BYJU'S EXAM PREP

Computer Science & IT

Discrete Mathematics

SHORT NOTES

Short Notes — DISCRETE MATHEMATICS

Chapter 1: Set Theory

A set is an unsorted array of distinct objects known as elements or set members. The elements of a set are said to be included within it. To denote that 'a' is a member of the set A, we write it as $a \in A$. The notation $a \notin A$ denotes the absence of 'a' from the set A.

- **Representation of a Set:**
  Various methods can represent a set. There are three standard methods used for representing set:
  1. Statement form.
  2. Roaster form or tabular form method.
  3. Set Builder method.

- **Cardinality / Size of a Set:**
  Number of elements in a set is called the Cardinality in a set. It is represented by |A|. For a finite set, the cardinality will always be a finite number.

- **Equality of Sets:**
  Consider two sets A and B. They are said to be following the property of equality if both have the same number of elements. For example: A = {1, 3, 9,} and B = {3, 1, 9} are equal sets.
  NOTE: Order of elements in a set do not matter.

- **Subset:**
  A set A is said to be a subset of another set B if and only if every element of set A is also a part of other set B. It is depicted by the symbol '⊆'. '$A \subseteq B$' denotes that A is a subset of B.

- **Power Sets:**
  The Power set denoted by P(A) of a set A is defined as the set all possible subset of the set A.
  Example: What will be Power set of {0, 1}? Solution: All possible subsets: {∅}, {0}, {1}, {0, 1}. Note: An Empty set and set itself is also the member of this set of subsets.
  Note: The power set's cardinality is 2^n, where n is the number of elements in the set A.
  - The Power set for a finite set for example A is always finite.

  Set S is a component of power set of S which can be written as S ε P(S).

- **Operation on Sets:**

The following are the various operations on Set.

1. Cartesian Product:

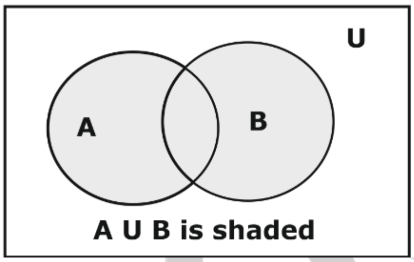
Let A and B be two sets. The Cartesian product of the set A and B is denoted by A × B, is the set of all ordered pairs (a,b), where a belongs to A and b belongs to B.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

The cardinality of A × B is P*Q, where P is the Cardinality of A and Q is the cardinality of B.

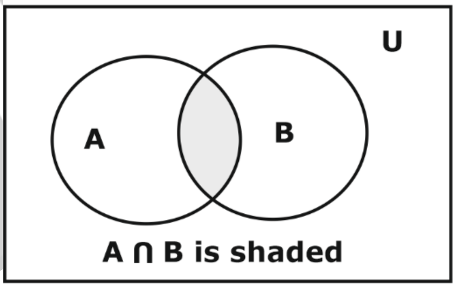
2. Union:

The set of distinct elements belonging to set A or set B, denoted by A∪B, is the union of the sets A ∪ B.



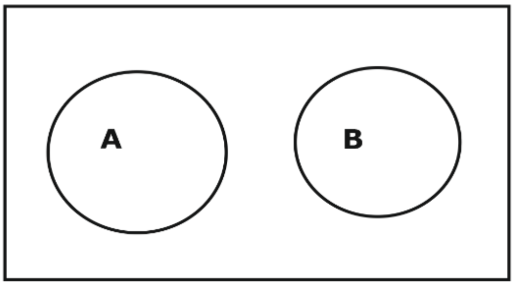
3. Intersection:

The set of elements belonging to both the set A and B, denoted by A∩B, is the intersection of the sets A and B, i.e., the set of the popular element in A and B.



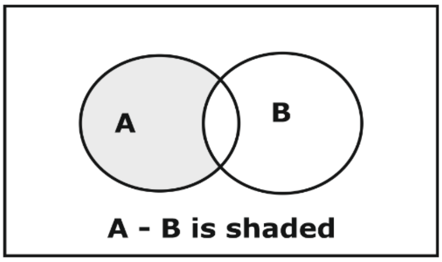
4. Disjoint:

If the intersection of two sets is the empty set, they are said to be disjoint. In other words, sets have no common components.



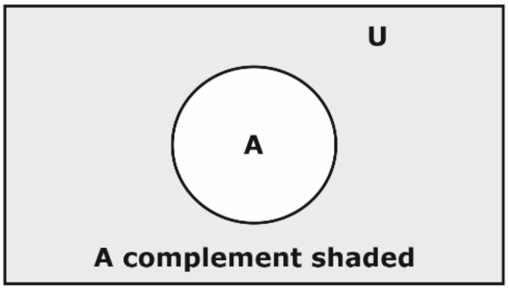
5. Set Difference:

The Difference between sets A and B is defined as the set which contains elements of set A but not of set B. i.e., all elements of A except the element of B. It is denoted by 'A – B'.



6. Complementation:

The Complementation operation of a set A is defined as the set that includes all the elements of the universal set that are not present in the given set. It is denoted by A^C.



- **SOME IMPORTANT RESULTS AND LAWS:**

1. $A - B = A \cap \overline{B}$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $A \cap U = A$, $A \cup \phi = A$ (Identity Laws)
4. $A \cup U = U$, $A \cap \phi = \phi$ (Domination Laws)
5. $A \cup A = A$, $A \cap A = A$ (Idempotent Laws)
6. $\overline{\overline{A}} = A$ (Complementation Law)
7. $A \cup B = B \cup A$, $A \cap B = B \cap A$ (Commutative Laws)
8. $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ (Associative Laws)
9. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, (Distributive Laws)

- **De Morgan's Laws:**

The complement of the union of two sets is equal to the intersection of their complements and the complement of the intersection of two sets is equal to the union of their complements. These are called **De Morgan's laws**.

