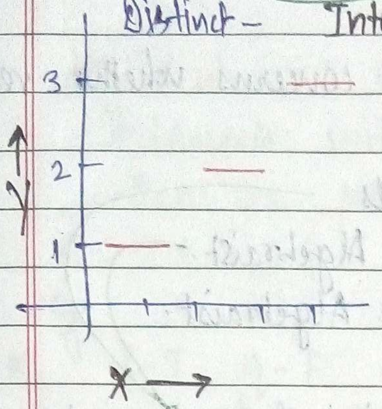
# DISCRETE STRUCTURES

Distinct – Integers




→ Study of mathematical structure.

→ Mathematical model with certain properties.

→ Study of mathematics of integers and of collection of objects that trigger the operation of digital computer, almost all fields of CS, programming & reasoning of data structure, algorithms, complexity

1. Set, Relation, Function
   - Language of Mathematics.
   - → A collection of distinct objects, order is not considered.

   Set, Sequence, String
   (Sequence → Order considered)

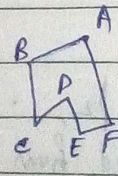
* Algorithm: Step by step solution to solve a problem

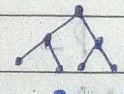
2. Logic & Proof (techniques)
   - → Study of Reasoning
   - → frame statements, syntactically, semantically correct or not.
   - → Proof by contradiction

3. Combinatorics

4. Algebraic Structures & Morphisms
   - Semigroups, monoid, group, ring, field.

5. Introduction ~~to~~ Graph Theory



## LOGIC and PROOFS

Logic is the study of reasoning; it concerns whether reason is correct or not.

Eg. → All mathematicians wear sandals
→ Anyone who wears sandals is an Algebraist.
→ Therefore all mathematicians are Algebraist.

Logic is of no use in determining the correctness of the statement

### Propositions

Def$^n$: A sentence that is either true or false but not both is called proposition

Declarative sentence T/F
(a) Earth is the only planet in Universe that contains life. T/F ✓
(b) The +ve integer that divides 7 are 1 & 7 T ✓
(c) Tom won Academic Award in 2016 for directing the picture 'Universe'. F ✓

If $p$ & $q$ are two propositions
propositions :-

| | | | |
|---|---|---|---|
| $p$ and $q$ | : $p \wedge q$ | – $\wedge$ | conjunction |
| $p$ or $q$ | : $p \vee q$ | – $\vee$ | disjunction |
| not $p$ | : $\neg p$ | – $\neg$ | negation |

$p$ : it is raining
$q$ : it is hot

| $p$ | $\neg p$ |
|---|---|
| T | F |
| F | T |

| $p$ | $q$ | P: $p \wedge q$ | Q: $p \vee q$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | F | T |
| F | F | F | F |

P – $p_1, p_2, \ldots p_n$
(Any produced from $n$ no. of propositions) is also a proposition

## Precedence

Statements without parenthesis
then the precedence of opⁿ - $\neg, \wedge, \vee$ (from left)
* / + -

eg:
* $p$-T $q$-F $r$-F
$\neg p \vee q \wedge r$
$\equiv F \vee F \equiv F$.

* p: Today is Monday F
q: it is not raining T
r: it is hot. T

1. $(p \wedge q) \wedge \neg(r \vee p)$
$F \wedge \neg(T)$
$F \wedge F$
$F$

2. $(p \vee \neg r) \wedge ((q \vee r) \vee \neg(r \vee p))$
$F \wedge (T \vee F)$
$F$

## Conditional Proposition

p & q propositions

If p then q $\quad p \rightarrow q$

p ⇒ hypothesis or antecedent
q ⇒ conclusion or consequent.

eg Director has announced that if CS Dept. gets INR 50 lakhs (p) then it will hire one new faculty member (q).

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

PAGE:
DATE: / /

eg:
For all real values of $x$, if $x > 0$ ; $x^2 > 0$

eg: $p - T$ $q - F$ $r - T$

(a) $p \wedge q \rightarrow r$ $T \wedge T \Rightarrow T$
(b) $p \vee q \rightarrow \neg r$ $T \vee T \Rightarrow T$ ? OR $F \rightarrow T \Rightarrow T$ ; ? $T \rightarrow F \Rightarrow F$
(c) $p \wedge (q \rightarrow r)$ $T \wedge T \Rightarrow T$
(d) $p \rightarrow (q \rightarrow r)$ $T \rightarrow T \Rightarrow T$

If the truth value of a conditional proposition is true because the hypothesis is false then it is called true by default or vacuously true.

Biconditional Proposition

p & q — If p then q
Converse — If q then p

roles of p & q are reversed

$p \leftrightarrow q$

| p | q | $p \Leftrightarrow q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

eg: If tom receives scholarship then he goes to college | If tom goes to college then he receives scholarship

P, Q have same truth values found out from truth value of n no. of propositions. $P \equiv Q$

# DE MORGAN'S LAWS

1. $\neg(p \vee q) \equiv \neg p \wedge \neg q$
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$

| | | P | Q |
|---|---|---|---|
| p | q | $\neg(p \vee q)$ | $\neg p \wedge \neg q$ |
| T | T | F | F |
| T | F | F | F |
| F | T | F | F |
| F | F | T | T |

Def$^n$ **Contrapositive**

If $p \to q$
then $\neg q \to \neg p$

not only the roles of p & q are reversed but also negates each of the proposition.

| | | P | Q | |
|---|---|---|---|---|
| p | q | $p \to q$ | $\neg q \to \neg p$ | |
| T | T | T | T | $(F \to F)$ |
| T | F | F | F | $(T \to F)$ |
| F | T | T | T | $(F \to T)$ |
| F | F | T | T | $(T \to T)$ |

Q. Show that negation of $p \to q$ is logically equivalent to $p \wedge \neg q$

$P : \neg(p \to q)$
$Q : p \wedge \neg q$

| | | | Q | | P |
|---|---|---|---|---|---|
| p | q | $\neg q$ | $p \wedge \neg q$ | $p \to q$ | $\neg(p \to q)$ |
| T | T | F | F | T | F |
| T | F | T | T | F | T |
| F | T | F | F | T | F |
| F | F | T | F | T | F |

Hence, $P \equiv Q$.

PAGE:
DATE: 21/07/16

Theorem

The conditional proposition $p \to q$ and its contrapositive $\neg q \to \neg p$ are equivalent.

Precedence Order :- $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$

Proposition
Hypothesis
Conclusion
De Morgan's Law
Logical equivalence

$$\underbrace{p \wedge q}_{2^{nd}} \to \underbrace{\neg r}_{1^{st}}$$

3rd

p: n is an odd integer
n is in set of integers
n is D, discourse of Domain
D is the set of integers

P(x) : n is an odd integer
P(1) : 1 T
P(2) : 2 F

★ P(x) is a proposition
P is not a proposition.

⇒ P(x) → Propositional function

Def$^n$ : Let P(x) be a statement involving the variable x and let D be a set. We call P a propositional function or predicate (with respect to D), if for each x in D, P(x) is a proposition. D is the domain of discourse of P.

Ex1. $n^2 + 2n$ is an odd integer.
odd or even, even

P(n) : $n^2 + 2n$ D: set of +ve integers.

$P(x) = x^2 - x - 6 = 0$ → is positive (or negative)
$(x-3)(x+2)$
D: set of real no's

# Quantifier

- → Universal Quantifier ($\forall x$ ; for all $x$)
- → Existential Quantifier ($\exists x$ ; there exists $x$)

## Universal Q.

$\forall x$, $P(x)$ is true if $P(x)$ is true for every value of $x$ in $D$
$\forall x$, $P(x)$ is false if $P(x)$ is false for at least one value of $x$ in $D$

**Ex1** $\forall x \; (\underbrace{x^2 \geq 0}_{P(x)})$ ; $D$ - set of Real no.s

→ T

- F → counter example
if it is false for atleast one value of $x$

$\forall x \; (x^2 > 0)$ → false for $x = 0$

$\forall x \; (x^2 - 1 > 0)$ → for $x = 1$, it is F

$\forall x \; P(x)$
→ free variable wrt $D$
→ bound variable

**Ex.** For any real no. $x$ if $x > 1$, then $x + 1 > 1$

$x > 1$
$x + 1 > 1 + 1$

$P(x) : x > 1$ is F at $x = -1$
But this proposition is always true.

$\boxed{R(x) : (x>1) \to (x+1>1) \to T}$ ($\forall x \in D$)

| p | q | |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

## Existential Q.

$\exists x \; P(x)$ - T if $P(x)$ is true for at least one value of $x$ in $D$

$\exists x \; P(x)$ - F if $P(x)$ is false for all values of $x$ in $D$.

**Ex.** $\exists x \left( \dfrac{x}{x^2+1} = \dfrac{2}{5} \right)$ $D \to$ set of real no.

True for $x = 2$ ⇒ True

Ex: $\exists x \left( \frac{1}{x^2+1} > 1 \right) \longrightarrow F$

$x$ real, $x^2 \geq 0$

$x^2+1 \geq 1$

$\frac{1}{x^2+1} \leq 1 \Rightarrow \frac{1}{x^2+1} \not> 1$

Ex: For some $n$,
if $n$ is prime then $n+1$, $n+2$, $n+3$ and $n+4$ are not prime.

$n=2$, $\overset{\checkmark}{3}, \overset{\times}{4}, \overset{\checkmark}{5}, \overset{\times}{6}$

$n=23$, $\overset{\times}{24}, \overset{\times}{25}, \overset{\times}{26}, \overset{\times}{27} \Rightarrow$ True

$\exists n \; P(n)$:

True.

25/07/16

## GENERALIZED DE MORGAN LAWS FOR LOGIC

Propositional function ($P$)

Quantifier: Universal, Existential

If $P$ is a propositional $f^n$ then each pair of propositions in (a) & (b) has the same value, true or false.

(a) $\neg(\forall x \, P(x))$ ; $\exists x \; (\neg P(x))$

(b) $\neg(\exists x \, P(x))$ ; $\forall x \; (\neg P(x))$

Proof :-

(a) Let $\neg(\forall x \, P(x)) \rightarrow$ true

$\Rightarrow \forall x \; P(x) \rightarrow$ false

At least for one value of $x$, $P(x)$ is false.

At least for one value of $x$, $\neg P(x)$ is true

$\Rightarrow \exists x \; (\neg P(x)) \rightarrow$ true.

$\neg(\forall x \, \neg P(x)) \equiv \exists x (\neg\neg P(x)) \equiv \exists x (P(x))$

Orion PAGE: DATE: / /

# Nested Quantifier - Multiple variables

Example

1. • If $(x>0) \land (y>0)$ then $(x+y)>0$ — D → +ve Real, $x, y \in D$

• The sum of two +ve real no. is a +ve real no.

$\forall x \forall y \, (x+y>0)$

2. $\forall m \exists n \, (m<n)$ — $m, n \in D$ → +ve Real no.

$\hookrightarrow n = m+1 \rightarrow$ True

3. If $(x>1) \land (y>1)$ — D → +ve integers.

then $(xy>6)$ ⟷ True or false.

$\exists x \exists y \, (\neg p(x)) \rightarrow$ True.

F ⇒ vacuously true.

4. If $(x>1) \land (y>1)$ — D → +ve integers.

then $xy=7$ → $P(x)$

$x=1, y=7$ or $x=7, y=1$ → $x=1, y=7$ → in Domain but violating hypothesis.

→ True

$\exists x \exists y \; P(x)$ → false. → D → +ve integer >1.

