Logic and Proofs

Evariste MIGABO. K

July 30, 2025

In this first set of notes, we explore basic proof techniques, and how they can be understood by a grounding in propositional logic. We will show how to use these proof techniques with simple examples, and demonstrate that they work using truth tables and other logical tools.

Definition 1. (Proof). A proof is a sequence of true statements, without logical gaps, that is a logical argument establishing some conclusion.

To prove things, we need to start from some assumptions. These assumptions are known as **axioms**. When we call something an axiom, it does not mean that we take these statements to be true without questioning. Instead, we are saying, "if we assume these axioms, then these results hold." Two people can disagree on what the axioms are and still be friends.

We also tend to define concepts as unambiguously as possible. Of course, just like a dictionary cannot define all words without being circular, we do not define everything in mathematics. To prove things, we have to start somewhere, with some agreed assumptions (axioms). We also don't define everything rigorously (or else how could one start speaking?).

In mathematics, we are often concerned about *truth*. Often, we only care about statements that can take some truth value.

Definition 2. (Statement/ Proposition). A statement (Proposition) is a sentence that can have a true value.

NOTE: Throughout these notes, we will use basic arithmetic properties to demonstrate concepts of proof. We will further develop a set of axioms and structure about arithmetic later; for now, assume that math works the way you think it does.

1 Proving conditional statements

While we have separated out the idea of proving conditional statements into a section here, it is also true that almost every proof you will ever write is, essentially, proving a conditional statement. In general, we have a statement of the form $p \Rightarrow q$, and we wish to prove it is true. Let us consider a simple example to see how we can interpret mathematical statements in this way.

Example 1. Consider the following statement: Let a and b be integers. If a is even and b divides b, then b is also even. We wish to consider how to phrase this as a single conditional statement, $p \Rightarrow q$. Recall that we can think of this as saying "anytime p is true, q must also be true." Hence, we could take the following assignments for the propositional variables:

$$p : (a \text{ and } b \text{ are integers}) \wedge (a \text{ is even}) \wedge (a \text{ divides } b)$$
$$q : b \text{ is even}$$

Then the statement we wish to prove can be interpreted as $p \Rightarrow q$ with these propositional variable assignments.

The direct approach to proving a statement like the one in Example 1 generally looks as follows: assume proposition p to be true, and by following a sequence of logical steps, demonstrate that proposition q must also be true. Fundamentally this structure relies on the following theorem:

Theorem 1. $[(p \Rightarrow r) \wedge (r \Rightarrow q)] \Rightarrow [p \Rightarrow q]$

Proof. To prove this theorem, we wish to show that the above proposition is always true. Recall that the conditional statement $p \Rightarrow q$ can be written as $\neg p \vee q$. Hence, we can rewrite the entire structure above as follows:

$$\begin{aligned}[(p \Rightarrow r) \wedge (r \Rightarrow q)] \Rightarrow [p \Rightarrow q] &= [(\neg p \vee r) \wedge (\neg r \vee q)] \Rightarrow (\neg p \vee q) \\ &= \neg[(\neg p \vee r) \wedge (\neg r \vee q)] \vee (\neg p \vee q) \\ &= \neg(\neg p \vee r) \vee \neg(\neg r \vee q) \vee (\neg p \vee q) \\ &= (p \wedge \neg r) \vee (r \wedge \neg q) \vee (\neg p \vee q).\end{aligned}$$

(by DeMorgan's Laws)

Hence, in order to prove the theorem true, it suffices to show that $(p \wedge \neg r) \vee (r \wedge \neg q) \vee (\neg p \vee q)$ is a tautology. We consider a truth table:

p	q	r	$p \wedge \neg r$	$r \wedge \neg q$	$(p \wedge \neg r) \vee (r \wedge \neg q)$	$\neg p \vee q$	$(p \wedge \neg r) \vee (r \wedge \neg q) \vee (\neg p \vee q)$
T	T	T	F	F	F	T	T
T	T	F	T	F	T	T	T
T	F	T	F	T	T	F	T
T	F	F	T	F	T	F	T
F	T	T	F	F	F	T	T
F	T	F	F	F	F	T	T
F	F	T	F	T	T	T	T
F	F	F	F	F	F	T	T

Therefore, the statement of the theorem is logically equivalent to a tautology, and thus it is itself a tautology. Therefore the theorem is true.
This may seem like a silly thing to prove, but it is essentially the crux of all mathematical proof. The idea being that if you wish to show that $p \implies q$ is true, it can be done by taking a series of implications, taking the form:

$$p \implies r_1, r_1 \implies r_2, r_2 \implies r_3, \ldots, r_{k-1} \implies r_k, r_k \implies q.$$

The previous theorem demonstrates that this is sufficient to prove the statement $p \implies q$. In general, we hope to take these intermediary propositions to be clearly true, or previously proven to be true. Hence, our basic direct proof structure will look as follows:

Direct Proof of $p \Rightarrow q$

1. Assume p to be true.
2. Conclude that r_1 must be true (for some r_1).
3. Conclude that r_2 must be true (for some r_2).
4. $\vdots$
5. Conclude that r_k must be true (for some r_k).
6. Conclude that q must be true.

I will note here that typically, we do not frame a mathematical proof using propositional logic. But the structure of propositional logic is what allows us to determine that the above described method of proving a statement will, in fact, work. Let us consider how this structure might look by returning to Example 1. We shall first write a proof of the statement in this example in the format given above, then reform it to comport with a traditional proof style.
Example 1. continued. Recall the statement we wish to prove:

Let a and b be integers. If a is even and a divides b, then b is also even.

The structure described above indicates that we can approach this proof by assuming p (as described previously) to be true, and following a series of conclusions until we can conclude that q is also true.

1. Assume p is true, so that a and b are integers, a is even, and $a \mid b$.
2. By definition, there exists an integer k with $a = 2k$, and there exists an integer ℓ with $b = a\ell$.
3. By substitution, we can write $b = a\ell = (2k)\ell = 2(k\ell)$.
4. Since $b = 2(k\ell)$, b is even.

In the above example, we can view the statements written in steps 2 and 3 as r_1 and r_2, and we note that each of these implications is clearly true by definition or basic multiplication properties. Structurally, this follows the basic idea described in our Direct Proof method: we can easily observe the implications $p \Rightarrow r_1$, $r_1 \Rightarrow r_2$, and $r_2 \Rightarrow q$. Chaining them together proves the entire statement.

Contentwise, the proof given here is excellent. However, it does not comport with standard mathematical style: a typical proof will omit the enumeration and present the proof as a single paragraph.

> Assume p is true, so that a and b are integers, a is even, and $a \mid b$. By definition, there exists an integer k with $a = 2k$, and there exists an integer ℓ with $b = a\ell$. By substitution, we can write $b = a\ell = (2k)\ell = 2(k\ell)$. Since $b = 2(k\ell)$, b is even.

Before we go further, let's take a look at one more example to be sure we understand the fundamental idea here.

Example 2. *Let a and b be real numbers. If a is rational and b is rational, then $a+b$ is also rational.*

Proof. Assume that a and b are real numbers, and that both a and b are rational. By definition, there exist integers n_1, d_1, n_2, and d_2 such that $a = \dfrac{n_1}{d_1}$ and $b = \dfrac{n_2}{d_2}$. Therefore, we can write:

$$a+b = \frac{n_1}{d_1} + \frac{n_2}{d_2}.$$

Multiplying by 1 in the form of $\dfrac{d_2}{d_2}$ and $\dfrac{d_1}{d_1}$, we get:

$$a+b = \frac{n_1 d_2}{d_1 d_2} + \frac{n_2 d_1}{d_1 d_2} = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}.$$

Since $n_1 d_2 + n_2 d_1$ and $d_1 d_2$ are both integers, it follows that $a+b$ is a ratio of two integers. Thus, by definition, $a+b$ is rational.