For any two finite sets A and B:

(i) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (which is a De Morgan's law of intersection).

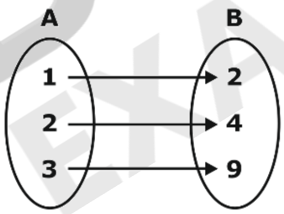
(ii) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (which is a De Morgan's law of union).

- **Properties of Union and Intersection of sets:**
  1. **Associative Properties:** A ∪ (B ∪ C) = (A ∪ B) ∪ C and A ∩ (B ∩ C) = (A ∩ B) ∩ C
  2. **Commutative Properties:** A ∪ B = B ∪ A and A ∩ B = B ∩ A
  3. **Identity Property for Union:** A ∪ ϕ = A
  4. **Intersection Property of the Empty Set:** A ∩ ϕ = ϕ .
  5. **Distributive Properties:** A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C) similarly for intersection.

- **FUNCTIONS:**

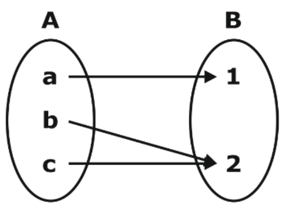
  A function f from A -> B is a relation R: A->B such that every element of the domain is mapped to exactly one element in the codomain. A is called Domain of function f and B is called co-domain of function f.
  - **Domain and co-domain** – Let f be a function from set A to set B i.e A->B, then the set A is called the Domain and the set B is called the co-domain of the function f.
  - **Range** – The Range of a function f is the set of all images of the elements of A. Basically Range is a subset of co- domain.
  - **Image and Preimage** – b is the image of a and a is the preimage of b if f(a)=b.

- **Types of functions:**
  1. **One to one function (Injective):** A function is called one to one if for all elements a and b in A, if f(a) = f(b), then it must be the case that a = b.



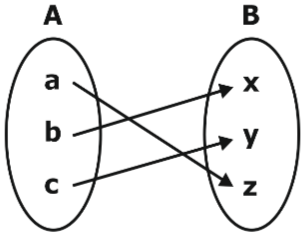
f: (A → B)

  2. **Onto function(surjective):** If every element b in B has a corresponding element a in A such that f(a) = b. It is not necessary that a is unique. The function f may map one or more elements of A to the same element of B.



f: (A → B)

One to one correspondence function (Bijective/Invertible): A function is Bijective function if it is both one to one and onto function.



f: (A → B)

3. **Many to One Function:** Here, at least one Image has at least 2 pre-images, i.e., there exists a 'b' which is an element of B such that there are at least two a1, a2 as element of A such that f(a1) = f(a2) = b.
   To check: Take f(x1) = f(x2) and prove that x1 ≠ x2.
   Note: Number of Many-one function = All Functions – One to one Function.

4. **Into Function:** Here, range must be a proper subset of Co-domain, i.e., there is at least one element b which is an element of B for which no element a which belongs to A exists such that f(a)=b.
   NOTE: Here we have at least one element which is not an image of any element of set A. Number of into function = All Functions – Onto Function.

5. **Inverse Functions:** Bijection functions are also known as invertible functions because they have inverse function properties. The inverse of bijection f is denoted as f^{-1}. It is a function which assigns to b, a unique element such that f(a) = b. Hence f^{-1} (b) = a.

- **Function Composition:** Let g be a function from B to C and f be a function from A to B, then the composition of f and g, is denoted as fog(a)= f(g(a)).
- **Properties of function composition:**
  1. fog ≠ gof
  2. $f^{-1}$of = f^{-1} (f(a)) = f^{-1}(b) = a.
  3. fof^{-1} = f(f^{-1} (b)) = f(a) = b.
  4. If f and g both are one to one function, then fog is also one to one.
  5. If f and g both are onto function, then fog is also onto.
  6. If f and fog both are one to one function, then g is also one to one.
  7. If f and fog are onto, then it is not necessary that g is also onto.
  8. $(fog)^{-1}$ = g^{-1}of^{-1}
- **Some Important Points:**
  1. A function f is defined to be one to one if it is either strictly increasing or strictly decreasing.
  2. One to one function never assigns the same value to two different domain elements.
  3. For onto function, range and co-domain are equal.
  4. If a function f is not bijective, the inverse function of function f cannot be defined.

- **Total Number of Functions:**

  Let |A| = p and |B| = q, then

  1. Total Number of functions from A to B = p^q
  2. No. of one - one function = (p, P, q) or ${}^pP_q$
  3. No. of onto function =

     p^q – (p, C, 1) *$(p-1)^q$ + (p, C, 2)*$(n-2)^q$ …. +$(-1)^q$*(p, C, p-1), if q >= p; 0 otherwise
  4. The Necessary condition for bijective function |A| = |B| and

     thus the No. of bijection function =n!

- **RELATION:**

  Given two sets A and B, a relation between A and B is any subset of the cross product of A X B. It can be defined as p R q ↔ (p, q) ∈ R ↔ R (p, q).

- **Domain and Range:**

  If there are two sets, like P and Q and Relation from P to Q is R(p, q), then the domain is defined as the set { p | (p, q) ∈ R for some q in Q} and Range is defined as the set {q | (p, q) ∈ R for some p in P}.