$\exists x \forall y \, (xy > < 7)$

Ex.1 Find the negation of $\forall x \exists y \, P(x,y)$

$\neg(\forall x \exists y \, P(x,y))$

$= \exists x \, \neg(\exists y \, P(x,y))$

$= \exists x \, \forall y \, (\neg P(x,y))$

Ex.2 Find the negation of $\exists x \forall y \, \underbrace{(xy<1)}_{P(x,y)}$

$\neg(\exists x \forall y \, (xy<1))$

$= \forall x \exists y \, (xy \geq 1)$

Orion
PAGE:
DATE: / /

Proof & Logic

Mathematical system → Axioms, already proved.
→ Definitions, new concepts in terms of existing concepts.
→ Term, already existing concepts.

Theorem → It is a proposition that has been proved.
Lemma → It is a theorem which is useful to prove other theorem.
Corollary → It is a theorem that follows easily from other theorems.

26/07/16

Gen De Morgan Laws
Nested Quantifiers
Theorem, Lemma, Corollary.

Proof Techniques.

Ex. If $(x>1) \wedge (y>1)$ (D: +ve integers)
then $(xy=7)$ → F.

$p \rightarrow q$ if p then q

$\exists x \exists y \; (\underbrace{\overset{p}{(x>1) \wedge (y>1)}}_{P(x,y)} \rightarrow \overset{q}{(xy=7)})$ → F

Here, we won't take the condition $x=1, y=7$ as we are analyzing conditional proposition.
Had it been a simple proposition → $xy=7$, we would have considered $x=1$ case.

PROOF TECHNIQUES

Theorem - It is proposition that has been proved to be true.
PROOF - Argument that establishes the value of the theorem.
LOGIC - It analyzes whether the proof is valid or not.

VANSHIKA TAIN NOTES

* Direct Proof
* Proof by contradiction
* Proof by contrapositive
* Proof by Cases
* Proof by equivalence

If $\underbrace{p(x_1, x_2, \ldots, x_n)}_{\text{true}}$ then $\underbrace{q(x_1, x_2, \ldots, x_n)}_{\text{true}}$.

| p | q | p→q |
|---|---|---|
| T | T | T ✓ |
| T | F | F ✗ |
| F | T | T |
| F | F | T |

In case of theorem, we take hypothesis true & prove consequent true.

Assuming the hypothesis is true, then taking $P(x_1, x_2, \ldots, x_n)$, previously derived result, axioms, values of inference, we will establish $q(x_1, x_2, \ldots, x_n)$.

Ex.1 Statement

If (m is odd and n is even) then (the sum of m & n is odd).

$m = 2k_1 + 1$

$n = 2k_2$

$m + n = 2(k_1 + k_2) + 1 = 2k_3 + 1 = \text{odd}$ (Direct Proof)

Ex.2 Statement

For all real no. $d, d_1, d_2, x$

if $\boxed{d = \min(d_1, d_2) \text{ and } x \le d}$

then, $x \le d_1$, $x \le d_2$

| | |
|---|---|
| $d = d_1$ | if $d_1 < d_2$ |
| $d = d_1$ | if $d_1 = d_2$ |
| $d = d_2$ | if $d_2 < d_1$ |

$d_1 < d_2$ $\quad d = d_1 \le d_2$

$d_2 < d_1$ $\quad d = d_2 \le d_1$

if $x \le d$ & $d \le d_1 \Rightarrow x \le d_1$

$x \le d$ & $d \le d_2 \Rightarrow x \le d_2$. Hence, Proved.

Orion
PAGE:
DATE: / /

## Disproving Universal Quantified Statements.

$\forall x \; P(x)$ – One member in $x$ in D is false

Cnf → $\wedge$

Dnf → $\vee$

Disjunction normal form

Ex. $\forall n \in Z^+$ ($2^n + 1$ is prime)

$n = 3 \rightarrow 2^n + 1 = 9 \rightarrow$ not prime → False

## Proof by contradiction:

Def^n → A proof by contradiction establishes $p \rightarrow q$ by assuming p is true & then conclusion q is false & then using p & $\boxed{\neg q}$ as well as other axioms, previously derived theorems, rules of inference decides (try to find) a contradiction.

$p \rightarrow \neg q$

$p \rightarrow q$ — r - true

$p \rightarrow \neg q$ — r -

---

$p \rightarrow q$ — equivalent

$(p \wedge \neg q) \rightarrow (r \wedge \neg r)$

| p | q | r | $p \rightarrow q$ | $p \wedge \neg q$ | $r \wedge \neg r$ | $(p \wedge \neg q) \rightarrow (r \wedge \neg r)$ |
|---|---|---|---|---|---|---|
| T | T | T | T | F | F | T |
| T | T | F | T | F | F | T |
| T | F | T | F | T | F | F |
| T | F | F | F | T | F | F |
| F | T | T | T | F | F | T |
| F | T | F | T | F | F | T |
| F | F | T | T | F | F | T |
| F | F | F | T | F | F | T |

Ex. 1

Statement

For every $n \in Z$, if $\underbrace{n^2 \text{ is even}}_{p}$ then $\underbrace{n \text{ is even}}_{q}$.

Direct Proof:- $n^2 = 2k_1$

$n = \sqrt{2k_1}$ → cannot say anything as $\sqrt{2}$ is irrational

$p \to n^2$ is even → True

$\neg q$ → $n$ is odd → $(2k+1)$

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2+2k)+1 = 2k_2+1$ → odd

Contradiction. ⇒ $\neg q \to F \Rightarrow q \to T \Rightarrow n$ is even.

Ex. 2

For all real no. $x$ & $y$ if $\underbrace{(x+y) \geq 2}_{p}$ then $\underbrace{\text{either } x \geq 1 \text{ or } y \geq 1}_{q}$

$$\neg q \equiv \neg((x \geq 1) \vee (y \geq 1))$$
$$\equiv (x<1) \wedge (y<1)$$
$$\Rightarrow x+y<2 \text{ — Contradiction.}$$

Ex. 3

$\sqrt{2}$ is irrational.

Assume $\sqrt{2}$ is rational. ⇒ $\sqrt{2} = \frac{p}{q}$, $p$ & $q$ are in lowest form.

$$2 = \frac{p^2}{q^2}$$

$p^2 = 2q^2$ = even. ⇒ $p$ = even $= 2k_1$

$(2k_1)^2 = 2q^2$

$2k_1^2 = q^2$ = even ⇒ $q$ = even $= 2k_2$

But $p$ & $q$ are in lowest form which contradicts that both $p$ & $q$ are even. ⇒ Contradiction ⇒ Our assumption was wrong.

⇒ $\sqrt{2}$ is irrational.

## Proof by contrapositive

Suppose we prove by contradiction $p \to q$ >
$\neg q \to \neg p$

Ex: for all $x \in R$
if $x^2$ is irrational then $x$ is irrational.
$p \to q$

if $x$ is rational then $x^2$ is rational. → True
$\neg q \to \neg p$ ⇒ $p \to q$ True.

## Proof by cases

Ex: $x \in R$ R = Real no.
$R^-$ $R^+$ Real nonnegative no.
Real -ve no

if $P(x_1, x_2, \dots, x_n)$ then $q$

$(P_1 \vee P_2 \vee P_3 \dots \vee P_n) \to q$ — (1) → True
$(P_1 \to q) \wedge (P_2 \to q) \wedge \dots \wedge (P_n \to q)$ — (2)

(1) true ⇒

| | p | q |
|---|---|---|
| (a) | T | T |
| (b) | F | T |
| (c) | F | F |

T

Case (a) take only one $P_i$ is true, q is true ⇒ $(\overset{T}{P_i} \to \overset{T}{q})$ True
$(\overset{F}{P_j} \to \overset{T}{q})$ True
⇒ (2) is true for case (a)

Case (b), (c) all $P_i$ = false ⇒ $(\overset{F}{P_i} \to \overset{T/F}{q})$ True ⇒ (2) is true for case (b), (c)
vacously True

| p | q | p→q |
|---|---|---|
| T | F | F |

Case (d) →

(1) is false. $P_i = T$, $P_j = F$ → $(\overset{T}{P_i} \to \overset{F}{q})$ F } (2) is ~~false~~ false
$(\overset{F}{P_j} \to q)$

Ex $2m^2 + 3n^2 = 40$ if $(m, n \in Z^+)$

$2m^2 < 40$ $m^2 < 20$ ; $m < 5$ $\rightarrow m = 1, 2, 3, 4$

$3n^2 < 40$ $n^2 < 40/3$ ; $n < 4$ $\rightarrow n = 1, 2, 3$

| n \ m | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 5 | 11 | 21 | 35 |
| 2 | 13 | 20 | 30 | 44 |
| 3 | 29 | 35 | 45 | 59 |

Exhaustive situation.

27/07/16

Theorem = Argument + Logic.

# RULES OF INFERENCE

Example

Set of propositions / hypothesis (or premises)

The bug is in either Module 17 or in Module 81.
The bug is a numerical error. — No bug in Module 17 → Bug is in Module 81
There is no numerical error in Module 17.

Conclusion (Deductive Reasoning) The bug is in module 81.

Def$^n$. An argument is a sequence of propositions.

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_n \\ \hline q \end{array} \quad \text{or} \quad p_1, p_2, p_3, \ldots p_n \;/\therefore q$$

If $\underbrace{(p_1, p_2, \cdots p_n)}$ are all true, then $q$ is true.

We assume it to be true despite of its actual truth value.

| $p$ | $q$ |
|---|---|
| T | T |
| T | F |
| F | T |
| F | F |

| $p \to q$ | $p$ | $q$ |
|---|---|---|
| T | T | T |
| F | T | F |
| T | F | T |
| T | F | F |

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

* Tautology — Set of propositions that are Always true
* Contradiction — Always false
* Contigency — Neither true nor false (Neither tautology nor contradiction)

| | Rules | Name | Tautology |
|---|---|---|---|
| 1. | $p \to q$, $p$, $\therefore q$ | Modus ponens | $p \wedge (p \to q) \to q$ |
| 2. | $p \to q$, $\neg q$, $\therefore \neg p$ | Modus tollens | $\neg q \wedge (p \to q) \to \neg p$ |
| 3. | $p$, $\therefore p \vee q$ | Addition | $p \to (p \vee q)$ |
| 4. | $p \wedge q$, $\therefore p$ | Simplification | $(p \wedge q) \to p$ |
| 5. | $p$, $q$, $\therefore p \wedge q$ | Conjunction | $((p) \wedge (q)) \to (p \wedge q)$ |
| 6 | $p \to q$, $q \to r$, $\therefore p \to r$ | Hypothetical syllogism | $((p \to q) \wedge (q \to r)) \to (p \to r)$ |
| 7. | $p \vee q$, $\neg p$, $\therefore q$ | Disjunctive syllogism | $((p \vee q) \wedge (\neg p)) \to q$ |

8. $p \vee q$ Resolution $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

$\neg p \vee r$

$\therefore q \vee r$

| $p$ | $q$ | $r$ | $\neg p$ | $p \vee q$ (A) | $\neg p \vee r$ (B) | $(A \wedge B)$ | $q \vee r$ | $(A \wedge B) \rightarrow (q \vee r)$ |
|---|---|---|---|---|---|---|---|---|
| T | T | T | F | T | T | T | T | T |
| T | T | F | F | T | F | F | T | T |
| T | F | T | F | T | T | T | T | T |
| T | F | F | F | T | F | F | F | T |
| F | T | T | T | T | T | T | T | T |
| F | T | F | T | T | T | T | T | T |
| F | F | T | T | F | T | F | T | T |
| F | F | F | T | F | T | F | F | T |

Hence, a tautology.

---

If a computer has 500 MB memory it can run a s/w (software) (say Blast.) If the computer can run 'Blast' then the sonics will be impressive

p: Computer has 500MB memory

q: Computer run the s/w 'Blast'.

r: the appl^n program running is $\leq 10$

and the no. of application program running in computer are 10.

if memory 500MB & the no. of appl^n program running < 10.

