

Basic Proof Techniques

Our experience with quantifiers enables us to establish a few basic techniques to prove mathematical statements. Below we discuss and verify the validity of the three most common techniques, *Direct Proof*, *Proof by Contradiction* (also called *Indirect Proof*), and *Proof by Contraposition*.

- **Direct Proof.** We now know that a compound statement of the form $P \Rightarrow Q$ is true if Q is true whenever P is true. That is, we cannot have P true and Q false at the same time. In our first method of proof, we begin by assuming P is true and deriving, through direct mathematical arguments, Q 's truth from this assumption.

Typically P will contain a universe of values x which must be considered. If P has the form “ $(\forall x \in S)$ blah blah blah...” we must verify that Q is true for *every* possible $x \in S$. Beware of “proof by example,” in which only a few values of x are considered; considering examples (I like to call it “play”) is an *excellent* way to gain intuition, but is ultimately not a substitute for a mathematical proof.

Let's do a few simple examples.

1. *If x and y are even integers, then $x + y$ is even.* Rewritten in quantifier notation, if E is the set of even integers this reads

$$(\forall x \in E)(\forall y \in E) x + y \in E.$$

Proof. Assume x and y are even. By the definition of an even integer, there exist integers m and n such that $x = 2m$ and $y = 2n$. Therefore

$$x + y = 2m + 2n = 2(m + n).$$

If we let $k = m + n$, $x + y = 2k$, showing that $x + y$ is even, again by the definition of an even integer. \diamond

Notes: there were a few facts we took as “given,” such as basic rules of multiplication and addition in \mathbb{R} . Such “givens” we'll call *axioms*, and will talk about soon. Also, notice how we wrapped up the proof with a nice little symbol, \diamond . It's never a bad idea to give the reader a visual cue that the proof is over (just like “**Proof.**” lets us know the proof has begun), even when writing on the board.

Ready for *your* first proof? Let's do it! We just need one simple definition that will be *incredibly* useful later on: if n and d are integers, we say that d *divides* n or n *divisible by* d (and write $d|n$) if there is some other integer, k , such that $n = dk$.

Now turn the page...

2. If x is an odd integer, then $x^2 - 1$ is divisible by 4.

Here's another, to prove which you may assume some basic geometric facts (involving certain kinds of triangles, maybe...):

3. If s and t are any natural numbers with $s > t$, then there is a triangle with side lengths st , $\frac{s^2-t^2}{2}$, and $\frac{s^2+t^2}{2}$.

Proof. Let s and t be given natural numbers, $s > t$. Draw segments of length st and $\frac{s^2-t^2}{s}$ which meet at a right angle. Then...

Make sense? So far we've just had to assume P and from it derive Q directly. Let's try a different method...

- **Proof by Contradiction.** We indicated above that $P \Rightarrow Q$ is false only when P is true and Q is false. From this it's easy to see that $(P \Rightarrow Q) \Leftrightarrow \neg[P \wedge (\neg Q)]$. Here's a wee bit of space for you to build a truth table demonstrating this carefully:

What's that mean for us? It means that instead of arguing directly, we could prove instead that $\neg[P \wedge (\neg Q)]$ holds. That is, if we assume both that P is true and that Q is *not* true, we must show that we encounter some logical obstacle, or *contradiction*. What this amounts to, ultimately, is showing that *something* in our hypotheses has to have been false.

Examples? You got 'em!

1. If a , b , and c are odd integers, then $ax^2 + bx + c = 0$ has no solutions in the set of rational numbers (fractions). (Please note what “ P ” and “ Q ” are in this statement!)

Proof. Suppose, by way of contradiction, that $\frac{p}{q}$ is a solution in the set of rational numbers (that is, “ $\neg Q$ ”), and that $\frac{p}{q}$ is in “lowest terms,” so that p and q have no *common divisor* larger than 1. We plug this into the equation:

$$a\frac{p^2}{q^2} + b\frac{p}{q} + c = 0 \Rightarrow ap^2 + bpq + cq^2 = 0,$$

after multiplying by q^2 .

Because 2 is assumed to not divide both p and q , at least one of p and q is odd. Assuming first that both are odd, then each of ap^2 , bpq , and cq^2 are odd, so their sum is odd, too. But this cannot then be 0, since 0 is even! This contradiction shows that one of p and q is odd, and the other is even. If p is odd and q is even, then ap^2 is odd while bpq and cq^2 are both even, so the sum is again odd, another contradiction. Finally, you should check that p even and q odd also yields a contradiction.

We have concluded that in every case of $P \wedge \neg Q$, some contradiction arises. Thus we have shown $\neg[P \wedge (\neg Q)]$. ◇

Notes: We assumed some of our earlier work with sums and products of even and odd numbers. We also assumed properties of rational numbers; namely, that the phrase “lowest terms” makes sense to us. Finally, note the phrase “by way of contradiction.” This is a common phrase in proofs by contradiction, indicating that what will follow is such an indirect proof. Please use this phrase when building such proofs!

2. *There is no largest real number x .*

Proof. Suppose, by way of contradiction...

3. *The Golden Ratio is irrational, where we define this ratio to be value ϕ satisfying $\phi = \frac{\phi+1}{\phi}$. (Hint: look back at the first proof by contradiction, above.)*

Proof. Suppose, by way of contradiction...

4. If x and y are both odd, then so is xy . (This can be proven directly, but try using contradiction instead!)

- **Proof by Contraposition.** There's another formulation of $P \Rightarrow Q$ that is logically equivalent. You should construct a truth table in the space below to show that $(P \Rightarrow Q) \Leftrightarrow [(\neg Q) \Rightarrow (\neg P)]$:

The statement $(\neg Q) \Rightarrow (\neg P)$ is called the *contrapositive* of $P \Rightarrow Q$, and is sometimes easier to prove than the original statement itself. Let's try some examples!

1. If x is a positive number, then so is $x + 1$.

Proof. Assume that $x + 1$ is *not* positive. That is, $x + 1 \leq 0$. Thus $x \leq 0 - 1 = -1$. Therefore $x \leq -1 < 0$, so that x itself is not positive. We have thus shown $\neg Q \Rightarrow \neg P$, the contrapositive of the statement we wished to derive. \diamond

Try your hand at contraposition in proving the following statement:

2. *If the square of a number is even, then the number itself is even.*

To summarize, in order to prove $P \Rightarrow Q$...

- ...in a **direct proof**, *assume* P and *conclude* Q .
- In a **proof by contradiction**, *assume* P and $\neg Q$ and *conclude* by reaching a logical contradiction.
- In a **proof by contraposition**, *assume* $\neg Q$ and *conclude* $\neg P$.