- **Types of Relation:**

  1. **Empty Relation:** A relation R on a set A is called Empty if the set A is an empty set.
  2. **Full Relation:** A binary relation R on a set A and B is called full if we have A X B.
  3. **Reflexive Relation:** A relation R on a set P is called reflexive if (p, p) ∈ R holds for every element p ∈ A, i.e., if set A = {p, q} then R = {(p, p), (q, q)} is reflexive relation.
  4. **Irreflexive relation:** A relation R on a set P is called irreflexive if no (p, p) ∈ R holds for every element p ∈ A. i.e., if set A = {a, b} then R = {(a, b), (b, a)} is an irreflexive relation.
  5. **Symmetric Relation:** A relation R on a set A is known as symmetric if (b, a) ∈ R holds when (a, b) ∈ R. i.e. The relation R= {(3,5), (5,3), (4,5), (5,4)} on set A= {4,5,3} is symmetric.
  6. **Antisymmetric Relation:** If (a, b) ∈ R and (b, a) ∈ R are both true for a relation R on a set A, then a = b is antisymmetric. The relation R = {(a, b) → R| a ≤ b} is anti-symmetric since a ≤ b and b ≤ a implies a = b.
  7. **Transitive Relation:** A relation R on a set A is called transitive if (a, b) ∈ R and (b, c) ∈ R then (a, c) ∈ R for all a, b, c ∈ A. i.e., Relation R = {(1,2), (2,3), (1,3)} on set A = {1,2,3} is transitive.
  8. **Equivalence Relation:** A relation R if it is reflexive, symmetrical, and transitive, it is called an Equivalence Relation. i.e., the equivalence relation R = {(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2), (1,3), (3,1)} on the set A = {1,2,3} is reflexive, symmetric, and transitive.
  9. **Asymmetric relation:**

     The asymmetric relationship is the polar opposite of the symmetric relationship. If there is no (b, a) ∈ R when (a, b) ∈ R, a relation R on a set A is said to be asymmetric.

- **Important Points:**
  1. Since a relation R may contain both properties or not, symmetric, and antisymmetric relations are not mutually exclusive.
  2. If and only if a relation is both antisymmetric and irreflexive, it is said to be asymmetric.
  3. Number of different relations from a set with n elements to a set with m elements is 2^{mn}.

- **Total Number of Relations:**

  1. Number of Reflexive Relations on a set with n elements: $2^{n(n-1)}$.

  2. Number of Symmetric Relations on a set with n elements: $2^{n(n+1)/2}$.

  3. Number of transitive relations = 1,2,13,171,3994 … for 1, 2, 3, 4, 5, ... elements.

  4. Number of Anti-Symmetric Relations on a set with n elements: 2^n. $3^{n(n-1)/2}$.

  5. Number of Asymmetric Relations on a set with n elements: $3^{n(n-1)/2}$.

  6. Number of Irreflexive Relations on a set with n elements: $2^{n(n-1)}$.

  7. Number of Reflexive and symmetric Relations on a set with n elements: $2^{n(n-1)/2}$.

  8. Number of reflexive and anti-symmetric relations = $3^{n(n-1)/2}$.

- **Closure of Relations:**

  Consider a relation S with property P having R such that S is the subset of any relation with property P containing R, it is called the closure of R with respect to P. Closures of relations concerning property P can be obtained in the following ways:

  1. **Reflexive closure** - $\Delta = \{(a, a) \mid a \in A\}$ is the diagonal relation on set A. The reflexive closure of relation R on set A is $R \cup \Delta$.
  2. **Symmetric Closure** – Let R be a relation on set A, and let R^{-1} be the inverse of R. The symmetric closure of relation R on set A is $R \cup R^{-1}$.

  3. **Transitive Closure** – Let R be a relation on set A. The connectivity relation is defined as :

     $R^* = \bigcup_{n=1}^{\infty} R^n$. The transitive closure of R is R*.

- **Equivalence Relations:** Let R be a relation on set A. If R is reflexive, symmetric, and transitive then it is said to be an equivalence relation. Consequently, two elements a and b related by an equivalence relation are are said to be equivalent.

- **Equivalence Classes:**

  Let R be an equivalence relation on set A.

  We know that if (a, b) ∈ R then a and b are said to be equivalent with respect to R.

  The set of all elements which are related to an element a of A is called the **equivalence class** of a. It is denoted by $[a]_R$ or simply [a] if there is only one relation to consider.

  Formally,

  $$[a]_R = \{s \mid (a, s) \in R\}$$

  Any element $b \in [a]_R$ is said to be the **representative** of $[a]_R$.

  Important Note: The set A is formed by the union of all the equivalence classes of a Relation R on set A, which are either equal or disjoint.

  $$\bigcup [a]_R = A$$

  Since the equivalence classes are disjoint and their union gives the set on which the relation is described, they are also known as partitions.

- **GROUP THEORY:**

  Algebraic Structure:

  If a non-empty set S obeys the following axioms in terms of binary operation (*), it is considered an algebraic structure:

  Closure: If (a*b) belongs to S for all a, b which are element of S, it is called as Closure.

- **Semi-Group:**

  A semigroup is a non-empty set S, (S,*) that follows the following axiom:

  For all a,b S, the closure (a*b) belongs to S and Associativity: if p*(q*r) = (p*q)*r ∀ p,q,r belongs to S, it satisfies Associativity property.

- **Monoid:**

  A non-empty set S denoted by (S,*) is said to satisfy the property of a monoid if it follows the following property:

  - Closure: If (a*b) belongs to S for all a, b which are element of S, it is called as Closure.
  - Associativity: if p*(q*r) = (p*q)*r ∀ p,q,r belongs to S, it satisfies Associativity property.
  - e ∈ S such that ∀ a ∈ S ,a*e = e*a = a. Such an element e is unique and called the Identity element for the monoid.

  Note: A Monoid is also a semi-group and also an algebraic structure.

- **Group:**

  An algebraic structure (S,*) is called a group if the binary operation satisfies the following property:

  - Closure: If (a*b) belongs to S for all a, b which are element of S, it is called as Closure.
  - Associativity: if p*(q*r) = (p*q)*r ∀ p,q,r belongs to S, it satisfies Associativity property.