A quick note: formally speaking, each equality sign in the above equation represents a separate proposition, which is why the sentence including these equalities has a separate justification for their truth. Now that we have a few proofs under our belt, let's discuss some good proofwriting rules of thumb that you may have noticed in the above examples.

Good Proofwriting Tips

1. Proofs should be composed of sentences that include verbs, nouns, and grammar
2. Never start a sentence with a mathematical symbol. In other words, always start a sentence with a word. This is to avoid confusion, as "." can also be a mathematical symbol, so you don't want people to believe you are performing multiplication when you are simply ending a sentence and beginning another.
3. When drawing a conclusion, it is generally good form to give a reason for that conclusion. You see above things like "by definition," "by arithmetic rules," etc. This can help explain the intermediary conclusions of the proof. If you can't come up with a reason like this for something to be true, it may not be a fair conclusion to draw.
4. If you'd like to introduce a new symbol, you should clearly define what kind of thing it is. For example, in the proofs in Examples 1 and 2, we introduced variables and specified that these variables represented integers.

We will add to these tips as we continue these notes.

One more quick note about the method of direct proof. We have phrased this method as a chain of implications $p \Rightarrow r_1$, $r_1 \Rightarrow r_2, \ldots, r_k \Rightarrow q$, but in fact we can do a bit better, and already have, in Example 2. When we begin, we assume p, and then prove r_1 to be true. But for the next implication, we need not prove that $r_1 \Rightarrow r_2$, but actually that $(p \wedge r_1) \Rightarrow r_2$. This is clearly sufficient, since we still know p to be true, so we have both the information from p and the information from r_1 available to draw the next conclusion.

You'll note that we used this type of structure in the proof shown in Example 2; we used the fact that

$$a+b = \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}$$

and the fact that $n_1d_2 + n_2d_1$ and d_1d_2 are integers to draw our final conclusion, using information from multiple previous propositions.

2 Proving biconditional statements (If and Only If)

Recall, a biconditional statement is a statement of the form $p \iff q$. As noted at the end of the previous set of notes, we have that $p \iff q$ is logically equivalent to $(p \implies q) \wedge (q \implies p)$. Hence, we can approach a proof of this type of proposition effectively as two proofs: prove that $p \implies q$ is true, **and** prove that $q \implies p$ is true. Indeed, it is common in proofs of biconditional statements to mark the two proofs using the symbols ($\implies$) and ($\impliedby$), to indicate $p \implies q$ and $p \impliedby q$, respectively. It is also common to refer to these types of statements as "if and only ifs," a silly but functional nounification of the operator $\iff$. It is also common to refer to the two parts of the proof as "directions," with $p \implies q$ called the *forward direction* and $p \impliedby q$ called the *backward direction*.

A useful note for proving $\iff$ statements, compared to $\implies$ statements as in the previous section. Typically, in a statement of a proof, there are a set of assumptions given prior to the statement of the proposition to be proven, often defining variables and terms. In the case of a simple conditional statement, we lumped these assumptions in with the proposition p. In a biconditional statement, these assumptions are true for both directions of the proof.

We first consider a simple example.
Example 3. Prove the following statement.
Let x be a real number. Define $\lceil x \rceil$ to be the smallest integer greater than or equal to x, and define $\lfloor x \rfloor$ to be the largest integer less than or equal to x. Then x is an integer if and only if $\lceil x \rceil = \lfloor x \rfloor$.

The first step here is to identify which assumptions will be true throughout the proof. Notice the word "then" at the beginning of the last sentence. It is common to use this word to indicate the statement to be proven, rather than assumptions made. So here, we have that everything written prior to the word "then" is an assumption that will be true throughout the proof, and everything written after the word "then" is something that requires proof.

The words "if and only if" indicate a biconditional statement: x is an integer $\iff \lceil x \rceil = \lfloor x \rfloor$. As we will do here, we can first do some "pre-processing" of assumptions before we dive into the meat of the two main parts of the proof.

Proof: Take x, $\lceil x \rceil$, and $\lfloor x \rfloor$ as defined in the statement of the proposition. Note that, by definition, we must have:

$$\lfloor x \rfloor \leq x \leq \lceil x \rceil.$$

($\Rightarrow$) Assume that x is an integer. Then, since $x \leq x$, the smallest integer greater than or equal to x is x itself, so $\lceil x \rceil = x$. Likewise, the largest integer less than or equal to x is also x, so $\lfloor x \rfloor = x$. Therefore, $\lceil x \rceil = \lfloor x \rfloor$.

($\Leftarrow$) Assume that $\lceil x \rceil = \lfloor x \rfloor$. Then since $\lfloor x \rfloor \leq x \leq \lceil x \rceil$, and $\lceil x \rceil = \lfloor x \rfloor$, we must have:

$$\lfloor x \rfloor = x = \lceil x \rceil.$$

Since $\lfloor x \rfloor$ is an integer by definition and $\lfloor x \rfloor = x$, it follows that x is an integer. ■

We note that each of the two propositions to be proved above—both the forward and backward directions—are treated separately as simple conditional statements, and the method of **direct proof** described in the previous section is used for each of them.

As we develop further proof techniques below, any one of these techniques can be applied to either of these two propositions.
Occasionally, a biconditional statement may be *hiding* inside a problem, waiting to be found. Consider, for example, the following.

Example 4. Find all real solutions x to the equation $x^2 - 2x = 0$.

Solution. First, consider that if x is a solution to the equation, we have that

$$x^2 - 2x = 0 \Rightarrow x(x-2) = 0 \Rightarrow x = 0 \text{ or } x = 2.$$

(You may be tempted to stop right here, but this is insufficient. All that has been demonstrated is that solutions must take the form $x = 0$ or $x = 2$, but we need to also verify that these are, in fact, solutions to the given equation. Indeed, what we have proven thus far is a conditional statement:

$$x \text{ is a solution} \Rightarrow x = 0 \text{ or } x = 2,$$

but we need a **biconditional** statement here.)

Moreover, we find that:

- If $x = 0$, then $x^2 - 2x = 0 - 0 = 0$;
- If $x = 2$, then $x^2 - 2x = 4 - 4 = 0$.

Hence, we conclude that:

$$x \text{ is a real-valued solution to } x^2 - 2x = 0 \iff x = 0 \text{ or } x = 2.$$

In this example, we see a **biconditional statement** hiding inside an innocuous-looking algebra problem. The problem asks us to find all real-valued solutions to an equation, which means we must do two things: we must figure out what the solutions are, and we must determine that these are *all* possible solutions.

By showing only the first part—that a solution takes the form of $x = 0$ or $x = 2$, we haven't done enough to ensure that these are even solutions at all. We have effectively done only the second part of the question: we have found that these are the *only possible* solutions, but we haven't checked whether they are *in fact* solutions.
While this may seem like a minor point, consider the following example.

Example 5. Find all real solutions x to the equation $x + \sqrt{2x} = 0$.

Solution. First, consider that if x is a solution to the equation, we have:

$$x + \sqrt{2x} = 0 \Rightarrow x = -\sqrt{2x} \Rightarrow x^2 = 2x \quad \text{(by squaring both sides)} \Rightarrow x = 0 \text{ or } x = 2 \quad \text{(by Example 4)}.$$

Moreover, we find that:

- If $x = 0$, then $x + \sqrt{2x} = 0 + 0 = 0$.
- If $x = 2$, then $x + \sqrt{2x} = 2 + \sqrt{4} = 2 + 2 = 4 \neq 0$.

