DISCRETE MATHEMATICS

LATTICE THEORY

Cartesian product: The Cartesian product of two sets A and B denoted $A \times B$ is the set of all ordered pairs of the form (a, b) where $a \in A$ and $b \in B$.

Binary relation: A binary relation from A to B is a subset of $A \times B$.

Reflexive relation: Let R be a binary relation on A. R is said to be reflexive relation if (a, a) is in R for every $a \in A$.

Symmetric relation: A binary relation R on a set A is said to be a symmetric relation if (a, b) in R implies that (b, a) is also in R.

Antisymmetric relation: Let R be a binary relation on A. R is said to be an antisymmetric relation if (a, b) in R implies that (b, a) is not in R unless $a = b$.

Transitive relation: Let R be a binary relation on A. R is said to be a transitive relation if (a, c) is in R whenever both (a, b) and (b, c) are in R.

Equivalence relation: A binary relation is said to an equivalence relation if it is reflexive, symmetric and transitive.

Partial ordering relation: A binary relation is said to be a partial ordering relation if it is reflexive, antisymmetric and transitive.

Partially ordered set (poset): Set A together with a partial ordering relation R on A is called a partially ordered set and is denoted by $(A, \leq)$.

Chain: Let $(A, \leq)$ be a partially ordered set. A subset of A is called a chain if every two elements in the subset are related.

Antichain: Let $(A, \leq)$ be a partially ordered set. A subset of A is called an antichain if no two elements in the subset are related.

Totally ordered set: A partially ordered set $(A, \leq)$ is called a totally ordered set if A is a chain and the binary relation is called a total ordering relation.

Maximal element: Let $(A, \leq)$ be a partially ordered set. An element a in A is called a maximal element if for no b in A, $a \neq b, a \leq b$.

Minimal element: Let $(A, \leq)$ be a partially ordered set. An element a in A is called a minimal element if for no b in A, $a \neq b, b \leq a$.

Upper bound: Let $(A, \leq)$ be a partially ordered set. An element = is said to be an upper bound of a and b if $a \leq c$ and $b \leq c$. An element c is said to be least upper bound of a and b if c is an upper bound of a and b, and if there is no other upper bound d of a and b such that $d \leq c$.

Universal upper bound: An element a in a lattice $(A, \leq)$ is called a universal upper bound if for every element b in A, $b \leq a$. It is unique if it exists and is denoted by 1.

Lower bound: Let $(A, \leq)$ be a partially ordered set. An element c is said to be a lower bound of a and b if $c \leq a$ and $c \leq b$. An element c is said to be greatest lowerbound of a and b if c is a lower bound of a and b, and if there is no other lower bound d of a and b such that $c \leq d$.

Universal lower bound: An element a in a lattice $(A, \leq)$ is called a universal lower bound if for every element b in A, $a \leq b$. It is unique if it exists and is denoted by 0.

Lattice: A partially ordered set is said to be a lattice if every two elements in the set have a unique least upper bound and a unique greatest lower bound.

For any a and b in the lattice $(A, \leq)$, $\mathrm{a} \leq \mathrm{a} \vee \mathrm{b}$ and $a \wedge b \leq a$

For any a, b, c, d in a lattice $(A, \leq)$, if $a \leq b$ and $c \leq d$ then $a \vee c \leq b \vee d$ and $a \wedge c \leq b \wedge d$

Commutative property: For any a and b in a lattice $(A, \leq)$, $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$

Associative property: For any a, b and c in a lattice $(A, \leq)$

a$\vee(b \vee c) = (a \vee b) \vee c$ and $a \wedge(b \wedge c) = (a \wedge b) \wedge c$

Idempotent property: For every a in a lattice $(A, \leq)$ $a \vee a = a$ and $a \wedge a = a$.

Absorption Property: For any a and b in a lattice $(A, \leq)$, $a \vee(a \wedge b) = a$ and $a \wedge(a \vee b) = a$

Cover: Let a and b be two elements in a lattice. Then a is said to cover b if $b < a$ and there is no element c such that $b < c < a$.

Atom: An element is called as an atom if it covers the universal lower bound.

Distributive lattice: A lattice $(A, \vee, \wedge)$ is said to be distributive if for all $a, b, c \in A$,

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

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Complement of an element: The complement of an element a of a lattice $(A, \vee, \wedge)$ with 0 and 1 is an element $b \in A$ such that $a \vee b = 1$ and $a \wedge b = 0$.