- $e \in S$ such that $\forall a \in S$,$a*e = e*a = a$. Such an element e is unique and called the Identity element for the group.
- Inverses: Each element of S possesses an inverse. For each $a \in S$, there exists an element $b \in S$ such that $a*b = e= b* a$. We write $b = a^{-1}$ to denote b is inverse of a.

Note: A group is also a monoid, semigroup, and algebraic structure.

- **Abelian Group or Commutative Group:**

  A non-empty set (S,*) is called a Abelian group if it follows the following property:
  - Closure: If (a*b) belongs to S for all a, b which are element of S, it is called as Closure.
  - Associativity: if $p*(q*r) = (p*q)*r \ \forall$ p,q,r belongs to S, it satisfies Associativity property.
  - $e \in S$ such that $\forall a \in S$, $a*e = e*a = a$. Such an element e is unique and called the Identity element for the group.
  - Inverses: Each element of S possesses an inverse. For each $a \in S$, there exists an element $b \in S$ such that $a*b = e= b* a$. We write $b = a^{-1}$ to denote b is inverse of a.
  - Commutative: if $a*b = b*a$ for all $a,b \in S$, it satisfies commutative property.

  Note: For finding a set lies in which category one must always check one by one starting from closure property and so on.

- **Partial Orders:**

  A non-empty set P together with a binary relation Relation R is said to form a partially ordered set or poset if the following condition are satisfied:
  1. **Reflexive Relation:** A relation R on a set P is called reflexive if $(p, p) \in R$ holds for every element $p \in A$, i.e., if set A = {p, q} then R = {(p, p), (q, q)} is reflexive relation.
  2. **Antisymmetric Relation:** If $(a, b) \in R$ and $(b, a) \in R$ are both true for a relation R on a set P, then $a = b$ is antisymmetric. The relation $R = \{(a, b) \to R \mid a \leq b\}$ is anti-symmetric since $a \leq b$ and $b \leq a$ implies $a = b$.
  3. **Transitive Relation:** if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$ for all $a, b, c \in A$, then a relation R on a set P is called transitive. Relation R = {(1,2), (2,3), (1,3)} on set A = {1,2,3} is transitive.

- **Comparability:**

  Let a and b be the elements of a poset $(S, \preccurlyeq)$ then a and b are said to **comparable** if either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, a and b are said to be **incomparable**.

- **Total Order:**

  A poset $(P, \preccurlyeq)$ where every pair of elements $a,b \in P$ are comparable is called **totally ordered** set(toset) or a chain.

- **Hasse Diagrams:**

  A Hasse diagram may represent the relation of elements of a partially ordered set (poset) with an implied upward orientation. Some extent is drawn for every element of the partially ordered set (poset) and joined with the segment consistent with the subsequent rules:

  - If $p<q$ in the poset, then the point like p appears lower in the drawing than the point-like q.
  - The two points p and q are going to be joined by line segment iff p is said to q i.e. p is related to q.

  To draw a Hasse diagram, provided set must be a poset.

- **Important terms in Posets:**
  - **Maximal Elements-** An element a in the poset is said to be maximal if there is no element b in the poset such that $a \prec b$.
  - **Minimal Elements-** An element a in the poset is said to be minimal if there is no element b in the poset such that $b \prec a$.

- **Bounds in Posets:**

  It is sometimes possible to find an element that is greater than or equal to all the elements in a subset A of poset $(S, \preccurlyeq)$. We call such an element to be the **upper bound** of A. Similarly, we can define the **lower bound** of A as the element that is less than or equal to all elements in a subset A of poset $(S, \preccurlyeq)$.

- **Lattices:**

  A Poset $(S, \preccurlyeq)$ where every pair of elements has a least upper bound(supremum) and a greatest lower bound(infimum) is called a lattice.

  There are two binary operations defined for lattices:

  1. **Join –** The join of two elements is their least upper bound. It is denoted by $\vee$, not to be confused with disjunction.
  2. **Meet –** The meet of two elements is their greatest lower bound. It is denoted by $\wedge$, not to be confused with conjunction.

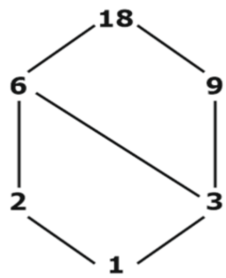
- **Types of Lattice:**

  1. **Bounded Lattice:**

     A lattice $(L, \preccurlyeq)$ is called bounded if the lattice has the greatest element and the least element sometimes denoted by 1 and 0(zero).

     E.g. – D_{18}= {1, 2, 3, 6, 9, 18} is a bounded lattice.

     Note: Every Finite lattice is always bounded.

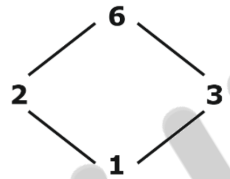


Hasse Diagram of D_{18}

2. Complemented Lattice:

A bounded lattice where every element has a complement is said to be complemented Lattice. Here, each element should have at least one complement.

E.g. – D_6 {1, 2, 3, 6} is a complemented lattice.

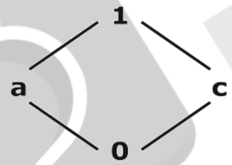


Hasse Diagram of D_6

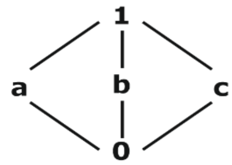
3. Distributive Lattice:

It is a lattice in which meet (∧) and join (∨) operations distribute over each other.

- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$



A distributive lattice



A non-distributive lattice

Note:

- A complemented distributive lattice is a boolean algebra or boolean lattice.
- For a distributive lattice each element has a unique complement.

Chapter 2: Propositional and First order logic

- **Propositional Logic** is concerned with the statements to which the truth values, "true" and "false", can be assigned. The purpose is to analyze these statements either individually or in a composite manner.