---

Ex

$p \rightarrow q$

$q \rightarrow r$

$q \rightarrow s$

$p$

If p attend classes, q also

p always attend classes

r and s always attend classes.

# Rules of Inference for Quantified Statements.

$$\frac{\forall x \ P(x)}{\therefore \forall \ P(d) \text{ for all } d \text{ in } D.}$$ Universal Instantiation (UI)

$$\frac{\forall \ P(d) \text{ for all } d \text{ in } D}{\therefore \forall x \ P(x)}$$ Universal Generalization (UG)

$$\frac{\exists x \ P(x)}{\therefore \exists \ P(d) \text{ for some } d \text{ in } D}$$ Existential Instantiation (EI)

$$\frac{\exists \ P(d) \text{ for some } d \text{ in } D}{\therefore \exists x \ P(x)}$$ Existential ~~Instantiation~~ Generalization (EG)

Everyone loves either Microsoft or Apple.
Amit does not love Microsoft → $\neg P(\text{Amit})$
∴ Amit loves Apple.

$Q(x)$ : x loves Apple  $\forall Q(\text{Amit})$
$P(x)$ : x loves Microsoft  $\forall P(\text{Amit})$ $\forall x P(x)$

$P(\text{Amit}) \vee Q(\text{Amit})$
$\neg P(\text{Amit})$
$\therefore Q(\text{Amit})$
Amit loves Apple.

## PROOF BY INDUCTION

Mathematical Induction.

$\boxed{1}$ $\boxed{2}$ $\boxed{3}$ $\boxed{4}$ ...... $\boxed{N}$
X X X X X

→ Some of the blocks are marked X.

Scanned by CamScanner

→ If the block N is marked X then block (N+1) is also marked X.

Let block 1 is marked X.

⇒ All blocks are marked X.

$S_n = 1+2+3+\dots+n$

$S_n = n+n-1+n-2+\dots+1$

$2S_n = (n+1)+(n+1)+(n+1)+\dots+(n+1)$

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

$S_1 = 1 = \frac{1\cdot 2}{2} = 1$

If it is true for $S_n$, then it is true for $S_{n+1}$.

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

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

**Ex.1** Proof by induction that $5^n - 1$ is divisible by 4.

* For $n=1$: $5^1 - 1 = 4 = 4(1)$ = divisible by 4.
* Assume that it is true for $n=n$ ⇒ $5^n - 1 = 4K$. $\{K \in N\}$
* for $n = n+1$, $5^{n+1} - 1 = 5 \cdot 5^n - 1$

$= 5(4k+1) - 1 = 20k + 5 - 1$

$= 4(5k+1)$ = divisible by 4.

Hence, Proved.

* **Basic Step** Verify that the corresponding statement to $n=1$ is true.
* **Inductive Step** Assume that the statement $n$ is true and then proof that statement $(n+1)$ is true.

Ex. 3 $\quad n! \geq 2^{n-1}$

B.S. $\quad n=1, \quad 1! = 1$
$\geq 1$
$\geq 2^{1-1}$

I.S: $n, \quad n! \geq 2^{n-1}$

$\longrightarrow (n+1 \geq 2)$

$n+1, \quad (n+1)! = (n+1)\cdot n! \geq (n+1)(2^{n-1})$
$\geq 2\cdot(2^{n-1}) = 2^n.$
$(n+1)! \geq 2^{(n+1)-1}$

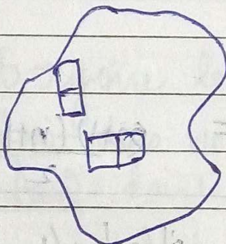
Hence, Proved.

---

## Tiling Problem :-

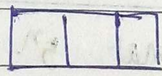
Exact covering a figure by a shape; without overlap to each other & external area:

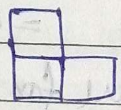
S. W. Golomb.



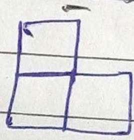
polyomino of order s


– domino (Order = 2)


– Triomino/Tromino (Order = 3)

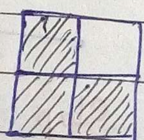


Problem. ★ Check if an $(n \times n)$ deficient board, where $n$ is a power of 2
1997. can be tiled by triominoes. ★

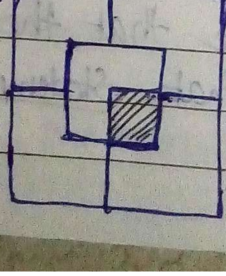

deficient board

$n \times n \rightarrow 2^k \times 2^k$.

$k=1$ $\quad - 2 \times 2$.

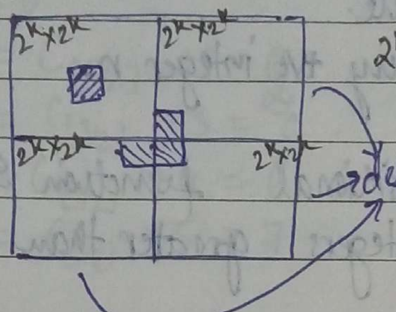


4x4. deficient board tiled up with triominoes :-



**I.S.**

We assume that it is true for $n = k$.
i.e. $n \times n$ or $(2^k \times 2^k)$ deficient board.
We have to check whether it is true for $(2^{k+1} \times 2^{k+1})$



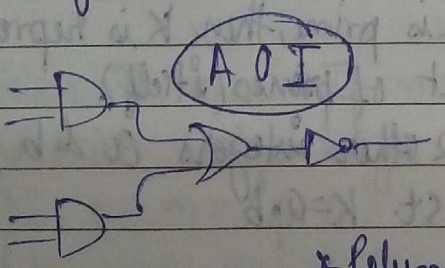

For $2^{k+1} \times 2^{k+1}$ board, place a triomino in the centre of the board directing the missing square to the direction of that $(2^k \times 2^k)$ deficient board.

1986 1. P Chu & R Johnsonbaugh.

→ If $n$ not necessarily a power of two then the no. of triominoes require to tile up $(n \times n)$ deficient board is $(n^2-1)$ where $(n^2-1)$ is divisible by 3.
(Except $n = 5$.)

**Converse**

If $(n^2-1)$ is divisible by 3 (except $n=5$), then any $(n \times n)$ deficient board can be tiled up by triominoes.




Induction & Recursion (4th Ch)

* Polynomials puzzles & problems in tiling
— Martin

# STRONG FORM OF MATHEMATICAL INDUCTION

## Principal of Mathematical Induction:-

**BS** $S(1)$ is true  If $S(n)$ is a propositional $f^n$

**IS** for all $n \geq 1$, if $S(n)$ is true
then $S(n+1)$ is true.

Then $S(n)$ is true for every +ve integer $n$.

Suppose we have a propositional function $S(n)$ whose domain of discourse is set of integers greater than or equal to $n_0$

BS. $S(n_0)$ is true

IS. for all $n > n_0$, if $S(k)$ is true then
$S(n)$ is true. $(n_0 \leq k < n)$

Then $S(n)$ is true for every integer $n \geq n_0$.

**Ex. 1** Show that if $n$ is an integer $\geq 1$, then $n$ can be written as the product of primes.

$n = p_1^{c_1} \cdot p_2^{c_2} \cdots p_m^{c_m}$

$n_0 = 1$
1 is thought of empty set of no primes.

$n_0 = 2$

**BS** $n_0 = 2$, so it is product of prime 2 (itself)

**IS** We consider one integer $k \geq 2$

Case I  $k$ is prime - If $k$ is prime, then $k$ is represented as the product of primes (itself).

Case II  $k$ is composite - Let 2 other integers $a$ & $b$,
$n_0 \leq a, b < k$, s.t. $k = a \cdot b$

Strong form of induction - then for all $a, b$
$2 \leq a, b < k$, proposition is true

Ex.2 Consider a sequence $C_1, C_2, \ldots, C_n$ given $C_1 = 10$ and $C_n = C_{\lfloor n/2 \rfloor} + n$ for all $n > 1$. Prove that $C_n < 4n$ for all $n > 1$.

$C_1 = 0$

$C_2 = C_{\lfloor 2/2 \rfloor} + 2 = 2$

$C_3 = C_{\lfloor 3/2 \rfloor} + 3 = 3$

$C_4 = C_{\lfloor 4/2 \rfloor} + 4 = 6$

$C_5 = C_{\lfloor 5/2 \rfloor} + 5 = 7$

* $\lfloor n/2 \rfloor < n$ $\qquad n_0 \le k < n$

Assume $k = \lfloor n/2 \rfloor$

$C_{\lfloor n/2 \rfloor} = C_k < 4k = 4\lfloor n/2 \rfloor$

strong form of induction.
for $n_0 \le i \le k$
$C_i < 4i$ (Assumption)

Now $C_n = C_{\lfloor n/2 \rfloor} + n$

$= C_k + n$

$< 4k + n \le 4 \cdot \frac{n}{2} + n = 3n < 4n$

$\Rightarrow C_n < 4n$. Hence proved.

---

## Well ordering Property

– non-negative integer

WOP states that every non-empty set of non-negative integers has a least element

Division Theorem – If $n$ is an integer, $d$ is a +ve integer then there exists unique integers $q$ and $r$ so that $n = dq + r$

$\frac{n}{d}$ $\qquad n = dq + r$.

Remainder $r < d$ $\qquad n - dq = r$

Quotient $q$ $\qquad n - dq_0 = r_0$

$n - d(q_0 + 1) = \underline{n - dq_0} - d = r_0 - d$

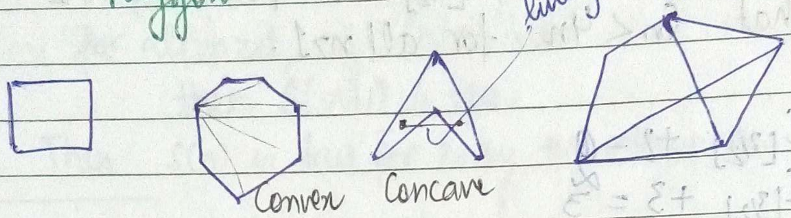
But $r_0 < d$

(See Logic in Rosen)

# Computational Geometry

Polygon

line joining pts inside polygon lie outside polygon ⇒ concave




Simple :- Consecutive Sides do not intersect.
Diagonal :- Line joining 2 vertices. (Interior)

**Theorem :-** A simple polygon with $n$ sides where $n$ is an integer $\geq 3$ can be <u>triangulated</u> with $(n-2)$ triangle

**Lemma :-** Every simple polygon has an interior diagonal.

1975

<u>Proposition</u> → $T(n)$ can be triangulated for all values of $n$ $n_0 \leq n \leq K$.

$T(K+1)$ ← can be triangulated.

<u>BS</u>: $n_0 = 3$

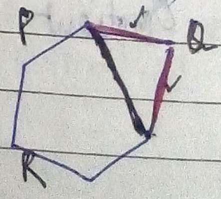
<u>IS</u>: Let $P$ be a simple polygon with $(K+1)$ sides.
Adding one diagonal we partition $P$ into $Q$ & $R$ having $s$ and $t$ no. of sides respt.

$$3 \leq s, t \leq K$$

$Q$ and $R$ can be triangulated with $(s-2)$ and $(t-2)$ triangles

$Q$ & $R$ sharing 2 sides from $P$ and moreover $Q$ & $R$ have one side extra which is added diagonal.
So, $P$ has at least one side fewer (lesser) than the no. of sides of $Q$ or $R$.

$$(K+1) = (s-1) + (t-1)$$
$$s + t = K + 3$$



Orion

PAGE:
DATE: / /

Total no. of triangulated Δ's $= (s-2)+(t-2) = s+t-4 = k+3-4 = k-1 = (k+1)-2$

$T(k+1)$ P can be triangulated with $\{(k+1)-2\}$ Δ's.