Complemented lattice: A lattice in which every element has a complement is called a complemented lattice.

Boolean lattice: A distributive, complemented lattice is called a Boolean lattice. In a such a lattice, every element a has a unique complement $\bar{a}$, and $^{-}$ is a unary operation on the lattice.

Boolean algebra: The algebraic structure $(A, \vee, \wedge, ^{-})$ formed by a Boolean lattice is called a Boolean algebra.

A Boolean expression over $(\{0,1\}, \vee, \wedge)$ is said to be in **disjunctive normal form** if it is join of minterms.

A Boolean expression over $(\{0,1\}, \vee, \wedge)$ is said to be in **conjunctive normal form** if it is meet of maxterms.

COMBINATORICS

Addition Principle. If there are m ways of doing A and n ways of doing B, with no way of doing both simultaneously, then the number of ways of doing A **or** B is $m + n$.

Multiplication Principle. If there are m ways of doing A and n ways of doing B independently, then there are mn ways of doing A **and** B (or A followed by B).

Permutations and Combinations

The number of permutations of n distinct objects is $n! = n(n-1)(n-2) \times \cdots 3 \times 2 \times 1$.

The number of ways of selecting and arranging r distinct objects from a collection of n distinct objects is ${}^nP_r = \frac{n!}{(n-r)!}$.

The number of ways of selecting r distinct objects from a collection of n distinct objects is ${}^nC_r$ or $\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$.

The number of ways of selecting any number of distinct objects from a collection of n distinct objects is 2^n.

The number of permutations of n objects where n_1 of them are alike of the first kind, n_2 of them are alike of the second kind, …, n_k of them are alike of the k^{th} kind is $\frac{n!}{n_1!n_2!\cdots n_k!}$.

The number of permutations of r objects selected from n types of objects with unlimited repetition of each type is n^r.

The number of selections of r objects from n types of objects with unlimited repetition of each type is $\binom{n+r-1}{r} = \binom{n+r-1}{n-1}$.

Basic identities

1. $n! = n(n-1)!$
2. $\binom{n}{r} = \binom{n}{n-r}$
3. $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$ for $n > r > 0$
4. $\sum_{r=0}^{n}\binom{n}{r} = 2^n$

Inclusion-Exclusion Principle

Let $a_1, a_2, \dots, a_n$ be n properties. In a collection of N objects, let $N(a_i)$ denote the number of objects with property a_i, let $N(a_i a_j)$ denote the number of objects with both properties $N(a_i a_j)$, etc. Then the number of objects in the collection that do **not** have any of the properties $a_1, a_2, \dots, a_n$ is

$$N(\overline{a_1}\,\overline{a_2}\cdots\overline{a_n}) = N - \sum_i N(a_i) + \sum_{i<j} N(a_i a_j) + \cdots + (-1)^k \sum_{i_1<i_2<\cdots<i_k} N(a_{i_1} a_{i_2}\cdots a_{i_k}) + \cdots + (-1)^n N(a_1 a_2 \cdots a_n).$$

Ordering of Permutations

Index sequence for k^{th} permutation of n distinct marks in lexicographical order: $c_{n-1}c_{n-2}\cdots c_1$ where

$$k - 1 = c_{n-1}(n-1)! + c_{n-2}(n-2)! + \cdots + c_1 1!$$

is the factorial base representation of $k-1$.

Fike's sequence for k^{th} permutation of n distinct marks: $d_1 d_2 \cdots d_{n-1}$, where $d_i = i - c_i$, and

$$k - 1 = c_1\frac{n!}{2!} + c_2\frac{n!}{3!} + \cdots + c_{n-1}\frac{n!}{(n-1)!}.$$

Generating Functions

The ordinary generating function for the number of selections of r distinct objects out of n distinct objects is $(1+x)^n = \sum_{r=0}^{n}\binom{n}{r}x^r$.

The ordinary generating function for the number of selections of r objects from n types of objects with unlimited repetition is $(1-x)^{-n} = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r$.

The exponential generating function for the number of permutations of n objects is $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Partitions and Compositions

The number of compositions of n into k positive parts is $\binom{n-1}{k-1}$.

The number of compositions of n into any number of positive parts is 2^{n-1}.

The ordinary generating function for the number of unrestricted partitions of n is $(1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}\cdots$.

