1 GRAPH THEORY

1.1 Basics of Graphs:

The number of vertices of odd degree in a graph is always even.

Every graph has an even number of odd vertices.

- Based on Parallel edges & self-loops graphs are classified into 3 types

	Parallel graph	Self-loops
Simple graph	×	×
Multi graph	✓	×
Pseudograph	✓	✓

(We mainly discuss simple graph in our syllabus)

1.1.1 Theorem1:

Maximum degree of a vertex, in a simple graph with n vertices, is ≤ n – 1.

Note:

Hand Shaking Lemma: Sum of all degrees = 2 × sum of all edges.

1.1.2 Theorem2 :

Maximum no. of edges, in a simple graph with n vertices, is ≤ $n_{c_2} = \frac{n(n-1)}{2}$

Note: No of different graphs possible with n distinct vertices is $= 2^{\frac{n(n-1)}{2}}$

No. of different graphs possible with n distinct vertices and 'e' edges is $\left[\frac{n(n-1)}{2}\right]_{C_e}$

1.1.3 Degree sequence:

If the degrees of a graph are written in increasing order or decreasing order, we call it a degree sequence

- Not all degree sequence forms simple graph.
- The degree sequence which forms simple graph is called graphical

1.1.4 Theorem 3:

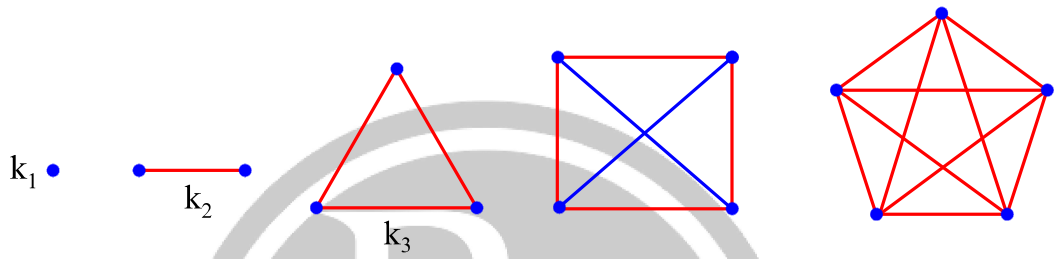
In a simple graph at least two vertices with have same degree ($n \geq 2$)
Example: {5, 4, 3, 2, 1} is not graphical

1.1.5 Theorem 4:

Max degrees in a given graph G is denoted as $\Delta(G)$ & Min degree is denoted as $\delta(G)$

$$\delta(G) \leq \frac{2e}{n} \leq \Delta(G) \leq n-1$$

1.1.6 Complete Graph (k_n) ($n \geq 1$):



Degree of every vertex is $n - 1$

(or)

There direct edge b/w every pair of vertices

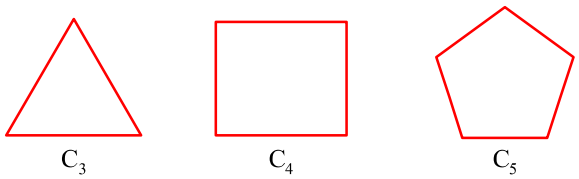
- no. of edges is,

$$e = \frac{n(n-1)}{2}$$

1.1.7 Regular Graph:

A graph in which degree of all vertices is same is called a regular graph.
$n.\delta(G) = 2e = n.\Delta(G)$

1.1.8 Cycle Graph (C_n) ($n \geq 3$):



If given degree sequence is all 2's, then it's not guaranteed that it's a cycle graph
G: [2, 2, 2, 2, 2, 2]

Degree of all vertices is 2 in a cycle graph

- Every Cn is a regular graph
- Number of Edges = n = Number of Vertex

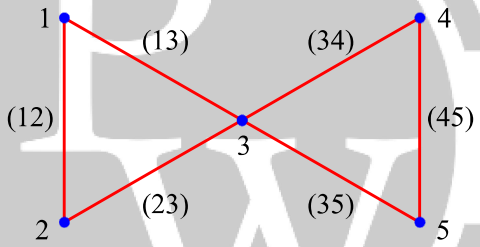
1.1.9 Wheel Graph (w_n) ($n \geq 4$):

A wheel graph w_n is obtained by adding a vertex (hub) to c_{n-1}(Cycle Graph) such that this vertex is adjacent to all the other vertices.

Number of edges = 2 (n - 1)

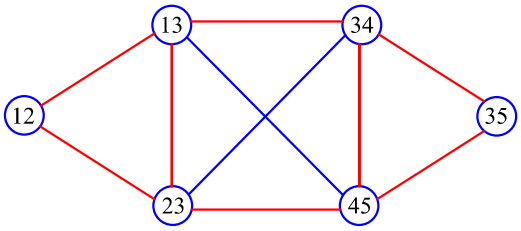
1.1.10 Line Graph (L(G)):

Consider below graph, G



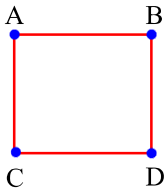
Step to construct L(G)

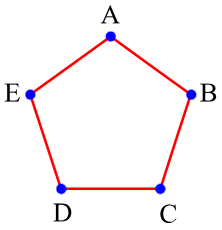
(i) define edges in G
(ii) label these edges as vertices in L(G)
(iii) Connect vertices with common number.

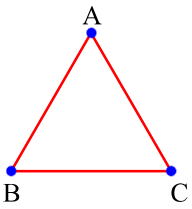


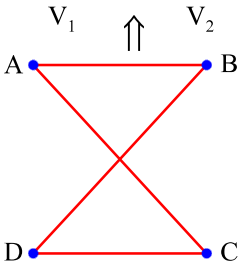
Line graph of every cycle graph is also a cycle.

1.1.11 Bipartite (L(G)):

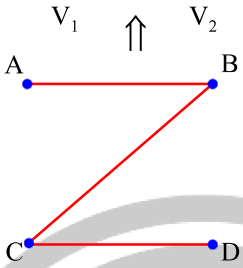








$\therefore C_4$ is a bipartite graph



Now adding E in either of the sets violates the property of bipartite graph

$\therefore C_5$ is not a bipartite graph

adding C is not possible

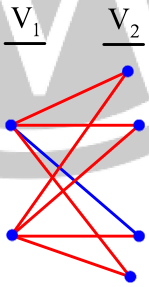
$\therefore C_3$ is not a bipartite graph

Note: Bi – partite graphs do not contain odd length cycle.

1.1.12 Complete bipartite graph ($k_{m,n}$) :

Each vertex in set v_1 is adjacent to all vertices in set v_2.

Example:



$K_2, 4$ $\quad |v_1| = m$

$|v_2| = n$

In $k_{m,n}$ number of vertices = m + n

number of edges = mn

$\Delta(k_{m,n}) = \max(m, n)$, $\quad \delta(k_{m,n}) = \min(m, n)$

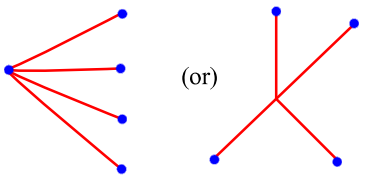
1.1.13 Theorem 5 :

- Maximum no. of edges passible is bipartite graph of n vertices is $\leq \left\lfloor \frac{n^2}{4} \right\rfloor$

1.1.14 Star graph ($k_{1,n-1}$) :

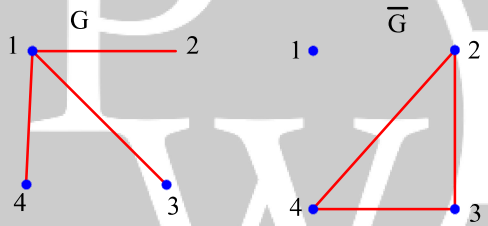
It is complete bipartite graph with one vertex in one set and rest of the vertices in other set.
(or)
Star graph (k_1, k_{n-1}) is complete bipartite graph possible with n vertices and minimum no. of edges.