Hence, x is a real-valued solution to $x + \sqrt{2x} = 0$ **if and only if** $x = 0$.
Here, the verification of the solution is critical. If we only took the first part of the problem, we would have found an incorrect set of solutions. To add to our good proofwriting guidelines, we have the following:

Good Proofwriting Tips

5. When proving a biconditional statement, clearly communicate when you are proving each direction.

To demonstrate the above, we give one final example of proof using a biconditional, in part because it is a classic example, and in part because it demonstrates the value of pre-processing the assumptions prior to delving into the two directions of the proof.

Example 6. Let n be a positive integer. Prove that n is divisible by 3 if and only if the sum of the base-10 digits of n is divisible by 3.

Proof. Let n be a positive integer, and write $n = d_n d_{n-1} d_{n-2} \cdots d_1 d_0$ in its base-10 expansion, so each d_i is between 0 and 9. Note that this is equivalent to writing

$$n = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10^1 + d_0 10^0.$$

By performing some algebra, we can write

$$\begin{aligned} n &= d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10^1 + d_0 10^0 \\ &= d_n (10^n - 1) + d_{n-1} (10^{n-1} - 1) + \cdots + d_1 (10^1 - 1) + (d_n + d_{n-1} + \cdots + d_1 + d_0). \end{aligned}$$

Notice that $10^1 - 1 = 9, 10^2 - 1 = 99, \ldots, 10^n - 1 = 99 \cdots 9$, where there are n 9s in the final expression. Hence, $10^n - 1 = 3(33 \cdots 3)$ for any choice of n, where there are n 3s in the parenthesized number. Therefore, $10^n - 1$ is

divisible by 3 for each n. By rules of arithmetic, that implies $d_n(10^n-1)+d_{n-1}(10^{n-1}-1)+\cdots+d_1(10^1-1)$ is also divisible by 3, since each term of the sum is divisible by 3. Hence, there exists an integer k such that $d_n(10^n-1)+d_{n-1}(10^{n-1}-1)+\cdots+d_1(10^1-1)=3k$, and therefore we may write n as

$$n = 3k+(d_n+d_{n-1}+\cdots+d_1+d_0).$$

Now, we wish to prove that n is divisible by 3 if and only if $d_n+d_{n-1}+\cdots+d_1+d_0$ is also divisible by 3.

($\Rightarrow$) Suppose that n is divisible by 3. Then there is an integer j so that $n=3j$. Therefore, we have

$$3j = 3k+(d_n+d_{n-1}+\cdots+d_1+d_0) \Rightarrow d_n+d_{n-1}+\cdots+d_1+d_0 = 3(j-k),$$

so $d_n+d_{n-1}+\cdots+d_1+d_0$ is also divisible by 3.

($\Leftarrow$) Suppose that $d_n+d_{n-1}+\cdots+d_1+d_0$ is divisible by 3. Then there exists an integer m so that $d_n+d_{n-1}+\cdots+d_1+d_0=3m$. Therefore, we have

$$n = 3k+(d_n+d_{n-1}+\cdots+d_1+d_0) = 3k+3m = 3(k+m),$$

so n is also divisible by 3.

Since both directions are true, the biconditional statement is therefore true. ■

3 Proof by contradiction

Now that we have a basic understanding of direct proof methods for conditional and biconditional statements, we will develop some more sophisticated approaches to proof. We begin here with the method of proof by contradiction.

3.1 Proving nonconditional propositions with contradiction

In general, to prove a proposition p by contradiction, we assume that p is false, and use the method of direct proof to derive a logically impossible conclusion. Essentially, we prove a statement of the form $\neg p \Rightarrow q$, where q is never true. Since q cannot be true, we also cannot have $\neg p$ is true, since $\neg p \Rightarrow q$. Therefore, if $\neg p$ is false, we must have that p is true, completing the proof of proposition p. Let's look at a few examples to understand this method more fully.

Example 7. Prove the following proposition: There are no integers a,b for which $2a+4b=1$.

Proof. Suppose the proposition is false, so that there are integers a,b for which $2a+4b=1$. Dividing both sides of this equation by 2, we conclude that $a+2b=\frac{1}{2}$. Since a and b are integers, $a+2b$ is also an integer. But $\frac{1}{2}$ is not an integer, so this is impossible. Therefore, the proposition cannot be false, so it must be true. ■

Example 8. Prove the following proposition: There is no smallest positive rational number.

Proof. Suppose that the proposition is false, and there is a smallest positive rational number. Let k be the smallest positive rational number, so there are positive integers a,b such that $k=\frac{a}{b}$. Consider $t=\frac{k}{2}=\frac{a}{2b}$. Notice that since a,b are integers, we also have $a,2b$ are integers, so t is rational. Also, since a,b are positive, we have that t is positive, and that $t<k$. Therefore, t is a smaller positive rational number than k. Since k is assumed to be the smallest positive rational number, we have arrived at a logically impossible conclusion. Therefore, the proposition cannot be false, and thus must be true. ■

Both Examples 7 and 8 have something in common: the proposition we wish to prove is asserting a negative. That is, in both cases, we wish to prove that something does NOT happen. This gives us a clue that we might consider contradiction as a proof technique. In general, recognizing that a proof should be pursued by contradiction can be a bit tricky, but it is often used in this type of case. It's also useful to note that this can be hidden; for example, using terms like "irrational" or "irregular" usually implies contradiction as a viable proof technique, since the definitions of these terms are themselves negative: something is irrational if it is NOT rational, etc.

In general, a proof by contradiction follows this basic structure:

Proof of p by contradiction

1. Assume p is false.
2. Follow the method of Direct Proof to conclude that q must be true (for some q that is observably false).
3. Conclude that p cannot be false.
4. Conclude that p is therefore true.

We close this section with a classic proof by contradiction. This proof will rely on the following proposition

Proposition 1. Let n be an integer. If n^2 is even, then n is also even.

We leave the proof of Proposition 1 as an exercise, but will use this proposition in the proof in Example 9. The proof of Proposition 1, itself, could be done by contradiction, following the technique that will be laid out in Section 3.2.

Example 9. $\sqrt{2}$ is irrational.

Proof. Suppose that the proposition is false, so $\sqrt{2}$ is rational. Then there exist integers a, b so that $\sqrt{2} = \frac{a}{b}$. We assume that a and b are chosen to have no common factors; that is, the rational $\frac{a}{b}$ is in lowest terms. By squaring both sides, we therefore have that $2 = \frac{a^2}{b^2}$, so $2b^2 = a^2$. Therefore, a^2 is even, and hence a must also be even. Thus, there exists an integer k so that $a = 2k$, and $a^2 = 4k^2$. We therefore have that $2b^2 = a^2 = 4k^2$, and dividing by 2 yields $b^2 = 2k^2$. Therefore, b^2 is even, and hence b must also be even. Since a and b are both even, they are both divisible by 2. But by assumption, a and b have no common factors, so this is impossible. Therefore, it cannot be the case that the proposition is false, so it must be true. Thus $\sqrt{2}$ is irrational.■

3.2 Proving conditional propositions with contradiction

As with proving simple conditional statements, we wish to prove a statement of the form $p \Rightarrow q$. Recall from the last set of notes that this statement is logically equivalent to $(\neg p) \vee q$. Now, we can rewrite this as follows:

$$\begin{aligned}(\neg p) \vee q &= \neg(\neg(\neg p) \vee q) \\ &= \neg(\neg(\neg(p) \vee q)) \\ &= \neg(p \wedge \neg q) \quad \text{(by De Morgan's Laws)}\end{aligned}$$

That is to say, $p \Rightarrow q$ is true if and only if $p \wedge (\neg q)$ is false. This allows us to rephrase any conditional proposition as a negative, and apply the strategy of proof by contradiction as in the previous section. In general, this is done by assuming that $p \wedge (\neg q)$ is true, and arriving at a logically impossible conclusion. Since $p \wedge (\neg q)$ is true is therefore impossible, it must be the case that $p \wedge (\neg q)$ is false, just like we desired.