- **CONNECTIVES:**

  In propositional logic generally we use five connectives which are :

  - **OR (∨) –** The OR operation of two propositional variables A and B (written as A∨B) is true if at least any of the propositional variable A or B is true.

A	B	A ∨ B
True	True	True
True	False	True
False	True	True
False	False	False

  - **AND (∧) –** The AND operation of two propositional variables A and B (written as A ∧ B) is true if both the propositional variable A and B is true.

A	B	A ∧ B
True	True	True
True	False	False
False	True	False
False	False	False

- **Negation (¬) –** The negation of a propositional variable A (written as ¬A) is false when A is true and is true when A is false.

- **Implication / if-then (→)** An implication A→B is denoted by the proposition "if A, then B". It is false only when A is true and B is false. The rest of the cases are true.

A	B	A → B
True	True	True
True	False	False
False	True	True
False	False	True

- **If and only if (⇔)** A⇔B is bi-conditional logical connective which is true when p and q are same, i.e., both are false or both are true.

A	B	A ⇔ B
True	True	True
True	False	False
False	True	False
False	False	True

- **Types of propositions based on Truth values:**
  - **1. Tautology** - A proposition which is always true, is called a tautology.
  - **2. Contradiction** - A proposition which is always false, is called a contradiction.
  - **3. Contingency** - A proposition that is neither a tautology nor a contradiction is called a contingency.

- **Inverse** – An inverse of the conditional statement is the negation of both the hypothesis and the conclusion. If the statement is written as "If p, then q", then the inverse will be "If not p, then not q". Thus the inverse of p→q is ¬p→¬q.

- **Converse** – The converse of the conditional statement is computed by interchanging the hypothesis and the conclusion. If the statement is written as "If p, then q", then converse will be "If q, then p". The converse of the proposition $p \to q$ is $q \to p$.

- **Contra-positive** – The contra-positive of the conditional is computed by interchanging the hypothesis and the conclusion of the inverse statement. If the statement is "If p, then q", the contra-positive will be "If not q, then not p". The contra-positive of $p \to q$ is $\neg q \to \neg p$.

- **Quantifiers:** The variable of predicates is quantified by the theory of quantifiers. The well-known two types of quantifiers in the field of predicate logic are – Universal Quantifier and Existential Quantifier.

- **Universal Quantifier:**
  Universal quantifier states that the statements within its scope are true for every value of the specific variable. It is denoted by the symbol $\forall$.
  $\forall x P(x)$ is read as for every value of x, P(x) is true.

- **Existential Quantifier:**
  Existential quantifier states that the statements within its scope are true for some values of the specific variable. It is denoted by the symbol $\exists$.
  $\exists x P(x)$ is read as for some values of x, P(x) is true.

- **Table of Rules of Inference:**

Rule of Inference	Name	Rule of Inference	Name
$\dfrac{P}{\therefore P \vee Q}$	Addition	$\dfrac{\begin{matrix} P \vee Q \\ \neg P \end{matrix}}{\therefore Q}$	Disjunctive Syllogism
$\dfrac{\begin{matrix} P \\ Q \end{matrix}}{\therefore P \wedge Q}$	Conjunction	$\dfrac{\begin{matrix} P \to Q \\ Q \to R \end{matrix}}{\therefore P \to R}$	Hypothetical Syllogism

Rule of Inference	Name	Rule of Inference	Name
$\dfrac{P \wedge Q}{\therefore P}$	Simplification	$(P \to Q)$ $\wedge (R \to S)$ $\dfrac{P \vee R}{\therefore Q \vee S}$	Constructive Dilemma
$P \to Q$ $\dfrac{P}{\therefore Q}$	Modus Ponens	$(P \to Q)$ $\wedge (R \to S)$ $\dfrac{\neg Q \vee \neg S}{\therefore \neg P \vee \neg R}$	Destructive Dilemma
$P \to Q$ $\dfrac{\neg Q}{\therefore \neg P}$	Modus Tollens		

- **Predicate Logic:** Predicate Logic is concerned with the predicates, which are Propositions containing variables.
- **Definition:**
  A predicate is an expression of one or more variables defined on some specific domain. A predicate with variables can be made a proposition by either assigning a value to the variable or by quantifying the variable.
- The following are some examples of predicates –
  - Let E(x, y) denoted "x = y"
  - Let X(a, b, c) denote "a + b + c = 0"
  - Let M(x, y) denote "x is married to y"

- **Aristotle Form:**
  We have four Aristotle forms:
  (i) All P's are Q's.

  $$\forall x\left[P(x) \to Q(x)\right]$$

  (ii) Some P's are Q' s.

  $$\exists x\left[P(x) \wedge Q(x)\right].$$

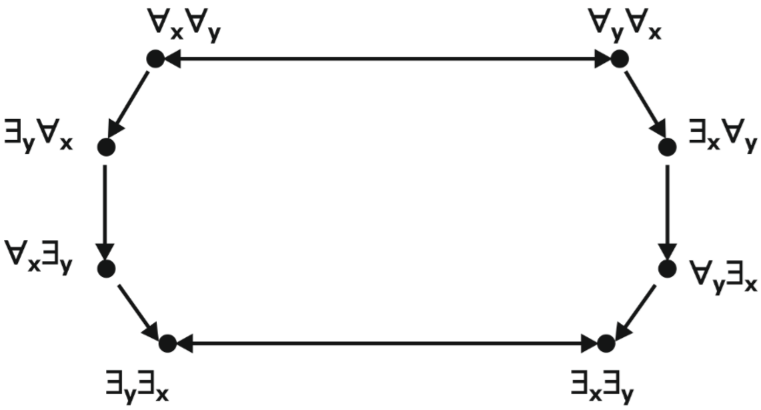
  (iii) Not all P's are Q's.

  $$\neg \forall x[P(x) \to Q(x)]$$
  $$\Rightarrow \exists x[P(x) \wedge \neg Q(x)].$$

  (iv) No P's are Q's.

