How to Always Be Right

Definition 3.1. *An **argument** begins with a set of propositions, called the **assumptions**. Each step is justified with a mathematical axiom or previously proven fact. It ends with a conclusion.*

In general, a proof is an argument that concludes with the proposition we are trying to prove. We will first examine two easy types of proofs, known as "trivial" and "vacuous" proofs.

Definition 3.2. *A **trivial proof** is one of the form $\forall x \in A, P(x) \Rightarrow Q(x)$, where $Q(x)$ is always true for any x.*

Did someone call Obama?
Remember that it helps to think of an implication like a *promise*. When looking at $P \Rightarrow Q$, if Q is always true, we will have always fulfilled our promise.

Example: For every person in America, if they are Obama, then Obama is not the president. Here, $P(x) := x$ is Obama, $Q(x) =$ Obama is not the president. $Q(x)$ is always true, and in fact has nothing to even do with x. So we are trivially done.

Example: For every $x \in \mathbb{R}$, $x > 0 \Rightarrow x^2 - 2x + 1 \geq 0$ `(x - 2x + 1 \geq 0)`. Note that $x^2 - 2x + 1 = (x-1)^2$, which is always non-negative. Thus $Q(x)$ is always true, regardless of $P(x)$.

Definition 3.3. *A **vacuous proof** is one of the form $\forall x \in A, P(x) \Rightarrow Q(x)$, where $P(x)$ is always false for any x.*

Effectively, this is the same idea as above. If $P(x)$ never happens, then we're good. There are *two* ways in which this can happen, although both are quite similar.

Example: Show that for any set A, $\varnothing \subseteq A$. To do this, we have to show $\forall x, x \in \varnothing \Rightarrow x \in A$. But $P(x)$ is always false, so our promise is upheld. We are done.

Note 3.4. *This **first** way in which we did a vacuous proof was clear, since we were obviously dealing with the empty set. But it's sometimes not clear that the set we are dealing with actually **is** empty!*

Example: Show that for any $x \in \mathbb{R}$, $x^2 < 0 \Rightarrow 3x + 3 > 0$. Clearly our $P(x)$ here is never true, so we are vacuously done. The implication is true.

Now on to *real* proofs.

Definition 3.5. *A **direct proof** is one in which we begin with the premises of the implication we are trying to prove, perform logical manipulations, and reach our conclusion directly.*

Not much really going on here, but the key is in actually structuring these things. There are really two things to look out for: Dealing with universal and existential quantifiers.

Suppose I am along my way proving a statement with a universal quantifier, $\forall x \in A$. There are two things I should keep in mind here. First - I can simply will a new x into existence, and continue doing my proof. Second - I *cannot* impose any restrictions on this x, other than that it is an element of A. If I were to do this, I would lose the generality of the universal quantifier, and I would not be proving the correct statement anymore.

Example: Prove that for any $x \in \mathbb{R}$, $x^2 \geq 0$.

"Proof:" Pick some $x \in \mathbb{R}$ such that $x > 0$. Then it follows that a positive number times a positive number is still positive - therefore, $x \cdot x = x^2 > 0$.

It is somewhat subtle if you are not expecting it, but basically the error is that I have imposed that $x > 0$ erroneously. I am not allowed to do this!

Now to discuss existential quantifiers: These ones are harder. You have to actually find the guy that satisfies the proposition that comes after, or prove in some non-constructive way that it ought to exist

somewhere.

Example: Prove that for all $x \in \mathbb{Z}$, there is some y such that $x + y = 0$.

Proof: Pick some integer x. Then let $y = -x$. Then, $x + y = x + (-x) = 0$. So we are done.

The reason this works is because I actually found a suitable value for y. Now, what happens if we cannot find the actual value, but still could manage to show it ought to exist?

Definition 3.6. *An integer x is even if there exists some integer k such that $x = 2k$.*

Definition 3.7. *An integer x is odd if there exists some integer k such that $x = 2k + 1$.*

Example: Prove that for any two consecutive integers, at least one is even.

Proof: Notice that we have to do a little bit of formalization here for what it means to be consecutive. It is not particularly complicated, but we should be careful in how we do it, lest we accidentally introduce a mistake. Let x and $x + 1$ be arbitrary consecutive integers. If x is even, then we are done. But if x is odd, then there is some integer k such that $x = 2k + 1$. Then, $x + 1 = 2k + 1 + 1 = 2(k + 1)$. Since $x + 1$ is double some integer, it must be even. So I am done.

Notice that I did not actually point out x or $x + 1$ specifically as even! I only showed that **at least one** is even.

Definition 3.8. *A **proof by cases** in one in which we split our proof into multiple cases, and they collectively cover all possible cases.*

Actually, we just did a proof by cases. Either x is even, or x is odd. In both cases, we saw that either x or $x + 1$ is even.

Note 3.9. *CS majors in particular are prone to resorting to proof by cases, akin to how they might try to create extra if branches to try and ease their line of thought. I suggest that before trying this, give a good think about whether or not you can simply reduce the proof to be without cases. Of course, sometimes a proof by cases is inevitable, but it is good to try and avoid it if possible, to reduce the complexity of the proof.*

Definition 3.10. *A **contrapositive proof** is one in which we prove $\neg q \Rightarrow \neg p$ instead of $p \Rightarrow q$.*

This isn't a super commonly used one, but consider the following example-
Example: For any integer x, if $x^2 - 6x + 7$ is odd, then x is even.