In plain English, if $p \Rightarrow q$ is true, we must have that every time p is true, q is also true. Proof by contradiction assumes p is true but q is false, and arrives at a logically impossible conclusion. Therefore, if p is true, it must be that q is also true, since q being false is logically impossible.

Before we outline the strategy in general, we begin with a small example.

Example 10. Let n be an integer. If $n^2 + 5$ is odd, then n is even.

Proof. Suppose, for the sake of contradiction, that $n^2 + 5$ is odd and n is also odd. By definition, then, there exist integers k and ℓ so that $n^2 + 5 = 2k + 1$ and $n = 2\ell + 1$. Hence, we have

$$\begin{aligned}2k + 1 &= n^2 + 5 \\ &= (2\ell + 1)^2 + 5 \\ &= 4\ell^2 + 4\ell + 1 + 5 \\ &= 2(2\ell^2 + 2\ell + 3).\end{aligned}$$

Therefore, $2k + 1$ is even. This is clearly impossible, and hence we cannot have that $n^2 + 5$ is odd and n is also odd. Therefore, if that $n^2 + 5$ is odd, we must have n is even.■

In general, the strategy for proving conditional propositions using contradiction looks as follows:

Proof of $p \implies q$ by contradiction

1. Assume p is true, and q is false.
2. Follow the method of Direct Proof to conclude that r must be true (for some r that is observably false).
3. Conclude that if p is true, q cannot be false.
4. Conclude that anytime p is true, q is also true, and thus $p \Rightarrow q$.

Example 11. Prove the following proposition: Let a and b be integers. If $a \geq 2$, then a does not divide one of b and $b+1$.

Proof. Suppose, for the sake of contradiction, that $a \geq 2$ but a does divide both of b and $b+1$. Then there are integers k, ℓ such that $b = ak$ and $b+1 = a\ell$. By substitution, we thus have $ak+1 = a\ell$, so $1 = a(\ell - k)$. Because $a \geq 2$, we have that $a \neq 0$, so we can divide by a on both sides, to obtain $\frac{1}{a} = \ell - k$. Since ℓ and k are integers, $\ell - k$ is also an integer, but since $a \geq 2$, $\frac{1}{a}$ is not an integer. This is impossible. Therefore, it must be that if $a \geq 2$, a must not divide at least one of b and $b+1$. ■

Example 12. Prove the following proposition:

If a, b, c are all odd integers, then there is no rational x such that $ax^2 + bx + c = 0$.

Proof. Suppose, for the sake of contradiction, that a, b, and c are all odd integers, and that there exists a rational number x such that

$$ax^2 + bx + c = 0.$$

Let $x = \frac{k}{\ell}$ where $k, \ell \in \mathbb{Z}$, $\ell \neq 0$, and $\gcd(k, \ell) = 1$ so that x is in lowest terms.

Substituting into the equation gives:

$$a\left(\frac{k}{\ell}\right)^2 + b\left(\frac{k}{\ell}\right) + c = 0 \quad \Rightarrow \quad a\frac{k^2}{\ell^2} + b\frac{k}{\ell} + c = 0.$$

Multiplying both sides by ℓ^2, we obtain:

$$ak^2 + bk\ell + c\ell^2 = 0.$$

The right-hand side is 0, an even number, so the left-hand side must also be even. Now observe:

- a, b, and c are all odd, - so ak^2, $bk\ell$, and $c\ell^2$ are all odd if k and ℓ are odd, - thus their sum would be odd + odd + odd = odd, which contradicts the left-hand side being even.

Hence, in order for the sum to be even, k and ℓ must both be even. But this contradicts the assumption that $\gcd(k, \ell) = 1$.

Therefore, no such rational x can exist. That is, if a, b, and c are all odd integers, then there is no rational solution to $ax^2 + bx + c = 0$. ■

note on the previous example: if you are not convinced by the assertion that k and ‘ must both be even, then you should prove it! This proof itself can be done by contradiction: you wish to prove that a, b, c are odd integers, k and l are integers, and $ak^2 + bkl + cl^2 = 0$ implies k and l are even. Assume that they are not; then one of them (at least) is odd, and you can arrive at a contradiction. This portion is not included in the above proof so as not to confuse the structure, but also because it’s a good exercise in ensuring that you understand how to construct a proof by contradiction!
A final note on proof by contradiction: as you may have noticed, all of our proofs by contradiction start with a sentence informing the reader that we are explicitly assuming the statement to be false, or that we plan to proceed by contradiction. This, in general, is standard practice: if you don’t communicate your plan to achieve contradiction, it can be confusing to the reader as to why you have made an assumption that, based on the statement of the desired proposition, seems nonsensical.

Good Proofwriting Tips

6. When proving a statement with the method of contradiction, inform your reader that you are planning to achieve contradiction with an introductory clause such as "Suppose, for the sake of contradiction" or "Suppose the proposition is false," followed by the assumptions you wish to make.

4 Proof by contrapositive

As with proving conditional statements by contradiction, a proof by contrapositive relies on the fact that $p \Rightarrow q$ is logically equivalent to $\neg(p \wedge \neg q)$, but takes a slightly different approach to the proof. Consider:

$$\begin{aligned} p \Rightarrow q &\equiv \neg(p \wedge \neg q) \\ &\equiv \neg(\neg(q \wedge p)) \\ &\equiv \neg(\neg(q \wedge \neg\neg p)) \\ &\equiv \neg q \Rightarrow \neg p \end{aligned}$$

In other words, $p \Rightarrow q$ is true means that if p is true, q is also true. Hence, if q is not true, we cannot have p true. This is the same as saying that $\neg q \Rightarrow \neg p$ is true. The method of proof by contrapositive uses this approach to prove conditional statements. In particular, to prove $p \Rightarrow q$, it is sufficient to prove $\neg q \Rightarrow \neg p$. This can be done by any method, but generally if contrapositive is used a direct proof method follows.

Example 13. Prove the following proposition: Let a, b be integers. If ab is even, then at least one of a or b is even.

Proof. We work by contrapositive. Suppose that a and b are both odd. Then there are integers k and ℓ so that $a = 2k+1$ and $b = 2\ell+1$. Therefore, we have

$$ab = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1,$$

so ab is odd. Thus, by contrapositive, if ab is even, we must have at least one of a or b is even. ■

In general, a proof by contrapositive follows this strategy:

Proof of $p \implies q$ by contrapositive

1. Assume q is false.
2. Follow the method of Direct Proof to conclude that p is also false.
3. Conclude that $\neg q \Rightarrow \neg p$ is true.
4. Since $(\neg q \Rightarrow \neg p) \equiv (p \Rightarrow q)$, conclude that $p \Rightarrow q$ is true.

It is common for students to be confused about the differences between a proof by contrapositive and a proof by contradiction, as in both cases, the first assumption includes the explicit assumption that q is false. However, there is a key difference here. In a proof by contrapositive, you have a specific goal: assuming q is false, you wish to prove that p is false. In a proof by contradiction, you have a nonspecific goal: you assume that q is false and p is true, and wish to arrive at any logically impossible conclusion.
There are a lot of different logically impossible conclusions, so proofs by contradiction have a less clear target than proofs by contrapositive. That said, why would anyone use a proof by contradiction instead of a proof by contrapositive? Since not having a clear goal makes a proof seem, well, harder, why go that route? It's a great question, and I would encourage you, every time you start a proof by contradiction, to think about whether you could just work by contrapositive instead. However, the method of contradiction can be helpful, because you make MORE assumptions at the outset than in a proof by contrapositive. That means that when you start writing conclusions, you have more information to work with than in a proof by contrapositive.