Eg: Star graph of 5 vertices, k_1, 4 is
total no of edges in $k_{1,n-1} = n - 1$
$\Delta(k_{1,n-1}) = n - 1$, $\delta(k_{1,n-1}) = 1$



1.1.15 Complement graph $(\bar{G})$:

For a graph G, complement of G$(\bar{G})$ is the graph which contains all the vertices present in G and does not contain the edges present in G.



$$\therefore \quad G + \bar{G} = k_n \Rightarrow e(G) + e(\bar{G}) = \frac{n(n-1)}{2}$$

If the degree of vertex v is x in graph G, then the degree of vertex v in $\bar{G}$ is [(n-1)-x]
If $d_1, d_2 \ldots\ldots d_n$ is degree sequence for G then
$(n-1-d_1), (n1-d_2), \ldots.. (n-1-d_n)$ is degree sequence of $\bar{G}$

Example:
consider a graph of degree sequence {5, 2, 2, 2, 2, 1}.
What is the degree sequence of complement graph?
Total vertices, n = 6

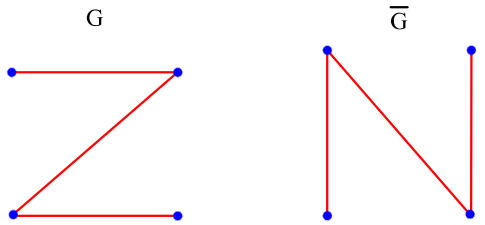
$$k_6 \rightarrow 5, 5, 5, 5, 5, 5$$
$$G \rightarrow 5, 2, 2, 2, 2, 1$$
$$\bar{G} \rightarrow \{0, 3, 3, 3, 3, 4\}$$

Isomorphic Graphs:
Let G1 = (V1, E1) and G2 = (V2, E2) be two undirected graphs. A function f: V1 → V2 is called a graph isomorphism if (a) f is one-to-one and onto, and (b) for all a, b ∈ V1. {a, b} ∈ E1 if and only if {f(a), f(b)} ∈ E2. When such a function exists, G1 and G2 are called isomorphic graphs.

(ii) Self-complement: $(G \equiv \bar{G})$

It is a graph which is isomorphic to-its own complement.

i.e., $G = \bar{G}$



It is clear that above two graphs are self-complement to each other.

w.r.t

$$e(G) + e(\bar{G}) = \frac{n(n-1)}{2}$$

Let e be no. of edges in G

$$e\ te = \frac{n(n-1)}{2}$$

- $e = \frac{n(n-1)}{4}$ i.e., no. of edges in a self-complement graph

Complement of star graph $k_{1, n-1}$ gives one isolated vertex and a complete graph k_{n-1}

n must be congruent to 0 or 1 mod 4.

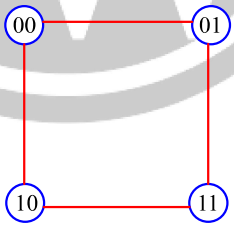
Hypercube (Q_n):

Q_1

2' vertices – 0, 1

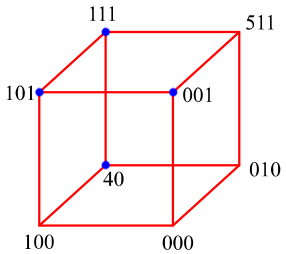
Q_2

4' vertices – 00, 01, 10, 11



Every cycle in hypercube B of even length (think why). So, every hypercube is bipartite graph

Q_3: 2^3 vertices



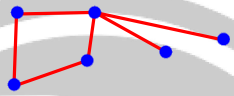
Number of edges = $\frac{n \times 2^n}{2} = n \times 2^{n-1}$

1.2 Connectivity

Name	Repeated Vertex (Vertices)	Repeated Edge(s)	Open	Closed
Walk (open)	Yes	Yes	Yes	
Walk (closed)	Yes	Yes		Yes
Trail	Yes	No	Yes	
Circuit	Yes	No		Yes
Path	No	No	Yes	
Cycle	No	No		Yes

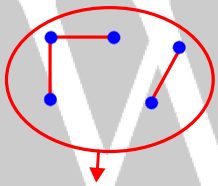
1.2.1 Connected graph:

For every two pair of vertices, there must exist a path between them.



1.2.2 Disconnected graph:

If we can find at least one pair of vertices, such that there is no path available b/w these 2 verities, then the graph is said to be disconnected graph.

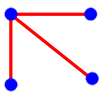


Disconnected graph

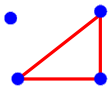
- If G is connected then $\bar{G}$ may be connected or disconnected

G Connected

$\overline{G}$ Connected



G Connected

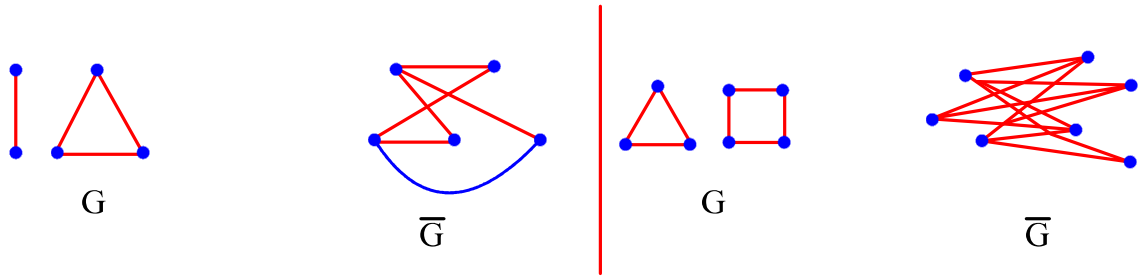


$\overline{G}$ disconnected

1.2.3 Theorem 6:

If G is disconnected, then $\bar{G}$ is connected.

Example:



1.2.4 Range of edges for a connected graph (k=1):

(k is connected components)

Tree

- Minimum no of edges required to get a possibility to make graph connected with in vertices is n-1.

$$(n-1)_{Tree} \le e \le \frac{n(n-1)}{2}$$

- The connected graph with n-1 edges is doesn't have a cycle.
- This graph is known as minimally connected graph.
- In this kind of graph, these will be a unique path b/w any two pair of vertices.
- This kind of graph is called a tree (a connected graph with no cycles)

1.2.5 Range of edges for a disconnected graph:

- Edges range b/w

$$n-k \le e \le \frac{(n-k)(n-k+1)}{2}$$

Proof:

Here lets say we have k components with $n_1, n_2 \ldots\ldots n_k$ components

$\therefore n_1 + n_2 + \ldots\ldots + n_2 : k$

For min no. of edge, each compared must be minimally connected.

$\therefore$ min no of edges is

$N_1 - 1 + n_2 - 1 + \ldots\ldots + n_k - 1$

$= (n_1 + n_2 + \ldots.. n_k) - k = n - k$

Note:

1. Let G be a graph of order n. If

deg u + deg v ≥ n – 1

nonadjacent vertices u and v of G, then G is connected and diam(G) ≤ 2.

2. If G is a graph of order n with $\delta(G) \ge (n-1)/2$, then G is connected.

3. A directed graph is strong connected if there is a path from a to b and from b to a whenever a and b are vertices in the graph.

4.A directed graph is weakly connected if there is a path between every two vertices in the underlying undirected graph.

5. $k(G) \le \lambda(G) \le \min_{v \in v} \deg(v)$.

6. Simple graph G with n vertices is connected if it has more than (n - 1) (n - 2)/2 edges.
7. Let G = (V, E) be a loop-free graph with n (≥2) vertices. If deg(v) ≥ (n - 1)/2 for all v ∈ V, then G has a Hamilton path.
8. If G = (V, E) is a loop-free undirected graph with $|V| = n \geq 3$, and if $|E| \geq \binom{n-1}{2} + 2$, then G has a Hamilton cycle.
9. If G = (V, E) is a loop-free undirected graph with $|V| = n \geq 3$, and $\deg(v) \geq n/2$ for all v ∈ V, then G has a Hamilton cycle.
(10) If G_1, G_2 are (loop-free) undirected graphs, G_1, G_2 are isomorphic if and only if $\bar{G}_1, \bar{G}_2$ are isomorphic.
(11) If G is an undirected graph or multigraph with no isolated vertices, then we can construct an Euler trail in G if and only if G is connected and has exactly two vertices of odd degree.
(12) $k(G) \leq \lambda(G) \leq \delta(G) \leq \Delta(G) \leq n-1$

1.3 Planarity

A graph (or multigraph) G is called planar if G can be drawn in the plane with its edges intersecting only at vertices of G. Such a drawing of G is called an embedding of G in the plane.

Kuratowski's Theorem. A graph is nonplanar if and only if it contains s subgraph that is homomorphic to either K_5 or $K_{3,3}$.

Let G = (V, E) be a connected planar graph or multigraph with |V| = ν and |E| = e. Let r be the number of regions in the plane determined by a planar embedding (or, depiction) of G; one of these regions has infinite area and is called the infinite region. Then ν – e + r = 2.
Let G = (V, E) be a loop-free connected planar graph with |V| = ν, |E| = e > 2, and r regions. Then 3r ≤ 2e and e ≤ 3ν – 6.