GRAPH THEORY

A graph G consists of a finite nonempty set $V = V(G)$ whose elements are called 'vertices' of G and a set $E = E(G)$ of unordered pairs of distinct vertices of $V(G)$ whose elements are called the 'edges' of G. A graph with p vertices and q edges is called a (p, q) graph.

The first theorem in graph theory due to Euler, popularly known as 'Hand shaking lemma'. It states that, "the sum of degrees of all the vertices in a graph is twice the number of edges".

There are several types of graphs namely: complete graph, regular graph, cycle graph, path graph, tree, bipartite graph etc.

Some of the preliminary terminologies to be noted are:

Distance: The distance $d(u, v)$ between the two vertices u and v in G is the length of a shortest path joining them if any, otherwise $d(u, v) = \infty$. In a connected graph, distance is a metric. That is, for all the vertices u, v, w

i. $d(u, v) \geq 0$ with $d(u, v) = 0$ if and only if $d(u, u) = 0$
ii. $d(u, v) = d(v, u)$
iii. $d(u, v) + d(v, w) \geq d(u, w)$

Geodesic: A shortest u-v path.

Girth: Girth $g(G)$ of a graph G is the length of the shortest cycle (if any) in G.

Circumference: Circumference $c(G)$ of a graph G is the length of the longest cycle (if any) in G.

Eccentricity: The eccentricity $e(v)$ of a vertex in a connected graph G is the distance from v to the vertex farthest from v in G. That is, $e(v) = \max_{u \in V(G)} \{d(v, u)\}$.

Radius: The radius $r(G)$ or $\mathrm{rad}(G)$ is the minimum eccentricity of the vertices, i.e. $\mathrm{rad}(G) = \min_{v \in V(G)} \{e(v)\}$.

Diameter: The diameter $\mathrm{diam}(G)$ is the maximum eccentricity of the vertices. In other words, the length of any longest geodesic. i.e., $\mathrm{diam}(G) = \max_{v \in V(G)} \{e(v)\}$.

Central vertex: A vertex v is a central vertex if $e(v) = \mathrm{rad}(G)$. And the set of all central vertices is called 'center' of the graph.

GROUP THEORY

Let G be a non-empty set and $*: G \times G \to G$ a binary operation on G. Then

1. Associativity axiom: $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$.
2. Identity axiom: There exists an element $e \in G$ such that $a * e = e * a = a$, for all $a \in G$.
3. Inverse axiom: For $a \in G$, there corresponds an element $b \in G$ such that $a * b = b * a = e$.
4. Commutativity or Abelian axiom: $a * b = b * a$, for all $a, b \in G$.

In the above, if $(G,*)$ satisfies 1 then $(G,*)$ is a **semigroup**.
If $(G,*)$ satisfies 1 and 2 then $(G,*)$ is a **monoid**.
If $(G,*)$ satisfies 1, 2, and 3 then $(G,*)$ is a **group**.
If $(G,*)$ satisfies 1, 2, 3, and 4 then $(G,*)$ is a **commutative** or **Abelian group**.

Definitions

Let $(G,\cdot)$ be a group.

1. A non-empty subset of $H \subseteq G$ is a **subgroup** of G if $(H,\cdot)$ itself is a group. Then we write $H \leq G$.
2. If $H \leq G$, and $a \in G$, then $Ha = \{ha \mid h \in H\}$. Then Ha is a **right coset** of H in G. Similarly, $aH = \{ah \mid h \in H\}$ is a **left coset** of H in G.
3. The number of elements in G is the **order of the group** G, denoted $o(G)$ or $|G|$.
4. Let $a \in G$. The **order of the element** a is the least positive integer m such that $a^m = e$, denoted $o(a)$ or $|a|$.
5. Let $a \in$ G. Then $\langle a \rangle = \{a^i \mid i = 0, \pm 1, \pm 2, \dots\}$ is the **cyclic subgroup** of G generated by a.
6. A subgroup N of G is a **normal subgroup** of G if for every $g \in G$ and every $n \in N$, $gng^{-1} \in N$.
7. The set $Z(G) = \{z \in G \mid xz = zx, \forall x \in G\}$ is the **center** of G.
8. Let $a \in G$. Then $N(a) = \{x \in G \mid ax = xa\}$ is the **normaliser** of a.
9. Let $(H,\circ)$ also be a group. Then a **group homomorphism** from G to H is a function $f: G \to H$ such that for all $x, y \in G$, $f(xy) = f(x) \circ f(y)$.
10. Let $f: G \to H$ be a group homomorphism. Then the **image** of f is $\operatorname{im} f = \{f(x) \mid x \in G\} \leq H$ and the **kernel** of f is $\ker f = \{x \in G \mid f(x) = e_H\} \leq G$ where e_H is the identity element of H.