* Proof by equivalence :- (If p then q) and (If q then p)

## Language of Mathematics

09/08/16

SET :- S: An unordered collection of objects

$S: \{1, 2, 3, 4, 5\}$

$S: \{x \mid x$ is even integer

* $x \in S \equiv x$ belongs to $S$ / $x$ is in $S$
* $x \notin S$.

empty set :- null, void — $\varphi$, $\phi$.

Universal set :- U (referred ~~to~~ in some context or it is inferred in some specific context).

Consider 2 sets C and A.

Let $x$ denote the element of C and $y$ denote the element of A.

* $C \overset{\text{subset}}{\subseteq} A$

$\forall x\ (\underbrace{x \in C}_{p} \rightarrow \underbrace{x \in A}_{q})$

* proper subset :- $C \subset A$.
* $C = A$ (All elements of C belongs to A and vice versa)

$\hookrightarrow \begin{cases} \forall x (x \in C \rightarrow x \in A) \\ \forall x (x \in A \rightarrow x \in C) \end{cases}$

$\neg(p \rightarrow q) \equiv p \wedge \neg q$

$\neg(\underbrace{x \in C}_{p} \rightarrow \underbrace{x \in A}_{q}) \equiv (x \in C) \wedge \{\neg(x \in A)\}$

$\equiv x \in C \wedge x \notin A$

$\Rightarrow \exists x\ (x \in C \wedge x \notin A) \Rightarrow$ (C is not subset of A.)

ANUBHAV JAIN NOTES

Orion

PAGE:
DATE: / /

$$(x+2)(x-1) \Rightarrow x = -2, +1.$$

Ex: $C : \{x \mid x^2 + x - 2 = 0\}$

$A : \{\text{Set of integers}\} = \{ ---, -2, -1, 1, --- \}$

$\Rightarrow C \subset A.$

---

$\forall x \, (x \in \phi \rightarrow x \in C)$

---

X : {a, b, c}

Cardinality of X = no. of elements of X. = 3. = |X|

Subsets of X : {ϕ} {a} {b} {c} {a, b} {b, c} {c, a} {a, b, c}

ϕ or { }

$c_1 a,\ c_2 b,\ c_3 c$

$c_1, c_2, c_3 \in \{0, 1\}$

All possible combinations of $c_1, c_2$ & $c_3$ gives all subsets of X.

Power Set : The set of all subsets of a given set is called the power set. → P(X)

$|X| = 3 \qquad |P(X)| = 2^3$

Imp. Observation

Consider a, one element of X.

| Subsets a belongs to | Subsets a does not belong to |
| --- | --- |
| {a} | ϕ |
| {a, b} | {b} |
| {a, c} | {c} |
| {a, b, c}. | {b, c} |

| | | |
| --- | --- | --- |
| a | $c_1$ | — o — o — o — o |
| b | $c_2$ | — — o o — — o o |
| c | $c_3$ | — — — — o o o o |

⇒ Every element appears in half of the subsets in Power set.

Orion

PAGE:
DATE: / /

**Theorem :-** If $|X| = n$
then $|P(x)| = 2^n$.

Prove by induction.

**Basic Step:** $n = 0$ implies $X$ is an empty set.
$|P(x)| = 1 = 2^0$ { contains empty set }.
$= 2^n$ when $n = 0$.

**Inductive step:** Let $X$ be a set having $(n+1)$ elements.
★(We have assumed for $X$ of $n$ elements, $|P(X)| = 2^n$)

Now, if we remove one element from $X$, the no. of elements become $n$.
Let $Y$ be set of $n$ elements and from ~~...~~ our induction assumption, $|P(Y)| = 2^n$ - true.
Now if we consider one element in $X$
So, from property of power set, that particular element belongs to the half of the total subsets. and does not belong to other half.

$$\Rightarrow |P(y)| = \frac{|P(x)|}{2}$$

$$\Rightarrow |P(x)| = 2\,|P(y)| = 2(2^n)$$

$$\boxed{|P(x)| = 2^{n+1}}$$

**OPERATIONS:-**

* Set Union $(\cup)$ → if element $x$ belongs to A or belongs to B.
* Set Intersection $(\cap)$ → ——— " ——— and ———
* Set Difference $(-)$ → ——— but not ———
  $(A-B)$



{1,2}

$A : \{1, 2, 5\}$ $B : \{3, 4, 5, 6\}$.

$A \cup B$ Union : $(x \in A) \vee (x \in B)$

$A \cap B$ Intersection : $(x \in A) \wedge (x \in B)$

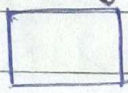
Difference : $A-B$ $(x \in A) \wedge (x \notin B)$

$B-A$ $(x \in B) \wedge (x \notin A)$

{3,4,6}

Scanned by CamScanner

# Venn diagrams

U – 

S – 

In a class there are 165 st.
Among them (Cal^culus^, Com^puter sc.^, Psy^chology^)

8 – Cal + Psy + Com
33 – Cal + Com                Cal + Psy – 24
20 – Com + Psy
79 – Cal
83 – Psy
63 – Com.

$$\text{Cal} + \text{Psy} + \text{Com} = 79 + 83 + 63 - 24 - 33 - 20 + 8 \quad \boxed{\text{Cal} + \text{Psy} + \text{Com}}$$

$$= 156.$$

⇒ No. of student with no subject $= 165 - 156$
$= 9.$

---

**Properties of set** : A, B, C        U, ∩, – complement.

Associative : $(A \cup B) \cup C = A \cup (B \cup C)$
$(A \cap B) \cap C = A \cap (B \cap C)$        $(\bar{A} = U - A)$

Commutative : $A \cup B = B \cup A$ , $A \cap B = B \cap A$.

Distributive : $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Identity : $A \cup \phi = A$ , $A \cap U = A$

(Always not same universal) → Complement : $A \cup \bar{A} = U$ , $A \cap \bar{A} = \phi$

Bound : $A \cup U = U$ , $A \cap \phi = \phi$

Absorption : $A \cup (A \cap B) = A$ , $A \cap (A \cup B) = A$.

Involution : $\overline{(\overline{A})} = A$

0/1 Law : $\overline{\phi} = U$ , $\overline{U} = \phi$

De Morgan : $\overline{A \cup B} = \overline{A} \cap \overline{B}$

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

---

Proof

Distributive: Let $x$ is an element of $A \cup (B \cap C)$

$\Rightarrow$ $x$ is an element of A

or $x$ is an element of $(B \cap C)$ $\Rightarrow$ $x$ is an element of B and C.

$\Rightarrow$ $x$ is an element of A or $x$ is an element of B and ($\cap$) C. $(A \cup B)$ $(A \cup C)$

~~$x$ is an element of A or x is ... A~~

{ $p \equiv q \iff p \to q$ and $q \to p$ }

Now, prove opp. also.

Now let $x \in (A \cup B) \cap (A \cup C)$

$x \in (A \cup B)$ and $\to$ $x \in A \vee x \in B$

$x \in (A \cup C)$ $\to x \in A \vee x \in C$

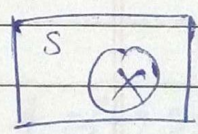
} $x \in A$ or $x \in B$ and $x \in C$

$x \in (A \cup (B \cap C))$

---

Consider an arbitrary family S of sets to be those element of X belong to atleast a set X in S

Universal S $\quad \cup S = \cup \{x \mid x \in X$ $\underbrace{\text{for some } x \in S}_{X \in S}$ $\}$




$\cap S = \{x \mid x \in X$ $\underbrace{\text{for all } x \in S}_{X \in S}$ $\}$

$\cup S = \bigcup_{i=1}^{n} A_i$

$\cap S = \bigcap_{i=1}^{n} A_i$

$\cup S = \bigcup_{i=1}^{\infty} A_i$

$\cap S = \bigcap_{i=1}^{\infty} A_i$

} Finite set.

Define a set $A_i = \{i, i+1, \ldots\}$

$A_1 = \{1, 2, 3, \ldots\}$

$A_2 = \{2, 3, 4, \ldots\}$

$\vdots$

$A_i = \{i, i+1, \ldots\}$

$\cup S =$ set of all integers

$\cap S = \phi$

11/08/16

## Partition of sets

A partition of a set X divides X into non-overlapping subsets.

Family of S consisting all the subsets of X, then every element of X must belong to one subset of S.

US.

$X = \{1, 2, \ldots, 8\}$

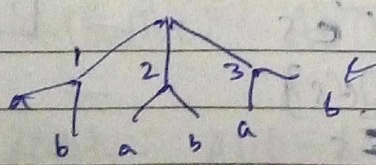
$S = \{\{1,2,3\}, \{4,5\}, \{6\}, \{7,8\}\}$

Partitions of S.

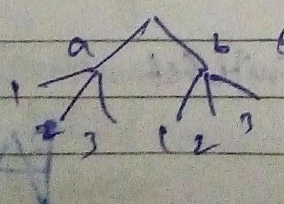
Let X & Y are the 2 sets then all possible set of ordered pairs of X & Y are defined as Cartesian Product of X and Y.

$X * Y$

$X = \{a, b\}$ $Y = \{c, d\}$.




$X \times Y = \{(1,a) \ldots (3,b)\}$




$\leftarrow Y \times X$

$X \times Y \neq Y \times X$

$|X \times Y| = |Y \times X|$

$|X| \cdot |Y| = |Y| \cdot |X|$

Orion

PAGE:
DATE: / /

$X = \{x_1, x_2, \ldots x_n\}$

$Y = \{y_1, y_2, \ldots y_m\}$

$|\underbrace{X \times Y}_{X'}| = m \times n$

$Z = \{z_1, z_2 \ldots z_p\}$

$|X' \times Z| = |X \times Y \times Z| = m \times n \times p.$

---

Ex: Let A : set of apetizers
{ ribs, shrimp, fried cheese }
E: set of entree
{ chicken, beef, trout }
D : {chocolate, vanila, pista}
All possible dinners → $A \times E \times D$.
No of ______ $= 4 \times 3 \times 3 = |A \times E \times D|$

---

Representing set in a computer
We considered a universal set $U$, $U$ must be finite.
No. of elements in $U$ must be lesser than the memory size.
Now if I want to represent a set $A = \{a_1, a_2 \ldots a_n\}$
$|U| = p$

p bit string

$a_i = 1$, if $a_i$ belongs to A

$p > n$

Ex. 1 $U = \{1, 2, 3, \ldots, 10\}$
A = set of odd integers $= \{1, 3, 5, 7, 9\}$
$|A| = 5$
B = set not exceeding 4 $= \{1, 2, 3, 4\}$
(odd) $A = \{1, 0, 1, 0, 1, 0, 1, 0, 1, 0\}$
(even) $\bar{A} = \{0, 1, 0, 1, 0, 1, 0, 1, 0, 1\}$
$B = \{1, 1, 1, 1, 0, 0, 0, 0, 0, 0\}$
$A \cap B = \{1, 0, 1, 0, 0, 0, 0, 0, 0, 0\}$ $A \cup B$ ✓
$A - B = \{0, 0, 0, 0, 1, 0, 1, 0, 1, 0\}$

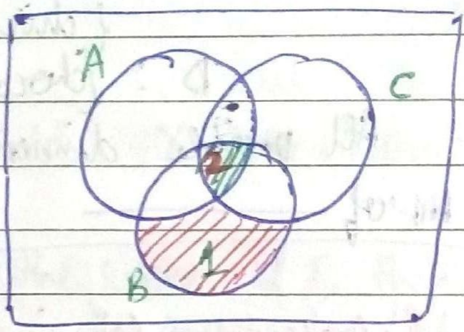
ANUBHAV JAIN NOTES

$A = \{1, 4, 7, 10\}$
$B = \{1, 2, 3, 4, 5\}$
$C = \{2, 4, 6, 8\}$
$U = \{1, 2, \ldots, 10\}$

$B \cap \phi = \phi$
$A \cup U = U$
$A \cap (B \cup C) = \{1, 4\}$
$B - A = \{2, 3, 5\}$
$\overline{B} \cap (C - A) = \overline{B} \cap \{2, 6, 8\} = \{6, 8\}$

Draw Venn Diagram.

