Math 127: Logic and Proof

Mary Radcliffe

In this 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.

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 a 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 and b are integers) $\wedge$ (a is even) $\wedge$ (a divides b)

q: b 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:

$$\begin{aligned}
[(p \Rightarrow r) \wedge (r \Rightarrow q)] \Rightarrow [p \Rightarrow q] &\equiv [(\neg p \vee r) \wedge (\neg r \vee q)] \Rightarrow (\neg p \vee q) \\
&\equiv \neg[(\neg p \vee r) \wedge (\neg r \vee q)] \vee (\neg p \vee q) \\
&\equiv [\neg(\neg p \vee r) \vee \neg(\neg r \vee q)] \vee (\neg p \vee q) \qquad \text{(by DeMorgan's Laws)} \\
&\equiv [(p \wedge \neg r) \vee (r \wedge \neg q)] \vee (\neg p \vee q).
\end{aligned}$$

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 $p \Rightarrow q$ is true, it can be done by taking a series of implications, taking the form

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

The previous theorem demonstrates that this is sufficient to prove the statement $p \Rightarrow q$. 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).

$\vdots$

4. Conclude that r_k must be true (for some r_k).
5. 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 divides 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 divides 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. Prove the following statement.

> 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 a is rational, and b is rational. By definition, then, there are integers n_1, d_1 and n_2, d_2 such that $a = \frac{n_1}{d_1}$ and $b = \frac{n_2}{d_2}$. Therefore, we can write $a + b = \frac{n_1}{d_1} + \frac{n_2}{d_2}$. Because multiplying by 1 does not change the value of a number, we have

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

where the last two equalities follow by arithmetic rules. Since n_1, d_1, n_2, d_2 are all integers, we also have that $n_1 d_2 + n_2 d_1$ and $d_1 d_2$ are integers. By definition, since $a + b$ can be written as a quotient of integers, it is therefore 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 $p \Rightarrow r_1$, $r_1 \Rightarrow r_2$, ..., $r_k \Rightarrow q$, 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 $n_1 d_2 + n_2 d_1$ and $d_1 d_2$ are integers to draw our final conclusion, using information from multiple previous propositions.

2 Proving biconditional statements

Recall, a biconditional statement is a statement of the form $p \Leftrightarrow q$. As noted at the end of the previous set of notes, we have that $p \Leftrightarrow q$ is logically equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Hence, we can approach a proof of this type of proposition effectively as two proofs: prove that $p \Rightarrow q$ is true, AND prove that $q \Rightarrow p$ is true. Indeed, it is common in proofs of biconditional statements to mark the two proofs using the symbols ($\Rightarrow$) and ($\Leftarrow$), to indicate $p \Rightarrow q$ and $p \Leftarrow q$, 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 $\Leftrightarrow$. It is also common to refer to the two parts of the proof as "directions," with $p \Rightarrow q$ called the "forward direction" and $p \Leftarrow q$ called the "backward direction."

A useful note for proving $\Leftrightarrow$ statements, compared to $\Rightarrow$ 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 $\Leftrightarrow \lceil x \rceil = \lfloor x \rfloor$. 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 $x, \lceil x \rceil, \lfloor x \rfloor$ as defined in the statement of the proposition. Note that, by definition, we must have that $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

($\Rightarrow$) Assume that x is an integer. Then as $x \leq x$, we must have that 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 itself, so $\lfloor x \rfloor = x$. Therefore, $\lfloor x \rfloor = \lceil x \rceil$.

(⇐) 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 that the inequalities are all equalities, so $\lfloor x \rfloor = x = \lceil x \rceil$. Since $\lfloor x \rfloor$ is an integer by definition, and $\lfloor x \rfloor = x$, we must have 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

$$\begin{aligned} x^2 - 2x = 0 \quad &\Rightarrow \quad x(x-2) = 0 \\ &\Rightarrow \quad x = 0 \text{ or } x = 2. \end{aligned}$$

(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 is a solution $\Rightarrow x = 0$ or $x = 2$, but we need a biconditional statement here.)