  $\neg \exists x\left[P(x) \wedge Q(x)\right]$ which is equivalent to $\forall x\left[P(x) \to \neg Q(x)\right]$

- **Relation Between Quantified 2-place Predicates:**



Note: $\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$

Chapter 3: COMBINATORICS

- **THE PRODUCT RULE:**

  Suppose that a procedure is often divided into a sequence of two tasks. If there are n1 ways to try and do the primary task and for every one of those ways of doing the primary task, there are n2 ways to try and do the second task, then there are n1.n2 ways to try and do the procedure.

  By the product rule, it follows that:

  $|A1 \times A2 \times \cdots \times Am| = |A1| \cdot |A2| \cdot \cdots \cdot |Am|$.

- **THE SUM RULE:**

  If a task is often done either in one among the n1 ways or in one among the n2 ways, where none of the set of n1 ways is that the same as any of the set of n2 ways, then there are n1 + n2 ways to try and do the task. The sum rule is often described in terms of sets as:

  We say a finite set S is partitioned into parts S1, . . ., Sk if the parts are disjoint, and their union is S. In other words, $Si \cap Sj = \emptyset$ for i j and $S1 \cup S2 \cup . . . \cup Sk = S$.

  So: $|S| = |S1| + |S2| + \cdot \cdot \cdot + |Sk|$.

- **Permutation:**

  A permutation of a group of distinct objects is an ordered arrangement of those objects. We are also curious about the ordered arrangements of some number of elements of a group. An ordered arrangement of r elements of a group is named an r-permutation.

  If n may be a positive integer and r is an integer with $1 \le r \le n$, then there are $P(n, r) = n.(n - 1). (n - 2) \cdots (n - r + 1)$

  r-permutations of a group with n distinct elements.

  If n and r are integers with $0 \le r \le n$, then $P(n, r) = \frac{n!}{(n-r)!}$.

- **Some important formulas of permutation:**

  1. Number of permutations of n distinct elements taking n elements at a time = $n_{p_n} = n!$
  2. The number of circular permutations of n different elements taken x elements at time = ${}^np_x/x$
  3. The number of circular permutations of n different things: ${}^np_n/n$

- **Combinations:**

  An r-combination of elements of a group is an unordered selection of r elements from the set. Thus, an r-combination is just a subset of the set with r elements.

  The number of r-combinations of a group with n elements, where n is a nonnegative integer and r is an integer with $0 \le r \le n$, equals

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

Combinations and Permutations with and without Repetition.		
Type	**Repetition Allowed?**	**Formula**
r-permutations	No	$\frac{n!}{(n-r)!}$
r-combinations	No	$\frac{n!}{r!(n-r)!}$
r-permutations	Yes	n^r
r-combinations	Yes	$\frac{(n+r-1)!}{r!(n-1!)}$

- **INCLUSION/ EXCLUSION PRINCIPLE:**
  The principle of inclusion and exclusion (PIE) may be defined as a counting technique that computes the number of elements that satisfy a minimum of one among several properties while guaranteeing that elements satisfying quite one property aren't counted twice.

  In the case of objects being separated into two (possibly disjoint) sets, the principle of inclusion and exclusion states |A ∪ B| = |A| + |B| − |A ∩ B|, where |S| denotes the cardinality, or the number of elements, of set S in set notation.

- **THE PIGEONHOLE PRINCIPLE:**
  If k is a positive integer and k + 1 or more objects are placed into k boxes, then there's a minimum of one box containing two or more of the objects.

- **THE GENERALIZED PIGEONHOLE PRINCIPLE:**
  If we have n pigeons and m holes such that n > m; then atleast $\left[\frac{n-1}{m}\right]+1$ pigeons will occupy one hole.

  Or: $\geq \left[\frac{n-1}{m}\right]+1$ pigeons will occupy the same hole.

  Or: $\exists$ a hole $\geq \left[\frac{n-1}{m}\right]+1$ pigeons.

- **DERANGEMENT:** Derangement is a permutation of the elements of a set such that no element appears in its original position.

[i.e. Arrangement → n!
Derangement → !n $\boxed{\text{opposite}}$]

Number of Derangements = total arrangements - total non-Derangements.

Note: Total no. of non-Derangements: $\left[\sum_{i=1}^{n}(-1)^{i+1}\ {}^{n}C_i * (n-i)!\right]$

- **TOTIENT FUNCTION:**

  Euler's totient function (also called the φ function) counts the number of positive integers less than n that are coprime to n. That is, φ(n) is the number of m ∈ N such that 1 ≤ m < n and gcd (m, n) = 1.

  The totient function appears in many applications of elementary number theory, including Euler's theorem, primitive roots of unity and constructible numbers in geometry.

- **The Binomial Theorem:**

  THE BINOMIAL THEOREM Let x and y be variables, and let n be a nonnegative integer.

  Then:

$$(x+y)^n = \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

- **GENERATING FUNCTION:**

  It is a powerful tool used in Discrete Mathematics for solving sequences.

Table: Useful Generating Functions

G(x)	**a_k**
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	C(n, k)
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^k x^k = 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	C(n, k)a^k
$\left(1+x^r\right)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	C(n, k/r) if r|k;0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if k ≤ n;0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k

G(x)	a_k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if r| k;0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	k = 1
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k$ $= 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n + k - 1, k) = C(n + k - 1, n - 1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k$ $= 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n + k - 1, k) = (-1)^k C(n + k - 1, n - 1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^k x^k$ $= 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n + k - 1, k)a^k = C(n + k - 1, n - 1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k!$

- **Application of generating function-**
  1. Solving Basic Counting problem
  2. Solving Complicated Counting Problems
  3. Solving Recurrence Relation.