It's not really clear how to tackle this immediately by direct proof. We could say, "okay, there must be some integer k such that $x^2 - 6x + 7 = 2k + 1$, blah blah blah ," but it's not really clear how to proceed from here.

Instead with the contrapositive, we have "If x is odd, then $x^2 - 6x + 7$ is even." This is a lot more tractable. We know that $x = 2k + 1$ for some integer k. Then, $x^2 - 6x + 7 = 2(2k^2 - 4k + 1)$ (after some invisible algebra). That means that $x^2 - 6x + 7$ is even, as it was double some integer. So the proof is done by its contrapositive.

Definition 3.11. *A **proof by contradiction** begins by assuming the **negation** of what we want to prove. For example, if we want to prove $p \Rightarrow q$, we assume the negation of the implication, which is $p \wedge \neg q$. From there, we prove some kind of contradiction (i.e., F). If all of our logic was sound, the only thing wrong was the initial assumption, $p \wedge \neg q$. Therefore the opposite is true; $p \Rightarrow q$.*

Note 3.12. *WARNING!!!!!!! The easiest thing to do when stuck is try contradiction. Don't do it. Do NOT jump to contradiction. Sure, there will be plenty of times where it actually is the easiest way to do the proof. But your instinct to jump to contradiction is likely misguided. Spend plenty of time understanding the problem well and trying a direct proof before going to contradiction.*

Note 3.13. *Whenever you begin a proof by contradiction, you MUST state "Assume for the sake of contradiction that..". Do not expect that the reader will look at your initial assumption and know that you are doing a proof by contradiction.*

Definition 3.14. $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z} \wedge q \neq 0 \wedge \gcd(p, q) = 1\}$

Note 3.15. *In the above definition, p and q should have no common prime factors, meaning that the fraction has been fully reduced.*

Example: Prove that $\sqrt{2}$ is irrational. This is actually kind of complicated, and we will need a lemma to do it.

Lemma 3.16. *If x^2 is even, then x is even as well.*

Proof. We will do this by proving the contrapositive. Suppose x is odd. Then $x = 2k + 1$ for some integer k. Then, $x^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore x^2 is odd. □

Assume for the sake of contradiction that $\sqrt{2}$ is rational. Then, there are some integers p and q such that $\sqrt{2} = p/q$, $q \neq 0$, and p and q are coprime.

Note 3.17. *Two integers are coprime if their gcd is 1.*

Then, $p^2/q^2 = 2$, and $p^2 = 2q^2$. This means that p^2 is even. From the lemma, we know that p must also be even. Therefore, there is some integer k such that $p = 2k$. Then $p^2 = 4k^2 = 2q^2$, so $2k^2 = q^2$. This means q^2 is even, so by the lemma, q is also even. This is a contradiction! The gcd of p and q was supposed to be 1, and yet both p and q are divisible by 2. Therefore, the assumption that $\sqrt{2}$ is rational is incorrect, and so it is actually irrational.

Homework

1. (a) Prove that for any real x, if $x^2 < 73$, then $0 < 1$.
   (b) Prove that for any integer x, if $-x^2 > 0$, then $x = 5$.

2. Prove the following by **direct** proof.
   (a) Prove that if x is an odd integer, then $7x - 5$ is even.
   (b) Let a, b, c be integers. Prove that if a and c are odd, then $ab + bc$ is even.

   Note 3.18. *It is a common mistake to do something like, if a is odd, then $a = 2k + 1$, and if c is also odd, then $c = 2k + 1$. The problem is that we used the same k for both of these, and that is not allowed. We used something known as existential instantiation to bring this k into existence. However, it cannot be a variable that we already used before. To fix this, do something like $c = 2k' + 1$ instead.*

   (c) Prove that every odd integer is the difference of two square integers.

3. (a) Prove that for an integer x, x is odd if and only if x^3 is odd. [Hint: You have to prove two directions for this, x is odd $\Rightarrow$ x^3 is odd, and x is odd $\Leftarrow$ x^3 is odd. It is customary to do this in two stages, where you label the direction you are proving with the relevant arrow. I would start the first stage by writing ($\Rightarrow$), and the second stage with a ($\Leftarrow$) to make it clear what I am doing. Also, for the second stage, the contrapositive may help you.]
   (b) Consider the following definition:

   Definition 3.19. *If x **divides** y, then there is some integer k such that $y = kx$.*

   Prove that if four does not divide x^2 when x is an integer, then x is odd.

4. (a) Prove that there is no largest integer.
   (b) Prove that there is no smallest positive rational number.
   (c) Prove or disprove: The product of two irrational numbers is irrational.
   (d) Prove or disprove: The sum of a rational and irrational number is irrational.

5. (a) **(Triangle Inequality).** Prove that for any $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$. [Hint: Proof by cases.]
   (b) **(Reverse Triangle Inequality).** Prove that for any $x, y \in \mathbb{R}$, $||x| - |y|| \leq |x - y|$. [Hint: $x = x - y + y$.]