(1) $B \cap (\overline{C \cup A})$




(2) $((C \cap A) - (\overline{B - A})) \cap C$

Prove the absorption law:-
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$.

Proof:-
Let $x$ be an element in $A \cup (A \cap B)$
$\Rightarrow$ $x$ is in $A$ or $x$ is in $A$ and $B$.
$\Rightarrow$ $x$ is in $A$ for sure.

$x$ in $A$.
$\Rightarrow$ $x$ is in $A \cup C$ ; $C \rightarrow$ any set.
$(A \cap B)$.

$x$ is in $A \cap B$
$\Rightarrow$ $x$ in $A$ & $B$. $\Rightarrow$ $x$ is in $A \cup (A \cap B)$.

$\overline{A} = U - A$

$\overline{\overline{A}} = U - (U - A) = A.$

1. Prove De Morgan's Law.
2. Use induction to prove that -
   if $X_1, X_2, \ldots, X_n$ are sets then
   $|X_1 \times X_2 \times \cdots X_n| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|$

16/08/16

## FUNCTIONS

$d = r \cdot t$ distance travelled = rate × time

$d = f(t)$

$t$ = set of non-zero +ve real no.

$r = 60$ $d$ = set of non-zero +ve real no.

$(1, 60), (2, 120), (1.5, 90), \ldots$

function: A set of ordered pairs.

Def^n: Let X and Y be two sets. The function is defined as a subset of cartesian Product $X \times Y$ where for each $x \in X$, there is exactly one element $y \in Y$ with the ordered pair $(x, y) \in f$.

X - domain of f

y - Range of f.

$y = f(x)$

$f(x) = x^2$

Ordered pair → $(x, x^2)$



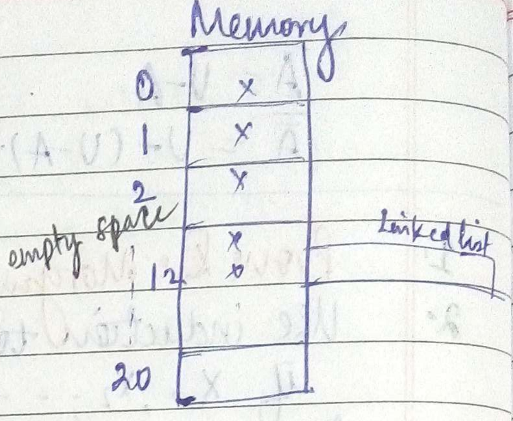
Book ISBN

International Standardary Book Number.

0 - 8065 - 9059 - ⓐ

gr. code, publisher code, book code by publisher, check code (obtained by function)

$(0 \times 8 \cdot 1 + 0 \cdot 2 + 6 \cdot 5 + \cdots + 9 \cdot 8)$ mod 11 ← $1 \times 1$, divide, polynomial




# Hash Function

Key to address mapping.

Store $x$ –

$h(x) = a_1$

$= \{1, 2, \ldots 20\}$

$h(x_1) = h(x_2)$

→ Many to one function.

Always collision will be there.

## Ideal hash function – Random function.

Key should be distributed over address spaces.

Random $f^n$: i) True random – no use
Pseudo-random

$x_n = (a x_{n-1} + c) \bmod m$

$m$ = modulus (+ve integer)

$a$ = multiplier $0 \le a < m$

$c$ = sum $0 \le c < m$

$s$ = seed

$x_0 = s$.

| | |
|---|---|
| $m=11$ | $x_0 = 3$ |
| $c=5$ | $x_1 = 4$ |
| $a=7$ | $x_2 = 0$ |
| $s=3$ | $x_3 = 5$ |
| | $x_4 = 7$ |
| | ⋮ |

→ Knuth – Vol 2 (The art of computing).

Random no. cannot be predicted (from prev. values).

A function is such that for each value of $y \in Y$, there is atmost one value of $x \in X$ $\Rightarrow$ One to one function

$$\forall x_1, \forall x_2 \ \left( \left( f(x_1) = f(x_2) \right) \rightarrow (x_1 = x_2) \right)$$

**Not one-to one :-**

$(\forall x_1 \forall x_2 ((f(x_1) - - - \cdot x_2)))$ is false.

$\neg ( \_\_\_\_\_\_ )$

$\Leftrightarrow \exists x_1 \exists x_2 (\neg(p \rightarrow q))$

$\neg(p \rightarrow q) = p \land \neg q$

$$\boxed{\exists x_1 \exists x_2 \left( (f(x_1) = f(x_2)) \land (x_1 \neq x_2) \right)}$$

$y = 2^x - x^2$

$x_1 = 2 \quad y = 0$

$x_2 = 4 \quad y = 0$

$1 \rightarrow a$
$2 \rightarrow c$
$3 \rightarrow b$
$d$

one to one but not onto

**Onto function :-** (X onto Y)

$$\exists x \in X \, \forall y \in Y \ (f(x) = y)$$

Into: $\neg (\quad)$

$= \forall x \exists y \ (f(x) \neq y)$.



$f(x) = y = 2x + 1 \rightarrow$ odd

Codomain :-

$Y$ : odd integer $\rightarrow$ onto

$Y$ : +ve integer $\rightarrow$ not onto.

one $1 \ x \in X$

Codomain = Range

One to One + Onto $\rightarrow$ Bijective function

Orion
PAGE:
DATE: / /

Ex. $y = f(x) = \frac{1}{x^2}$

Check the type of function:
① Domain → nonzero Real nos.
Codomain → R → not onto
+ve Real no → onto.

Many to one

---

Composition
$f \circ g(x) = f(g(x))$

Operators :- binary or unary operators.
$\times$ $+$

---

22/08/16

Relations

Relations generalize the notion of functions.

Students $X = \{A, B, C, D\}$
Course $Y = \{$Comp Sc., Math, Hum., Hist.$\}$ $\rangle$ R
Subset of Cartesian product of $X$ & $Y$. → Relation
$R = \{$(A, Comp Sc), (A, Hum), (B, Hist), (B, Hum) - - $\}$

Def

Relation from a set X to Set Y is a subset of Cartesian product $X \times Y$ $xRy$ : where $x \in X$, $y \in Y$, $(x, y) \in R$
* if $X = Y$, Relation is on Set X.

Function is a Special class of Relation.
$Y = f(x)$, $(x, y) \in (X \times Y)$

properties of function.
1. X is the domain
2. for each $Y \in Y$, $(x, y) \in f$, Y is the range

Orion

PAGE:
DATE: / /

x can relate to only one y.

Function v/s Relation → one x can relate to more than one y.

* Both are cartesian product

but function is a special class of Relation with 2 properties.

---

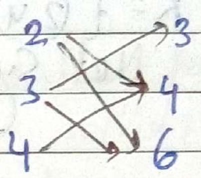
$X = \{2, 3, 4\}$

$Y = \{3, 4, 5, 6, 7\}$

$R = \{(x,y) \mid x \text{ divides } y\}$

$= \{(2,4), (2,6), (3,3), (3,6), (4,4)\}$

$R = \{(x,y) \mid x \in X, y \in Y, x, y \in X\}$



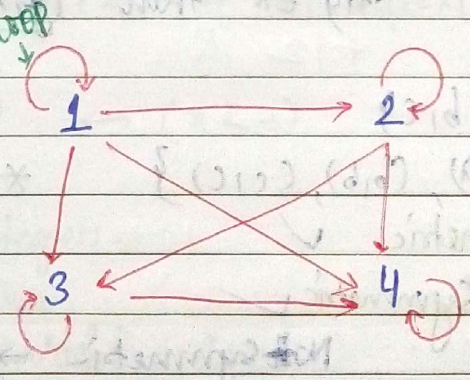
$X = \{1, 2, 3, 4\}$

$R = \{(x,y) \mid x \leq y \;\&\; x, y \in X\}$

$R = \{(1,1) (1,2) (1,3) (1,4) (2,2) (\_\_) \_\_ (4,4)\}$.

* Digraph is the another notation of relation (Directed graph)

Graph = {V, E}




---

1. Reflexive A relation R on set X is reflexive if $(x,x) \in R$, for all $x \in X$.

$X = \{a, b, c, d\}$

$R = \{(a,a) (b,c) (c,b), (d,d)\}$.


Not Reflexive.

ANUBHAV JAIN NOTES

Orion

PAGE:
DATE: / /

2. Symmetric A relation R from a set X to a set Y is symmetric if $\forall (x,y) \in R$ and $x \in X, y \in Y$ then $(y,x) \in R$.

$X = \{2,3,4\}$
$Y = \{3,4,5,6,7\}$
$R = \{(2,4)\ (2,6)\ (3,3)\ (3,6)\ (4,4)\}$

Not Symmetric
if $\exists (x,y) \in R$ $x \in X, y \in Y$,
then $(y,x) \notin R$

Anti symmetric A relation R on a set X is called anti symmetric if $\forall (x,y) \in R$, $\{x,y\} \in X$ then $(y,x) \notin R$

If no member $(x,y) \in R$ where $x \neq y$.
$x,y \in X$ then $(y,x) \notin R$.

$X = \{a,b,c\}$
$R = \{(a,a), (b,b), (c,c)\}$ * Reflexive
* Symmetric ✓
* Anti-symmetric ✓
~~Not~~ symmetric → false.

3. Transitive A relation R on set X is transitive if $(x,y) \in R$, $(y,z) \in R$, $\{x,y,z\} \in X$ $(x=y=z)$

Ex:
$X = \{1,2,3,4\}$ $(x,y) \in R$ $x \leq y$
$R = \{(1,1), (1,2), (1,3)\ (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$.

Reflexive, Transitive, Anti-symmetric

Scanned by CamScanner

**PARTIAL ORDER** A relation R on a set X is called a partial order if the relation is Reflexive, anti-symmetric, and transitive.

X $x, y \in X$ $x \leq y$ → Partial order.

$X = \{2, 3, 5, 1, 9\}$

A set X together with the relation R is called partially ordered set or poset.

members of X with R, is the element of poset.

---

Ex: $x = \{2, 3, 4\}$
$y = \{3, 4, 5, 6, 7\}$

$(x, y) \in R$ x divides y $x \in X$, $y \in Y$.

$(2, 2)$ → not there in R ⇒ not reflexive ⇒ Not partial order.

$(xRy), (yRz) \rightarrow (xRz)$

---

$Z^+$ → set of the integers.
R – division, /
$(Z^+, /)$ → partial order.
Reflexive – $xRx$
transitive – $xRy$, $yRz \Rightarrow xRz$
Anti-symmetric – $x/y$, $y/x$ ⇒ Antisymmetric

Hence, it is partial order.

---

<or>

Ex: We considered people who are older $(x > y)$. ($x \geq y$ ⇒ partial order.)

* $xRx$ X ($\not{x}R$)
* $xRy$, $yRz \Rightarrow xRz$ ✓ (✓T)
* $xRy$; $yRx$ ⇒ (✓AS)

} Not a partial order

Orion
PAGE:
DATE: / /

$x \geq y$

$x \leq y$ denotes relation of ordering (not less than or equal to)

$x, y \in X$

$(x,y) \in R$, R-partial order

if either $x \geq y$ or $x \leq y$
then $x$ & $y$ are comparable.

