BCSE304L - Theory of Computation

L	T	P	C
3	0	0	3

Dr. M. Bhuvaneswari

Assistant Professor Senior Gr.2

School of Computer Science and Engineering

Vellore Institute of Technology, Vellore

m.bhuvaneswari@vit.ac.in

Thanks To: Dr. Gunavathi and Dr. Somasundaram, SCOPE, VIT, Vellore

Proof Techniques

A proof involves a **statement of the form p → q (p implies q)**

There are several methods for establishing a proof of statements.

Some of them are

1. Direct proof
2. By contradiction
3. By mathematical induction.
4. Indirect proof / By Contrapositive
5. Deductive proof

Direct proof

If we have to prove that $p \rightarrow q$, then a direct proof assumes p is true and try to prove q is true.

<u>Example: 1</u>

Prove for any integer a and b if a and b are odd then ab is odd.

Solution: Any odd integer u, can be written as $2v+1$, where v is an integer.

Given that a and b are odd integer, by the above statement

$$a = 2x + 1 \quad \text{and} \quad b = 2y + 1\text{, where } x, y \text{ are integers.}$$

Use this fact and prove the product ab is also odd.

$ab = (2x + 1)(2y+1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1 = \mathbf{2w+1}$

where $w = 2xy + x + y$ is an integer.

Hence, ab is an odd number.

Proof by contradiction

- We need to prove **$p \rightarrow q$**.
- A contradiction is a propositional form which is always false.
- Assume that P is true and Assume that ¬Q is true.
- Use P and ¬Q to demonstrate a contradiction. ¬Q must be false. Q is true

Proof by contradiction

- **Example 1:**
- If a and b are consecutive integers, then the sum a + b is odd.
- Assume a and b are consecutive integers and the sum a + b is not odd
- Since sum a + b is not odd, **there exists no number k** such that **a + b = 2k + 1**
- However, the integers a and b are consecutive, means a+b=2a+1
- we have derived that a + b ≠ 2k + 1 for any integer k and also that

a + b = 2a + 1. This is a contradiction.

sum a + b is not odd is false. sum a + b is odd

Proof by contradiction

Example 2:

Prove for any integer a and b if a and b are odd then ab is odd.

Solution: To prove this, assume the contrary that ab is even.

ab is even implies, $ab = 2z$, for some integer z.

Given that a and b are odd integer, by the above statement

$a = 2x + 1$ and $b = 2y + 1$, where x, y are integers.

Therefore, $ab = 4xy + 2x + 2y + 1 = 2z$

$$z = 2xy + x + y + (½)$$

z is not an integer and hence a contradiction. ab odd an number.

Example 3:

A rational number is a number that can be expressed as the ratio of two integers n and m have no common factor. A real number that is not rational is said to be irrational.

Show that $\sqrt{2}$ is irrational.

Solution: Assume the contrary that $\sqrt{2}$ is rational.

$\sqrt{2}$ is rational implies, $\sqrt{2} = n/m$ ---------------- (1)

where n and m are integers andhave no common factor.

From (1), $2m^2 = n^2$ ---------------- (2)

implies n^2 is even and hence n is even.

Therefore, we can write $n = 2k$ for some integer k.

From (2), $2m^2 = 4k^2$

$m^2 = 2k^2$ implies m^2 is even and hence $m$is even.

This is contradiction to the fact that n and m have no common factor.

Proof by mathematical induction

Proof by mathematical induction consists of three basic steps. If the statement **p** is to be proved then:

1) Show that **p** is true for some particular integer n_0

   - this is called **Basis**

2) Assume **p** is true for some particular integer $k \geq n_0$

   - this is called **Induction hypothesis**

3) Then to prove is true for $k+1$

   - this is called **Induction step**

Example 1

Show that for any $n \geq 1$, $1 + 2 + . . . + n = n(n+1)/2$

Solution:

Let P(n) : $1 + 2 + . . . + n = n(n+1)/2$

Basis step: P(1) : $1 = 1(1+1)/2 = 1$

P(1) is true.

Induction hypothesis: Assume that P(k) is true for some k.

P(k): $1 + 2 + . . . + k = k(k+1)/2$ ------------(1)

Induction step: To prove P(k+1) is also true.

Take the LHS P(k+1) and prove the RHS.

$1 + 2 + . . . + k + (k+1) = k(k+1)/2 + (k+1) = (k+1)\ (k/2 +1)$ using (1)

$= (k+1)(k+2)/2$

Therefore, P(k+1) is true and hence P(n) is true for any n.

