Lecture 11

Proof by Exhaustion (contd.), Existence Proof, Forward & Backward Reasoning

More on Proof by Exhaustion

When to use Proof by Exhaustion?

When extra information in each case helps move the proof forward.

Do we always need to prove all the cases?

No. Sometimes proof of one case follows by making small changes to the proof of another case.

Example on the next slide.

Leaving Cases: Proof by Exhaustion

Theorem: Suppose $x, y \in \mathbb{Z}$. If both xy and $x + y$ are even, then both x and y are even.

Proof: We will prove the contrapositive of the theorem. That is,

Suppose $x, y \in \mathbb{Z}$. If either x or y is odd, then either xy or $x + y$ is odd.

Case 1: Assume both x and y are odd.

By the definition of an odd integer, $x = 2k + 1$ and $y = 2k' + 1$, for some integers k and k'.

So,

$$xy = (2k + 1)(2k' + 1) = 4kk' + 2k + 2k' + 1 = 2(2kk' + k + k') + 1$$

Thus, $xy = 2k'' + 1$, where k'' is an integer. Hence, xy is an odd integer.

continue…

Leaving Cases: Proof by Exhaustion

Case 2: *Without loss of generality* assume that x is odd and y is even.

By the definition of an odd integer, $x = 2k + 1$, for some integer k.

By the definition of an even integer, $y = 2k'$, for some integer k'.

So,

$$x + y = 2k + 1 + 2k' = 2(k + k') + 1$$

Thus, $x + y = 2k'' + 1$, where k'' is an integer. Hence, $x + y$ is an odd integer. ■

Note: A third case, where x is even and y is odd, is not required because proof for this case is the same as the proof of Case 2 where x and y are interchanged.

Existence Proofs

A proof of a proposition such as $\exists x P(x)$ (or $\exists x \exists y P(x, y)$, etc.) is called an **existence proof**.

An existence proof of proposition $\exists x P(x)$ that actually gives a c, such that $P(c)$ is true is called **constructive proof**.

For instance, for a non-zero rational number r, we actually constructed two irrational numbers, $\sqrt{2}$ and $\frac{r}{\sqrt{2}}$, whose product is r.

An existence proof of proposition $\exists x P(x)$ that proves the existence of a c for which $P(c)$ is true without actually giving a c is called **nonconstructive proof**.

Example on the next slide.

Example: Non-constructive Existence Proof

Theorem: There exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational.

Consider the number $\sqrt{2}^{\sqrt{2}}$. If $\sqrt{2}^{\sqrt{2}}$ is rational, then $x = y = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ because,

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$$

■

Note: Above is an example of non-constructive proof because theorem is true for either $x = \sqrt{2}$ and $y = \sqrt{2}$ or $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, but we do not know for which one.

Forward and Backward Reasoning

Two strategies to prove a mathematical statement, say p:

Forward Reasoning:

Try to find proof of p using premises, axioms, and existing theorems in a straightforward manner.

Backward Reasoning:

Assume p and try to deduce a true statement q in such a way so that you can also deduce p from q.

Example: Backward Reasoning

Theorem: For any two positive real numbers x and y, their arithmetic mean is greater than or equal to their geometric mean.

Reasoning: Arithmetic mean $= \dfrac{x+y}{2}$ Geometric mean $= \sqrt{xy}$

$$\left.\begin{aligned}
(x+y)/2 &\geq \sqrt{xy} \\
(x+y)^2/4 &\geq xy \\
(x+y)^2 &\geq 4xy \\
x^2+y^2+2xy &\geq 4xy \\
x^2+y^2-2xy &\geq 0 \\
(x-y)^2 &\geq 0
\end{aligned}\right\} \longleftarrow$$

Last inequality can be deduced from first inequality and vice versa.

Note: The actual proof must deduce the first inequality from the last inequality.

Disproving Mathematical Statements

How to disprove a mathematical statement, say p?

Prove $\neg p$. (Be careful while forming $\neg p$.)