Writing Proofs

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

TAKE-AWAYS

- Direct proofs are used prove implications of the form $\forall x\ P(x) \quad \rightarrow \quad Q(x)$. The proof begins by assuming that $P(x)$ holds for an arbitrary element x, and tries to show that $Q(x)$ must hold.
- Proofs by contraposition prove the contrapositive of $\forall x\ P(x) \rightarrow Q(x)$ to establish $\forall x\ P(x) \rightarrow Q(x)$.
- To prove if and only if statements $\forall x\ P(x) \quad \leftrightarrow \quad Q(x)$, we need to show $\forall x\ P(x) \rightarrow Q(x)$ and $\forall x\ Q(x) \rightarrow P(x)$.
- Proofs are often broken into cases, where each case is proved separately.
- Proof by contradiction is an indirect proof method to prove a proposition P. In the first step of such a proof, $\neg P$ is assumed, and one tries to derive a contradiction.

Proofs are arguments that convince us about the truth of a proposition. They are a series of logical deductions, starting from a set of common understood facts called *axioms*, that establish the proposition being proved. In most cases, proofs follow a few standard templates that we will look at in these notes. As we shall see, the templates are often closely tied to the form of the statement one is trying to establish. Thus these templates provide an initial outline with details to be filled in based on the task at hand. Before looking at these proof templates, let us consider the types of statements one usually encounters.

Statements

Statements are one of two forms: existentially quantified statements or universally quantified statements. The general template used to establish these differs, and it is useful to highlight this difference.

Existentially quantified statements are of the form $\exists x\ P(x)$. To prove such a statement, one usually finds an example value for x such that $P(x)$ holds [1]. Let us look at an example.

[1] There are certain cases when the proof of an existential statement is *non-constructive*. We will not encounter such proofs in this class.

Definition 1. A non-negative integer $n \in \mathbb{N}$ is a perfect square if there is another integer a such that $n = a^2$. For example, $1, 4, 9, 16, \ldots$ are all perfect squares, while 2 and 3 are not perfect squares.

Proposition 2. *There is an integer n that is not the sum of two perfect squares.*

Proof. To prove the statement, all we need to do is find an integer that is not the sum of two perfect squares. In this case we can take $n = -1$. Observe that since all perfect squares are non-negative, the sum of any two perfect squares will also be non-negative. Therefore, -1 cannot be the sum of two perfect squares. □

Universally quantified statements are of the form $\forall x\ P(x)$. They are typically more difficult to prove than existentially quantified statements. Their proofs begin by starting with an arbitrary value for x (and not a specific one), and showing the predicate P is true for this arbitrary value. Let us look at an example.

Example 3. Suppose we want to prove that if $n \in \mathbb{Z}$ is odd then n^2 is also odd. To prove such a statement, it is not sufficient to take a specific odd value for n (say 5) and showing that $5^2 = 25$ is also odd. Instead, its proof will begin by picking an *arbitrary* odd number as n and then showing that n^2 is odd. We will write a proof for this statement later in these notes.

We conclude this section by observing that the statement in Example 3 — if $n \in \mathbb{Z}$ is odd then n^2 is also odd — does not explicitly quantify n. We assume that it is universally quantified. That is, "if $n \in \mathbb{Z}$ is odd then n^2 is also odd" really means "for every integer n, if n is odd then n^2 is odd". This is typical: if a variable in a statement is not quantified, like n in this example, it will be assumed to be universally quantified.

Direct Proofs

The first proof template we will consider is for a conditional statement of the form

$$\forall x\ (P(x) \to Q(x)).$$

Since this is a universal statement, such proofs begin by taking x to be an arbitrary value. Recall that an implication $P(x) \to Q(x)$ is false in only one scenario: when $P(x)$ is true and $Q(x)$ is false. Thus, for an implication to be true, we need to argue that the combination of $P(x)$ being true and $Q(x)$ being false cannot occur. A direct proof, therefore, proves an implication by showing that if we assume $P(x)$

to be true then $Q(x)$ must also be true. Thus such a proof template looks as follows

> Let x be an arbitrary element.
> Assume $P(x)$ holds.
> $\vdots$
> Goal: $Q(x)$

Let us look at an example.

