SUBJECT NAME : **Discrete Mathematics**

SUBJECT CODE : **MA 2265**

MATERIAL NAME : **Formula Material**

MATERIAL CODE : **JM08ADM009**

Name of the Student: Branch:

Unit – I (Logic and Proofs)

1) **Truth Table**:

Conjunction

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

Disjunction

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

Conditional

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional

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

Negation

p	$\sim p$
T	F
F	T

2) **Tautology and Contradiction**:

A Compound proposition $P = (P_1, P_2, \ldots P_n)$ where $P_1, P_2, \ldots P_n$ variables are called tautology if it is true for every truth assignment for $P_1, P_2, \ldots P_n$.

P is called a Contradiction if it is false for every truth assignment for $P_1, P_2, \ldots P_n$.

If a proposition is neither a tautology nor a Contradiction is called contingency.

3) **Laws of algebra of proposition**:

Name of Law	Primal form	Dual form
Idempotent law	$p \vee p \equiv p$	$p \wedge p \equiv p$
Identity law	$p \vee F \equiv p$	$p \wedge T \equiv p$

Dominant law	$p \vee T \equiv T$	$p \wedge F \equiv F$
Complement law	$p \vee \sim p \equiv T$	$p \wedge \sim p \equiv F$
Commutative law	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Associative law	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive law	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Absorption law	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Demorgan's law	$\sim (p \vee q) \equiv \sim p \wedge \sim q$	$\sim (p \wedge q) \equiv \sim q \vee \sim p$
Double Negation law	$\sim\sim p \equiv p$	

4) **Equivalence involving Conditionals**:

Sl.No.	Propositions
1.	$p \rightarrow q \equiv \sim p \vee q$
2.	$p \rightarrow q \equiv \sim q \rightarrow \sim p$
3.	$p \vee q \equiv \sim p \rightarrow q$
4.	$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
5.	$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$

5) **Equivalence involving Biconditionals**:

Sl.No.	Propositions
1.	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
2.	$p \leftrightarrow q \equiv \sim p \leftrightarrow \sim q$
3.	$p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$

4.	$\sim(p \leftrightarrow q) \equiv p \leftrightarrow \sim q$

6) **Tautological Implication**:
$A \Rightarrow B$ if and only if $A \rightarrow B$ is tautology. (i.e) To prove $A \Rightarrow B$, it enough to prove $A \rightarrow B$ is tautology.

7) **The Theory of Inferences**:
The analysis of the validity of the formula from the given set of premises by using derivation is called "theory of inferences"

8) **Rules for inferences theory**:
Rule P:
A given premise may be introduced at any stage in the derivation.
Rule T:
A formula S may be introduced in a derivation if S is tautologically implied by one or more of the preceding formulae in the derivation.
Rule CP:
If we can drive S from R and a set of given premises, then we can derive $R \rightarrow S$ from the set of premises alone. In such a case R is taken as an additional premise (assumed premise). Rule CP is also called the deduction theorem.

9) **Indirect Method of Derivation**:
Whenever the assumed premise is used in the derivation, then the method of derivation is called indirect method of derivation.

10) **Table of Logical Implications:**

Name of Law	Primal form
Simplification	$p \wedge q \Rightarrow p$ $p \wedge q \Rightarrow q$
Addition	$p \Rightarrow p \vee q$ $q \Rightarrow p \vee q$
Disjunctive Syllogism	$\sim p \wedge (p \vee q) \Rightarrow q$ $\sim q \wedge (p \vee q) \Rightarrow p$
Modus Ponens	$p \wedge (p \rightarrow q) \Rightarrow q$
Modus Tollens	$(p \rightarrow q) \wedge \sim q \Rightarrow \sim p$
Hypothetical Syllogism	$(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow p \rightarrow r$

$$p \to q \Rightarrow \ \sim q \to \sim p$$

Unit – II (Combinatorics)

1) **Principle of Mathematical Induction**:

   Let $P(n)$ be a statement or proposition involving for all positive integers n.