- **RECURRENCE:**

  For all integers n with n>= n0, a recurrence relation for the series a_n is an equation that expresses that in terms of one or more of the previous terms a0, a1,.. a_n.

  1. Many sequences can be a solution for the same recurrence relation.

     $a_n = 2a_n-1 - a_n-2$, for n ≥ 2

     The following sequences are recurrence relation solutions:

     - $a_n = 3n$, for all n ≥ 0,
     - $a_n = 5$, for all n ≥ 0,

  2. The terms before n0 are defined in the sequence's initial conditions (before the recurrence relation takes effect).

     The series is determined by the recurrence relations and the initial conditions.

     For the instance above, the initial conditions are: a0 = 0, a1 = 3; and a0 = 5, a1 = 5; respectively.

Chapter 4: Graph Theory

The two sets V and E make up the graph G = (V, E). The vertices of V are called Vertices and the edges of G are called edges. Each edge consists of two vertices.

- **Basics of Graph:**
  1. If $(u, v) \in E(G)$, then u, v are said to be adjacent. Now in this case we say that u is connected to v or u is a neighbor of v. If $u, v \notin E(G)$, then u and v are nonadjacent (not connected, non-neighbors).
  2. If e = (u, v) is an edge of G, then e is incident to u and v. We also say that u and v are the endpoints of e.
  3. The degree of $v \in V(G)$, denoted by deg(v), is the number of edges incident to v.

- **Adjacent vertices:**
  Two vertices when they are connected by an edge are said to be adjacent. Two edges are said to be adjacent if they share a vertex.

- **Adjacent edges:**
  Adjacent edges are defined as those edges that share a common vertex. The degree of a vertex is defined as the number of edges incident with that vertex. A path is a sequence of vertices following the property that each vertex in the sequence is adjacent to the vertex next to it.

- **Simple Graphs**: A finite undirected graph with no self-loops and multiple edges is called a simple graph. Unless otherwise noted, all graphs in these notes are simple.

- **Mixed Graph**: The graph in which some edges are directional, and some are unidirectional is called a Mixed Graph. Ex: The real-world road networks are all mixed graphs as some are one way while others are bidirectional.

- **Self-loop:**
  A degenerate edge of a graph which joins a vertex to itself, is called a self-loop. A simple graph cannot contain any loops, but a pseudograph can contain both multiple edges and loops.

- **Parallel edges:**
  In graph theory, multiple edges (also called parallel edges or a multi-edge), are, in an undirected graph, two or more edges that are incident to the same two vertices, or in a directed graph, two

or more edges with both the same tail vertex and the same head vertex. A simple graph has no multiple edges.

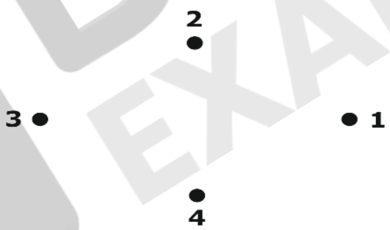
- **Size of a Graph(G)** = Number of edges.
- **Order of a Graph(O(G))** =Number of vertices

Type of graph	Self-loops	Multi edges
Simple graph	No	No
Multigraph	No	Yes
General or pseudo graph	Yes	Yes

- **TYPES OF GRAPHS:**

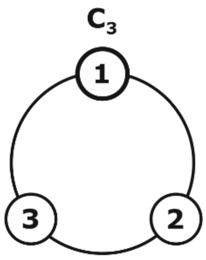
Some important types of graphs are:

1. A **null graph** is a graph that includes only isolated nodes; thus the set of edges in a null graph is empty. Null graph is denoted on 'n' vertices by N_n.

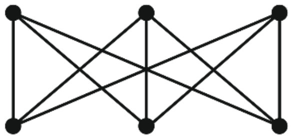


2. A **complete graph** is a simple and a undirected graph with a unique edge connecting every pair of distinct vertices, as described by graph theory. Example of a complete graph with 4 vertices.

3. **Regular Graph:** A Regular graph is one in which all of the vertices have the same degree.
4. **Cyclic Graph -** A graph with **continuous sequence of vertices and edges** is called a cyclic graph. Cyclic graph is denoted on 'n' vertices by C_n where n >=3.



5. **Wheel Graph** - A graph formed by adding a vertex inside a cycle and connecting it to every other vertex is known as wheel graph. Wheel graph is denoted on 'n' vertices by W_n where n>=4 and number of Edges(e) = 2(n-1).
6. **Bipartite Graph:** It is a graph G(V,E) where vertices can be partitioned into two sets such that there is no edge between vertices of the same partition. There can be no loop in a bipartite graph.



7. **Complete Bipartite Graph -** A graph where a set of vertices of a graph can be partitioned into two subsets in such a way that no pair of vertices in the same set are adjacent to each other and every vertex of the first set is adjacent to the second set.

- **Some Important Results:**
  1. Let G be a simple graph with n vertices.
     i) Max degree of a vertex in G = n – 1
     ii) Max. no. of edges in G = ${}^{n}c_2 = \frac{n(n-1)}{2}$
  2. Consider a simple graph with n labelled vertices.
     The number of distinct simple graphs with n labelled vertices is $2^{n(n-1)/2}$.
  3. In a graph G, sum of degree of all vertices is equal to twice the number of edges (Handshaking Lemma)
  4. Maximum number of connected components in graph with n vertices = n
  5. Minimum number of connected components = 0 (null graph) and 1 (for a non-null graph)
  6. Minimum number of edges to be present to have a connected graph with n vertices = n-1.
  7. To guarantee that a graph with n vertices is connected, minimum number of edges required will be = {(n-1) *(n-2)/2} + 1.
- **Clique, Independent set:**
  - In a graph, a set of pairwise adjacent vertices is called a clique.
    The size of a maximum clique in G is called the clique number of G and is denoted ω(G).
  - A set of pairwise non-adjacent vertices is called an independent set (also known as a stable set).