1.3.1 Coloring:

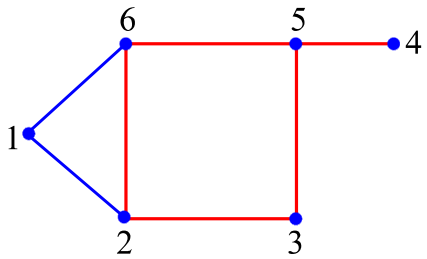
Note: Every MIS will always be MDS. But reverse need not to be true
Domination number ≤ Independence number.
α(G) = ≤ β(G

1.3.2 Theorem 7 :

Sum of size of minimum vertex cover and size of maximum independent set is equal to number of vertices

1.4 Covering:

It is set of edges such that all vertices should incident on at least one edge.



{16, 12, 65, 53, 54}
{16, 54, 23}, {16, 12, 53, 54}
{12, 16, 65, 23, 53, 62, 54}

Set of all edge is also a covering set

- It is also known as edge covering set.

1.4.1 Minimal Covering set:

It is a covering set from which we can't remove new elements(edge).
{16, 12, 53, 54} . {16, 54, 23} are MCS

1.4.2 Covering Number (C(G)):

It is no of edges present smallest covering set.
For above graph C(G) = 3

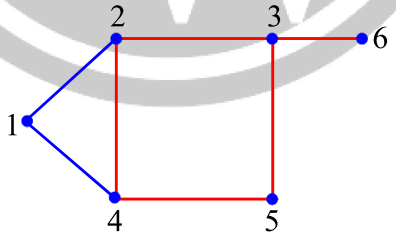
1.5 Perfect Matching:

A matching is said to be prefect matching if every vertex in the graph is matched
(or)
Induced degree of all the vertices is 1.

1.5.1 Induced degree:

The degree of a vertex in a matching is called indeed degree

Example:



{12, 45, 36} is perfect matching

Note: Every perfect matching is maximal, but reverse need not to be true.
If prefect matching exists, then no. of vertices will always be even but reverse need not to be true.
A graph may contain more than one perfect matching.
Total no. of prefect matching possible for a complete graph with 2n vertices is $\frac{(2n)!}{2^n.n!}$

❑❑❑

2 LOGIC HANDBOOK

2.1 Introduction

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "if p, then q."

The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p is called the hypothesis (or *antecedent* or *premise*) and q is called the conclusion (*or consequence*).

"if p, then q"	"p implies q"
"if p, q"	"p only if q"
"p is sufficient for q"	"a sufficient condition for q is p"
"q if p"	"q whenever p"
"q when p"	"q is necessary for p"
"a necessary condition for p is q"	"q follows from p"
"q unless $\neg p$"	"q provided that p"

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ is the proposition "p if and only if q". The biconditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise. Biconditional statements are also called bi-implications.

Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. A compound proposition that is neither a tautology nor a contradiction is called contingency.

→ Every contingency is satisfiable, but reverse need not to be true 1.

→ Every tautology is satisfiable, but revers need not to be true.

For any primitive statements p, q, r, any tautology 'T' and any contradiction 'F'.

(1) $\neg \neg p \Leftrightarrow p$ Law of Double Negation

(2) $\neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$ DeMorgan's Laws

$\neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$

(3) $p \vee q \Leftrightarrow q \vee p$ Commutative Laws

$p \wedge q \Leftrightarrow q \wedge p$

(4) $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ Associative Laws

$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$

(5) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ Distributive Laws

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

(6) $p \vee p \Leftrightarrow p$ Idempotent Laws

$p \wedge p \Leftrightarrow p$

(7) $p \vee F \Leftrightarrow p$ Identity Laws

$p \vee T \Leftrightarrow p$

(8) $p \vee \neg p \Leftrightarrow T$ Inverse Laws

$p \wedge \neg p \Leftrightarrow F$

(9) $p \vee T \Leftrightarrow T$ Domination Laws

$p \wedge F \Leftrightarrow F$

(10) $p \vee (p \wedge q) \Leftrightarrow p$ Absorption Laws

$p \vee (p \wedge q) \Leftrightarrow p$

$p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to \neg q$

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

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

$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Rule of Inference	Related Logical Implications	Name of Rule
1) $\dfrac{p \quad p \to q}{\therefore q}$	$[p \wedge (p \to q)] \to q$	Rule of Detachment (Modus Ponens)
2) $\dfrac{p \to q \quad q \to r}{\therefore p \to r}$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Law of the syllogism
3) $\dfrac{p \to q \quad \neg q}{\therefore \neg p}$	$[(p \to q) \wedge \neg q] \to \neg p$	Modus Tollens

4) $\dfrac{p}{q}$ $\therefore p \wedge q$		Rules of Conjunction
5) $\dfrac{p \vee q}{\neg p}$ $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Rule of Disjunctive Syllogism
6) $\dfrac{\neg p \rightarrow F}{\therefore p}$	$(\neg p \rightarrow F_0) \rightarrow p$	Rule of Contradiction
7) $\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Rule of Conjunctive simplification
8) $\dfrac{p}{\therefore p \vee q}$	$p \rightarrow p \vee q$	Rule of Disjunctive Amplification
9) $\dfrac{p \wedge q}{p \rightarrow (q \rightarrow r)}$ $\therefore r$	$[(p \wedge q) \wedge [p \rightarrow (q \rightarrow r)]] \rightarrow r$	Rule of Conditional Proof
10) $\dfrac{p \rightarrow q}{q \rightarrow r}$ $\therefore (p \vee q) \rightarrow r$	$[(p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow [(p \vee q) \rightarrow r]$	Rule for Proof by Cases
11) $\dfrac{p \rightarrow q}{r \rightarrow s}$ $\dfrac{p \vee r}{\therefore q \vee s}$	$[(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r)] \rightarrow (q \vee s)$	Rule of the Constructive Dilemma
12) $\dfrac{p \rightarrow q}{r \rightarrow s}$ $\dfrac{\neg q \vee \neg s}{\therefore \neg p \vee \neg r}$	$[(p \rightarrow q) \wedge (r \rightarrow s) \wedge (\neg q \vee \neg s)] \rightarrow (\neg p \vee \neg r)$	Rule of the Destructive Dilemma

$\exists x\, p(x)$	For some (at least one) a in the universe, $p(a)$ is true.	For every a in the universe, $p(a)$ is false.
$\forall x\, p(x)$	For every replacement a from The universe, $p(a)$ is true.	There is at least one replacement a from the universe for which $p(a)$ is false.
$\exists x \neg p(x)$	For at least one choice a in The universe, $p(a)$ is false, so Its negation $\neg p(a)$ is true.	For every replacement a in the universe, $p(a)$ is true.

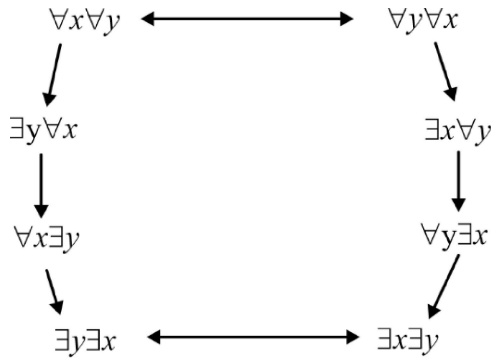
$\forall x \neg p(x)$	For every replacement a from The universe, $p(a)$ is false and its negation $\neg p(a)$ is true	There is at least one replacement a from the universe for which $\neg p(a)$ is false and $p(a)$ is true.

$$\neg [\forall x\, p(x)] \Leftrightarrow \exists x \neg p(x)$$
$$\neg [\exists x\, p(x)] \Leftrightarrow \forall x \neg p(x)$$
$$\neg [\forall x \neg p(x)] \Leftrightarrow \exists x \neg\neg p(x) \Leftrightarrow \exists x\, p(x)$$
$$\neg [\exists x \neg p(x)] \Leftrightarrow \forall x \neg\neg p(x) \Leftrightarrow \forall x\, p(x)$$