Neither $x \geq y$ nor $x \leq y$ ⇒ $x, y$ are incomparable
not ($x \geq y$ and $x \leq y$) Not satisfying P.O.

If for a set X, each pair of elements (for all $x, y$) are comparable then we define the relation as a total order or linear order, chain.

$x, y$ $2|4$ ✓ (2 divides 4)
$4|2$ ✗

---

$X = \{1,2,3,4,5,6,7\}$

$(x,y) \in R$ , $x, y \in X$ , $x < y$

* (1,1) (2,2) ... (7,7) → ✗ Not Reflexive
* (1,2)(1,3) ... (1,7) (2,3)(2,4) ... (2,7) ...
(1,2), (2,4) → (1,4) ✓ Transitive
* (1,2) → ~~(2,1)~~ ✓ Antisymm.

Example of. Task Scheduling

Taking a photo by a camera.

Tasks

1. Remove the lens cap
2. Focus the camera
3. Unlock the safety button
4. Click the button to take photos.

Can be done in any order → (2,3) (3,2) (1,3) (3,1)

Order → {(1,1) (2,2) (3,3) (4,4)
(1,2) (1,4) (2,4) (3,4)}

Example. $(x,y) \in R$
$(Z^+, /)$ $x$ divides $y$, $x, y \in X$
$X = \{1, 2, 3, 4, 5, 6\}$
$R = \{(1,1), (1,2), \ldots, (1,6),$
$(2,2), (2,4), (2,6), (3,3), (3,6), (4,4)$
$(5,5), (6,6)\}$

Reflexive
Anti-Symmetric
Transitive
} P.O. not total order - for not each pair $\underbrace{\text{either } xRy \text{ or } yRx}$.
(2,3) are not comparable.
etc.

---

## Well Ordered Set :

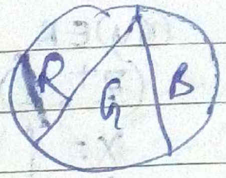
$(X, \leq)$ is a well ordered set if it a poset and the relation $R$ $(\leq)$ is a total order and every non-empty subset has a least element.

eg Set of ordered pairs
$(a_1, a_2)$ $(b_1, b_2)$
$a_1 < a_2$
$a_2 \leq b_2$ $Z^+ \times Z^+$

Theorem :- The principle of well induction
Suppose $X$ is a well ordered set
Then $P(x)$ (for all $x \in X$) is true.
Induction step - If for every $y \in X$, if $P(x)$ is true for all $x \in X$ with $x < y$ then $P(y)$ is true.

$y < x_0$
$P(x_0)$

S




Equivalence Relation $X = \{R\ G\ B\}$
$= \{\{R\}, \{G\}, \{B\}\}$

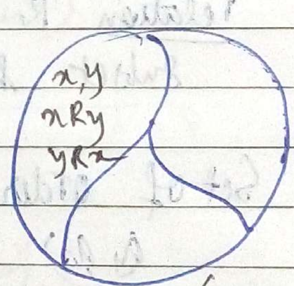
Set X of ~~n~~ no. of balls with colors R, G, B.
Consider R - is same colour.

Theorem: Let S be a partition of a set X. Define $xRy$ to mean for some set $S \in S$, both x & y belong to S, then R is reflexive, symm. & Transitive.

Reflexive
Consider of element $x \in S$
$xRx$ $x \in S$, $S \in S$ →
→ must belong to one partition S.

$S = \{R, G, B\}$

~~Anti~~ Symmetric
$x, y \in S$
$xRS \in S$
$yRx \in S$




Symmetric

Transitive $xRy$ $x\,y\,z \in T$ ~~$x\,y\,\in S$~~
$yRZ$ $T \in S$
$\Rightarrow xRZ \in S$
y belong to one partition.
$T = S$

$xRy \in S$, $yRz \in S$
$xRz \in S$

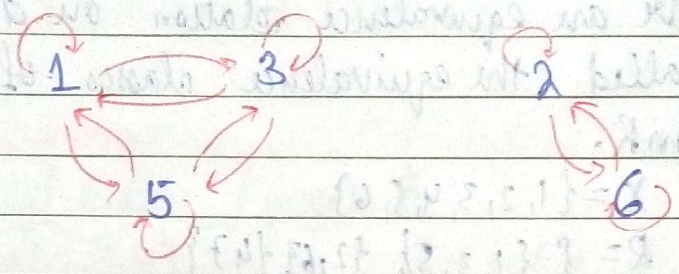
Equivalence Relation:-
A relation on a set X is equivalence relation if the relation is reflexive, symmetric & transitive.

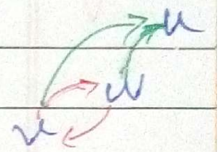
PAGE:
DATE: / /

(c) $X = \{1, 2, 3, 4, 5, 6\}$

$S = \{\{1, 3, 5\}, \{2, 6\}, \{4\}\}$

$R = \{(1,1), (1,3), (1,5), (3,1), (3,3), (3,5), (5,1), (5,3), (5,5), (2,2),$
$(2,6), (6,2), (6,6), (4,4)\}$.





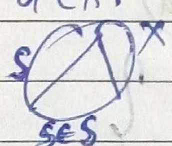
25/08/16

## Equivalence Class

Equivalence Relation → Reflexive, Symmetric, Transitive.

Theorem:- Let $R$ be a equivalence relation on a set $X$, and
$[a] = \{x \in X \mid xRa\}$
Then $S = \{[a] \mid a \in X\}$ is a partition on $X$

Here $[a]$ is set of elements of $X$ that are related to $a$, $a \in X$.



$yRa$, $y \in [a]$.

Proof:- We have to prove that each element belongs to one and exactly one subset of $X$. Let $a$ is one element of $X$, $a \in X$. So, $aRa \in [a]$.

If we consider each element of $X$. $x$ is one element related to $a$.

$x \in [a]$

If $x \in [a]$ and $x \in [a] \cap [b]$

then $[a] = [b]$

Consider 2 elements $c$ & $d$ $\in X$, $[c]$, $[d]$

$cRc \in [c]$.

Let $x$ is the element related to $[c]$ & $[d]$

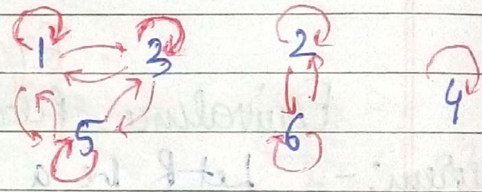
$cRx \in [c]$, $xRd \in [d]$

cRd - true since R is transitive, [c] = [d].
c=a , d=b } , aRx, xRb
aRb.

**Def$^n$:-** Let R be an equivalence relation on a set X. The sets [a] are called the equivalence classes of X given by the relation R.

$X = \{1,2,3,4,5,6\}$
$R = \{ \{1,3,5\}, \{2,6\} \{4\} \}$
$= (1,1)\ (1,3) \ldots\ldots$

31/8/19




$R = \{(a,a), (b,b), (c,c)\}$
$= \{\{a\}, \{b\}, \{c\}\}$
not transitive

Ex. Let $X = \{1,2,3,\ldots,10\}$
xRa = 3 divides $(x-a)$.
$[a]$ , $a \in \{1,2, \ldots 10\}$
$[1] = \{1,4,7,10\}$
$[2] = \{2,5,8\}$
$[3] = \{3,6,9\}$
3 Partitions

$R = (a,b)$, $a \equiv b \bmod m$
$a \bmod m = b \bmod m$
$a-b$ is divisible by m.

$m=3$

Congruence modulo m forms the equivalence classes.

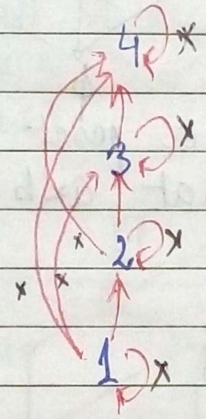
**Theorem** Let R be an equivalence relation on a finite set, X. If each sequence class has r elements then there are $|X|/r$ equivalence classes.

$$|X| = |X_1| + |X_2| + |X_3| + \dots$$

## Hasse Diagram

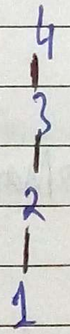
★ for Partial order / poset ★

$X = \{1, 2, 3, 4\}$ $\qquad R - a \le b \quad , a, b \in X$



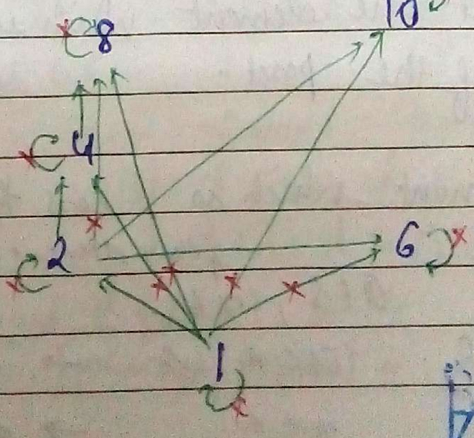

Minimisation of Digraph for poset.

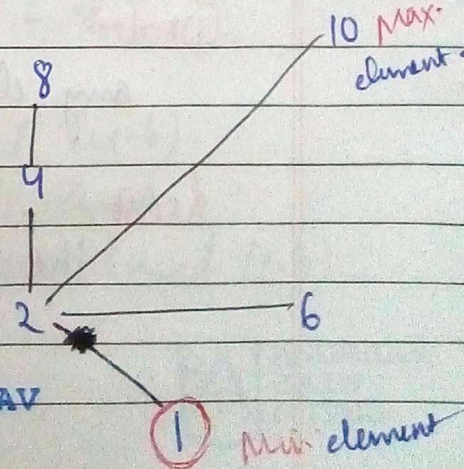
1. delete all the loop.
2. delete all the directed edges showing transitivity.
3. Re~~position~~ present some relations by their positions (top, bottom)
4. Remove the arrow i.e. replace the directed edge by undirected edge




Hasse Diagram & poset
$\{1, 2, 3, 4\}$ with R $a \le b$, $a, b \in X$.

$X = \{1, 2, 4, 6, 8, 10\}$ $\qquad R \in a/b \quad , a, b \in X.$



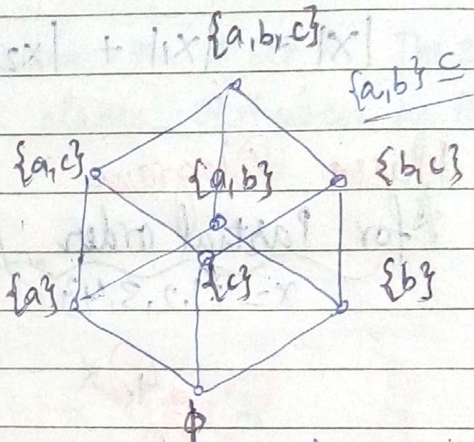



# Hasse Diagram

Power Set $P(S)$

where $S = \{a, b, c\}$

$P(S) = \{ \phi, \{a\}, \{b\}, \{c\}, \{a,b\}\ \{b,c\}\ \{c,a\}\ \{a,b,c\} \}$

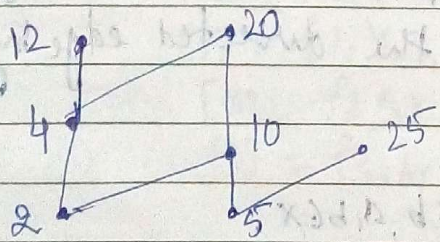



$\{a,b\} \subseteq \{a,b,c\}$

**Maximal** – An element $a$ of a poset is maximal if there is no $b$ such that $a \not< b$ (not a less than b)

**Minimal** – $b < a$

Ex. $\{\underbrace{\{2, 4, 5, 10, 12, 20, 25\}}_{S}, /\}$




$a < b$

$12, 20, 25 \rightarrow$ Maximal

$b < a$

$2, 5 \rightarrow$ Minimal

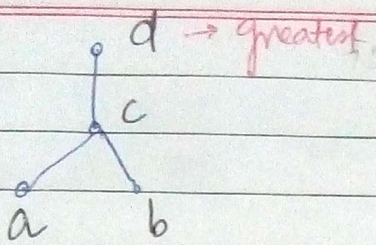
**Greatest** – We get one element which is greater than any element of the poset.