Let's look at another example of proof by contrapositive. In this example, we introduce a useful mathematical tool, namely, "without loss of generality;" more on that after the proof.
Example 14. Prove the following proposition: Let a and b be integers. If $a+b$ is even, then a and b are either both odd or both even.

Proof. We work by contrapositive. Suppose that a and b are not both odd and not both even, so that one of a and b is odd, and the other is even. Without loss of generality (WLOG), suppose that a is odd and b is even. Then there

are integers k and ℓ such that $a = 2k+1$ and $b = 2\ell$. Therefore, $a+b = (2k+1)+2\ell = 2(k+\ell)+1$, so $a+b$ is odd. Hence, by contrapositive, if $a+b$ is even, then a and b are either both odd or both even.

A note here on "without loss of generality": Since it doesn't make a difference to the proof structure which one is odd or even, we can just assign one possibility: if we were wrong, just switch which numbers we label as a and b. The phrase "without loss of generality" generally communicates that we do not lose any abstraction from the problem when we make such a declaration.

Typically, we can WLOG only in the case that all the variables we care about act symmetrically in a proposition. If they play different roles, though, we need to treat each variable differently. If you aren't sure if you can WLOG, then don't. Just write separate proofs for each of the cases; proofs by cases will be discussed more in Section 5. We will see many more examples of WOLOG throughout the class.

5 Proof by cases

Our first look at proof by cases will involve explicitly stated cases in the statement of a proposition. That is, suppose we have a proposition $p \Rightarrow q$, where p itself takes the form $p = r \vee s$, that is, p can be written as a propositional formula using the disjunction operator. If we follow the method of Direct Proof to consider a proposition of this form, we would start by assuming that p is true. But if p is true, that leaves us with two possibilities: either r is true, or s is true, or both. We can break these possibilities up into cases, essentially writing two proofs: one that shows $r \Rightarrow q$ is true, and a second proof that shows $s \Rightarrow q$ is true. By examining the following truth table, we see that $(r \vee s) \Rightarrow q$ is logically equivalent to $(r \Rightarrow q) \wedge (s \Rightarrow q)$, so this approach of proving two separate cases is sufficient to prove the proposition.

r	s	q	$r \vee s$	$(r \vee s) \Rightarrow q$	$r \Rightarrow q$	$s \Rightarrow q$	$(r \Rightarrow q) \wedge (s \Rightarrow q)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

In plain English, if p as a proposition involves an "or" statement, it is sufficient to consider each of the two possibilities for p separately.

Now, most often, a proof by cases does not appear in this format. It is common for the proofwriter to have to define cases themselves, often hinging on some fundamental property of the objects involved. Often, this involves an application of the Law of Excluded Middle. That is, we can think of breaking up according to a proposition r, where we clearly have that $r \vee (\neg r)$ is always true. Think: a number is either negative or nonnegative, an integer is either even or odd, etc.

Example 15. Prove the following proposition: If x is a real number, then $|x+3| - x > 2$.

Proof. We consider two cases: $x \geq -3$ and $x < -3$.

Case 1: $x \geq -3$. Then $|x+3| = x+3$, so we have $|x+3| - x = x+3-x = 3 > 2$, so the proposition holds.

Case 2: $x < -3$. Then $|x+3| = -(x+3)$, so we have $|x+3| - x = -3-x-x = -3-2x$. Since $x < -3$, we must have $-x > 3$, so $-3-2x > -3+2(3) = 3 > 2$. Therefore, the proposition holds.

Since the proposition holds in all cases, it must be true that if x is a real number, then $|x+3| - x > 2$. ■

In the above example, there is a clear reason to break out the proof by cases. We know that the absolute value function itself involves cases: we take one number if the argument is nonnegative, and a second number if the argument is negative. Hence, it seems sensible to consider a proof by cases.

In some circumstances, though, using only two cases may not be enough. In some circumstances, we may wish to divide proposition p up into a variety of cases, and prove each of these separately. This is also acceptable, as we

will see in the next example; so long as we can be sure that $p = r_1 \vee r_2 \vee \cdots \vee r_k$, then we will have

$$p \Rightarrow q \equiv (r_1 \vee r_2 \vee \cdots \vee r_k) \Rightarrow q \equiv (r_1 \Rightarrow q) \wedge (r_2 \Rightarrow q) \wedge \cdots \wedge (r_k \Rightarrow q),$$

that is, we can prove each $r_i \Rightarrow q$ independently.

Example 16. Prove the following proposition:
Given real numbers a and b, define the operation $a \mathbin{@} b = \max\{a,b\}$; that is,

$$a \mathbin{@} b = \begin{cases} a & \text{if } a \geq b, \\ b & \text{otherwise.} \end{cases}$$

Then, for all real numbers a, b, and c, we have

$$(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} (b \mathbin{@} c).$$

Proof. Suppose $a,b,c \in \mathbb{R}$. We consider all possible orderings of a,b,c. There are six distinct orderings:

- **Case 1:** $a \leq b \leq c$.
  Then $a \mathbin{@} b = b$, $b \mathbin{@} c = c$, and $a \mathbin{@} c = c$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = b \mathbin{@} c = c = a \mathbin{@} c = a \mathbin{@} (b \mathbin{@} c).$$

- **Case 2:** $a \leq c \leq b$.
  Then $a \mathbin{@} b = b$, $b \mathbin{@} c = b$, and $a \mathbin{@} c = c$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = b \mathbin{@} c = b = a \mathbin{@} b = a \mathbin{@} (b \mathbin{@} c).$$

- **Case 3:** $b \leq a \leq c$.
  Then $a \mathbin{@} b = a$, $b \mathbin{@} c = c$, and $a \mathbin{@} c = c$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} c = c = a \mathbin{@} (b \mathbin{@} c).$$

- **Case 4:** $b \leq c \leq a$.
  Then $a \mathbin{@} b = a$, $b \mathbin{@} c = c$, and $a \mathbin{@} c = a$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c).$$

- **Case 5:** $c \leq a \leq b$.
  Then $a \mathbin{@} b = b$, $b \mathbin{@} c = b$, and $a \mathbin{@} c = a$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = b \mathbin{@} c = b = a \mathbin{@} b = a \mathbin{@} (b \mathbin{@} c).$$

- **Case 6:** $c \leq b \leq a$.
  Then $a \mathbin{@} b = a$, $b \mathbin{@} c = b$, and $a \mathbin{@} c = a$.
  Thus,
  $$(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c).$$

Since the equality $(a \mathbin{@} b) \mathbin{@} c = a \mathbin{@} (b \mathbin{@} c)$ holds in all cases, the proposition is true for all real numbers a, b, and c. ■

This may seem like a lot of work to do in a case like this (and it is!), which is why proof by cases is sometimes called "Proof by Exhaustion."

In general, proof by cases looks as follows:

Direct Proof of $p \Rightarrow q$ by cases

1. Write $p \equiv r_1 \vee r_2 \vee \cdots \vee r_k$.
2. Separately prove $r_i \Rightarrow q$ for each i, using any method.
3. Conclude that $p \Rightarrow q$, since $p \Rightarrow q \equiv (r_1 \Rightarrow q) \wedge (r_2 \Rightarrow q) \wedge \ldots (r_k \Rightarrow q)$.

A word of caution! If you're going to use proof by cases, you should be absolutely sure that all cases are covered. For example, if you have a statement about a real number a, and you split into the cases that a is positive or a is negative, this is not sufficient; you have not considered the case that $a = 0$. So please be careful with how cases are defined, and ensure that all possibilities are met.

As with the above examples, it is generally good form to announce that you are considering cases, and clearly label what those cases are.