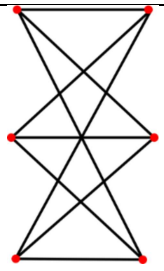
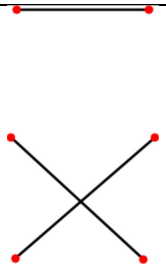
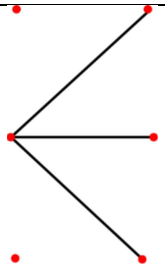
$\exists x\, [P(x) \vee Q(x)] \equiv \exists x\, P(x) \vee \exists x\, Q(x)$
$\forall x\, [P(x) \vee Q(x)] \equiv \forall x\, P(x) \vee \forall x\, Q(x)$
$\exists x\, [P(x) \wedge Q(x)] \rightarrow \exists x\, P(x) \wedge \exists x\, Q(x)$
$\forall x\, [P(x) \wedge \forall\, Q(x)] \rightarrow \forall x\, [P(x) \vee Q(x)]$
$\forall x\, [P(x) \rightarrow\ Q(x)] \rightarrow \forall x\, P(x) \rightarrow \forall x\, Q(x)$
$\forall x\, [P(x) \leftrightarrow\ Q(x)] \rightarrow \forall\, P(x) \leftrightarrow \forall x\, Q(x)$
$(\forall x)\, P(x) \wedge (\forall x)\, Q(x) \Leftrightarrow (\forall x)\, [P(x) \wedge Q(x)]$
$(\forall x)\, P(x) \wedge (\forall x)\, Q(x) \Leftrightarrow (\forall x)\, (\forall y)\, [P(x) \vee Q(y)]$
$(\exists x)\, P(x) \vee (\exists x)\, Q(x) \Leftrightarrow (\exists x)\, (\exists y)\, [P(x) \wedge Q(y)]$
$(\exists x)\, P(x) \vee (\exists x)\, Q(x) \Leftrightarrow (\exists x)\, [P(x) \vee Q(y)]$
$(\forall x)\, P(x) \wedge (\exists x)\, Q(x) \Leftrightarrow (\forall x)\, (\exists y)\, [\, P(x) \wedge Q(y)]$
$(\forall x)\, P(x) \vee (\exists x)\, Q(x) \Leftrightarrow (\forall x)\, (\exists y)\, [\, P(x) \vee Q(y)]$
$A \vee (\forall x)\, P(x) \Leftrightarrow (\forall x)\, [A \vee P(x)]$
$A \vee (\exists x)\, P(x) \Leftrightarrow (\exists x)\, [A \vee P(x)]$
$A \wedge (\forall x)\, P(x) \Leftrightarrow (\forall x)\, [A \wedge P(x)]$
$A \wedge (\exists x)\, P(x) \Leftrightarrow (\exists x)\, [A \wedge P(x)]$

Statement	When True?	When False?
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which P(x, y) is true for every y.	For every x there is a y for which P(x, y) is false.

$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	The is a pair x, y for which P(x, y) is true	P(x, y) is false for every pair x, y



Rule of Inference	***Name***
$\dfrac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\dfrac{P(c) \text{for an arbitary } c}{\therefore \forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{\therefore \text{for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{for some elemet } c}{\therefore \exists x P(x)}$	Existential generalization

Number of non-equivalent propositional function possible with 'n' propositional variable			
2^{2^n}			
Nested Quantifier			
$\forall x \forall y$	$\forall x \exists y$	$\exists y \forall x$	$\exists x \exists y$
			
English statements		**Logical Expressions**	

All graphs are connected	$\forall x[G(x) \rightarrow C(x)]$
Not all graphs are connected	$\neg\forall x[G(x) \rightarrow C(x)]$
All graphs are not connected ≡ No graphs are connected	$\forall x[G(x) \rightarrow \neg C(x)] \equiv \forall x[G(x) \rightarrow \neg C(x)]$

❑❑❑

3 SET THEORY

3.1 Introduction

Collection of unordered, district and well defined objects.

- $\{1, 2\} = \{2, 1\} = \{1, 2, 1\}$ (order & repetition doesn't matter)

  Set representation: A $\{1, 2, 3\}$ - Roaster form

  $A = \{z|z \in N \quad x \leq 3\}$ – Set builder form
- Set with one element is known as singleton set.
- Set with zero element is known as empty set or null set.
- No of elements in a set is known as cardinality of set.
- If a set A contains an element a, it is denoted as:

  $a \in A$.

3.1.1 Equal sets (Axiom of extension):

Two sets A and B are said to be equal iff they have same set of elements.

$A = B \Leftrightarrow \forall_x (x \in A \leftrightarrow x \in B) \Leftrightarrow A \subseteq B \wedge B \supseteq A$

3.1.2 Subset:

- A is said to be subset of B iff every element in A is also then in B. Denoted as $A \subseteq B$

  $\forall x (x \in A \Rightarrow x \in B)$

3.1.3 Proper subset:

- 'A' is said to be a proper subset of B if every element in A. exist in B and $A \neq B$. Denoted as $A \subset B$

  i.e., $A \subset B \Leftrightarrow \forall x (x \in A \rightarrow x \in B) \wedge \exists x. (x \in B \wedge x \notin A)$

  or

  $A \subset B \Leftrightarrow \forall x (x \in A \rightarrow x \in B) \wedge (|A| \neq |B|)$

3.1.4 Powerset:

Powerset of a set A is set of all subsets of A. Denoted as P(A)

- if |A| = n

  $|P(A)| = 2^n$

- For any set A

  $\phi \subseteq A$

  If A = ϕ, then

  $\phi \subset A$

3.1.5 Operations on set:

(i) **Union:**

$A \cup B = \{x | x \in A \vee x \in B\}$

(ii) **Intersection:**

$A \cap B = \{x | x \in A \wedge x \in B\}$

(iii) **Complement:**

If A is a set,

Complement of A, $\bar{A} = A^c = \{x | x \in \cup \wedge x \notin A\}$

i.e., $\bar{A} = U - A = U \cap \bar{A}$

(iv) **Difference:**

$A/B = A - B = \{x | x \in A \wedge x \notin B\} = A \cap \bar{B}$

$A - \bar{B}$ is also called complement of B w.r.t. to A.

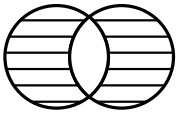
"complement of B in A"

(v) **Symmetric Difference:**

$A \Delta B = \{x | x \in A \vee x \in B$, but not both$\}$

Since it corresponds to XOR operator, it is also denoted as $A \oplus B$

$A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$



- Two sets are said to be disjoint if their intersection ϕ.

3.1.6 Loss involving set operations:

- $\left.\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}\right\}$ Idempotent law
- $\left.\begin{aligned} A \cap \phi &= \phi \\ A \cup U &= U \end{aligned}\right\}$ Domination law
- $\left.\begin{aligned} A \cap U &= A \\ A \cup \phi &= A \end{aligned}\right\}$ Indentity law
- $\left.\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cup (B \cap C) &= (A \cap B) \cap C \\ A \oplus (B \oplus C) &= (A \oplus B) \oplus C \end{aligned}\right\}$ Associative law

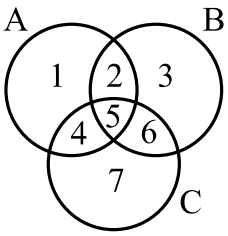
  $\because$ XOR operation is associative
- $\left.\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup (A \cup c) \\ A \cap (B \cap C) &= (A \cap B) \cup (A \cap C) \end{aligned}\right\}$ Distributive law
- $\left.\begin{aligned} A \cup (A \cap B) &= A \\ A \cap (A \cup B) &= A \end{aligned}\right\}$ absorption law
- $\left.\begin{aligned} \overline{A \cup B} &= \bar{A} \cup \bar{B} \\ \overline{A \cup B} &= \bar{A} \cap \bar{B} \end{aligned}\right\}$ Demorgan's law

Note:

$\left.\begin{aligned} A \oplus B = A \oplus C &\Rightarrow B = C \\ A \oplus C = B \oplus C &\Rightarrow A = C \end{aligned}\right\}$ *The proot can be obtained by relating this to XOR operation in* logic.

3.1.7 Representation of sets using Venn diagrams:

Rather than direct calculations we sometimes represent sets with Venn diagram and see them as regions.
Let A, B, C be 3 sets



The region 1 is represented by $A \cap \overline{B} \cap \overline{c}$

The region 2 is represented by $A \cap B \cap \overline{c}$

Similarly, we have 8 regions including region outside of A, B, C

The principle of duality:

Let s denote a theorem dealing with the equality at two expressions which involve only operation $\cup$ and $\cap$. The dual of s(sd) (i.e., expression obtained by interchanging $\cup$ and $\cap$) is also a theorem.

Finding dual of $A \subseteq B$

$A \subseteq B$ can be written as

$A \cup B = B$

Dual is $A \cap B = B$

i.e., $B \subseteq A$

$\therefore$ Dual of $A \subseteq B$ is $B \subseteq A$

Duality principle should be applied only for general can but no for particular cases

3.1.8 Cartesian Product:

$A \times B = \{(a, b) | a \in A \wedge \text{be } B\}$

- Cartesian product is associative

  However

$$\underset{\text{it has ordered pairs t type } ((a,b),c)}{(A \times B) \times C} \neq \underset{(a,(b,c))}{A \times (B \times C)}$$

  $A \times B \neq B \times A$

  If $A \times B = B \times A$ then $(A = B \vee (A = \phi) \vee (B = \phi)$

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$

  $A \times (B \cup C) = (A \times B) \cup (A \times C)$

  $\overline{A} \times \overline{B} \neq \overline{A \times B}$

$\overline{A} \times \overline{B} \leq \overline{A \times B}$

3.1.9 Multisets:

Multiset is an unordered collection of elements where on element can occur more than once.