Definition 4. An integer $n \in \mathbb{Z}$ is *even* if there is an integer k such that $n = 2k$. An integer n is *odd* if there is an integer k such that $n = 2k + 1$.

Proposition 5. *If n is an odd integer then n^2 is an odd integer.*

Proof. Let n be an arbitrary integer. Assume that n is odd. Since n is odd, there an integer k such that $n = 2k + 1$. Now,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Observe that since k is an integer, $2k^2 + 2k$ is also an integer, and so n^2 is two times an integer (namely, $2k^2 + 2k$) plus 1. Hence, n^2 is odd. □

More generally, direct proofs can be written for statements of the form

$$\forall x((P_1(x) \wedge P_2(x) \wedge \cdots \wedge P_k(x)) \to Q(x)).$$

The proof template follows the same pattern as before starting from assuming the antecedent and trying to prove the consequent. The only difference is that when you start the proof, you may now assume that each of the conjuncts in the antecedent holds.

> Let x be an arbitrary element.
> Assume $P_1(x), P_2(x), \ldots P_k(x)$ hold.
> $\vdots$
> Goal: $Q(x)$

Let us look at an example.

Proposition 6. *If n is an odd integer and m is an odd integer then nm is an odd integer.*

Proof. Let n, m be arbitrary integers. Assume that n and m are both odd. Then there are integers k, ℓ such that

$$n = 2k + 1 \qquad m = 2\ell + 1.$$

Observe that $nm = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1 = 2(k\ell + k + \ell) + 1$. Now since k and ℓ are integers, so is $k\ell + k + \ell$, and hence nm is odd. □

Proofs by Contraposition

PROOFS BY CONTRAPOSITION is another method to proof an implication statement. The difference from a direct proof is that in a proof by contraposition we prove the equivalent contrapositive form, instead of the original statement. Thus, to show $\forall x\ (P(x) \to Q(x))$, we prove the contrapositive $\forall x\ (\neg Q(x) \to \neg P(x))$. Let us look at an example to see how this works.

Proposition 7. *For any integer n, if n^2 is even then n is even.*

Proof. Let n be an arbitrary integer.

A direct proof starting with the assumption that n^2 is even, cannot be advanced. Let us write out the first few steps to see where we get stuck. So assuming n^2 is even, we know that there is an integer k such that $n^2 = 2k$. What can we say about n? Is $n = \sqrt{2k}$ even? We can't even argue that $\sqrt{2k}$ is an integer!

Instead, it is easier to prove the contrapositive. The contrapositive is "if n is not even then n^2 is not even". Observe that an integer that is not even is odd. So we can rewrite the contrapositive as "if n is an odd integer then n^2 is odd". This can be established by a direct proof as we saw in Proposition 5. □

One case where proofs by contraposition are useful, is when trying to prove a statement of the form

$$\forall x\ (P(x) \to (Q_1(x) \vee Q_2(x) \vee \cdots \vee Q_k(x))).$$

Observe that the contrapositive of such a statement is

$$\forall x\ ((\neg Q_1(x) \wedge \neg Q_2(x) \wedge \cdots \wedge \neg Q_k(x)) \to \neg P(x)).$$

Thus the contrapositive in this case is consistent with the form of statements that can be established by a direct proof.

Proposition 8. *Let m, n be integers. If mn is even then either m is even or n is even.*

Proof. Let m, n be arbitrary integers. The contrapositive of the proposition is "if m is not even and n is not even then mn is not even". Using the duality of odd and even, the contrapositve can be rewritten as "if m is odd and n is odd then mn is odd". This can be proved using a direct proof as we saw in Proposition 6. □

Proving if and only if statements

Recall that if and only if statements are equivalent to the conjunction of two implications. Thus, proving $\forall x\ (P(x) \leftrightarrow Q(x))$ is equivalent

to proving $\forall x\ (P(x) \to Q(x))$ and $\forall x\ (Q(x) \to P(x))$. Therefore, proving an if and only if statement requires proving an implication in each direction. Let us look at an example.