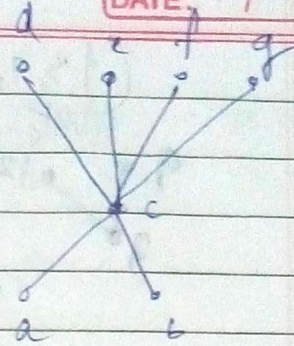
**Least** – One element which is less than any element of the poset

$a \in S$, $x \in S$. (any element in S)

$S$, $a < x$ ✓ $\rightarrow$ a least

$x < a$ $\rightarrow$ greatest



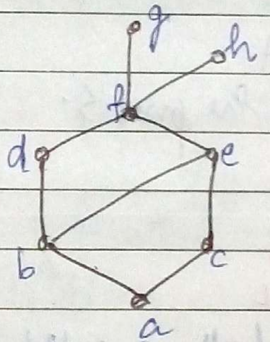




a,b → Minimal
But no ~~least~~ element

---

In case of Powerset, set itself is the greatest element.

Poset – S
Subset of a poset S is A.
$u \in S$
$a \in A$. $a \leq u$




a,b,c < g,h,f,e

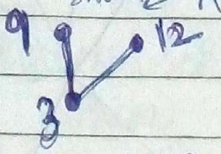
A{a,b,c}
a → least $a \in S$
$a \leq a$ $a \in A$.
$a \leq b$
$a \leq c$

A = {b, d}
ub – d,f,g,h
lb – b,a
least upper bound
lub(A) = d
greatest lower bound
glb = b

We get an element that is greater than equal to all the elements in a subset A of a poset $(S, \preceq)$.
If $u \in S$, $a \preceq u$, for all $a \in A$
then u is called the upper bound (u.b)
Similarly, if $l \in S$, $l \preceq a$ for all $a \in A$.
then l is called the lower bound (l.b).
Lower bound of {a,b,c} is a
Upper bound of {a,b,c} is f, g, h, e.

Ex. $(\{3,9,12\}, |)$ poset

subset ← A  $Z^+$ → set




$3|9$, $3|12$

$1 \in Z^+$
$3 \in A$.

lower bound → 1, 3

glb (A) = 3

no greatest element.

LCM(3, 9, 12) → 36 & its multiples.

ub = {36, 72, ... multiples of 36}

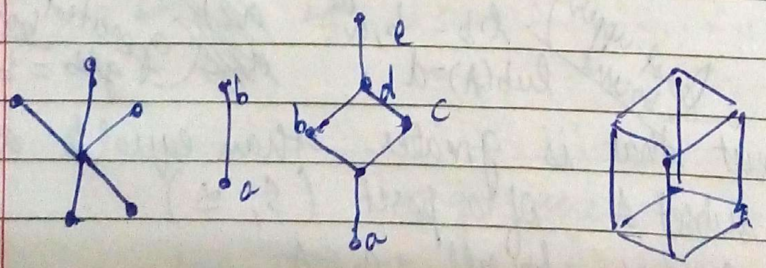
☆ lub(A) = 36 → not contained in A itself

Class Test upto functions

glb (A)
lub (A) — subset A wrt the poset S.

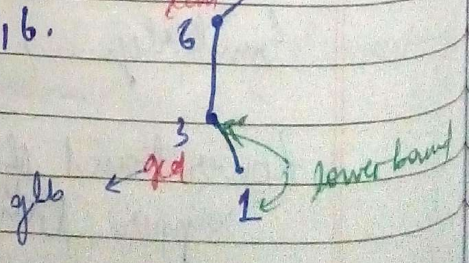
## Application of poset – Lattice

In a poset if every pair has both greatest lower bound (glb) and least upper bound (lub) then it is called a lattice.




S = {a, b, c}.

poset $(Z^+, |)$ – LCM – 3, 6.

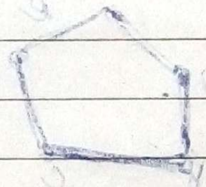


Join  Poset $(P, \leq)$  $((A,C), \leq)$
Meet  $a, b \in P$

join – $a \vee b$ is least upper bound.
meet – $a \wedge b$ is greatest lower bound.

Boolean Algebra
Lattice based cryptography
A – B
 └ C    post quantum cryptography
code based cryptography, lattice based cryptography
Hash based ,, .

Govt



Set of authorities $A = \{$scientist, officers, Director$\}$
$C = \{$Spies, SWs, Agents$\}$
$\{Sp, S, A\}$
$(A, C) = ($Scientist, $\{Sp, S\})$
$= ($Officer, $\{S, A\})$

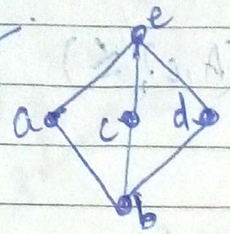
In a lattice

$L_1$  ex.1 $x \wedge y = x$ and ex.2 $x \vee y = x$
$L_2$  $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$
$L_3$  $(x \wedge y) \wedge z = x \wedge (y \wedge z)$  $(x \vee y) \vee z = x \vee (y \vee z)$
$L_4$  $\cancel{x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)}$
$\longrightarrow x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$.

Distributive Law:-
$L_5$. $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$  $(\leq)$
$L_6$. $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$  $(\geq)$

Sublattice S of Lattice L then
$a, b \in S$, $a \wedge b \in S$, $a \vee b \in S$.

Rossen



To prove:- $a \wedge (e \vee d) = (a \wedge e) \vee (a \wedge d)$

LHS.

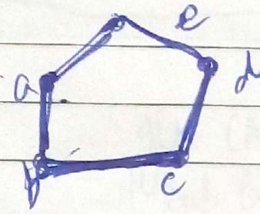
$a \wedge (e \vee d)$
$= a \wedge e$
$= a$

RHS

$(a \wedge e) \vee (a \wedge d)$
$= a \vee b$
$= a$

Lattice ⟹ Distributive Law hold.

---



least.

$d \wedge (a \vee c) = (d \wedge a) \vee (d \wedge c)$

LHS.

$d \wedge e = d$

RHS.

$b \vee c = c$

⟹ Doesnot hold.

**Theorem:**

In any distributive lattice, if $a \wedge x = a \wedge y$ and $a \vee x = a \vee y$

then, togther they imply $x = y$.

Sol:
$x = x \vee (x \wedge a)$
$= x \vee (y \wedge a)$
$= (x \vee y) \wedge (x \vee a)$
$= (y \vee x) \wedge (x \vee a) \longrightarrow (y \vee x) \wedge (y \vee a)$
$= (y \vee x \vee a) \wedge (x \wedge (x \wedge a))$ $= y \vee (x \wedge a)$
$= y \vee (y \wedge a)$
$= y$.

• Apply commutative (in every step if applicable)

$I$ - greatest
$0$ - least

$(a, x)$ - complementary

If $a \wedge x = 0$ (glb)
$a \vee x = I$ (lub)
$x$ is complement of $a$
$a \mid a'$

$(0, I) \rightarrow$ Trivially complemented pair

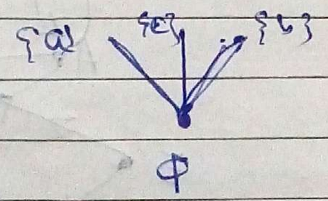
**Theorem**

In a distributive lattice $L$, a given element $a$ can have atmost one complement.

$x = y$
$a = a'$
$a = x$

$a \wedge x = a \wedge y$
$a \vee x = a \vee y$
$\Rightarrow x = y$

$S = \{a, b, c\}$, $\subseteq$
$= \{\phi, \{a\} \{b\}, \{c\}$.



# Closures of Relations

* Computer Network
* Connectivity.

Let R be a relation on a set A with some property P, reflexivity, symmetry, transitivity. If S be a relation containing R with property P such that S contains all the relations (R) with property P then S is the closure of R.

$A = \{1,2,3\}$

$R = \{(1,1), (2,1), (2,3), (1,3)\}$

P → reflexivity $(a,a) \to (2,2), (3,3)$

P → symmetric – if $(a,b), (b,a)$

$(1,2), (3,2), (3,1)$

## Reflexive closure

If we consider the $R = \{(a,b) \mid a<b\}$

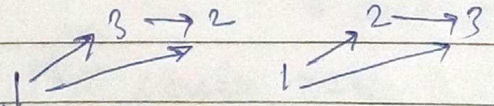
Reflexive closure $R \cup \Delta = \{(a,b) \mid a<b\} \cup \{(a,a) \mid a \in Z\}$

$S = \{(a,b) \mid a \leq b\}$

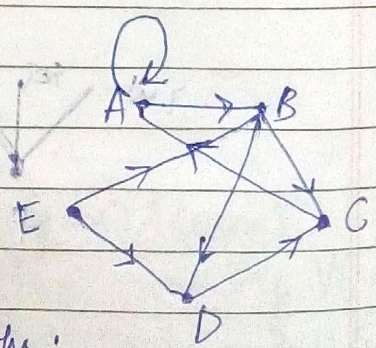
## Symmetric Closure

$R \cup R^{-1} = \{(a,b) \mid a<b\} \cup \{(b,a) \mid a<b\}$

P → transitivity – $(3,2), (1,2)$




## How to find the transitive closure?




Paths :–

A,B, A,B,C, A,B,C,A

D,C,A ✓ D,C,B ✗

Def$^n$:- A path from A to B in a directed graph G is a sequence of edges $(x_0, x_1)$ $(x_1, x_2)$ . . . $(x_{n-1}, x_n)$ in G where $n$ is a non-negative integer and $x_0 = a$ and $x_n = b$.

empty set of edges - loop $a \to a$.

Theorem:- Let R be a relation on a set A. There is a path of length n from a to b, where n is +ve integer. iff $(a,b) \in R^n$.

$R^1$ - if $(a,b) \in R$

$(a,b) \in R^1$

$R^n$-

Proof: by induction

BS if $(a,b) \in R$, there exists a path $R^1$

IS if it holds for $n$ i.e there is $R^n$ then $R^{n+1}$ also exists in R.

$R^{n+1}$ will exist if in between a & b, there is one node c such that $(a,c) \in R$ and $(a,c) \in R^1$ and $(c,b) \in R$ & $(c,b) \in R^n$.

---

Def$^n$ !- Let R be a relation on a set A. The connectivity relation $R^*$ consists of the pairs $(a,b)$ such that there is a path of length atleast one from a to b in R.

$R^*$ is the union of all the sets $R^n$.

$$R^* = \bigcup_{n=1}^{\infty} R^n$$

Theorem:- The transitivity closure of a relation R equals the connectivity relation $R^*$.

by def$^n$ - $R^*$ contains the set of R.

$R^*$ is transitive and $R^* \subseteq S$ where S is transitive and S contains R.

$f(S \cup T) \underset{\subseteq}{=} f(S) \cup f(T)$

## Transitive Closure

**Theorem 1**

$R^*$ – pairs of $(a,b)$ iff $(a,b) \in R^n$

$R^*$ – connectivity relation

**Theorem 2**

The transitive closure of $R$ is the connectivity relation $R^*$.