Moreover, we find that if $x = 0$, then $x^2 - 2x = 0 - 0 = 0$, and if $x = 2$, then $x^2 - 2x = 4 - 4 = 0$. Hence, we have that x is a real-valued solution to $x^2 - 2x = 0$ if and only if $x = 0$ 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 this is 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 at all. While this may seem like a silliness, 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 that

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

Moreover, we find that if $x = 0$, then $x + \sqrt{2x} = 0 + 0 = 0$, and if $x = 2$, then $x + \sqrt{2x} = 2 + \sqrt{4} = 4 \neq 0$. 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 $n = d_r d_{r-1} d_{r-2} \dots d_1 d_0$ in its base-10 expansion, so each d_i is between 0 and 9. Note that this is equivalent to writing

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

By performing some algebra, we can write

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

Notice that $10^1 - 1 = 9$, $10^2 - 1 = 99$, $\dots$, $10^r - 1 = 99 \cdots 9$, where there are r 9s in the final expression. Hence, $10^\ell - 1 = 3(33 \cdots 3)$ for any choice of ℓ, where there are ℓ 3s in the parenthesized number. Therefore, $10^\ell - 1$ is divisible by 3 for each ℓ. By rules of arithmetic, that implies $d_r(10^r - 1) + d_{r-1}(10^{r-1} - 1) + \cdots + d_1(10^1 - 1)$ is also divisible by 3, since each term of the sum is divisible by 3. Hence, there exists an integer k such that $d_r(10^r - 1) + d_{r-1}(10^{r-1} - 1) + \cdots + d_1(10^1 - 1) = 3k$, and therefore we may write n as

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

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

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

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

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

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

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 $\ell = \frac{k}{2} = \frac{a}{2b}$. Notice that since a, b are integers, we also have $a, 2b$ are integers, so ℓ is rational. Also, since a, b are positive, we have that ℓ is positive, and that $\ell < k$. Therefore, ℓ 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:

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

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 exists 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 $p \Rightarrow q$ 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 $p \Rightarrow q$.

Another way to think about this is to consider the truth table corresponding to $p \Rightarrow q$. By definition in the previous set of notes, we have that $p \Rightarrow q$ is a false proposition if p is true and q is false, otherwise, it is a true proposition. So, the truth table is as follows:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The goal of a proof by contradiction is to consider the second row of the table. If we can show that the assignment of truth values of p and q in the second row is not possible, then we know that the truth values must be from one of the other rows. In any of those rows, $p \Rightarrow q$ is true, and hence $p \Rightarrow q$ must always be true if the second row is logically impossible.

We close this section with a two more examples of proofs of implications using contradiction. In both of the following examples, there is a clue that a contradiction proof might be useful: both statements that follow have a conclusion q that is effectively a negative; that is, we wish to prove that something does NOT happen. As with proving nonconditional propositions using contradiction, it is frequently useful to prove something does not happen by showing that if it does happen, something logically impossible must occur.

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 $b+1$.

Note: here we have the implication $p \Rightarrow q$, where p is "$a \geq 2$" and q is "a does not divide one of b and $b+1$." To follow proof by contradiction, we wish to assume p and $\neg q$. Note that to negate q, we can use De Morgan's laws; think of q as "(a does not divide b)$\vee$ (a does not divide $b+1$)." De Morgan's laws then say that $\neg q$ can be written as

$$\neg q \equiv \neg(a \text{ does not divide } b) \wedge \neg(a \text{ does not divide } b+1).$$

The negation of "does not divide" is clearly "does divide," so to negate q we assume that a divides both 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, c are all odd integers, but that there is a rational x such that $ax^2 + bx + c = 0$. Let k, ℓ be integers with $x = \frac{k}{\ell}$, and suppose that k and ℓ share no common factors, so that x is written in lowest terms. Then we have

$$\begin{aligned} ax^2 + bx + c = 0 \quad &\Rightarrow \quad a\left(\frac{k}{\ell}\right)^2 + b\left(\frac{k}{\ell}\right) + c = 0 \\ &\Rightarrow \quad ak^2 + bk\ell + c\ell^2 = 0 \quad \text{(by multiplying by } \ell^2\text{)} \end{aligned}$$

Notice that the right hand side of the final equation is 0, which is even, so the left hand side must also be even. As a, b, c are all odd, we observe that this can only occur if both k and ℓ are even. Therefore, both k and ℓ are divisible by 2. But this is impossible, since we have chosen k and ℓ to share no common factors.

Therefore, if a, b, c are all odd integers, there cannot exist any rational number x such that $ax^2 + bx + c = 0$.

