For instance, when presenting this proof and showing that any strategy will fail to avoid putting two pigeons in the same hole, you will start by saying something like: let's place pigeon 1 in hole 1. One might say in response to that: but what if there is another strategy? You are going to say: well it does not matter which hole you choose for pigeon 1. So, basically you have to articulate your proof. Here's an easier proof using a technique called proof by contradiction. In a proof by contradiction you start by the opposite of what you claim, and then try to reach something that is false (yes that's funny!). If your logic is correct, this can only mean one thing: your starting point is false.

So, what is the opposite of our claim? Our claim is that at last one hole will contain at least two pigeons. The opposite of the claim is that every hole has at most one pigeon. Assume every hole has at most one pigeon. Then the total number of pigeons is at most $1+1+\ldots+1$ (n times), which is n, a contradiction!

Dirichlet was the first to articulate this principle in proving that for any real number α and any integer n, there exist integers p and $1 \leq q \leq n$, such that:

$$|q\alpha - p| \leq \frac{1}{n+1}$$

2 Primes are infinite - a proof by contradiction

Here's another famous proof by contradiction due to Euclid. We want to prove that primes are infinite. The opposite of this claim is that they are finite.

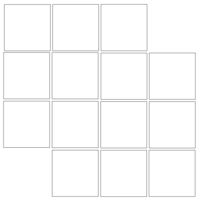
Assume we have a finite number of primes, let's call them $p_1, p_2, \ldots, p_k$ (in ascending order). Construct the following integer

$$n = p_1 p_2 \ldots p_k + 1$$

Every integer can be factored into primes. This integer is not divisible by any prime (because the division will result in a remainder of 1). Therefore, it is either a prime, or must have a prime factor larger than p_k. In both cases, we reach a contradiction because we find yet another prime. Therefore, primes must be infinite.

3 Trap the mouse - another proof by contradiction

Imagine a grid of $n \times n$ squares with two squares missing at $(0,0)$ and $(n-1, n-1)$. The following figure shows the case of $n = 4$.



We have mouse traps with dimensions 1×2 each, so each trap can cover two squares either vertically or horizontally. We want to cover the entire grid with mouse traps. This cannot be done, and we can prove it by contradiction. So let us assume that we can cover the entire grid. We call each square on the grid *even* or *odd*. Square (x, y) is even iff $x + y$ is even; otherwise, it is odd. Every trap must cover one even and one odd square because it must lie either vertically or horizontally and, therefore, either the x coordinates or (exclusive or) the y coordinates of the two squares differ by 1, thus $x+y$ is even of one and odd for the other. This means that we have the same number of even and odd squares; a contradiction since we are missing squares $(0,0)$ and $(n-1, n-1)$, both even, which makes the number of even squares less than the number of odd squares (do a case analysis on n for even or odd).

4 A water juggling puzzle

Here's another setting inspired by Euclid's work. Consider two containers of sizes 4 and 7 units respectively. We can fill these containers with water and, therefore, all we can measure accurately is 4 and 7. However, We would like to juggle water between the two containers to obtain 2 units of water. This problems appears to be abstract, but it is related to the concept of the greatest common divisor. The greatest common divisor of two integers is the largest integer that evenly divides both. The greatest common divisor of 4 and 7 is 1 (verify that this is true). When the greatest common divisor of two integers is 1, we call the integers co-primes or relatively prime. The theory tells us in this case, that we can use 4 and 7 not only to obtain 2 but also to obtain any number from 0 to 6. This is related to the Euclidean algorithm for finding the greatest common divisor and has important application in cryptography. For now, let us just verify that we can obtain 2. We will repeatedly fill the container of size 4 and empty it in the container of size 7. Every time the container of size 7 is full, we empty it. The amount of water in the container of size 7 will progress as follows: 0, 4, 1, 5, 2, 6, 3, and back to 0.

