Fall, 2024

DISCRETE MATHEMATIC LEC-02:

Method of Proofs

Instructor: MS.c Nguyen Thi Huong

Lecture 2

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction
- Proof by Cases.

Definitions

- **<u>Why proof?</u>**
- **<u>Proof:</u>** A sequence of statements, ending with the proposition being proved; each statement is either an axiom or can be deduced easily from the previous statements.
- In proving theorems or solving problems, creativity and insight are needed, which cannot be taught.

Definitions

- **<u>Theorem</u>**: a true proposition that is guaranteed by a proof.
- **<u>Axiom:</u>** an assertion we accept without proof.

Example 1

- Theorem:

  If n^2 is odd, then n is odd.

- Axiom:

  If equals are added to equals, the wholes are equal.

Types of Proof

Direct Proof

Direct proof of P=>Q

Assume P

=>A

=>B

…

Therefore Q

Example 2

- Theorem: If x is odd, then $x + 1$ is even.
- Proof
  Assume x is odd
  => $x = 2k + 1$
  => $x + 1 = 2(k + 1)$
  Therefore, x + 1 is even

Example 3

- Theorem: Let n be a positive integer less than 1000. If the sum of the digits of n is divisible by 9, then n is divisible by 9.
- Proof
  Let n be abc. Assume (a + b + c) is divisible by 9.
  n = abc
  => n = 100a + 10b + c
  => n = 99a + 9b + (a + b + c)
  since a + b + c is divisible by 9
  Therefore, n is divisible by 9

Example 4

- **<u>Theorem:</u>** n is divisible by 9 iff the sum of digits is divisible by 9.
- Proof: n is divisible by 9

$$
\begin{aligned}
\Leftrightarrow \quad & n = 9l, && l \in Z && (1)\\
\Leftrightarrow \quad & 100a + 10b + c = 9l, && l \in Z && (2)\\
\Leftrightarrow \quad & 99a + 9b + (a + b + c) = 9l, && l \in Z && (3)\\
\Leftrightarrow \quad & (a + b + c) = 9l - 99a - 9b, && l \in Z && (4)\\
\Leftrightarrow \quad & (a + b + c) = 9(l - 11a - b), && l \in Z && (5)\\
\Leftrightarrow \quad & (a + b + c) = 9k, && k, l \in Z, (k = l - 11a - b) && (6)\\
\Leftrightarrow \quad & (a + b + c) \text{ is divisible by } 9 && && (7)
\end{aligned}
$$

Example 5

- Proof: $$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

- **Binomial Coefficients:** The number of distinct subsets with *k* elements that can be chosen from a set with *n* elements is denoted by $\binom{n}{k}$

, and is pronounced "*n choose k*." The number $\binom{n}{k}$ is called a binomial coefficient.

$$\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}$$

Example 5

- Proof: $$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

$$\begin{aligned}
\text{LHS} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\
&= \frac{n!}{k(k-1)!(n-k)!} + \frac{n!}{(k-1)!(n-k)!(n-k+1)} \\
&= \frac{n!(n-k+1) + n!k}{k!(n-k+1)!} \\
&= \frac{n!(n+1)}{k!(n+1-k)!} = \text{RHS}
\end{aligned}$$

Indirect Proofs

Proof by Contraposition

Proof by contraposition of P=>Q

Assume ¬Q.

…

Therefore ¬P.

So ¬Q=>¬P ≡ P=>Q

Example 6

- <u>Theorem:</u> If n^2 is even, then n is even
- <u>Proof:</u>
  Assume n is odd
  => $n = 2k + 1$
  => $n^2 = 2(2k^2 + 2k) + 1$
  Therefore n^2 is odd
  So if n is odd then n^2 is odd. This is equivalent to if n^2 is even then n is even.

Example 7

- Prove that if $n \in \mathbb{Z}$ and $3n+2$ is odd, then n is odd.
- <u>Proof:</u>
  Assume the ¬(conclusion): *n* is even

$$\Rightarrow n = 2k \tag{1}$$

$$\Rightarrow 3n+2 = 3(2k)+2 = 2(3k+1) \tag{2}$$

Therefore 3*n*+2 is odd: ¬(hypothesis)
So if *n* is odd then 3*n*+2 is odd. This is equivalent to if *n* is even then 3*n*+2 is even.