Eg: $\{m_1.a_1, m_2.a_2 \text{ --- } m_n a_n\}$

Where m_1 is called multiplicity of set

3.1.10 Operations on multisets:

- Union: Maximum of multiplicities is considered.
- Intersection: Minimum of multiplicities is considered
- Difference: Difference of multiplicities is considered.

  If the difference is -ve, it is considered 0.
- Sum: Sum of multiplicities is considered.

  It is denoted as P + Q

3.2 Relations:

A binary relation from set A to set B is any subset of A × B.

If |A| = M and |B| = n, then |A × B| = mn

∴ number of relations possible from A to B = 2^{mn}

If relation B from A to A we say it relation on A.

∴ Number of relations possible on a set A = 2^{n^2}, |A| = n

Domain of relation : $\{ x \mid (x, y) \in R\}$

Range of relation : $\{y \mid (x, y) \in R\}$

- (x, y) ∈R is written as 'xRy' on 'k' relates y

3.2.1 Inverse of relations:

Inverse of a relation, $R^{-1} = \{(y, x) | (x, y) \in R\}$

3.2.2 Diagonal relation:

Diagonal relation on set A is

$\Delta_A = \{(a,a) \mid \forall a \in A\}$

3.2.3 Reflexive relations:

Relation R defined on set A is reflexive

$\Leftrightarrow aRa\ \forall a \in A$

i.e., if R is a reflexive relation then $\Delta_A \leq R$

3.2.4 Important type of relations:

Type of relation	Condition	No. of relatives possible	Union	Intersection
Reflective	aRa, ∀a∈A	2^{n^2-n}	✓	✓
Irreflective	∀a∈A (a $\not R$ a)	2^{n^2-n}	✓	✓
Symmetric	∀x, y∈A($xR_y \Rightarrow yR_x$)	$2^n.2^{\frac{n^2-n}{2}}$	✓	✓
Antisymmetric	∀x, ∀y ($xR_y \wedge yR_x \Rightarrow x = y$)	$2^n\ 3^{\frac{n^2-n}{2}}$	×	✓
Asymmetric	∀x, ∀y ($xR_y \Rightarrow y \not R_x$)	$3^{\frac{n^2-n}{2}}$	×	✓
Transitive	∀x, ∀y (∀z($xR_y \wedge yR_z \Rightarrow xR_z$)	—	×	✓

- Note that all the above relations are defined on a single set.
- Also to prove any relation is not of certain type we need to P.T the logical formula for that relation is false.
- Every Asymmetric relation is antisymmetric relation.

3.2.5 Composition of relations:

If R is a relation from A to B, S is a relation from B to C, the composition of R & S is given by

SoR from A to C.

S.R = {(a, c)|(a, b)∈R and (b, c)∈S}

If R is relation on A, then composition is denoted as R^2, R^3.

Note:

If R is any relation on set A, then

$R_o\Delta_A = R$ and Δ_A oR = R

3.2.6 Closure:

Clause of a relation R under given property is smallest possible relation that contains R and Satisfy the prpperty.

(i) **Reflexive Closure (R*):**

Reflexive clouse of a relation R,

$R^{\#} = RU\Delta_A$

(ii) **Symmetric closure:**

$R^{+} = RUR^{-1}$

(iii) **Transitive closure:**

- Finding transitive closure has no formula, but we have a procedure as shown below.
  Steps: Represent relation R with a directed graph such that whenever aRb draw a directed edge from a to b.

  Steps: Now from each vertex, find all reachable vertices and for each reachable vertex b from a add the ordered pair (a, b) to the closure.

- The standard procedure for finding transitive closes is
  $R\# = R \cup R^2 . \cup R^3 \cup \ldots\ldots . R^{n-1} \cup R^n$
  'n' is a positive integer such that $R^{n-1} = R^n$
- when a relation is represent as a graph,
  If $(a, b) \in R^n$, we can say that there exists an n-length path from a to b.
- when asked to find more than one closure, the order to be followed is reflexive, symmetric, transitive.
  Following any other order may give redundancy.
- The closure of a relation, if exists, under a property is intersection of the relations with that property containing R.
- If R is a transitive relation,
- $Rn \leq R \ \forall n \geq 1$
- also R^n is transitive relation.

3.2.7 Partion:

A partition of set s is dividing s in disjoint subsets such that

$A_1 \cup A_2 \cup \ldots \cup A_n = s$

$A_i \cap A_j = \phi \ \forall i, j \leq n$

3.2.8 Refinement:

Partition P_2 is called refinement of partition p_1.

if every partitioned subset of P_2 is subset to some partitioned subset of P_1.

3.2.9 Equivalence Relation:

A relation which is reflexive

Symmetric

Transitive

is called an equivalence relation.

- Equivalence relation creates partition.
- Each set of the partition is called an equivalence class.
- Every element of same equivalence class are related to each other.
- No two element of different classes of related to each other

- Equivalence class is represented by
  [a] R

Where a is any element of the equivalence classes

- It R is an equivalence relation, the below two sentences means the same
  (i) aRb
  (ii) $[a]_R = [b]_R$

  aRb & $[a]R \phi [b]$ also mean same.

  If R is an equivalence relation.

  aRb is read as "a is equivalent to b".

- If R_1, R_2 are two equivalence relations
  $R_1 \cup R_2$ need not to be an equivalence relation

  $R_1 \cup R_2$ is an equivalence relation.

3.2.10 Finding number of equivalence relations:

- No of equivalence relations on a set with n elements is given by

  Bell number $B_n = \sum_{k=1}^{n} s(n,k)$

  Where sterling 2nd kind number

  $$s(m,n) = \frac{1}{n!}\sum_{i=0}^{n}(-1)^i \, nc_i \, (n-i)^m$$

  The below is a shortcut to find the Bell number

  $B_0 \rightarrow (1)$

  $B_1 \rightarrow (1)\quad 2$

  $B_2 \rightarrow (2)\quad 3 \qquad 5$

  $B_3 \rightarrow (5)\quad 7 \qquad 10 \qquad 15$

  $B_4 \rightarrow (15)\quad 20 \qquad 27 \qquad 37 \qquad 52$

  Find no. of equivalence relations is nothing but find no. of way we can partition the set.

3.3 Partial Ordering Relations:

A relation R on a set A is called a partial order if R is reflexive, antisymmetric and transitive.

3.3.1 Poset:

A set 'A' together with a partial order R is called a poset

It is denoted as [A:R]. In a poset aRb is denoted as $a \leq b$. $a < b$ means $a \leq b$ and $a \neq b$.

3.3.2 To set:

A post [A;R] is called toset it every pair of element of set A are comparable.

Toset is also known as linearly ordered set (or) chain.

If [A, R] is a poset, then

$[A ; R^{-1}]$ is called dual of the poset.

i.e., these diagram of $[A : R^{-1}]$ can be obtained by turning the hasse diagram of [A, R] upside down.

3.3.3 Hasse Diagram (Poset Diagram):

- It is graphical representation of a poset.
  It is constructed as below:

  (i) Create vertex corresponding to every element of set A.
  (ii) All loops & Edges implied from transitivity are not shown.

- Let $[A, \leq]$ be a poset
  We say yes, covers $x \in s$, if $x < y$ such that there doesn't exist any $z \in s$, $x < z < y$
- Thus hasse diagram shows edges b/w two elements x & y only if x covers y (or) y covers x. The set of such pairs $x < y$ is called covering relation of $(s, \leq)$.
- Thus applying reflexive transitive closure on covering relation of a poset gives the poset.
- Hasse Diagram of a toset is a chain.

3.3.4 Maximum Element:

In a poset an element is called maximal if it is not related to any other element.

3.3.5 Greatest element (or) Maximum element:

In a poset an element is called greatest if every element of the set relates to that element.

3.3.6 Minimal element:

In a poset an element is called minimal, if no other element is related to it.

3.3.7 Least element (or) Minimum Element:

In a poset least element is the one which relates to every other element of the set.

- Every finite, nonempty lattice has at least one minimal and one maximal element.
- Greatest or least element if exists is unique.
- Greatest and least elements may or may not exist if they exist they are the only maximal and only minimal elements respectively.

