Discrete Mathematics (CSA103)

Ganga Ram

DST-Centre for Interdisciplinary Mathematical Sciences

Institute of Science, Banaras Hindu University

gangaiitr11@gmail.com; gangacims@bhu.ac.in

Mathematical Logic: Propositional and Predicate Logic, Propositional Equivalences, Normal Forms, Predicates and Quantifiers, Nested Quantifiers, Rules of Inference.

Sets and Relations: Set Operations, Representation and Properties of Relations, Equivalence Relations, Partially Ordering. Counting,

Mathematical Induction and Discrete Probability: Basics of Counting, Pigeonhole Principle, Permutations and Combinations, Inclusion- Exclusion Principle, Mathematical Induction, Probability, Bayes Theorem.

Group Theory: Groups, Subgroups, Semi Groups, Product and Quotients of Algebraic Structures, Isomorphism, Homomorphism, Automorphism, Rings, Integral Domains, Fields, Applications of Group Theory.

Graph Theory: Simple Graph, Multigraph, Weighted Graph, Paths and Circuits, Shortest Paths in Weighted Graphs, Eulerian Paths and Circuits, Hamiltonian Paths and Circuits, Planner graph, Graph Coloring, Bipartite Graphs, Trees and Rooted Trees, Prefix Codes, Tree Traversals, Spanning Trees and Cut-Sets.

Boolean Algebra: Boolean Functions and its Representation, Simplifications of Boolean Functions.

Optimization: Linear Programming - Mathematical Model, Graphical Solution, Simplex and Dual Simplex Method, Sensitive Analysis; Integer Programming, Transportation and Assignment Models,

PERT-CPM: Diagram Representation, Critical Path Calculations, Resource Levelling, Cost Consideration in Project Scheduling.

Books Recommended:

- J.P. Trembley and R.P.Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill.
- Dornhoff and Hohn, Applied Modern Algebra, McMillan.
- N. Deo, Graph Theory with Applications to Engineering and Computer Science, PHI.
- C.L. Liu, Elements of Discrete Mathematics, McGraw-Hill.
- Kenneth H Rosen, Discrete Mathematics, Tata McGraw Hill.
- K.L.P. Mishra, N. Chandrasekaran, Theory of Computer Science: Automata, Languages and Computation, PHI.

Set: A set is a collection of well-defined objects, called elements (or members) of the set.

Examples:

1. $S = \{1, 2, 3, 4, 5\}$
2. $S = \{x : \text{x is a month of the year with exactly 30 days}\}$
3. $S = \{1, 2, 3, 4, 5, \ldots\}$ or $S = \{1, 2, 3, 4, 5, (1)\}$

There are three methods of defining sets.

1. Listing Method/ Tabular Method
2. Set-Builder Method/Pradicate Method
3. Missing Element Method

Now, we present several relationships between sets.

1. Subset: $A \subseteq B$
2. Proper subset: $A \subset B$
3. Equal Set: $A = B$ if $(A \subseteq B) \wedge (B \subseteq A)$.
4. Empty Set: ϕ
5. Singleton Set: $\{a\}$
6. Universal Set: $U(\neq \phi)$
7. Disjoint Sets: Not have common elements.
8. Power Set: The family of subsets of a set
9. Finite and Infinite Sets: Number of element finite or infinite
10. Intervals: [a, b] where $a < b, a, b \in \mathbb{R}$

Venn Diagrams: Relationships between sets can be displayed using diagrams.

Truth Sets of Quantifier: Given a predicate P, and a domain D, we define the truth set of P to be the set of elements of x in D for which $P(x)$ is true.

Examples:

1. What is the truth sets of the predicate $P(x)$, where the domain is the set of integers and $P(x)$ is "$|x| = 1$"
2. What is the truth sets of the predicate $Q(x)$, where the domain is the set of integers and $Q(x)$ is "$x^2 = 2$"

Operations with sets:

1. Union: $A \cup B$
2. Intersection: $A \cap B$
3. Difference: $A - B$
4. Complement: $A' = U - A$
5. Symmetric Difference: $A \oplus B = (A - B) \cup (B - A)$.
6. Cartesian Product: $A \times B$

Laws of Sets: Let A, B, and C be any three sets and U the universal set.