The size of a maximum independent set in G is called the independence number (also known as stability number) of G and is denoted α(G).

- **Havel Hakimi Algorithm:**
  The Havel Hakimi Algorithm is used to check whether a given degree sequence is graphic or not. A degree sequence is graphic if there exists a simple graph corresponding to it.
- **Algorithm:**
  1. Arrange the degree in non- increasing order.
  2. Delete the first entry (say k) then subtract 1 from next k entries.
  3. Repeat steps 1 and 2 until the stop condition is reached.
- **Stop condition:**
  1. All entries are zero: graphic
  2. Any negative entry: not graphic
  3. Not enough entries: not graphic
- **GRAPH CONNECTIVITY:**
  - **Cut Vertex:** Vertex whose removal from the graph either disconnects the connected graph or increases the number of connected components is called a Cut Vertex.
  - **Cut Edge:** Edge whose removal from the graph either disconnects the graph or increases the number of connected components is called a Cut Edge.

  Note: Removal of a vertex removes the associated edge.

  Note: Removal of a edge doesn't removes the associated vertex.

- **Vertex / Edge Connectivity Number:**
  - **Vertex Connectivity Number:** Minimum number of vertices required to disconnect the graph or increase the number of connected components.
  - **Edge Connectivity Number:** Minimum number of edges required to disconnect the graph or increase the number of connected components.

- **EULER GRAPH:** In a graph G(V,E) a trial is called Euler trial if it covers or visits every edge of the graph exactly once. A connected graph is called a Euler trial iff it has at most two odd degree vertices. A connected graph is having the Euler circuit iff it has no odd degree vertex. A graph is called Eulerian Graph if it contains an Eulerian Circuit.

  Note: (i) Degree of all vertices must be even for a Euler graph.

  (ii)Atmost two odd degree vertices are possible in a Euler Trial.

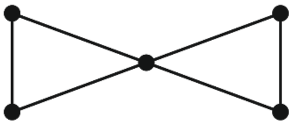
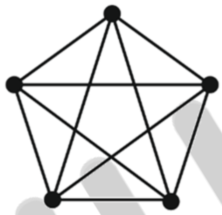
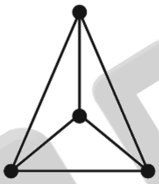
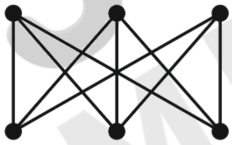
- **HAMILTONIAN GRAPH:**
  A graph where we can go through all the vertices without repeating vertices or edges more than once is called a Hamiltonian graph.

In a graph G(V,E); path p is called a Hamiltonian path if it covers or visits every vertex exactly once.

Note: Edge should not be visited more than once.

- **Planar graph:**

  A graph G is called a planar graph if it can be drawn in the plane without any edges crossing i.e edges do not intersect.

Example graphs	
Planar	Nonplanar
 **Butterfly graph**	 **Complete graph K_5**
 **Complete graph K_4**	 **Utility graph $K_{3,3}$**

- **Some Important Results:**

  1) Euler's formula

     Let G be a connected planar graph with N vertices, e-edges & r-regions.

     Then: $v - e + r = 2$

  2) In a connected planar graph the sum of degrees of regions ≤ twice the no. of edges

     i.e. $\sum d(r) \le 2e$

     Note: When there are no interior edges

     $\sum d(r) = 2e$

  3) Let G be connected planar graph with v-vertices, e-edges, r-regions

     If min. degree of region = 3

     Then:

     1. $3r \le 2e$

     2. $e \le 3v - 6$

4) Kuratowski's Graph:

1) K_5 and $K_{3,3}$
2) Both are non-planar
3) K_5 is a non-planar graph with min. no. of vertices.
4) $K_{3,3}$ is a non-planar graph with min. no. of edges.
5) Four Color Theorem: The chromatic number of any planar graph is at most 4.

- **Kuratowski's theorem:**
  A graph is planar if it does not contain any subgraph homeomorphic to K_5 or $K_{3,3}$.

- **Tree:**
  A graph G(V,E) is called a Tree if there is exactly one path between every two vertices. A graph is tree iff it is connected and it does not contain cycle.

- **Forest**: A graph of every connected component of which is a tree is called a forest. In other words, a forest is a graph without cycles. Forests are also known as acyclic graphs.

- **Matching:**
  A set of pairwise non-adjacent edges in a graph is called a matching. The maximum number of edges in a matching in a graph G is called the matching number of G and denoted by $\mu(G)$.

- **Maximal Matching**: Matching, which is not a proper subset of any matching is called maximal matching.

- **Maximum Matching**: Matching, whose size is maximum is called maximum matching.

- **Perfect Matching**: If every vertex in the graph gets matched or is a matched vertex due to matching; it is called as perfect matching.

- **Complete Matching**: It is generally defined for Bipartite Graph. Here, the idea is to have every vertex of partition or else domain to have a matched vertex in our matching. Then such matching is called as Complete Matching.

- **Covering:**
  For a graph G = (V, E) a set $U \subseteq V$ is called a vertex cover if it covers all the edges of G, i.e. if every edge of G is incident to at least one vertex in U. The minimum number of vertices in a vertex cover of a graph G is called the vertex cover number of G and is denoted by $\beta(G)$.

- **GRAPH COLORING:**

  A vertex coloring of a graph G is an assignment of colors to the vertices of G in such a way that no two adjacent vertices receive the same color.

  Every bipartite graph is two colorable and vice versa. Graphs of chromatic number 1 are empty (edgeless) graphs.

  Note:(i) Star Graphs are always two colorable.

  (ii)Complete Graph requires n colors to color it properly.

  (iii)Complement of a Complete Graph is 1-colourable.

  (iv)Peterson's Graph is 3-colourable.

****