In effect, what we have achieved here is numbers of the form $4r - 7s$, where $r, s \geq 0$. To prove that we can obtain all numbers from 0 to 6, all we have to do is find values for r and s in each case. This is manageable and such an attempt constitutes a proof by case analysis (not by example!). Guided by the above sequence of numbers, here are possible values for r and s:

$$0 = 4(0) - 7(0)$$

$$4 = 4(1) - 7(0)$$

$$1 = 4(2) - 7(1)$$

$$5 = 4(3) - 7(1)$$

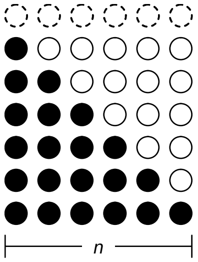
$$2 = 4(4) - 7(2)$$

$$6 = 4(5) - 7(2)$$

$$3 = 4(6) - 7(3)$$

5 What are proofs?

We have seen proofs by contradiction and case analysis in the previous sections. Not all proofs are like that. In fact, here's a proof by picture (which you should try to avoid because a picture could be misleading and might fail to capture the general case).



Based on the picture above,

$$n^2 = (1 + 2 + \ldots + n) + (1 + 2 + \ldots + n - 1)$$

$$= (1 + 2 + \ldots + n) + (1 + 2 + \ldots + n) - n$$

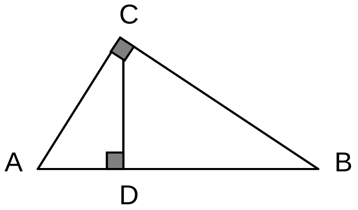
Therefore,

$$2(1 + 2 + \ldots + n) = n^2 + n = n(n + 1)$$

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

So what makes a proof? To answer this question, you might want to see a **false proof** first. Even smart people make mistakes. There are a lot of published false proofs in mathematics. Sometimes we learn from these proof because they give useful ideas. Perhaps the most famous false proof is Kemp's proof of the 4 color theorem: Given any map, the regions can be colored with at most four colors and no two neighboring regions will share the same color. Kemp gave a proof that was deemed false 11 years after it was published! His proof, however, contains the essential ideas that were used in subsequent proofs. In our case, we will not learn much from a false proof now, but it will give some insight about the nature of what a proof really is.

Consider the Pythagoras theorem, most famously know as $c^2 = a^2 + b^2$. I am sure everyone knows this fact, but only few actually know the proof. In fact, there are many proofs for the Pythagoras theorem and you are encourage to find one either on your own or by doing some little research. But here's a false proof:



Assume that the Pythagoras theorem holds. Then $AB^2 = AC^2 + CB^2$. Applying the theorem again on AC^2 and CB^2, we have $AB^2 = CD^2 + AD^2 + CD^2 + DB^2 = AD^2 + DB^2 + 2CD^2$. But the triangles ACD and CBD are similar; therefore $CD/AD = DB/CD$ and hence $CD^2 = AD \cdot DB$. So

$$AB^2 = AD^2 + DB^2 + 2AD \cdot DB = (AD + DB)^2$$

This mean $AB = AD + DB$ which is true.

Why is the above proof false? There is nothing wrong about the sequence of logical implications that we made. Isn't that what a proof is supposed to be? Yes, but one has to understand precisely what the logic of implication is.

Let us start by saying that a proposition can be either true or false, and that given two propositions P and Q, the implication $P \Rightarrow Q$ (P implies Q) is also a proposition that can be either true or false. But here's the catch. If an implication $P \Rightarrow Q$ is true (which is the case for all implications in our proof above), this does not necessarily mean anything about the truth of P or the truth of Q. So, let's look at some logic. Before we do, here's a more obvious example of a false proof. I will prove that $1 = 2$. Assume $1 = 2$. This implies that adding 2 to 1 will have the same result as adding 1 to 2. Therefore, $1 + 2 = 2 + 1$. In other words, $3 = 3$ which is true. Does that prove that $1 = 2$? This is the same type of error done above with one exception: The Pythagoras theorem is true.

