Proof by Contradiction

Introduction

A *direct proof* is where we begin with a valid statement (which can be from the theorem's hypothesis) and make logical deductions to arrive at the theorem's conclusion. For example, if the theorem is "*if A, then B*", then we start with assuming A and make deductions until we arrive at B.

A *proof by contradiction*, on the other hand, is a type of *indirect proof*. With this we begin by negating what we want to prove ("suppose not") and make logical deductions from this to arrive at something that contradicts an accepted fact (which can be from the theorem's hypothesis). For example, if the theorem is "*if A, then B*", then a proof by contradiction would start with assuming that there is a situation where A is true but B is false. We then make logical deductions from this until we we arrive at something that cannot be, and conclude that if A is true then B must be true.

Example 1

We now consider some examples. The first proof we will look at is a very old one. Rational numbers are numbers that can be expressed in the form $\frac{p}{q}$, where $p, q \in \mathbb{Z}$, the set of integers. The set of rational numbers is denoted $\mathbb{Q}$. The existence of irrational numbers was first discovered in Ancient Greece around 500BC by the Pythagoreans (a group following the beliefs of Pythagoras, which included a rule against eating beans). They kept the existence of irrational numbers secret, and drowned Hippasus of Metapontum at sea for divulging the secret. Although historians do not know who initially proved the existence of the irrationals, many attribute it to Hippasus.

Proposition 1. *The equation $p^2 = 2$ is not satisfied by any $p \in \mathbb{Q}$.*

Proof. We need to show that p cannot be a rational number. We do this by contradiction. We suppose that the equation $p^2 = 2$ is satisfied by a $p \in \mathbb{Q}$. We will then proceed with this until we find a contradiction.

If $p \in \mathbb{Q}$, then we can write it as a fraction of two integers. We reduce this fraction using greatest common divisors until it is irreducible and arrive at $p = \frac{m}{n}$, with $m, n \in \mathbb{Z}$. Here one of m or n must be an odd number, because otherwise the fraction could be simplified further.

Because $p^2 = 2$, we have:

$$\left(\frac{m}{n}\right)^2 = 2$$

This implies $m^2 = 2n^2$. Regardless of whether n is an even or odd number, $2n^2$ is even. Thus m^2 must be even. It must also be then that m is even, because if m where odd then m^2 would be odd.

If m is even then it is divisible by 2. Therefore m^2 is divisible by 4. But because $m^2 = 2n^2$, then $2n^2$ is also divisible by 4, and so n^2 divisible by 2. But if n^2 is divisible by 2 it must be even, and therefore n must be even as well (because if n was odd, then n^2 would be odd). Thus we arrive at a contradiction because if p was rational we require one of m and n to be odd. □

Thus we assumed the converse of the proposition, and used valid logical steps to arrive at a contradiction, leading us to conclude that the proposition is true.

Example 2

For we next proof we note that if we need to prove a statement like "*A if and only if B*" (often shortened to "*A iff B*") then we need to do 2 proofs: we need to prove both "*if A, then B*" and "*if B, then A*". For shorthand, we usually write the first step as ($\Rightarrow$) and the second step as ($\Leftarrow$).

Proposition 2. *For $a, b \in \mathbb{R}$, $a = b$ if and only if $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$.*

Proof. ($\Rightarrow$) What we want to show: If $a = b$, then $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$.

This direction of the proof is very straightforward and we will do it with a direct proof. If $a = b$, then $|a - b| = 0$. Then, for any $\varepsilon > 0$, it follows that $|a - b| = 0 < \varepsilon$. Therefore it follows that if $a = b$, then $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$.

($\Leftarrow$) What we want to show: If $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$, then it must be that $a = b$.

For this we will use a proof by contradiction. We say "suppose not". That is, suppose that $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$, but that $a \neq b$.

If $a \neq b$, then $|a - b| > 0$. There is a real number $\varepsilon_0 > 0$ satisfying $\varepsilon_0 = |a - b|$. The assumption of the theorem, however, is that $\forall \varepsilon > 0$ it follows that $|a - b| < \varepsilon$. Because $\varepsilon_0 > 0$ it must follow that $|a - b| < \varepsilon_0$. But this is a contradiction because we cannot have both (i) $|a - b| = \varepsilon_0$ and (ii) $|a - b| < \varepsilon_0$ at the same time. Therefore it must be the case that $a = b$. □