Example 2

prove the following by Induction for all n=0

$$1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

(or)

$$\sum_{i}^{n+1} n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 2 - IH:

Let n = 1,

$$1^2 = \frac{1(1+1)(2+1)}{6}$$

$$1 = \frac{(2)(3)}{6}$$

$$1 = 1$$

Let n = 2,

$$1^2+2^2 = \frac{2(2+1)(4+1)}{6}$$

$$5 = \frac{2(3)(5)}{6}$$

$$5 = 5$$

Step 1 - Basis

Basis : Let n = 0,

$$0^2 = \frac{0(0+1)(0+1)}{6}$$

$$\Longrightarrow 0 = 0$$

Step 3 - IS:

$5 = 5$

By Induction : ~~K~~ $n \geq i$, $i \Rightarrow$ basis integer

$$S(n) = 1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

is true for all 'n' values.

S(n) is true for all $n \geq i$

Now, we have to prove S(n+1) is also true

$$S(n+1) = 1^2+2^2+\dots+(n+1)^2 = \frac{(n+1)(n+2)(2(n+}{6}$$

LHS:

$$S(n+1) = 1^2+2^2+\dots+n^2+(n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6}+(n+1)^2$$

$$= \frac{n(n+1)(2n+1)+6(n+1)^2}{6}$$

$$= \frac{(n+1)[n(2n+1)+6(n+1)]}{6}$$

$$= \frac{(n+1)[2n^2+n+6n+6]}{6}$$

Cont...

[I-13]

$$= \frac{(n+1)\left[2n^2+7n+6\right]}{6}$$

$$= \frac{(n+1)\left[(n+2)(2n+3)\right]}{6}$$

$$= \frac{(n+1)\left[(n+1)+1\right]\left[2(n+1)+1\right]}{6}$$

$$= \frac{(n+1)(n+2)(2(n+1)+1)}{6}$$

$$= RHS$$

$$\therefore \boxed{LHS = RHS}$$

Hence, proved.

So, $S(n+1)$ is also true.

$$\therefore S(n) = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Example 3

Prove $1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$ by Mathematical Induction.

Basis: Let $n=0 \Rightarrow 0^3 = \frac{0^2(0+1)^2}{4} \Rightarrow 0=0$

$n=1 \Rightarrow 1^3 = \frac{1^2(1+1)^2}{4} \Rightarrow 1=1$

$n=2 \Rightarrow 2^3+1^3 = \frac{2^2(2+1)^2}{4} \Rightarrow 9=9$

By Induction:

$S(n) = 1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$

$S(n)$ is true (i.e.) $n \geq i$

Cont..

We have to prove $S(n+1)$ is also true

$$S(n+1) = 1^3+2^3+\dots+(n+1)^3$$

$$= \frac{(n+1)^2\,(n+1+1)^2}{4}$$

LHS

$$S(n+1) = 1^3+2^3+\dots\overset{n^3}{+}(n+1)^3 = \cancel{S(n+1)}$$

$$= \frac{(n^2(n+1)^2)}{4} + (n+1)^3$$

$$= \frac{(n^2(n+1)^2) + 4(n+1)^3}{4}$$

$$= \frac{(n+1)^2\,[n^2+4(n+1)]}{4}$$

$$= \frac{(n+1)^2\,[n^2+4n+4]}{4}$$

$$= \frac{(n+1)^2\,(n+2)^2}{4}$$

$$= \frac{(n+1)^2\,[(n+1)+1]^2}{4}$$

LHS = RHS

Thus,

$$S(n) = 1^3+2^3+\dots+n^3 = \frac{n^2(n+1)^2}{4}$$

Example 4

Prove that $S(n) = a^n - b^n$ is divisible by $(a-b)$ for all $n>0$

Soln:

Given: For $n>0$, $a^n - b^n$ is divisible by $(a-b)$

Basis:

$n=1 \Rightarrow a-b$ is divisible by $a-b$

$n=2 \Rightarrow a^2-b^2$ is divisible by $a-b$

Induction: $S(n)$ is true for $n \geq 1$

Such that, $S(n) = a^n - b^n$ is divisible by $a-b$

To prove $S(n+1) = a^{n+1} - b^{n+1}$ is also divisible by $a-b$

LHS

$$S(n+1) = a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot b^n \longrightarrow (1)$$

We know that

$$\Rightarrow S(n) = \frac{(a^n - b^n)}{(a-b)} = K \Rightarrow [\text{Constant}]$$

$$(a^n - b^n) = K(a-b)$$

$$a^n = b^n + K(a-b) \longrightarrow (2)$$

Sub. (2) in (1),

$$= [b^n + K(a-b)]\, a - b^n \cdot b$$

$$= [K(a-b) + b^n]\, a - b^n \cdot b$$

$$= K(a-b)a + b^n a - b^n \cdot b$$

$$= Ka(a-b) + b^n(a-b)$$

$$= (a-b)[Ka + b^n] \text{ is divisible by } (a-b)$$

$$= \text{RHS}$$

$S(n+1) = a^{n+1} - b^{n+1}$ is also divisible by $(a-b)$

$S(n) = a^n - b^n$ is divisible by 3.