6 Some logic

A proposition is either true of false. Here's one:

$$\forall n \in \mathbb{N} \cup \{0\}, n^2 + n + 41 \text{ is a prime number}$$

The symbol $\forall$ is called a quantifier and it signifies "for all". Therefore, the above is stating that for every integer $n \geq 0$, $n^2 + n + 41$ is a prime number. Is this true or false? This is actually true for many values of n. In fact, if you attempt to try it for $n = 0, 1, 2, \ldots$, you will almost believe that it is always true. You will discover that it is false when you get to $n = 40$, because $40^2 + 40 + 41 = 1681 = 41^2$ (not a prime). Interestingly, one can actually prove that no polynomial of the form $a_d n^d + a_{d-1} n^{d-1} + \ldots + a_1 n + a_0$ can produce only primes when $d \geq 1$. Otherwise, it would be really easy to generate large primes (something often required in cryptography). We will later explore practical ways of generating large primes. The following proposition is true:

$$\exists n \in \mathbb{N} \cup \{0\}, n^2 + n + 41 \text{ is a prime number}$$

The symbol $\exists$ is another quantifier and it means "there exists". With this modification, it should be obvious that the proposition is true.

One can use logical operator to create more complex logical statements. The three famous operators are AND denoted by $\wedge$, OR denoted by $\vee$, and NOT, denoted by $\neg$. If we represent false by 0 and true by 1, here are the rules for the three operators (these are called truth tables, and in general one could define other Boolean function in the same way on any number of inputs).

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

P	$\neg P$
0	1
1	0

The operators AND, OR, and NOT are universal in the sense that any Boolean function of any number of inputs can be implemented using those operators. In computer science, we often refer to them as Boolean gates. Boolean gates implement the logic of their corresponding operators by using two levels (digital) of voltages, e.g. Low for 0, and High for 1. For instance, here's how to implement a 1-bit adder (in binary):

0	0	1	1
+ 0	+ 1	+ 0	+ 1
--	--	--	--
00	01	01	10

The most significant bit of the result (the carry) is obviousyly $x \wedge y$. The least significant bit is $(x \wedge \neg y) \vee (\neg x \wedge y)$ (verify).

How do we prove that any Boolean function can be implemented using AND, OR, and NOT gates? I will illustrate this by an example, but the argument can be easily generalized. Consider the following Boolean function of three inputs:

x	y	z	?
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

For each row that evaluates to 1, I will NOT all inputs that correspond to 0, then AND all the inputs, then OR the results of all ANDs.

$$(\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge y \wedge z)$$

Observe that every term between parenthesis evaluates to 1 only when the correct input pattern is provided. Since $(a \wedge b \wedge c)$ is $(a \wedge b) \wedge c$ and similarly $(a \vee b \vee c)$ is $(a \vee b) \vee c$, we can use AND and OR gates with only two inputs.

One could live with either AND gates or OR gates, but will definitely need NOT gates. This can be seen by verifying the following equivalences (the symbol $\Leftrightarrow$ means equivalent and often expressed as **if and only if**, abbreviated **iff**).

$$P \wedge Q \Leftrightarrow \neg(\neg P \vee \neg Q)$$

$$P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$$

Here's the truth table for equivalence:

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

7 What is implication?

Implication is described by the following truth table (it's a relaxation of equivalence):

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

Do not confuse ($P \Rightarrow Q$) with (Q is true). ($P \Rightarrow Q$) is by itself a proposition, different than Q. We often say $P \Rightarrow Q$ (P implies Q) to implicitly mean ($P \Rightarrow Q$) **is true**; still that does not necessarily say anything about the truth of Q. It is not hard to see that

$$(P \Rightarrow Q) \Leftrightarrow \neg P \vee Q$$

In English, $P \Rightarrow Q$ is true iff whenever P is true, Q is true. In other words, either P is false, or else Q is true. The first two rows of the truth table above can be confusing. But as a matter of fact, the implication $P \Rightarrow Q$ is trivially true when P is false. Here's an example that illustrates the idea. Consider the following proposition:

$$\forall n \in \mathbb{Z}, (n \geq 2) \Rightarrow (n^2 \geq 4)$$

One could easily prove this algebraically knowing what we know about algebra. However, let's say that we want to try a few cases first. Which value of n do we start with? Obviously, we will start with 2 because we don't care what happens when $n < 2$. In fact, when $n < 2$ the statement is trivially true! Here's another example that might enlighten the situation. Let's say that I have a principle in life which is to carry an umbrella whenever there is rain. Now, if you see me walking the streets on a sunny day carrying an umbrella, am I violating my principle? Of course not, because nothing I do on a sunny day affects my principle. This is similar to saying $P \Rightarrow Q$ is true whenever P is false.