□

A note on the previous example: if you are not convinced by the assertion that k and ℓ 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 $ak^2 + bk\ell + c\ell^2 = 0$ 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 $\neg q$ is true implies $\neg p$ 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 $p \Rightarrow q$ 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, 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" (often abbreviated as WLOG or WOLOG). Here, we actually have two different possibilities: either a is odd and b is even, or a is even and b is odd. However, notice that the proofs of these two distinct possibilities are actually the same: a and b are performing symmetric roles in the proposition. 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 WOLOG 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 WOLOG, 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 have a proposition $p \Rightarrow q$, where p itself takes the form $p \equiv r \vee s$; 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 from the last set of notes. 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 $p \equiv r_1 \vee r_2 \vee \cdots \vee r_k$, then we will have

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

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

Example 16. Prove the following proposition:

> Given a, b real numbers, define $a@b = \max\{a, b\}$; that is, $a@b = a$ if $a \geq b$, and b otherwise.
>
> If a, b, c are real numbers, then $(a@b)@c = a@(b@c)$.

Proof. Suppose a, b, c are real numbers. We shall consider 6 cases, according to the order in which they appear.

Case 1: $a \leq b \leq c$. Then $a@b = b$, since $b \geq a$, and $b@c = c$, since $c \geq b$, and $a@c = c$, since $c \geq a$. Therefore,

$$(a@b)@c = b@c = c = a@c = a@(b@c),$$

and the proposition holds.

Case 2: $a \leq c \leq b$. Then $a@b = b$, since $b \geq a$, and $b@c = b$, since $b \geq c$, and $a@c = c$, since $c \geq a$. Therefore,

$$(a@b)@c = b@c = b = a@b = a@(b@c),$$

and the proposition holds.

Case 3: $b \leq a \leq c$. Then $a@b = a$, since $a \geq b$, and $b@c = c$, since $c \geq b$, and $a@c = c$, since $c \geq a$. Therefore,

$$(a@b)@c = a@c = a@(b@c),$$

and the proposition holds.

Case 4: $b \leq c \leq a$. Then $a@b = a$, since $a \geq b$, and $b@c = c$, since $c \geq b$, and $a@c = a$, since $a \geq c$. Therefore,

$$(a@b)@c = a@c = a@(b@c),$$

and the proposition holds.

Case 5: $c \leq a \leq b$. Then $a@b = b$, since $b \geq a$, and $b@c = b$, since $b \geq c$, and $a@c = a$, since $a \geq c$. Therefore,

$$(a@b)@c = b@c = b = a@b = a@(b@c),$$

and the proposition holds.

Case 6: $c \leq b \leq a$. Then $a@b = a$, since $a \geq b$, and $b@c = b$, since $b \geq c$, and $a@c = a$, since $a \geq c$. Therefore,

$$(a@b)@c = a@c = a = a@b = a@(b@c),$$

and the proposition holds.

Since the proposition holds under any ordering of a, b, c, it must hold in general. □

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.[1]"

In general, proof by cases looks as follows:

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

[1] This, of course, is a joke. It's called Proof by Exhaustion because you exhaust all possible outcomes, as in, you run out of options.

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 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.).

6.1 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 1. 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

Let a, b integers. Then $a + b$ 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

For all integers a, $a^2 + a$ 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 2. 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, $x^2 > 0$.

Proof. Let $x = 0$. Then x is a real number, but $x^2 = 0$, which is not greater than 0. Therefore the proposition is false. □

In the above example, it does not matter that the proposition $x^2 > 0$ 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 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.

6.2 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 3. 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 18. Prove the following proposition:

There exists a real number x such that $x(x + \sin x - x^2 + \sin^2 x \cos x + e^x) = 0$.

Proof. Let $x = 0$. Then $x(x+\sin x-x^2+\sin^2 x\cos x+e^x) = 0(0+\sin 0-0^2+\sin^2 0\cos 0+e^0) = 0$. Hence there exists an x that satisfies the proposition. □

In this example, it would be awful to have to spend time doing algebra on $x(x+\sin x-x^2+\sin^2 x\cos x+e^x)$ for an arbitrary x. Fortunately, though, we don't have to: because this is an existentially quantified x, it is enough to just demonstrate a single value of x that makes the proposition true. This is easy to do, since 0 times anything is 0.

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

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 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 "$\forall \varepsilon > 0,\ \exists \delta > 0$ such that...." Here, and in many other kinds of circumstance, 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 "$\forall x \in X$, [more words next]," it is assume that whatever words follow $\forall x \in X$ should actually be true for all x in the range of 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, that 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 existential quantifier; we can exchange two universally or two existentially quantified variables willy nilly. It is only the case that we have one of each that can cause potential problems.