   Step 1: $P(1)$ is true.

   Step2: Assume that $P(k)$ is true.

   Step3: We have to prove $P(k+1)$ is true.

2) **Principle of Strong induction**.

   Let $P(n)$ be a statement or proposition involving for all positive integers n.

   Step 1: $P(1)$ is true.

   Step2: Assume that $P(n)$ is true for all integers $1 \le n \le k$.

   Step3: We have to prove $P(k+1)$ is true.

3) **The Pigeonhole Principle**:

   If n pigeons are assigned to m pigeonholes and $m < n$, than at least one pigeonhole contains two or more pigeons.

4) **The Extended Pigeonhole Principle**:

   If n pigeons are assigned to m pigeonholes than one pigeonhole must contains at least $\left[\frac{(n-1)}{m}\right]+1$ pigeons.

5) **Recurrence relation**:

   An equation that expresses a_n, the general term of the sequence $\{a_n\}$ in terms of one or more of the previous terms of the sequence, namely $a_0, a_1, \ldots a_{n-1}$, for all integers n is called a recurrence relation for $\{a_n\}$ or a difference equation.

6) **Working rule for solving homogeneous recurrence relation**:

   Step 1: The given recurrence relation of the form

   $$C_0(n)a_n + C_1(n)a_{n-1} + \ldots + C_k(n)a_{n-k} = 0$$

   Step 2: Write the characteristic equation of the recurrence relation

   $$C_0 r_{n+k} + C_1 r_{n+(k+1)} + \ldots + C_k r_n = 0$$

   Step 3: Find all the roots of the characteristic equation namely $r_1, r_2, \ldots r_k$.

   Step 4:

   Case (i): If all the roots are distinct then the general solution is

   $$a_n = b_1 r_1^n + b_2 r_2^n + \ldots + b_k r_k^n$$

   Case (ii): If all the roots are equal then the general solution is

   $$a_n = \left(b_1 + nb_2 + n^2 b_3 + \ldots\right) r^n$$

Unit – III (Graph Theory)

1) **Graph**:
   A graph G=(V,E) consists of two sets $V = \{v_1, v_2, ...v_\upsilon\}$, called the set of vertices and $E = \{e_1, e_2, ...e_\epsilon\}$, called the set of edges of G.
2) **Simple graph**:
   A graph is said to be simple graph if it has no loops and parallel edges. Otherwise it is multi graph.
3) **Regular graph**:
   If every vertex of a simple graph has the same degree, then the graph is called a regular graph. If every vertex in a regular graph has degree n, then the graph is called n-regular.
4) **Complete graph**:
   A simple graph in which each pair of distinct vertices is joined by an edge is called a complete graph. The complete graph on "n" vertices is denoted by K_n.
5) **Pendent vertex and Pendent edge**:
   A vertex with degree one is called a pendent vertex and the only edge which is incident with a pendent vertex is called the pendent edge.
6) **Matrix representation of a graph**:
   There are two ways of representing a graph by a matrix namely adjacent matrix and incidence matrix as follows:
   Adjacency matrices:
   Let G be a graph with n vertices, then the adjacency matrix, $A_G = (A_{ij})$ defined by $A_{ij} = \begin{cases} 1, & \text{if } u_i, v_j \text{ are adjacent} \\ 0, & \text{otherwise} \end{cases}$.
   Incidence matrix:
   Let G be a graph with n vertices, then the incidence matrix of G is an n x e matrix $B_G = (B_{ij})$ defined by $B_{ij} = \begin{cases} 1, & \text{if } j^{th} \text{ edge is incident on the } i^{th} \text{ vertex} \\ 0, & \text{otherwise} \end{cases}$
7) **Bipartite graph**:
   A graph G=(V,E) is called a bipartite graph if its vertex set V can be partitioned into two subsets V_1 and V_2 such that each edge of G connects and vertex of V_1 to a vertex of V_2. In other words, no edge joining two vertices, in V_1 or two vertices in V_2.
8) **Isomorphism of a graph**:
   The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a one to one and onto function f from V_1 to V_2 with the property that a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all a and b in V_1.