Examples of Groups

1. $(\mathbb{Z}, +)$ – Group of integers under addition
2. $(\mathbb{Q}, +)$ – Group of rational numbers under addition
3. $(\mathbb{R}, +)$ – Group of real numbers under addition
4. $(\mathbb{C}, +)$ – Group of complex numbers under addition
5. $\mathbb{Q}^\times$ – Group of non-zero rational numbers under multiplication
6. $\mathbb{R}^\times$ – Group of non-zero real numbers under multiplication
7. $\mathbb{C}^\times$ – Group of non-zero complex numbers under multiplication
8. $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ – Group of integers modulo n under addition modulo n
9. $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$, where $\omega = e^{\frac{2i\pi}{n}}$ – Group of complex n^{th} roots of unity under multiplication
10. S_n – Group of all permutations of $\{1, 2, \dots, n\}$ under composition of permutations
11. $\mathrm{GL}_n(\mathbb{R})$ – Group of $n \times n$ invertible real matrices

Basic Results

Let $(G,\cdot)$ be any group.

1. **Uniqueness of identity:** G has a unique identity element.
2. **Uniqueness of inverses:** Every element $x \in G$ has a unique inverse $x^{-1} \in G$, and $(x^{-1})^{-1} = x$.

3. **Shoe-sock property:** $\forall x, y \in G, (xy)^{-1} = y^{-1}x^{-1}$.
4. **Cancellation laws**: Let $x, y \in G$. If $\exists a \in G$ such that $ax = ay$, then $x = y$. If $\exists b \in G$ such that $xb = yb$, then $x = y$.
5. If G is finite of order n, then $\forall x \in G, x^n = e$.
6. If $f: G \to H$ is a homomorphism, then $\ker f$ is an normal subgroup of G
7. $Z(G)$ is a normal subgroup of G.

PROPOSITIONAL CALCULUS

Implications

I_1: $P \wedge Q \Rightarrow P$(Simplification)	I_8: $\neg(P \to Q) \Rightarrow Q$	
I_2: $P \wedge Q \Rightarrow Q$(Simplification)	I_9: $P, Q \Rightarrow P \wedge Q$	
I_3: $P \Rightarrow P \vee Q$(Addition)	I_{10}: $\neg P, P \vee Q \Rightarrow Q$	(Disjunctive syllogism)
I_4: $Q \Rightarrow P \vee Q$(Addition)	I_{11}: $P, P \to Q \Rightarrow Q$	(Modus ponens)
I_5: $\neg P \Rightarrow P \to Q$	I_{12}: $\neg Q, P \to Q \Rightarrow \neg P$	(Modus tollens)
I_6: $Q \Rightarrow P \to Q$	I_{13}: $P \to Q, Q \to R \Rightarrow P \to R$	(Hypothetical syllogism)
I_7: $\neg(P \to Q) \Rightarrow P$	I_{14}: $P \vee Q, P \to R, Q \to R \Rightarrow R$	(Dilemma)

Equivalences

E_1: $\neg\neg P \Leftrightarrow P$	E_{12}: $R \vee (P \wedge \neg P) \Leftrightarrow R$
E_2: $P \wedge Q \Leftrightarrow Q \wedge P$	E_{13}: $R \wedge (P \vee \neg P) \Leftrightarrow R$
E_3: $P \vee Q \Leftrightarrow Q \vee P$	E_{14}: $R \vee (P \vee \neg P) \Leftrightarrow \mathbf{T}$
E_4: $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	E_{15}: $R \wedge (P \wedge \neg P) \Leftrightarrow \mathbf{F}$
E_5: $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	E_{16}: $P \to Q \Leftrightarrow \neg P \vee Q$
E_6: $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	E_{17}: $\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$
E_7: $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	E_{18}: $P \to Q \Leftrightarrow \neg Q \to \neg P$
E_8: $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	E_{19}: $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$
E_9: $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	E_{20}: $\neg(P \rightleftarrows Q) \Leftrightarrow P \rightleftarrows \neg Q$
E_{10}: $P \vee P \Leftrightarrow P$	E_{21}: $P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$
E_{11}: $P \wedge P \Leftrightarrow P$	E_{22}: $P \rightleftarrows Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$