Good Proofwriting Tips

7. When proving by cases, clearly communicate to the reader that cases will be considered, and label the cases as they occur. Tell the reader how you will split by cases before you do it.

6 Well-ordering and induction

The Well-Ordering Property. Every nonempty set of nonnegative integers has a least element.

The well-ordering property can often be used directly in proofs.

(Weak Principle of Induction). Let $P(n)$ be a statement about the natural number n. Suppose that:

1. $P(1)$ is true,
2. $\forall n,\ P(n) \implies P(n+1)$.

Then $P(n)$ is true for all $n \geq 1$.

Example 18. Show that if n is a positive integer, then

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

proof. Let $P(n)$ be the proposition that the sum of the first n positive integers,

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

We must do two things to prove that $P(n)$ is true for $n = 1,2,3,\ldots$: namely, show that $P(1)$ is true, and that the conditional statement $P(k) \implies P(k+1)$ is true for $k = 1,2,3,\ldots$.

Basis step: $P(1)$ is true because

$$1 = \frac{1(1+1)}{2},$$

since 1 is the sum of the first positive integer. The right-hand side is found by substituting 1 for n in $\frac{n(n+1)}{2}$.

Inductive step: Assume $P(k)$ holds for an arbitrary positive integer k, i.e.,

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

Under this assumption, we must show that $P(k+1)$ is true, namely,

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

Adding $k+1$ to both sides of the equation in $P(k)$ gives:

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

This shows that $P(k+1)$ is true under the assumption that $P(k)$ is true. This completes the inductive step.

Since we have completed both the basis step and the inductive step, by mathematical induction we conclude that $P(n)$ is true for all positive integers n. That is, we have proven

$$1+2+\cdots+n=\frac{n(n+1)}{2}, \text{ for all positive integers } n \text{ .}\blacksquare$$

As noted, mathematical induction is not a tool for discovering theorems about all positive integers, but rather a proof method to confirm results once they are conjectured.

(Strong Principle of Induction). Let $P(n)$ be a statement about $n \in \mathbb{N}$. Suppose that:

1. $P(1)$ is true,
2. For all $n \in \mathbb{N}$, if $P(k)$ is true for all $k < n$, then $P(n)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 19. Given $n \in \mathbb{N}$, define a_n recursively as follows:

$$a_0 = 1, \quad a_1 = 3, \quad a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 2.$$

Prove that for all $n \geq 0$, we have

$$a_n = 2n+1.$$

Proof. We proceed by strong induction on n.

Base cases:

- For $n = 0$, we have $a_0 = 1 = 2 \cdot 0 + 1$, so the result holds.
- For $n = 1$, we have $a_1 = 3 = 2 \cdot 1 + 1$, so the result holds.

Inductive step: Assume that for some $n \geq 1$, we have

$$a_k = 2k+1 \quad \text{for all } 0 \leq k \leq n.$$

We want to show that $a_{n+1} = 2(n+1)+1$.

Using the recursive definition:

$$a_{n+1} = 2a_n - a_{n-1}.$$

By the inductive hypothesis:

$$a_n = 2n+1, \quad a_{n-1} = 2(n-1)+1 = 2n-2+1 = 2n-1.$$

Substituting in:

$$a_{n+1} = 2(2n+1) - (2n-1) = 4n+2-2n+1 = 2n+3 = 2(n+1)+1.$$

Thus, the result holds for $n+1$. We conclude that by the Principle of Strong Induction, for all $n \geq 0$,

$$a_n = 2n+1. \quad \blacksquare$$

7 Variables and quantification

We end this set of notes on proofwriting techniques with a conversation about variables. Throughout these notes, to this point, we have seen variables show up without yet having a robust discussion on how to determine what kinds of values these variables might take. At the very beginning of the first set of notes, we mentioned the need to clearly define all variables involved in a problem, and we have seen that throughout these notes: each time a letter appears, it is specified what kind of value it can take (an integer, a rational, etc.).

7.1 Universal quantification

For most of our work to this point, our variables have been permitted to take any value in the set from which they came, i.e., they could be any integer, any odd integer, etc. Let's formalize this a bit.

Definition 3. Given a variable x, the range of x is the set of possible values that x can take. If the range is X, we write $x \in X$ to indicate that x is a member of X. If x is permitted to take any value in its range, then we say that x is universally quantified.

In most of our examples to this point, then, we have used universal quantification. That is, we have phrased our propositions in the form "Let x be in range X. Then [proposition about x]." Here are several other, common rephrasings of this proposition:

- Let $x \in X$. Then [proposition about x].
- For all $x \in X$. [proposition about x].
- Given $x \in X$. [proposition about x].

All of these constructions indicate that the proposition we wish to prove is universally true, that is, it applies to every member of the range, no matter what it looks like. In all of these cases, our proofs can use no information about x beyond the fact that it is a member of the specified range.

Symbolically, we express universal quantification with the symbol $\forall$. This symbol is read as "for all" or "for any." So we could express the statement

$$\text{Let } a, b \text{ integers. Then } a+b \text{ is also an integer.}$$

using the symbols

$$\forall a, b \in \mathbb{Z}, a+b \in \mathbb{Z}.$$

[Here $\mathbb{Z}$ is a symbol representing the set of integers. More on that later.]

In the setting of propositional logic, now that we have a better understanding of universal quantification, we can rephrase many things that we have previously considered as conditional propositions as nonconditional, universally quantified propositions.

For example, consider the proposition

$$\text{For all integers } a,\ a^2+a \text{ is even.}$$

Up until now, we may have viewed this as conditional, under the structure p: "a is an integer", q: "a^2+a is even," we can see this statement as $p \Rightarrow q$. However, we could redefine this structure by taking a logical proposition that has a variable; that is, let $p(a)$ be the logical statement a^2+a is even. We can then rephrase the structure of this proposition as

$$\forall a \in \mathbb{Z}, p(a).$$

In this way we can see many of the propositions we have handled thus far as in fact propositional formulae containing variables, as above. Formally, we have the following

Definition 4. Let $p(x)$ be a logical formula that takes a variable x from range X. The proposition "$\forall x \in X, p(x)$" is true if $p(x)$ is true for every choice of $x \in X$, and false otherwise.

It is worth mentioning here that this gives us an inkling of how to disprove statements of the type $\forall x \in X, p(x)$. Since this proposition can only be true if it is in fact true for every choice of x, then all that is needed to prove this proposition false is to demonstrate ONE value of x for which the proposition $p(x)$ fails to hold. For example:

Example 17. Disprove the following proposition: For all real numbers $x, x^3 > 0$.

Proof. Let $x = 0$. Then x is a real number, but $x^3 = 0$, which is not greater than 0. Therefore the proposition is false. ■

In the above example, it does not matter that the proposition $x^3 > 0$ is true for every single other choice of x. The fact that it is false even once is enough to prove that it is not true "for ALL real numbers." It is sufficient, to demonstrate its falsehood, that there is a single example of x in the proper range that fails to satisfy $p(x)$.

A quick note: please please please do not use the word "random" to describe a universally quantified variable. It is common parlance to use, but in mathematics, writing "for any random integer" carries deeper, more complicated

meaning than you intend. If you'd like to be verbose about your quantification instead of using the $\forall$ symbol, consider using the word "arbitrary" in place of random, since it is (a) correct and (b) does not carry the freighted problem of making the reader worry about probability distributions.

7.2 Existential quantification

Although we have seen relatively little existential quantification thus far, it is equally important to understanding mathematical structure. We first consider what a proposition that has an existentially quantified variable looks like.

Definition 5. Let $p(x)$ be a logical formula that takes a variable x from range X. The proposition "$\exists x \in X, p(x)$" is true if $p(x)$ is true for some value of $x \in X$, and false otherwise.