What about the following proposition?

$$\forall a, b \in \mathbb{Z}, (a/b > 1) \Rightarrow (a > b)$$

While there is no proof by example, there is proof by counter example. We can easily prove that the above proposition is false by providing a counter example: $a = -5$ and $b = -1$.

Looking at the table above, If $P \Rightarrow Q$ is true, and Q is true, nothing can be inferred about the truth of P! That's the flaw in our proof for the Pythagoras theorem. Here are five correct uses of implication (all can be verified from the truth table):

- Modus ponens: If P is true and $(P \Rightarrow Q)$ is true, then Q is true.
- Transitivity: If $(P \Rightarrow Q)$ is true and $(Q \Rightarrow R)$ is true, then $(P \Rightarrow R)$ is true.
- Contrapositive: If $(P \Rightarrow Q)$ is true, then $(\neg Q \Rightarrow \neg P)$ is true. In fact, $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$.
- Counter example: If $P(n)$ is true and $Q(n)$ is false for some n, then $[\forall n, P(n) \Rightarrow Q(n)]$ is false.
- Contradiction: If $(\neg P \Rightarrow \text{false})$ is true, then P is true.

Modus ponens is a mechanism by which we can establish the truth of a proposition Q starting from another proposition P that is known to be true. This is sometimes called a direct proof. The transitive property allows us to collapse a chain of implications to a single implication, as in $P_1 \Rightarrow P_2 \Rightarrow \ldots \Rightarrow P_n$ reduces to $P_1 \Rightarrow P_n$. The contrapositive provides some flexibility in proving that $P \Rightarrow Q$ is true by going the other way from $\neg Q$ to $\neg P$. A counter example is enough to disprove an implication, as we have seen before. Finally, the notion of proof by contradiction lies in the fact that if we start with $\neg P$, and reach through a sequence of true implications a proposition that is false, we know that $\neg P$ must be false. Therefore, P must be true. Proof by contradiction is sometimes called an indirect proof.

Here's a famous proof that $\sqrt{2}$ is irrational, by contradiction: Assume $\sqrt{2} = a/b$ where $a, b \in \mathbb{N}$ (rational). Then $a^2/b^2 = 2$ and $a^2 = 2b^2$. This means a^2 is even which in turn means that a is even. Now $b^2 = a^2/2 = a(a/2)$ is even. This means b is even. Now both a and b are even. This is a contradiction because we could have easily started with a reduced fraction a/b.

Here's a proof by contrapositive: Assume $r > 0$. If r is irrational, then $\sqrt{r}$ is irrational. This is equivalent to saying that if $\sqrt{r}$ is rational, then r is rational. Proving this statement is equivalent to proving to original one. If $\sqrt{r}$ is rational, then $\sqrt{r} = a/b$ where $a, b \in \mathbb{N}$. Therefore, $r = a^2/b^2$, so r is rational.

8 Self reference and diagonalization

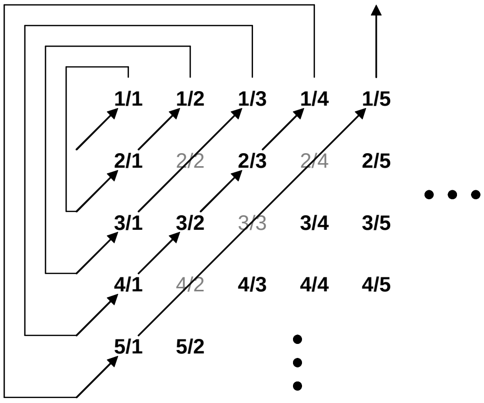
There is a town with a barber who shaves all and only those who do not shave themselves. This sounds like a fairly ordinary statement, but once it is given enough thought, a contradiction will emerge. In fact, such a town does not exist. This can be seen by asking the following question: who shaves the barber? If the barber does not shave himself, then he must shave himself. If the barber shaves himself, then he must not shave himself. The self reference creates the contradiction. There will be no contradiction, however, if the barber is considered not to be among those who live "in town". In other words, the shaving rule would not apply to the barber himself.

