Lecture 10

Proofs by Contradiction (contd.), Proof by Exhaustion

Examples: Proof by Contradiction

Theorem: There are infinitely many prime numbers.

Proof: For the sake of contradiction, suppose there are only finitely many primes.

Let $p_1, p_2, \ldots, p_n$ denote the list of all the primes in ascending order.

Consider the number $a = p_1 . p_2 . p_3 . \ldots . p_n + 1$.

Clearly, $a \; > p_n$ and thus cannot be a prime number.

Since $a > 1$, there must exist a prime divisor of a, say p_k.

Thus, there is an integer c for which $a = cp_k$, which is to say

$$p_1 . p_2 . \ldots . p_{k-1} p_k p_{k+1} . \ldots . p_n + 1 \; = cp_k$$

…

Examples: Proof by Contradiction

Dividing both sides with p_k gives us,

$$p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1} p_{k+1} \cdot \ldots \cdot p_n + \frac{1}{p_k} = c$$

So,

$$\frac{1}{p_k} = c - (p_1 \cdot p_2 \cdot \ldots \cdot p_{k-1} p_{k+1} \cdot \ldots \cdot p_n).$$

This is the q we mentioned in the outline of Proof by Contradiction.

$\neg p =$ *There are finitely many primes.*

The expression on the right is an integer, while the expression on the left is not an integer.

Since this is a contradiction, our assumption that there are finitely many primes is false.

Hence, there are infinitely many primes.

■

More on Proof by Contradiction

- Deducing p from $\neg p$ also proves p is true.

  If $\neg p \implies q_1 \implies q_2 \implies q_3 \quad \ldots\ldots \quad \implies q_k \ (= p)$

  Then, we can say that $\neg p \to p$ is true.

  If $\neg p \to p$ is true, then p is true.

- Proof by Contradiction can be applied on conditional statements as well.

  Suppose we want to prove $p \to q$ true using proof by contradiction.

  We start by assuming $\neg(p \to q)$ as true, which is the same as assuming both $\neg q$ and p as true. $(\because \neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q)$

  Then, we try to arrive at a contradiction.

Mixed Proofs

You are free to use more than one methods of proof while proving a statement.

Here's an example.

Theorem: Every non-zero rational number can be expressed as a product to two irrational numbers.

Proof: We can reword the theorem as follows:

If r is a non-zero rational number, then r is a product of two irrational numbers.

Since r is a non-zero rational number, $r = \frac{a}{b}$, where $a \neq 0$ and $b \neq 0$ are integers.

Also, r can be written as a product of two numbers as follows:

$$r = \sqrt{2} . \frac{r}{\sqrt{2}}$$

Mixed Proofs

We will show now that $\dfrac{r}{\sqrt{2}}$ is also irrational using proof by contradiction.

Suppose $\dfrac{r}{\sqrt{2}}$ is rational. Then, for integers c and $d \neq 0$, $\dfrac{r}{\sqrt{2}} = \dfrac{c}{d}$.

$\neg p$

So,

$$\sqrt{2} = r\frac{d}{c} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}$$

q

This means $\sqrt{2}$ is rational, which is a contradiction because we know it is irrational.

Therefore, $\dfrac{r}{\sqrt{2}}$ is irrational.

Proof by Exhaustion

In **Proof by Exhaustion (aka Proof by Cases)** mathematical statement that has to be proven is split into a finite number of cases, where each case is proved separately.

A proof by exhaustion typically contains **two stages**:

- A proof that the set of cases is exhaustive. ← *Skipped when obvious.*
- A proof of each of the cases.

Proof by Exhaustion are usually avoided due to following reasons:

- They are viewed as inelegant.
- It's easy to miss out on a few cases.

Example: Proof by Exhaustion

Theorem: If an integer n is a perfect cube, then n must be either a multiple of 9, 1 more than a multiple of 9, or 1 less than a multiple of 9.

Proof: If n is a perfect cube, then $n = k^3$, where k is an integer.

We will consider three cases based on the value of $k \,\%\, 3$.

Case 1: When $k \,\%\, 3 = 0$

If $k \,\%\, 3 = 0$, then $k = 3q$, for some integer q.

Then, $n = k^3 = (3q)^3 = 27q^3$, which is a multiple of 9.

Case 2: When $k \,\%\, 3 = 1$

If $k \,\%\, 3 = 1$, then $k = 3q + 1$, for some integer q.

Then, $n = k^3 = (3q+1)^3 = 27q^3 + 27q^2 + 9q + 1 = 9(3q^3 + 3q^2 + q) + 1$, which is 1 more than a multiple of 9.

…

Example: Proof by Exhaustion

Case 3: When $k \% 3 = 2$

If $k \% 3 = 2$, then $k = 3q + 2$, for some integer q.

If $k = 3q + 2$, then $k = 3q + 3 - 1 = 3(q + 1) - 1 = 3q' - 1$, for some integer q'.

Then, $n = k^3 = (3q' - 1)^3 = 27q'^3 - 27q'^2 + 9q' - 1 = 9(3q'^3 - 3q'^2 + q') - 1$,

which is 1 less than a multiple of 9.

$\blacksquare$