We read the symbol $\exists$ as "there exists" or "for some." Compared to universal quantification, a proposition of this type only requires that $p(x)$ is true for at least one choice of x. To prove a proposition of the form $\exists x \in X, p(x)$, it suffices simply to demonstrate one value of x for which the statement $p(x)$ is true.
Consider the following example.

Example 20. Prove the following proposition:

There exists a real number x such that

$$x\big(x+\sin x - x^2 + \sin^2 x \cos x + e^x\big) = 0.$$

Proof. Let $x = 0$. Then

$$x\big(x+\sin x - x^2 + \sin^2 x \cos x + e^x\big) = 0 \times \big(0+\sin 0 - 0^2 + \sin^2 0 \cdot \cos 0 + e^0\big) = 0.$$

Hence, there exists a real number x that satisfies the proposition.
In this example, it would be quite cumbersome to perform algebraic manipulations on

$$x\big(x+\sin x - x^2 + \sin^2 x \cos x + e^x\big)$$

for an arbitrary value of x. Fortunately, because the proposition is existentially quantified, it suffices to demonstrate a single value of x that makes the proposition true. This is straightforward, since 0 times anything is 0.

7.3 Universal and existential quantifiers are friends

The universal and existential quantifiers play quite nicely together and help each other out. We have already seen one small example of this: to **disprove** a statement

$$\forall x \in X,\ p(x),$$

it suffices to show just *one* x with $\neg p(x)$. This is, effectively, an existential question, and it is formalized with a new version of De Morgan's Laws just for quantifiers.

theorem 2. [De Morgan's Laws for Quantifiers] Let $p(x)$ be a logical formula that takes a variable x from range X. Then:

1. $\neg(\forall x \in X,\ p(x)) \equiv \exists x \in X,\ \neg p(x)$.
2. $\neg(\exists x \in X,\ p(x)) \equiv \forall x \in X,\ \neg p(x)$.

We omit the proof of this theorem, leaving it as an exercise. Fundamentally, the proof is definitional: if it is not true that $p(x)$ holds for every x, then there must be some choice of x for which $p(x)$ is false (this is essentially part 1). Likewise, if there does not exist an x for which $p(x)$ is true, then it must be the case that $p(x)$ is always false (this is essentially part 2).

While we were not quite explicit about it, we quietly used De Morgan's Laws for Quantifiers in Example 17, by reasoning logically rather than appealing directly to the theorem.

In addition to helping each other out in negations, the universal and existential quantifiers often appear together in a single statement. You may recall from calculus (or perhaps you've blocked it out; no matter, we shall not dwell on this) a definition of continuity that took the form

$$\forall \varepsilon > 0,\ \exists \delta > 0 \text{ such that } \ldots$$

Here, and in many other circumstances, a formal statement of the proposition we wish to consider requires two variables to be quantified, in different ways. And there is a critical point to be made here **ORDER MATTERS**.

When we read quantifiers in a mathematical statement, we always give precedence to the first quantifier. If you make a statement of the form

$$\forall x \in X, \text{ [more words next]},$$

it is assumed that whatever words follow $\forall x \in X$ should actually be true for *all* x in the range X. Hence, there is a big difference between a statement that takes the form

$$\forall \varepsilon > 0, \exists \delta > 0,$$

and one that takes the form

$$\exists \delta > 0, \forall \varepsilon > 0.$$

To illustrate, let's take a look at an example that has absolutely nothing to do with calculus. Let's look at two statements involving both a universal and existential quantifier, and think about how they differ when the quantifiers switch order:

1. $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a+b=0$.
2. $\exists b \in \mathbb{Z}, \forall a \in \mathbb{Z}, a+b=0$.

For the first statement, we are saying the following: first, select an arbitrary integer a. Then, based on a, select a particular integer b. Because the existential quantifier comes after the universal quantifier, we can use a to choose b (so, in this case, we would set $b=-a$). This makes sense here, and it is true: for every integer a, there is definitely a choice of integer b satisfying the condition that $a+b=0$. For the second statement, however, things go a little haywire. Because the existential quantifier comes first, we are forced to select b first. That is, before we get to even think about a, we have to determine a choice of b. Then, once we have a choice of b, we would like that for **every** integer a, the statement $a+b=0$ is true. This is obviously ludicrous, since $a+b=0$ can only be true for one value of a, not every value of a. Obviously, this is something of a cautionary note, and a reminder to keep precedence order in mind when considering quantified variables. It is also worth noting that this kind of issue can only occur when we are interchanging the order of a universal and an existential quantifier; we can exchange two universally quantified variables or two existentially quantified variables willy-nilly. It is only the case that we have one of each that can cause potential problems.

8 Sets and Functions

8.1 Sets

Like Georg Cantor (1845-1918) we understand by a set an unordered collection of well defined objects, called elements or members of the set. Usually, sets are denoted by capital letters A, B, C, etc. and elements of sets by lower-case letters a, b, c etc. If a set is said to contain some elements, we write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.
More generally, the $\in$- relation is asymmetric, i.e. , if A, B are sets with $A \in B$, then $B \notin A$. (If one uses A as an element of B, then one cannot use B as an element of A. For the same reason, a chain like $A_1 \in A_2 \in \cdots \in A_n = A_1, n \geq 2$, is not possible.) For example, the set U of all sets does not exist, since such a set U would be an element of itself.

A set can be described by explicitly listing its elements — this is called the *enumerative notation* — or by characterizing its elements using a property $P(x)$ defined for objects x. In the latter case, one uses the notation

$$\{x \mid P(x)\}$$

and reads it as "the set of all x such that $P(x)$ is true."

For example,

$$\{1,-1\} = \{1,-1,1\} = \{x \mid x \text{ is a real number and } x^2 = 1\} = \{x \in \mathbb{R} \mid x^2 = 1\}$$

are all notations for the set that contains exactly the two real numbers 1 and -1.

A single set can be described in many different ways. For two sets to be equal, it only matters that they contain the same elements.
We shall use the following standard notations for some frequently occurring sets:

$\mathbb{N} = \{0,1,2,3,\dots\}$	set of natural numbers,
$\mathbb{N}^* = \{1,2,3,\dots\}$	set of positive natural numbers,
$\mathbb{N}_n = \{x \in \mathbb{N} \mid x \le n\} = \{0,1,\dots,n\}$,	
$\mathbb{N}_n^* = \{x \in \mathbb{N}^* \mid x \le n\} = \{1,\dots,n\} \quad (n \in \mathbb{N})$,	
$\mathbb{Z} = \{0,1,-1,2,-2,3,-3,\dots\}$	set of integers,
$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a,b \in \mathbb{Z}, b \neq 0 \right\}$	set of rational numbers,
$\mathbb{R}$	set of real numbers,
$\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$	set of non-zero real numbers,
$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \ge 0\}$	set of non-negative real numbers,
$\mathbb{R}^- = \{x \in \mathbb{R} \mid x \le 0\}$	set of non-positive real numbers,
$\mathbb{R}^{\times +} = \{x \in \mathbb{R} \mid x > 0\}$	set of positive real numbers,
$\mathbb{C} = \{x+iy \mid x,y \in \mathbb{R}\}$	set of complex numbers,
$\mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$	set of non-zero complex numbers.