**Proof:**

$R^*$ contains $R$

We have to prove

(i) $R^*$ is transitive

(ii) $R^* \subseteq S$, where $S$, a transitive relation that contains $R$.

If $(a,b) \in R^*$ if $(b,c) \in R^*$, there exists a to c
$(a,c) \in R^*$, $R^*$ is transitive.

Suppose $S$ is a transitive relation containing $R$.

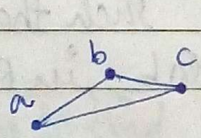
$S^n$ containing $R$

$S^i$ or

$$S^* = \bigcup_{i=1}^{\infty} S^i \qquad S^* \subseteq S.$$

$R \,\&\, S$

$R \subseteq S \qquad R^* \subseteq S^* \subseteq S.$




$(a,b)$

$(a,c)$

**Theorem 3**

Let $M_R$ be the zero-one matrix of the relation $R$ on a set with $n$ elements. Then the zero one matrix of Transitive closure $R^*$ is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \ldots \vee M_R^{[n]}$$

$R = (a,b)$

$a_i, b_j$

Orion

PAGE:
DATE: / /

$M \rightarrow m_{ij} = 1$ if the relation holds for $(a_i, b_j)$

$M = [m_{ij}]$

$S = \{1, 2, 3\}$

Ex1 $R = \{(1,1), (2,1), (3,1), (3,3)\}$

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}_{3\times3}$$

Reflexive → Diagonal = 1.

Symm. → $M = M^T$

Anti-sy → $m_{ji} \neq m_{ij}$ $(j \neq i)$

Relation on one set → square matrix

$A = \{1, 2, 3, 4\}$ $B = \{4, 6\}$

$M \rightarrow (4\times2)$.

---

Composition of 2 relation matrix

$M_{R\circ S} = M_S \odot M_R$

Boolean product of two relation-matrix.

Multiplication $\wedge$ Addition $\vee$

$M_{R^2} = M_R^{[2]} = M_R \odot M_R$

$R = \{(1,1), (2,2), (2,3), (3,1), (3,2)\}$

$$M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}_{n\times n}$$

1, 2, 3

$$M_{R^2} = M_R^{[2]} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$(1,2)\ (2,3) \Rightarrow (1,3)$

2n-1 operations ← $(1\wedge1) \vee (0\wedge0) \vee (0\wedge1)$

$$M_R^{[3]} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

↓

$M_R \odot M_R^{[2]}$

ANUBHAV JAIN NOTES

$$M_{R^*} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = M_R \vee M_R^{[2]} \vee M_R^{[3]}$$

Scanned by CamScanner

Orion
PAGE:
DATE: / /

{(1,1) (2,1) (2,2) (2,3) (3,1) (3,2) (3,3)} → Transitive closure of R.

Complexity

Boolean product of two Matrix.

multiplication

$n^2\,(2n-1)$ $(n-1)$, → no. of products.

$n^2(n-1)$ → Disjunctions (Mr ∨ Mr[2] ...)

$= \boxed{2n^3(n-1)}$ → bit operation

n multiplications $n^2$ times

2n-1 operations

∧, ∨, ...

Algo computing Transitive Closure

Procedure Transitive Closure (Mr - zero one relation Matrix)

$A = M_R$

$B = A$

for i=2 to n

{ $A = A \odot M_R$

$B = B \vee A$

}

$B - R^*$

Warshall's Algorithm → complexity is $\boxed{2n^3}$.

$W_{ij}^{k}$ computed from $W_{ij}^{k-1}$

$R^*$ $M_R^{[k]} - W^k$.

$W_0 = M_R$

$W_0 \cdot W_0$

$M_R \odot M_R$

$W_2$

$W_n$

$M_R^{[2]}$

$R^*$

$W_n$

(1,3)

(3,1)

(1,2)

Orion

PAGE:
DATE: 06 /09 /16

# Warshall's Algorithm

Given a relation / directed graph

$$M_R = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}_{n \times n}$$

$M_R^{[2]}$ - - - - . $M_R^{[n]}$

(Transitive closure) $T.C. = M_R \vee M_R^{[2]} \vee \dots \vee M_R^{[n]}$

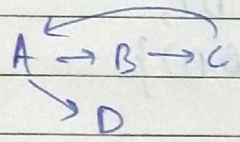
Interior Vertices

Path A to H    $\underline{A}$ B C D E F G $\underline{H}$

└ interior vertices

$\underline{A}$ B C D A E G F $\underline{H}$.

treated as interior

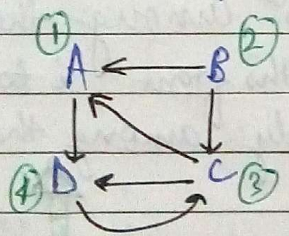



Warshall Matrix $W = [W_{ij}]$

$\boxed{W_{ij}^{k} = 1}$ if there is a path from i to j where the interior vertices is the set.

$\{1, 2, \dots k\}$ or $W_{ik}^{k-1} = 1$, $W_{kj}^{k-1} = 1$.

$W^k$ is computed from previously computed $W^{k-1}$, where $W^0 = M_R$




$$M_R = W^0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$ik - kj \Rightarrow ij$

$$W^1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \rightarrow k = 1 = A$$

ANUBHAV JAIN NOTES

Orion

PAGE:
DATE: / /

$K=2=B$. $W^2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

$K=3=C$ $W^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ → path DCD ⇒ D to D

$K=3$ $(i\,3)(3\,j)$

$(W^2_{i3} = W^2_{3j} = 1)$

$W^3_{ij} = 1$

$K=4=D$ $W^4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ ← $R^*$

$R^* = \{(A,A), (A,C), (A,D), (B,A) (B,C), (B,D), (C,A), (C,C), (C,D), (D,A), (D,C), (D,D)\}$

$R = \{(A,D), (B,A) (B,C) (C,D) (C,A) (D,C)\}$ (given in digraph)

**Compute $W^k$ from $W^{k-1}$**

Lemma: There is a path from $i$ to $j$ with no vertices other than $1, 2, \ldots k$ as interior vertices iff either there is a path from $i$ to $j$ with its interior vertices among the first $k-1$ vertices or there are paths from $i$ to $k$ & $k$ to $j$ that have interior vertices only among the $1^{st}$ $(k-1)$ vertices.

Let $W_k = W_{ij}^k$ be the $k^{th}$ interior matrix that has 1 in $ij^{th}$ position iff there is a path between $i$ & $j$ with interior vertices $\{1, 2, \ldots k\}$ then

$$\boxed{W_{ij}^k = W_{ij}^{k-1} \vee \left(W_{ik}^{k-1} \wedge W_{kj}^{k-1}\right)}$$

Procedure Warshall ($W_0 = M_R = n \times n$ matrix)

```
W = M_R
for k = 1 to n
{
    for j = 1 to n
    {
        for i = 1 to n
        {
            W = W_ij ∨ (W_ik ∧ W_kj)
        }
    }
}
W = R*
```

($2n^2$ bit operation in 1 matrix) $\times$ ($n$ matrices)

$\Rightarrow \boxed{\text{Complexity} = 2n^3}$

Q25, 26.

25(d) (1,1) (1,4) (2,1) (2,3)
(3,1) (3,2) (3,4) (4,2)

$$M_R = W^0 = \begin{bmatrix} 1&0&0&1\\1&0&1&0\\1&1&0&1\\0&1&0&0 \end{bmatrix} \rightarrow W^1_{(k=1)} = \begin{bmatrix} 1&0&0&1\\1&0&1&1\\1&1&0&1\\0&1&0&0 \end{bmatrix} \rightarrow W^2 = \begin{bmatrix} 1&0&0&1\\1&0&1&1\\1&1&1&1\\1&1&1&1 \end{bmatrix} \rightarrow W^3 = \begin{bmatrix} 1&0&0&1\\1&1&1&1\\1&1&1&1\\1&1&1&1 \end{bmatrix} \rightarrow W^4 = \begin{bmatrix} 1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1 \end{bmatrix}$$

$$M_R^{[2]} = M_R \odot M_R = \begin{bmatrix} 1&1&0&1\\1&1&0&1\\1&1&1&1\\1&0&1&0 \end{bmatrix}$$

$$M_R^{[3]} = M_R \odot M_R^{[2]} = \begin{bmatrix} 1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&0&1 \end{bmatrix} \longrightarrow$$

$$M_R^{[4]} = M_R \odot M_R^{[3]} = \begin{bmatrix} 1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1 \end{bmatrix}$$

Orion
PAGE:
DATE: 08/09/16

**Theorem** Let R be an equivalence relation on a set A. statements for elements a, b of A are equivalent.

(i) $aRb$ (ii) $[a]=[b]$ (iii) $[a]\cap[b] \neq \phi$

(i) $def^n$ $aRb$
(ii) $[a]=[b]$
(iii) $[a] - aRc$

Subsets are either disjoint or equal.

$aRb$, $aRc$, $bRa$, $aRc$, $bRc$

---

Inverse function

$f: A \to B$

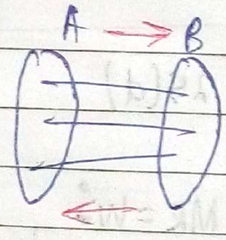
one to one correspondence between elements of A and that of B.

f is one to one and onto

$g: B \to A$

g is defined as inverse of f,

f is bijective



---

**Theorem** Suppose $f: A \to B$ is a bijective function, $f^{-1}$ is its inverse.

for each $x \in B$, $f o f^{-1}(x) = x$

for each $x \in A$, $f^{-1} o f(x) = x$.

$A \to B$

$x \in B$

Let $f^{-1}(x) = Z$

then $f(Z) = x$ by $def^n$

$x \in A$

Let $f(x) = Z$

then $f^{-1}(Z) = x$

$A = \{a, b, c\}$ $B = \{1, 2, 3\}$

$f = \{(a, 1), (b, 3) (c, 2)\}$

$f^{-1} = \{(1, a), (3, b) (2, c)\}$

Scanned by CamScanner

**Ex.** Show $f(x) = x^3$
and $g(x) = x^{1/3}$ are inverse of each other.

$fog(x) = f(x^{1/3}) = (x^{1/3})^3 = x$
$gof(x) = g(x^3) = (x^3)^{1/3} = x$

$\Rightarrow$ Hence, Proved.

---

$f^2 \equiv fof$
$f^3 \equiv fofof$

---

**Ex.** Let $f$ be a function for $X$ onto $Y$.
Let $S = \{f^{-1}(\{y\}) \mid y \in Y\}$
Show that $S$ is a partition of $X$. Describe an equivalence relation that gives rise to the partition.

$f$ is a bijection, one to one & onto.
$f: X \to Y$, $f^{-1}$ $Y \to X$
$f^{-1} = \{(y, x) \mid (x, y) \in f\}$

$S = \{f^{-1}(\{y\}) \mid y \in Y\}$ Let $x \in X$
$y = f(x)$
$s \in S$
$S = \{f^{-1}(f(x)) \mid x \in X, y \in Y\}$

$\bigcup_{x \in X} s \mid s \in S = X$

Let $a \in \{f^{-1}(\{y\})\} \cap \{f^{-1}(\{z\})\}$

$y = f(a)$ — $a \in \{f^{-1}(\{y\})\}$
$z = f(a)$ — $a \in \{f^{-1}(\{z\})\}$

$y = z$ → Not possible for $\Rightarrow$ This assumption is wrong $\Rightarrow$ $S$ is disjoint subset
$\hookrightarrow y = z$

partition
$\Uparrow$

$x R y$ if $f(x) = f(y)$

$f$ be a function from $X$ to $Y$

$R$ is an equivalence relation $R$ on $X$.