1. Idempotent laws: $A \cup A = A$
2. Identity laws: $A \cup \phi = A$
3. Inverse laws: $A \cup A' = U$
4. Domination laws: $A \cup U = U$
5. Commutative laws: $A \cup B = B \cup A$
6. Double complementation law: $(A')' = A$
7. Associative laws: $A \cup (B \cup C) = (A \cup B) \cup C$
8. Distributive laws: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
9. De Morgan's laws: $(A \cup B)' - A' \cap B'$
10. Absorption laws: $A \cup (A \cap B) = A$
11. If $A \subseteq B$, then $A \cap B = A$.
12. If $A \subseteq B$, then $A \cup B = B$.
13. If $A \subseteq B$, then $B' \subseteq A'$
14. $A - B - A \cap B'$
15. $A \oplus B = A \cup B - A \cap B$

Data Structure for Representing Set:

1. Linked List
2. Hash Table
3. Bit Vector
4. Graph
5. Array

Relations: Let A and B be sets. A binary relation from A to B is a subset of $A \times B$.

Relations on a Set: Relations from a set to itself. i.e. subset of $A \times A$.

Examples:

1. Let $A = \{1, 2, 3, 4, \}$ and $R = \{(a, b) \in A \times A | a \text{ divides } b\}$
2. $R = \{(a, b) \in I \times I | a \leq b\}$
3. $R = \{(a, b) \in I \times I | a = b\}$
4. $R = \{(a, b) \in I \times I | a = b + 1\}$

Properties of Relation:

1. Reflexivity: $aRa \ \forall a \ \in A$
2. Symmetry: bRa whenever aRb, $\forall a \ b \ \in A$
3. Anti-symmetry: aRb, bRa then $a = b$
4. Transitivity: aRb, bRc then aRc

Combining Relations:

1. Union: $R \cup S$
2. Intersection: $R \cap S$
3. Differences: $R - S$
4. Direct sum : $R \oplus S$
5. Composition: RoS

Representing Relations:

1. Matrix
2. Digraph

N-ary Relations: Let $A_1, A_2, (1), A_n$ be sets. A N-ary relation on these sets is a subset of $A_1 \times A_2 \times (1), \times A_n$.

Equivalence Relations:

1. Reflexivity: $aRa \ \ \forall a \ \in A$
2. Symmetry: bRa whenever $aRb, \ \ \forall a \ b \ \in A$
3. Transitivity: $aRb, \ \ bRc$ then aRc

Examples:

1. For $aRb \Leftrightarrow a = b \ or \ a = -b, \ \ a, b \in I$
2. $R = \{(a, b) | a \equiv b(mod(m))\}$

Closures of Relations: Let R be a relation on a set A. R may or may not have some property P, such as reflexivity, symmetry, or transitivity. If there is a relation S with property P containing R such that S is a subset of every relation with property P containing R then S is called closure of R with respect to P.

Formally, Let R be any binary relation on a set A. The **Reflexive Closure or Symmetric Closure or Transitive Closure** of R is the relation R^+ such that

1. R^+ is reflexive, or symmetric, or transitive.
2. $R^+ \supset R$
3. For any reflexive, or symmetric, or transitive relation R^{++}, if $R^{++} \supset R$, then $R^{++} \supset R^+$

Examples:

1. Let the relation $R = \{(1,1),(1,2),(2,1),(3,2)\}$ on the set $A = \{1,2,3\}$.
   Then Reflexive Closure
   $R_r^+ = \{(1,1),(1,2),(2,1),(3,2),\mathbf{(2,2)},\mathbf{(3,3)}\}$
2. Let the relation $R = \{(1,1),(1,2),(2,2),(2,3),(3,1),(3,2)\}$ on the set $A = \{1,2,3\}$.
   Then Symmetric Closure
   $R_s^+ = \{(1,1),(1,2),(2,2),(2,3),(3,1),(3,2),\mathbf{(2,1)},\mathbf{(1,3)}\}$
3. Let the relation $R = \{(1,1),(2,3),(3,1)\}$ on the set $A = \{1,2,3\}$.
   Then Transitive Closure $R_t^+ = \{(1,1),(2,3),(3,1),\mathbf{(2,1)}\}$
4. Let the relation $R = \{(1,2),(2,1),(2,3),(3,4),(4,1)\}$ on the set $A = \{1,2,3,4\}$.
   Then Transitive Closure $R_t^+ =$
   $\{(1,2),(2,1),(2,3),(3,4),(4,1),\mathbf{(1,1)},\mathbf{(1,4)},\mathbf{(2,2)},\mathbf{(3,3)},\ \mathbf{(4,2)},\mathbf{(4,4)}\}$

Equivalence Classes: Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the equivalence class of a.

Examples:

1. For $aRb \Leftrightarrow a = b \; or \; a = -b, \;\; a, b \in I \;\; [a] = \{-a, a\}$
2. $R = \{(a, b) | a \equiv b(mod(4)), \;\; a, b \in I\}$
   $[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}$ and $[1] = \{\dots, -7, -3, 1, 3, 7, \dots\}$

Partition: A partition of a set A is a collection of disjoint non empty subsets of A that have A as their union.