3.3.8 Upper Bound:

If $[A : R]$ is a poset and $B \leq A$

Upper band of $B = \{x | \forall b \in B, x \leq b \text{ and } x \in A\}$

3.3.9 Least Upper Bound (lub or join or Supremum):

In a poset [A : R] lub of two elemis a, b ∈ A is least element of upper bound of {a, b}. It is denoted as a∨b.

i.e., a∨b ≤ x ∀x∈ upper band of [a, b]

- If no least element exists in the upper bound, we say lub doesn't exist.
- In other word,

  If a∨b = c then

  aRc & bRc and

  If aRd ∧ bRd ⇒ cRd

3.3.10 Greatest lower Bound (glb or meet or infimum)

In a poset [A, R] glb of a, b is greatest element of lower bound of {a, b}. It is denoted as a ∧ b

- If no such element exists we say glb doesn't exist.
- Other way to define glb is

  If a ∧ b = c, then

  [eRa ∧ cRb] ∧ [(dRa ∧ dRb) ⇒ dRc]

- For poset [D_n ; 1]

  Lub (a, b) = LCM (a, b)

  Glb (a, b) = GCD (a, b)

- For poset [P(A) ; ≤], where P(A) is power set of A

  lub (x, y) = x∪y

  lub (x, y) = x∩y

- The hasse diagram of [P(A); ≤] forms a hypercube on, where |A| = n

3.3.11 Join Semi Lattice:

It is a poset in which every pair of elements has lub.

3.3.12 Meet Semi Lattice:

It is a poset in which every pair of elements has glb.

3.4 Lattice

A lattice is a poset in which every pair of elements has both glb & lub.

i.e., Lattice is both join semi lattice & meet semi lattice.

A lattice L is denoted as (L, ∧, ∨)

- It is not needed that every lattice has greatest and least element.
- Every finite lattice has least and greatest elements.

3.4.1 Properties of Lattice:

- $\left.\begin{matrix} a \wedge a = a \\ a \vee a = a \end{matrix}\right\}$ Idempotent
- $\left.\begin{matrix} a \vee b = a \vee a \\ a \wedge v = a \wedge a \end{matrix}\right\}$ Commutative
- $\left.\begin{matrix} a \vee (b \vee c) = (a \vee b) \vee c \\ a \wedge (b \wedge c) = (a \wedge b) \wedge c \end{matrix}\right\}$ Associative
- $\left.\begin{matrix} a \vee (a \wedge b) = a \\ a \wedge (a \vee b) = a \end{matrix}\right\}$ Absorption law
- $a \le b \Rightarrow a \vee c \le b \vee c$
  $a \le b \Rightarrow a \wedge c \le b \wedge c$

  If a ≤ b and c ≤ d then

  a ∨ c ≤ b ∨ d

  a ∧ c ≤ b ∧ d

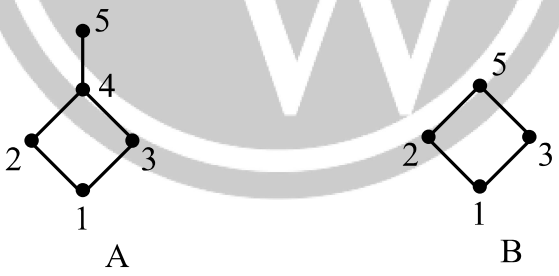
3.4.2 Sublattice:

If A is a lattice B is called

Sublattice of A iff

(i) B itself is a lattice.

(ii) lub of any two element of B is same as lub of the two elements in A.



In above figure B is subset of A and B is a lattice still B is not a sublattice of A.

Because $\left.\begin{matrix} in\ A\ glb\ (2,3) = 4 \\ in\ \text{B}\ glb\ (2,3) = 5 \end{matrix}\right\}$ not equal $\therefore$ not sublatice

3.4.3 Types of Lattices:

(1) Bounded Lattice:

- A lattice with greatest element and least element is called bounded lattice.
- Every finite lattice is bounded lattice.

(2) Complemented Lattice:

- Complemented lattice is a bounded in which every element has atleast one complement.
  B is said to be complement of a iff.
- glb (a, b) = greatest element and lub (a, b) = least element.

(3) Distributive Lattice:

- A lattice is said to be distributive if following distributive laws hold.
- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Note: If L is a bounded distributive lattice then complement of an element if exists, is unique. The reverse need not to be true.

Hence if we find more than one complement for an element, we can conclude that the lattice is not distributive

(4) Boolean Algebra:

- A lattice which is both distributive and complemented is known as Boolean algebra
- It is called so because it satisfises all the properties of Boolean algebra. Thus when given lattice is a Boolean algebra we can apply all the rules that we apply in logic.
- In Boolean algebra every element has exactly one complement.
- [Dn : 1] is a distributive lattice for any n.
- It is because distributive properties hold for lcm & gcd.
- [Dn : 1] is a Boolean lattice if n is a square free number.
- [P(s); ≤] is a Boolean lattice.
- Every Boolean lattice with 2n elements, $\forall \cap \geq 0$.
  Every Boolean lattice contains 2^nelements is isomorphic to the lattice (P(s); ≤) where s is a set with n elements.
  Also this Boolean lattice is a hypercube Q_n.
- Sublattice of a complemented lattice need not to be a complemented lattice.
- Sublattice of a bounded lattice is a bounded lattice.

3.5 Function (or) Mapping (or) Transformation

A function F from set A to set B is an assignment of exactly in one element of B to each element of A. It is denoted as: F : A → B

Here A is called Domain B is called codomain

Function is a special type of relation.

- Consider f(a) = b
  b is called image of a
  a is called preimage of b.

- Range: It is set of images of all the elements of A.
  Range ≠ Co-domain (Range need not to be equal to co-domain)
- If f_1, f_2 are two functions
  $f_1(x) + f_2(x)$ is denoted as $(f_1 + f_2)(x)$
  $f_1(x).\ f_2(x)$ is denoted as $(f_1.f_2)(x)$
  $\frac{1}{f(x)}$ is denoted as $\frac{1}{f}(x)$, ($\frac{1}{f}$ is not equal to inverse function)
- If A and B are two sets with
  $|A| = n$ $|B| = m$ then
  number of functions possible from A to B = m^n

3.6 Types of functions:

3.6.1 One - One function (Injection):

$f : A \to B$ is one to one
iff
$\forall a \forall b(f(a) = f(b) \Rightarrow a = b)$

- It $f : A \to B$ is 1–1 then $|A| \leq |B|$
- If $|A| = m$ and $|B| = n$
  no of 1 – 1 function possible from A to B = ${}_nP_m$
- If m = n = k, then number of 1:1 function = k!

3.6.2 Onto function (Surjection):

$f : A \to B$ is onto iff
$\forall b \in B \quad \exists a \in A$ such that $f(a) = b$

- If $f : A \to B$ is onto then $|A| \geq |B|$
- If $|A| = m$ $|B| = n$ then

$$\therefore \text{ number of onto functions} = \sum_{i=0}^{n} (-1)^i \, {}^nC_i \, (n-i)^m$$

- If m = n = k, then number of 1:1 function = k!

3.6.3 One-to-One Correspondence (or) Bijection:

A function $f : A \to B$ is Bijection iff
f is both one-one and onto

- If $f : A \to B$ is bijection, then $|A| = |B|$
- If $f : A \to B$ is 1 – 1 and $|A| = |B|$
  then f is a bijection
- If $f : A \to B$ is onto and $|A| = |B|$
  then f is a bijection

- If $|A| = |B| = n$ then no of bijections possible from A to B are n!
- If $f : A \to A$ is a function and A is a finite set then
  A is 1–1 $\Leftrightarrow$ A is onto

3.6.4 Inverse of a function:

$f : A \to B$ is invertible if its inverse relation f^{-1} is a function from B to A.

$f : A \to B$ is invertible $\Leftrightarrow$ f is a bijection

- Inverse doesn't exist if a function is not bijection. However, we can find inverse image of subset of codomain. If $f : A \to B$ is a function and $S \leq B$

Inverse image of $S = \{a \in A | f(a) \subseteq S\}$

- If f is a function from A to B and let S, T be subsets of A.

  $f(S \cup T) = f(S) \cup f(T)$

  $f(S \cap T) = f(S) \cap f(T)$

  However, $f(S \cap T) = f(S) \cap f(T)$ if f is a bijection
- If f is a function from A to B and let S, T be subsets of B

  $f^{-1}(S \cup T) = f^{-1}(s) \cup f^{-1}(T)$

  $f^{-1}(S \cap T) = f^{-1}(s) \cap f^{-1}(T)$

  $f^{-1}(\overline{s}) = \overline{f^{-1}(s)}$

3.6.5 Identity function:

A mapping $I_A : A \to A$ is called an identity function if

$I_A = \{(x, x)/x \in A\}$

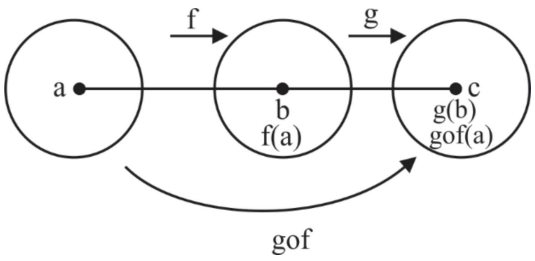
3.6.7 Constant function:

A function $f : A \to B$ is said to be a constant function if

$f(x) = c \quad \forall x \in A$

3.6.8 Composition of functions:

If $f : A \to B$ and $g : B \to C$ are two function then gof: $A \to C$ is called a composition function of f & g.