Open Question

- Show a direct proof of the following theorem.
- Theorem: if n^2 is odd, then n is odd.

$$
\begin{aligned}
& n^2 \text{ is odd} && (1)\\
\Rightarrow\quad & (n^2-1) \text{ is even} && (2)\\
\Rightarrow\quad & (n-1)(n+1) \text{ is even} && (3)\\
\Rightarrow\quad & \begin{cases} (n-1) \text{ is even} \\ (n+1) \text{ is even} \end{cases} && (4)\\
\Rightarrow\quad & n \text{ is odd} && (5)
\end{aligned}
$$

Proof by Contradiction

Proof by contradiction of P

Assume ¬P

…

R

…

¬R

Contradiction

Therefore P

Example 8

- Theorem: There are infinitely many prime.
- Proof:
  Assume there are only finitely many primes.
  => p_1, p_2, .., p_k are all primes.
  => $p_1p_2\ldots p_k + 1$ is not a prime.
  => $p_1p_2\ldots p_k + 1$ has a prime divisor $p > 1$.
  => p must be one of $p_1,p_2,\ldots,p_k$
  => p divides 1 => $p \leq 1$. Contradiction.
  Therefore there are infinitely many primes.

Example 9

- Theorem: $\sqrt{2}$ is irrational
- Proof:

Assume $\sqrt{2} = a/b$. 2 is not a common factor of a and b

$\Rightarrow 2 = a^2/b^2$

$\Rightarrow a^2 = 2b^2$

$\Rightarrow a^2$ is even

$\Rightarrow a$ is even

$\Rightarrow a = 2c$.

$\Rightarrow 2b^2 = 4c^2$

$\Rightarrow b^2 = 2c^2$.

$\Rightarrow a$ and b have a common factor 2

Contradiction. Therefore $\sqrt{2}$ must be irrational.

Open Question

- Show a proof by contradiction of the following theorem.
- Theorem: if n^2 is odd, then n is odd.
- How to make a negation of proposition?

$$P \Rightarrow Q \text{ is false only when P is true, Q is false}$$

$$\text{Assume that } n^2 \text{ is odd, and } n \text{ is even} \tag{1}$$

Proof by Cases

Sometime we don’t know which of a set of possible cases is true, but we know that at least one of the cases is true. If we can prove at least one of possible cases is true then we have a proof.

Example 10

- Theorem: For some irrational number *x* and *y*, x^y is rational.
- Proof:
  Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational (done.)

  Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

  $$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$$ is rational (done.)

Test 1

- Show that the square of an even number is an even number using direct proof.

$$\text{if } x \text{ is even then } x = 2k, k \in \mathbb{Z}$$

$$\Rightarrow x^2 = 4k^2$$

$$\Rightarrow x^2 = 2(2k^2)$$

$$x^2 \text{ is even}$$

Test 2

- Show that if n is an integer and $n^3 + 5$ is odd, then n is even using:
  - A proof by contraposition.
  - A proof by contradiction.

Test 3

- Proof by contraposition:

$$\text{Assume } n \text{ is odd then}$$

$$\Rightarrow n^2 \text{ is odd}$$

$$\Rightarrow n^3 \text{ is odd}$$

$$\Rightarrow n^3 + 5 \text{ is even}$$

Test 4

- Proof by contradiction:

Suppose there is an integer n such that

$$\boxed{n^3 + 5 \text{ is odd}} \text{ then } n \text{ is odd}$$

$$\Rightarrow n = 2k + 1, k \in \mathbb{Z}$$

$$\Rightarrow n^3 + 5 = (2k+1)^3 + 5$$

$$= 8k^3 + 12k^2 + 6k + 6$$

$$= 2(4k^3 + 6k^2 + 3k + 3)$$

$$\Rightarrow \boxed{n^3 + 5 \text{ is even}}$$

Contradiction

Test 5

- Show that if n is an integer and n^3+5 is odd, then n is even by using direct proof?

$$
\begin{aligned}
n^3+5-n &= n(n^2-1)+5 \\
&= (n-1)n(n+1)+5
\end{aligned}
$$

$$(n-1)n(n+1) \text{ is even}$$

$$\Rightarrow (n-1)n(n+1)+5 \text{ is odd}$$

$$\Rightarrow \begin{cases} n^3+5 \text{ is odd} & \text{then } n \text{ is even} \\ n^3+5 \text{ is even} & \text{then } n \text{ is odd} \end{cases}$$

Summary

- Direct proofs
- Proofs by contraposition
- Proofs by contradiction
- Proofs by cases
- Homework: Problem Set 2