We assume that the reader is familiar with the standard arithmetical operations and the elementary computational rules for these number systems.
Let A and B be sets. Then A is said to be a subset of B if every element of A is also an element of B. In this case, we write

$$A \subseteq B \text{ or } B \supseteq A.$$

We speak of the *inclusion* of the set A in the set B when every element of A is also an element of B, and we write

$$A \subseteq B.$$

If, in addition, $A \neq B$, then the inclusion is called *proper*. In this case, we also write

$$A \subset B \quad \text{or} \quad B \supset A.$$

Obviously, from the inclusions $A \subseteq B$ and $B \subseteq C$, it follows that

$$A \subseteq C.$$

The equality $A = B$ holds if and only if both inclusions are true:

$$A \subseteq B \quad \text{and} \quad B \subseteq A.$$

To prove the equality of two sets A and B, one typically verifies both these inclusions. That is, for all x, one shows:

1. From $x \in A$ it follows that $x \in B$, and
2. From $x \in B$ it follows that $x \in A$.

The set which has no element at all is called the empty set and is denoted by $\emptyset$.
It is a subset of every set. For example, $\mathbb{N}_0^* = \emptyset \subseteq \mathbb{N}^*$.

The set $\mathfrak{P}(A)$ of all subsets of a set A is called the *power set* of A.

For example,

$$\mathfrak{P}(\{1,2,3\}) = \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$$

is the power set of $\{1,2,3\}$.

The power set of the empty set is not empty:

$$\mathfrak{P}(\emptyset) = \{\emptyset\}.$$

Important set operations applied to elements of $\mathfrak{P}(A)$ again yield elements of $\mathfrak{P}(A)$. We describe some of these operations:

Let A and B be sets. Then:

- The set
$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}$$
is called the *intersection* of A and B.
- The set
$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}$$
is called the *union* of A and B.
- The set
$$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}$$
is called the *difference* of the sets A and B.

In the definition of the union of two sets, the term "or" means — as is generally the case in mathematics — the *disjunctive conjunction*, i.e., it does **not** have the meaning of "either-or".

Hence, the intersection $A \cap B$ is always a subset of the union $A \cup B$ i.e. $A \cap B \subseteq A \cup B$. The set

$$A \triangle B := \{x \mid \text{either } x \in A \text{ or } x \in B \text{ (but not both)}\} = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

is called the *symmetric difference* of A and B.

Two sets with empty intersection, i.e., $A \cap B = \emptyset$, are called *disjoint*. In this case, $A \triangle B = A \cup B$. *Euler–Venn diagrams* are often used to illustrate such (more or less) abstract concepts visually.

Computational Rules for Set Operations

Let A, B, and C be arbitrary sets. Then:

1. $A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset.$
2. $A \cup A = A, \quad A \cap A = A$ (Idempotency)
3. $A \setminus (A \setminus B) = B.$
4. $A \cup B = B \cup A, \quad A \cap B = B \cap A$ (Commutativity)
5. $A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$ (Associativity)
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributivity)
7. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
   $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ (De Morgan's Laws)

For sets A and B, the set of *(ordered) pairs* (x, y) with $x \in A$ and $y \in B$ is called the *Cartesian product* or *cross product* of A and B, and is denoted by $A \times B$. Formally,

$$A \times B := \{(x, y) \mid x \in A, y \in B\}.$$

8.2 Functions

Let A and B be sets. A *map* (or *function*) f from A *into* B associates or prescribes for every element $x \in A$ exactly one element $y \in B$, usually denoted by $f(x)$. A map f from A into B is written in the form:

$$f : A \to B, \quad x \mapsto f(x).$$

The set A is called the *domain* (or *domain of definition*), denoted by $\mathrm{Dom}\, f$, and the set B is called the *codomain*, denoted by $\mathrm{Cod}\, f$, of the map f.

For $x \in A$, the element $f(x) \in B$ is called the *image* of x under f, or the *value* of f at the *argument* $x \in A$, or the value of f *at the place* $x \in A$.

In order to make the concept of a map more precise, one considers the so-called *graph* of f. By definition, this is the subset

$$\Gamma := \Gamma(f) := \Gamma_f := \{(x, f(x)) \mid x \in A\} \subseteq A \times B$$

of $A \times B$. The graph $\Gamma(f)$ characterizes the map f uniquely. Therefore, one identifies maps with their graphs.

A subset $R \subseteq A \times B$ defines (i.e., is the graph of) a map

$$f : A \to B$$

if and only if, for every $x \in A$, there exists a unique $y = f(x) \in B$ with $(x, y) \in R$.

Two maps f and g are equal if and only if their domains and codomains coincide and if $f(x) = g(x)$ for all x in their (common) domain of definition.

Very often, maps with values in a set of numbers are called *functions*. In this case, the sum, product, or similar operations of functions f, g with values in a set of numbers are defined by applying the corresponding operations to the values of f and g. For example,

$$(f+g)(x) := f(x) + g(x), \quad \text{and} \quad (fg)(x) := f(x)g(x)$$

for all x in the common domain of definition of f and g.

Similarly, the multiplication of a function f by a number a is defined by

$$(af)(x) := a \cdot f(x).$$

The *constant function* which assigns the value a for every x is simply denoted by a.

Let $f : A \to B$ be a map and let $A_0 \subseteq A$ (resp. $B_0 \subseteq B$) be subsets with $f(A_0) \subseteq B_0$. Then f defines, in a natural way, a map $A_0 \to B_0$ with A_0 as domain of definition and B_0 as codomain: by definition, for every argument $x \in A_0$ it has the same value $f(x)$ as f. This map is called the *restriction of* f and is denoted by $f|_{A_0}$ (whereby the change of the codomain from B to B_0 is not indicated).

We will denote the set of all maps from a set A to a set B by B^A or $\mathrm{Map}(A, B)$.

8.2.1 Injectivity, Surjectivity and Bijectivity

Definition 6. A function $f : A \longrightarrow B$ is said to be *injective* if $f(a) = f(b) \implies a = b$. In other words, if for every $b \in B$ there is at most one $a \in A$ with $f(a) = b$. (Sometimes also called one-to-one.)

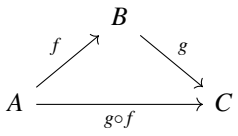
Definition 7. A function $f : A \longrightarrow B$ is said to be *surjective* if for all $b \in B$, there exist atleast one $a \in A$ such that $f(a) = b$. (Sometimes also called onto.)

Definition 8. A function $f : A \longrightarrow B$ is said to be *bijective* if it is both injective and surjective. In other words, for every $b \in B$, there is exactly one $x \in A$ with $f(a) = b$

Example 18. The map $\mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, is neither injective nor surjective. The map $\mathbb{R}^+ \to \mathbb{R}$, $x \mapsto x^2$, is injective but not surjective, and the map $\mathbb{R} \to \mathbb{R}^+$, $x \mapsto x^2$, is surjective but not injective. Finally, the map $\mathbb{R}^+ \to \mathbb{R}^+$, $x \mapsto x^2$, is bijective. — The sine function $\sin : \mathbb{R} \to [-1, 1]$ and the cosine function $\cos : \mathbb{R} \to [-1, 1]$ are surjective functions which are not injective.

Let A, B and C be sets, and let $f : A \to B$ and $g : B \to C$ be maps. Then the map $A \to C$ defined by $x \mapsto g(f(x))$ is called the *composition* of f and g. It is usually denoted by $g \circ f$ or just by gf.

This situation is well described by the following diagram (which is *commutative*):



Note that the composition gf is defined only if $\operatorname{Cod} f = \operatorname{Dom} g$ (or at least $\operatorname{Im} f \subseteq \operatorname{Dom} g$). Trivially, $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$ for every map $f : A \to B$.

Example 19. Even if both the compositions $f \circ g$ and $g \circ f$ are defined, in general, they do not coincide. For example, for the functions $f : x \mapsto x+1$ and $g : x \mapsto x^2$ from $\mathbb{R}$ into $\mathbb{R}$, we have:

$$f \circ g : x \mapsto x^2 + 1, \quad \text{and} \quad g \circ f : x \mapsto (x+1)^2 = x^2 + 2x + 1.$$

Therefore, $f \circ g \neq g \circ f$.

For the composition of maps, the commutative law does not hold in general.