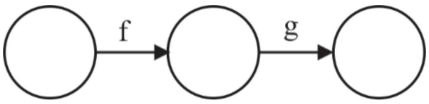


gof(x) = g(f(x))

- In gof : $A \to C$
  A is domain of gof
  C is codomain of gof

Range of gof is image of (range of f under g)

- If $f : A \to B$ and $g : B \to C$ are tow functions
  gof is defined for every case



But fog is defined iff
range of g ≤ domain of f
fog maps from B to B i.e., $fog : B \to B$
fog ≠ gof (i.e., composition is not commutative)
(fog)oh = fo(goh) (i.e., Associative)
$(fog)^{-1} = g^{-1}$ of^{-1} (Think why)
Let $f : A \to B$ be an invertible function then
$f^{-1} : B \to A$ is a inverse of f
$f^{-1}$of : $A \to A$ is an identity function I_A
fof^{-1} : $B \to B$ is an identity function I_B

Note:

- f is 1–1 & g is 1–1 ⇒ gof is 1–1
- f is onto & g is onto ⇒ gof is onto
- f is bijection & g is bijection ⇒ gof is bijection
- If gof is onto then g is onto
- If gof is 1–1 then f is 1–1
- If gof is a bijection then f is onto ⇔ g is 1–1

3.6.9 Partial Functions:

f: $A \to B$ is called partial function if 'f' is defined only for some of $a \in A$.
The subset of A on which f is defined is called domain definition of f.

3.7 Groups:

3.7.1 Binary Operation:

The binary operator * is said to be a binary operation on a non-empty set A if the set is closed under the operation.
i.e., $(a*b) \in A \ \forall a,b \in A$

3.7.2 Binary Structure (or) Algebraic Structure:

A nonempty set A is called binary structure with respect is a binary operator *, if * is binary operation on A. it is demoted as (A, *)

3.7.3 Semi Group:

(A, *) is semigroup iff
(i) is closed operation
(ii) is an associative property

3.7.4 Monoid:

(A, *) is called monoid iff:
(i) is closed operation
(ii) is an associative property
(iii) Identity element exists

3.7.5 Group:

(A, *) is called monoid iff:
(i) is closed operation
(ii) is an associative property
(iii) Identity element exists in A
(iv) Every element of A has inverse

- Identity element if exists is unique.
- Inverse element if exist is unique.
- Finite Group:
  A group with finite number of elements
- Order of a group: It is number of elements in the group.
- In a group of 2 element
  $a^{-1} = a, \forall a \in G$
- $(\{0,1,2,3 \ldots\ldots m\text{-}1\}, \oplus_m)$ is a group
- Let S_n be set of positive integers less than n and relatively prime to n. then
  $(S_n, \otimes_n)$ is a group.
- Abelian Group:
  A group (G,*) is called abelian if * is commutative.

3.7.6 Properties of Groups

- Let (G,*) be a group
  if $ab = ac \Rightarrow b = c$ (Left cancellation property)
  $ba = ca \Rightarrow b = c$ (Right cancellation property)
  due to these property ever raw and column in Caley table has exactly one element
- If G is a group and $a,b \in G$
  then $(ab)^{-1} = b^{-1}a^{-1}$
- Group G is abelian $\Leftrightarrow (ab)^{-1} = b^{-1}a^{-1} \ \forall a, b \in G$
- $\forall a \in G, a^{\circ} = e$

3.7.7 Homomorphism

- If (G, *) and (G', $\oplus$) are two groups then a function $f : G \to G'$ is called a homomorphism
  if $f(a*b) = f(a) \oplus f(b)$
- If $f : G \to G'$ is a bijection, then we call the homomorphism isomorphism. It is denote as $G \cong G'$
- If e_1, e_2 are identity elements of G and G' respectively then $f(e_1) = e_2$
- If $a \in G$, and $f : G \to G'$ is a homomorphism $f(a^{-1}) = (f(a))^{-1}$

3.7.8 Order of an element:

The smallest positive integer n such that $a^n = e$ is called of order of an element a in the group.

- The order of an element is divisor of order of the group.
- Order (a) = order (a^{-1}) $\forall a \in G$
- $a^{-n} = b^n$ if $a^{-1} = b$ and n is any positive integer.

3.7.9 Subgroup:

A non-empty subset H of a group G is called subgroup of G if (H, *) is also a group.

- For every group G, {e} and G are called trivial subgroups of G.
- Every subgroup contains identity element of its parent group.
- If H is a subgroup of G then order(H) divides order(G) (Lagrange's theorem). The converse of Lagrange's theorem holds only for abelian groups.
- If H and k are two subgroups of same group, then
  $H \cap k$ is also, a subgroup
  $H \cup k$ need not to be a subgroup.
- If $H \subseteq G$, then H is called subgroup of G iff:
  (i) $(a*b) \in H \quad \forall a, b \in H$
  (ii) $a^{-1} \in H \qquad \forall a, b \in H$
- If $H \subseteq G$, and if H is finite $\rightarrow$ (applies only when H is finite) and nonempty, then H is called subgroup iff:
  $(a*b) \in H \quad \forall a, b \in H$
- If G is a subgroup of composite order, then G necessarily has non-trivial subgroup.

3.7.10 Cyclic Groups:

A group G is called cyclic, if $\exists a \in G$ such that every element can be written as an integral power of a such an element 'a' is called generator.

- The order of generator is order of the group.
- If 'a' is a generator then a^{-1} is also a generator.
- All subgroups of a cyclic group are cyclic.
- If G is a cyclic group of order n, then no of generator of G is given by $\phi(n)$ (Euler's phi function)
- If 'a' is a generator of G, and let m be an integer such that $1 < m \leq n$ then

$$\text{order}(a^m) = \frac{n}{\gcd(n,m)}$$

- If G is a cyclic group with generator a and let d be divisor of |G|.
  For every d there exists exactly one subgroup of order d. this subgroup is generated by $a^{n/d}$ where n = |G|

$\therefore$ No of subgroup of a cyclic group = no. of divisors of |G| each subgroup is generated by $a^{n/d}$. (d is divisor of |G|)

3.7.11 Cyclic subgroup of a group:

If (G,*) is any group and let $a \in G$.
The smallest subgroup of G containing a is <a> where

$\langle a \rangle = \{a^n / \forall n \in Z\}$

Also <a> is a cyclic subgroup.
order of the subgroup <a> = order of element 'a' in G.

- If H is any subgroup of G and if H contains 'a' then
  $\langle a \rangle \subseteq H$
- Thus if G is a group
  $\langle a \rangle$ is a cyclic subgroup of G, $\forall a \in G$.
  Such subgroups are called generating sets

Note:

- Every group of prime order is cyclic in which every element (except e) is a generator element.
- Every cyclic group is abelian.
- A group is cyclic $\Leftrightarrow$ it can't be expressed as union of two proper subgroups.
- If (G,*) and (H,$\oplus$) are two groups
  $(G \times H, \bullet)$ is a group where $\bullet$ is defined as
  $(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \oplus h_2)$
  This group is called direct product of G and H.
- Every group of order less than or equal to 5 is abelian.
- There is only one unique group for each of the order 1,2,3.

❑❑❑

4 COMBINATORICS

4.1 Introduction

Let $m \in \mathbb{N}$. For a procedure of m successive distinct and independent steps with n1 outcomes possible for the first step, n_2 outcomes possible for the second step, ... , and nm outcomes possible for the mth step, the total number of possible outcomes is

$$n_1 \cdot n_2 \cdots n_m$$

For a collection of m disjoint sets with n_1 elements in the first, n_2 elements in the second, . . ., and nm elements in the mth, the number of ways to choose one element from the collection is

$$n_1 + n_2 + \cdots + n_m$$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{n-k} x^k y^{n-k}.$$

$$\sum_{i=0}^{n} C(n,i)(-1)^i = 0$$

For n even,

$$\sum_{i=0}^{n/2} C(n,2i) = \sum_{i=0}^{n/2-1} C(n,2i+1)$$

For n odd,

$$\sum_{i=0}^{\lfloor n/2 \rfloor} C(n,2i) = \sum_{i=0}^{\lfloor n/2 \rfloor+1} C(n,2i+1)$$

$$\sum_{i=1}^{n} iC(n,i) = n2^{n-1}.$$

For positive integers n, t, the coefficient of $x_1^{n1}\, x_2^{n2} x_3^{n3} \ldots x_t^{nt}$ in the expansion of $(x_1 + x_2 + x_3 + \ldots + x_t)^n$ is

$$\frac{n!}{n_1!n_2!n_3!\ldots n_t!},$$

where each n_i is an integer with $0 \le n_i \le n$, for all $1 \le i \le t$, and $n_1 + n_2 + n_3 + \cdots + n_t = n$.