Formally, consider a set $S = \{e_0, e_1, e_2, \ldots\}$ where every element $e_i \in S$ must satisfy a property $P(e_i, e_0)$. Further, $P(e, e)$ is false for every e. No such set can be constructed, because the condition fails for e_0. The use of self reference to create a contradiction is at the heart of a proof technique known as diagonalization.

Let's revisit the concept of the size of a set. If we have two infinite sets, how can we tell whether one is larger than the other or whether they are of the same size? Observe that two finite sets have the same size if there exists a one-to-one correspondence between them. This method compares the sizes without explicitly referring to a count of the elements. The idea can be extended to infinite sets. We say that two sets have the same size if and only if there exists a one-to-one correspondence between them (recall that a one-to-one correspondence is a bijection). A set is **countable** if either it is finite or it has the same size as $\mathbb{N}$.

We can show that $\mathbb{E} = \{2, 4, 6, \ldots\}$ is countable. Consider $f : \mathbb{N} \to \mathbb{E}$ such that $f(n) = 2n$. It is obvious that f is a one-to-one correspondence between $\mathbb{N}$ and $\mathbb{E}$. Therefore, the two sets have the same size. This example seems a bit weird. Intuitively, $\mathbb{E}$ is smaller than $\mathbb{N}$ because $\mathbb{E}$ is a proper subset of $\mathbb{N}$. But pairing each number of $\mathbb{N}$ with its own number of $\mathbb{E}$ is possible, so we declare these two sets to be the same size.

Here's a stranger result. Consider the set of positive rational numbers, let's call it $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{N}\}$. $\mathbb{Q}$ seems to be much larger than $\mathbb{N}$, yet these two sets are the same size. The following diagram illustrates a one-to-one correspondence between $\mathbb{Q}$ and $\mathbb{N}$ by making $\mathbb{Q}$ into an infinite ordered list that is guaranteed to contain every element of $\mathbb{Q}$ exactly once. The one-to-one correspondence is given by that order. Make sure you understand why listing $\mathbb{Q}$ row by row for instance will not provide you with the desired one-to-one correspondence.



The set of real numbers is an example of an uncountable set. A real number is one that has a decimal representation, e.g. $\pi = 3.1415926...$ and $\sqrt{2} = 1.4142135...$ are examples of real numbers. Let $\mathbb{R}$ be the set of real numbers. We can prove that $\mathbb{R}$ is uncountable. In other words, we prove that no one-to-one correspondence exists between $\mathbb{N}$ and $\mathbb{R}$. In doing so, we use a proof technique known as the diagonalization method.

Suppose a one-to-one correspondence $f : \mathbb{N} \to \mathbb{R}$ exists. For the sake of illustration, let $f(1) = 3.14159...$, $f(2) = 55.55555...$, $f(3) = 0.12345...$, $f_4 = 0.50000...$, and so on. The following table shows the few values of this correspondence $f : \mathbb{N} \to \mathbb{R}$.

$n \in \mathbb{N}$	$f(n) \in \mathbb{R}$
1	$3.\underline{1}4159...$
2	$55.5\underline{5}555...$
3	$0.12\underline{3}45...$
4	$0.500\underline{0}0...$
$\vdots$	$\vdots$

We construct $x \in \mathbb{R}$ that contradicts the existence of $\mathbb{R}$ in the same way the barber of the town contradicts the existence of the town. We make x a number between 0 and 1, so we are only concerned with the digits following the decimal point, we call them first, second, third, etc... The first digit of x will be different than the first digit of $f(1)$. The second digit of x will be different than the second digit of $f(2)$. The third digit of x will be different than the third digit of $f(3)$. Continuing this way down the **diagonal** of the table for f, we obtain all the digits of x. Now x differs from $f(n)$ in the n^{th} fractional digit (a slight technicality is that numbers such as 0.1999... and 0.2... are equal even though their decimal representations are different; we avoid this problem by never selecting the digits 0 or 9 when we construct x). If x is $f(n)$ for some n, then we have just constructed a set $\mathbb{R}$ that satisfies the following: $x \in \mathbb{R}$ and $r \in \mathbb{R} \Leftrightarrow r \neq x$. This gives a contradiction because the condition fails for x.