Examples:

1. Let $S = \{1, 2, 3, 4, 5, 6\}$ The collections of the sets
   $A_1 = \{1, 2, 3\}, \;\; A_2\{4, 5\}$ and $A_3 = \{6\}$ forms a partition of S.

Partially Ordered Sets

Definition: A relation R on a set A is said to be partial order if R is

1. Reflexivity: $aRa \ \forall a \ \in A$
2. Anti-symmetry: $aRb, \ \ bRa$ then $a = b$
3. Transitivity: $aRb, \ \ bRc$ then aRc

The set A together with the partial order R is called **partially ordered set (poset)**. It is denoted by (A, R) or $(A, \leq)$

Examples:

1. A collection of subsets A of a sets with the inclusion relation $(\subseteq .)$ $\surd$
2. A set of natural number N with the divisibility relation $(a|b \ \ a$ divides b). $\surd$
3. A set of natural number N with the less than relation $(<)$. $\times$

Definition: Let $(A, \leq)$ be a poset. The elements a and b of A are said to be **comparable** if $a \leq b$ or $b \leq a$. And a and b of A are **non-comparable** if neither $a \leq b$ nor $b \leq a$.

Examples:

1. A set of natural number N with the divisibility relation ($a|b$ a divides b). Thus $(N, |)$ is a poset. The elements 2 and 5 are not comparable.

Note: Let $(A, \leq)$ be a poset. We say b is larger than equal to a if $a \leq b$.

Definition: Let $(A, \leq)$ be a poset. $(A, \leq)$ is called **totally ordered set or Chain** (linearly orderly sets) if every two elements in A are comparable.

Examples:

1. The set of real number with less than or equal to relation $(\leq)$. Thus $(R, \leq)$ is a poset. $\surd$
2. A poset $(N, |)$. $\times$

Definition: A partial ordering say $\leq$ on a poset can be represented by a diagram known as a **Hasse diagram** of $(A, \leq)$.

Examples:

1. Let $X = \{2, 3, 6, 12, 24, 36\}$ and the division relation $(a|b)$.

Note: Any two comparable elements are joined by lines in such a way that if aRb than a lies below b in diagram, and there will not be any horizontal lines in the diagram of a post.

Minimal and maximal elements: An element a in a poset $(A, \leq)$ is a maximal element if A has no element b such that $a < b$. Similarly, an element a in A is a minimal element if A has no element $b < a$.

Least and greatest elements: If a poset A contains an element a such that $b \leq a$ for every element b in A, a is the greatest element of the poset. If it contains an element a such that $a \leq b$ for every b in A, a is the least element.

Upper bounds and lower bound: If u is an element of A such that $a \leq b$ for all elements $a \in A$, then u is an upper bound of A. Likewise, there may be an element less than or equal to all the elements in A. If l is an element of A such that $l \leq a$ for all elements $a \in A$, then l is called a lower bound of A.

Least lower bounds and greatest lower bound: The element x is called the least upper bound of the subset A if x is an upper bound that is less than every other upper bound of A. That is x is a least upper bound of the subset A if $a \leq x$ whenever $a \in A$, and $x \leq z$ whenever $z$is upper bound of A. Similarly, the element y is called the greatest lower bound of the subset A if x is an lower bound and $z \leq y$ whenever z is a lower bound of A.

Lattices as Partially ordered sets

Definition: A **lattice** is a poset $(L, \leq)$ in which every subset $\{a, b\}$ of two elements of L has greatest lower bound (inf) and a least upper bound (sup).

— **Examples:**

1. The power set $P(S)$ of any non-empty set S with inclusion relation $(\subseteq)$. Thus $(P(S), \subseteq)$ is a poset. It is lattice. $\surd$
2. Let $L = \{2, 3, 4, 6\}$ and the division relation $(a|b)$. Then $(L, |)$ is a poset. $\times$

Definition: Let (L, R) be a lattice with relation R which is defined as aRb for $a, b \in L$. Then $(L, \bar{R})$ is said to be **dual** of (L, R) if $(L, \bar{R})$ is a lattice, where $\bar{R}$ is the dual of R.

Further topics

Following topics can see in the reference books.

Some Properties of Lattices: likes Indempotent, Commutative, Associative, Absorption

Definition: Lattices as Algebraic system

Definition: Direct Product of two Lattices

Definition: Isomorphic Lattices

Questions/Query ?