When we wish to select, with repetition, r of n distinct objects, we are considering all arrangements of r x's and n – 1 |'s and that their number is

$$\frac{(n+r-1)!}{r!(n-1)!}=\binom{n+r-1}{r}.$$

Consequently, the number of combinations of n objects taken r at a time, with repetition, is C(n + r – 1, r).

4.1.1 we recognize the equivalence of the following:

(a) The number of integer solutions of the equation

$x_1 + x_2 + \ldots + x_n = r,\ x_i \geq 0,\ 1 \leq i \leq n.$

(b) The number of selections, with repetition, of size r from a collection of size n.

(c) The number of ways r identical objects can be distributed among n distinct containers.

$$b_n=\binom{2n}{n}-\binom{2n}{n-1}=\frac{1}{n+1}\binom{2n}{n},\qquad n\geq 1, b_0=1.$$

The numbers $b_0, b_1, b_2, \ldots$ are called the Catalan numbers, after the Belgian mathematician

Order Is Relevant	Repetitions Are Allowed	Type of Result	Formula
Yes	No	Permutation	P(n, r) = n!/(n – r)!, $0 \leq r \leq n$
Yes	Yes	Arrangement	N^r, n, $r \geq 0$
No	No	Combination	C(n, r) = n!/[r!(n – r)!] = $\binom{n}{r}$, $0 \leq r \leq n$
No	Yes	Combination with repetition	$\binom{n+r-1}{r}$, n, $r \geq 0$

If there are n objects with n_1 indistinguishable objects of a first type, n_2 indistinguishable objects of a second type, . . . and n_r indistinguishable objects of an rth type, where $n_1 + n_2 + \ldots + n_r = n$, then there are $\frac{n!}{n_1!n_2!\ldots n_r!}$ (linear) arrangements of the given n objects.

Let A and B be subsets of a finite universal set U. Then

(a) $|A\cup B|=|A|+|B|-|A\cap B|$

(b) $|A\cap B| \leq \min\{|A|, |B|\}$, the minimum of |A| and |B|

(c) $|A\backslash B| = |A| - |A\cap B| \geq |A| - |B|$

(d) $|A^c| = |U| - |A|$

(e) $|A \oplus B| = |A\cup B|-|A\cap B|=|A|+|B|-2|A\cap B|=|A/B|+|B/A|$

(f) $|A \times B| = |A| - |B|$

Given a finite number of finite sets, $A_1, A_2, \ldots, A_n$, the number of elements in the union $A_1 \cup A_2 \cup \ldots \cup A_n$ is

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|,$$

where the first sum is over all i, the second sum is over all pairs i, j with $i < j$, the third sum is over all triples i, j, k with $i < j < k$, and so forth.

The number of derangements of $n \geq 1$ ordered symbol is

$$\boxed{D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right).}$$

Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers. The function

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{i=0}^{\infty} a_i x^i$$

is called the generating function for the given sequence.

4.1.2 Extended Binomial coefficient

$$\binom{-n}{r} = \frac{(-n)(-n-1)(-n-2)\ldots(-n-r+1)}{r!}$$

$$= \frac{(-1)^r (n)(n+1)(n+2)\ldots(n+r-1)}{r!}$$

$$= \frac{(-1)^n (n+r-1)!}{(n-1)!r!} = (-1)^r \binom{n+r-1}{r}.$$

For all $m, n \in Z^+$, $a \in R$,

(1) $(1 + x)^n = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \ldots + \binom{n}{n} x^n$

(2) $(1 + ax)^n = \binom{n}{0} + \binom{n}{1} ax + \binom{n}{2} a^2 x^2 + \ldots + \binom{n}{n} a^n x^n$

(3) $(1 + x^m)^n = \binom{n}{0} + \binom{n}{1} x^m + \binom{n}{2} x^{2m} + \ldots + \binom{n}{n} x^{nm}$

(4) $(1 - x^{n+1})/(1 - x) = 1 + x + x^2 + \ldots. + x^n$

(5) $1/(1 - x) = 1 + x + x^2 + x^3 + \ldots = \sum_{i=0}^{\infty} x^i$

(6) $1/(1 - ax) = 1 + (ax) + (ax)^2 + (ax)^3 + \ldots$

$= \sum_{i=0}^{\infty} (ax)^i = \sum_{i=0}^{\infty} a^i x^i$

$= 1 + ax + a^2x^2 + a^3x^3 + \ldots$

(7) $1/(1+x)^n = \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \ldots$

$= \sum_{i=0}^{\infty}\binom{-n}{i}x^i$

$= 1 + (-1)\binom{n+1-1}{1}x + (-1)^2\binom{n+2-1}{2}x^2 + \ldots$

$= \sum_{i=0}^{\infty}(-1)^i\binom{n+i-1}{i}x^i$

(8) $1/(1-x)^n = \binom{-n}{0} + \binom{-n}{1}(-x) + \binom{-n}{2}(-x)^2 + \ldots$

$= \sum_{i=0}^{\infty}\binom{-n}{i}(-x)^i$

$= 1 + (-1)\binom{n+1-1}{1}(-x) + (-1)^2\binom{n+2-1}{2}(-x)^2 + \ldots$

$= \sum_{i=0}^{\infty}\binom{n+i-1}{i}x^i$

If $f(x) = \sum_{i=0}^{\infty}a_ix^i, g(x) = \sum_{i=0}^{\infty}b_ix^i$, and h(x) = f(x)g(x), then

$h(x) = \sum_{i=0}^{\infty}c_ix^i$, where for all $k \geq 0$,

$$c_k = a_0b_x + a_1b_{x-1} + \ldots + a_{k-1}b_1 + a_kb_0 = \sum_{j=0}^{k}a_jb_{k-j}.$$

Objects Are Distinct	Containers Are Distinct	Some Container(s) May Be Empty	Number of Distributions
No	Yes	Yes	$\binom{n+m-1}{m}$
No	No	Yes	(1) p(m), for n = m (2) p(m, 1) + p(m, 2) + … + p(m, n), for n < m
No	Yes	No	$\binom{n+(m-n)-1}{(m-n)} = \binom{m-1}{m-n} = \binom{m-1}{n-1}$
No	No	No	p(m, n)

Consider the nonhomogeneous first-order relation

$$a_n + C_1a_{n-1} = kr^n,$$

where k is a constant and $n \in Z^+$. If r^n is not a solution of the associated homogeneous relation

$$a_n + C1a_{n-1} = 0,$$

then $a_n^{(p)} = Ar^n$, where A is a constant. When r^n is a solution of the associated homogeneous relation, then $a_n^{(p)} = Bnr^n$, for B a constant.

Now consider the case of the nonhomogeneous second-order relation

$$a_n + C_1a_{n-1} + C_2a_{n-2} = kr^n,$$

Where k is a constant. Here we find that

(a) $a_n^{(p)} = Ar^n$, for A a constant, if r^n is not a solution of the associated homogeneous relation;

(b) $a_n^{(p)} = Bnr^n$, where B is a constant, if $a_n^{(h)} = c_1r^n + c_2r_n^n$, where $r_1 \neq r$; and

(c) $a_n^{(p)} = Cn^2r^n$, for C a constant, when $a_n^{(h)} = (c_1 + c_2n)r^n$.

Given a linear nonhomogeneous recurrence relation (with constant coefficients) of the form $C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \ldots + C_ka_{n-k} = f(n)$, where $C_0 \neq 0$ and $C_k \neq 0$, let $a_n^{(h)}$ denote the homogeneous part of the solution a_n.

	$a_n^{(p)}$
c, a constant	A, a constant
n	$A_1n + A_0$
n^2	$A_2n^2 + A_1n + A_0$
n^t, $t \in Z^+$	$A_tn^t + A_{t-1}n^{t-1} + \ldots. + A_1n + A_0$
r^n, $r \in R$	Ar^n
sin θn	A sin θn + B cos θn
cos θn	A sin θn + B cos θn
$n^t r^n$	$r^n (A_tn^t + A_{t-1}n^{t-1} + \ldots + A_1n + A_0)$
r^n sin θn	Ar^n sin θn + Br^n cos θn
r^n cos θn	Ar^n sin θn + Br^n cos θn

❑❑❑