Proposition 9. *For any integer n, n is odd if and only if n^2 is odd.*

Proof. This requires us to prove two implications: "if n is odd then n^2 is odd" and "if n^2 is odd then n is odd". We prove them in order, and it is typical of the proof to have "directions" to indicate which we are proving.

($\Rightarrow$) Need to prove "if n is odd then n^2 is odd". This is exactly what we showed in Proposition 5. We skip repeating this proof.

($\Leftarrow$) Now we need to prove "if n^2 is odd then n is odd". This is difficult to prove directly. Therefore, we will use a proof by contraposition. The contrapositive of our statement is "if n is not odd then n^2 is not odd". Again by using the relationship between odd and even, we can rewrite the contrapositive as saying "if n is even then n^2 is even". Proving this statement directly is similar to the proof of Proposition 5. We present it here for completeness.

Suppose n is an arbitrary even integer. Then there is an integer k such that $n = 2k$. Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since k is an integer, $2k^2$ is an integer, and so n^2 is even. □

Proof by Cases

BREAKING A COMPLICATED PROOF into cases, and proving each case separately, is a useful proof strategy. Let us look at an example to see how this works.

Definition 10. For any real number x,

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Proposition 11. *For any two real numbers x and y, $|xy| = |x||y|$.*

Proof. We will prove this by cases.

$x, y \geq 0$: In this case $xy \geq 0$, $|x| = x$, and $|y| = y$. Thus, $|xy| = xy = |x||y|$.

$x, y < 0$: In this case $xy \geq 0$, $|x| = -x$, and $|y| = -y$. Thus, $|xy| = xy = (-x)(-y) = |x||y|$.

$x \geq 0$, $y < 0$: In this case, $xy < 0$, $|x| = x$, and $|y| = -y$. Thus, $|xy| = -xy = x(-y) = |x||y|$.

$x < 0,\ y \geq 0$: This is similar to the previous case, and therefore the proof is skipped.

□

Proof by Contradiction

PROOF BY CONTRADICTION is an indirect way to prove that a proposition P holds. In such a proof, we try to establish P by proving that if P does not hold then both R and $\neg R$ hold, for some proposition R. The reason why this is a sound argument is because, using truth tables one can observe that, $P \equiv ((\neg P) \rightarrow (R \wedge (\neg R)))$, for any propositions P and R. To prove $\neg P \rightarrow (R \wedge \neg R)$, we begin by assuming that $\neg P$ holds, and proceed to show that some proposition R and its negation also hold as a consequence. The conjunction $R \wedge \neg R$ is said to be a contradiction. Often when writing a proof by contradiction, the contradiction itself or the proposition R is not known, and it is discovered through the process of writing the proof. Such proofs are not always possible and tend to be a bit convoluted. Hence, direct proofs are often prefered to a proof by contradiction. Let us look at a classical example to illustrate this proof template.

Definition 12. A real number $r \in \mathbb{R}$ is a *rational* number if there are integers $a, b \in \mathbb{Z}$ such that $b \neq 0$ and $r = \frac{a}{b}$. If r is a rational number, one can assume that the integers a, b are in lowest terms, i.e., they do not share any common factors. The set of all rational numbers is denoted by $\mathbb{Q}$.

A real number r is *irrational* if r is not rational.

Theorem 13. *$\sqrt{2}$ is irrational.*

Proof. Assume (for contradiction) that $\sqrt{2}$ is rational. Then there are integers a, b such that $b \neq 0$, a, b don't share any common factors, and

$$\sqrt{2} = \frac{a}{b}.$$

Squaring both sides and cross multiplying, we can conclude that $a^2 = 2b^2$, and so a^2 is even. From Proposition 7, this means that a is even. Thus there is some integer k such that $a = 2k$. Substituting this back, we get that

$$2b^2 = a^2 = (2k)^2 = 4k^2.$$

Or $b^2 = 2k^2$. Thus, b^2 is also even. Again by Proposition 7, we can conclude that b is even. Hence, a and b share 2 as a common factor. But a, b were not supposed to have any common factors. Thus, we have a contradiction. Our initial assumption that $\sqrt{2}$ is rational must be false and so $\sqrt{2}$ is irrational. □