BCSE304L - Theory of Computation

L	\mathbf{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

Proof Techniques

A proof involves a statement of the form $p \rightarrow q$ (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.

Example: 1

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

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

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

ab =
$$(2x + 1)(2y+1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1 = 2w+1$$

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 $\neg Q$ is true.
- Use P and $\neg Q$ to demonstrate a contradiction. $\neg Q$ 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 $a + b \ne 2k + 1$ 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,
$$ab = 4xy + 2x + 2y + 1 = 2z$$

 $z = 2xy + x + y + (\frac{1}{2})$

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 n² 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 mis 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 n₀
 - this is called **Basis**
- 2) Assume p is true for some particular integer $k \ge n_0$
 - this is called **Induction hypothesis**
- 3) Then to prove is true for k+1
 - this is called **Induction step**

Show that for any $n \ge 1$, 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.

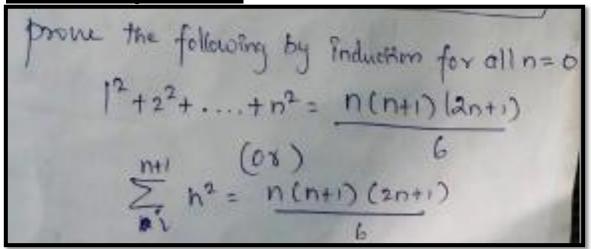
$$P(k): 1 + 2 + ... + k = k(k+1)/2$$
 -----(1)

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

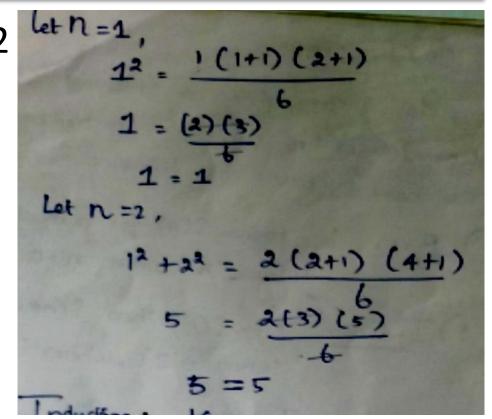
Take the LHS P(k+1) and prove the RHS.

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

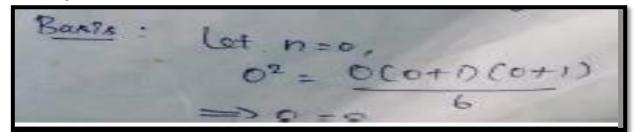
Therefore, P(k+1) is true and hence P(n) is true for any n.

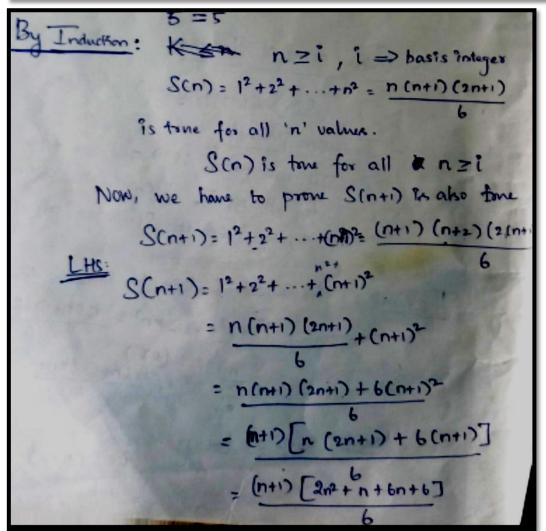


Step 2 - IH:



Step 1 - Basis





Step 3
- IS:

Cont...

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

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

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

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

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

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

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

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

Basis: Let
$$ne = 0 = > 0^3 = 0^2 (0+1)^2 = > 0 = 0$$
 $n = 1 \Rightarrow 1^3 = 1^2 (1+1)^2 = > 1 = 1$
 $n = 2 \Rightarrow 2^3 + 1^3 = 2^2 (2+1)^2 \Rightarrow 9 = 9$

By Industron:

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

Cont..

We have to prove
$$S(n+1)$$
 is also true
$$S(n+1) = 1^{3} + 2^{3} + ... + (n+1)^{3}$$

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

$$S(n+1) = 1^{3} + 2^{3} + ... + (n+1)^{3} = S(n+1)$$

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

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

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

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

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

$$= \frac{(n+1)^2 \left[(n+1) + 1\right]^2}{4}$$
Lets = RHs

Schr.

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 $n \ge i$

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

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

LHS

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

We know that

$$\Rightarrow S(n) = (a^n - b^n) = K \Rightarrow Constant$$

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

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

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

Sub. 2 in D, = [b"+ k(a-b)] a - b". b = [k(a-b)+bn] a - bn. b = K(a-b)a+bna-bn.b = ka(a-b) + bn (a-b) = (a-b) [Ka + bm] is divisible by (a-b) = RHS S(n+1) = ant | - bn+1 is also divisible by (a-b) S(n) = an - bn is divisible by 3.