9) **Complementary and Self complementary graph**:

Let G be a graph. The complement $\overline{G}$ of G is defined by any two vertices are adjacent in $\overline{G}$ if and only if they are not adjacent in G.

G is said to be a self complementary graph if G is isomorphic to $\overline{G}$.

10) **Connected graph**:

A graph G is said to be connected if there is at least one path between every pair of vertices in G. Otherwise G is disconnected. A disconnected graph consists of two or more connected sub graphs and each of them is called a component. It is denoted by $\omega(G)$.

11) **Cut edge**:

A cut edge of a graph G is an edge "e" such that $\omega(G-e) > \omega(G)$. (i.e) If G is connected and "e" is a cut edge of G, then $G-e$ is disconnected.

12) **Cut vertex**:

A cut vertex of a graph G is a vertex "v" such $\omega(G-v) > \omega(G)$. (i.e) If G is connected and "v" is a cut vertex of G, then $G-v$ is disconnected.

13) **Define vertex connectivity**.

The connectivity $\kappa(G)$ of G is the minimum "k" for which G has a k-vertex cut. If G is either trivial or disconnected then $\kappa(G) = 0$.

14) **Define edge connectivity**.

The edge connectivity $\kappa'(G)$ of G is the minimum "k" for which G has a k-edge cut. If G is either trivial or disconnected then $\kappa'(G) = 0$

15) **Define Eulerian graph**.

A path of graph G is called an Eulerian path, if it includes each edge of G exactly once. A circuit of a graph G is called an Eulerian circuit, if it includes each edge of G exactly one. A graph containing an Eulerian circuit is called an Eulerian graph.

16) **Define Hamiltonian graph**.

A simple path in a graph G that passes through every vertex exactly once is called a Hamilton path. A circuit in a graph G that passes through every vertex exactly once is called a Hamilton circuit. A graph containing a Hamiltonian circuit.

Unit – IV (Algebraic Structures)

1) **Semi group**:

If G is a non-empty set and * be a binary operation on G, then the algebraic system $(G,*)$ is called a semi group, if G is closed under * and * is associative.

Example: If Z' is the set of positive even numbers, then $(Z',+)$ and $(Z',\times)$ are semi groups.

2) **Monoid**:

If a semi group $(G,*)$ has an identity element with respect to the operation *, then $(G,*)$ is called a monoid. It is denoted by $(G,*,e)$.

Example: If N is the set of natural numbers, then $(N,+)$ and $(N,\times)$ are monoids with the identity elements 0 and 1 respectively. $(Z',+)$ and $(Z',\times)$ are semi groups with out monoids, where Z' is the set of all positive even numbers

3) **Sub semi groups**:

If $(G,*)$ is a semi group and $H \subseteq G$ is called under the operation *, then $(H,*)$ is called a sub semi group of $(G,*)$.

Example: If the set E of all even non-negative integers, the $(E,+)$ is a sub semi group of the semi group $(N,+)$, where N is the set of natural numbers.

4) **Semi group homomorphism**:

If $(G,*)$ and (G',Δ) are two semi groups, then a mapping $f: G \to G'$ is called a semi group homomorphism, if for any $a,b \in G$, $f(a*b) = f(a)\Delta f(b)$. A homomorphism f is called isomorphism if f is 1-1 and onto.

5) **Group**:

If G is a non-empty set and * is a binary operation of G, then the algebraic system $(G,*)$ is called a group if the following conditions are satisfied.

(i) Closure property
(ii) Associative property
(iii) Existence of identity element
(iv) Existence of inverse element

Example: $(Z,+)$ is a group and $(Z,\bullet)$ is not a group.

6) **Abelian group**:

A group $(G,*)$, in which the binary operation * is commutative, is called a commutative group or abelian group.

Example: The set of rational numbers excluding zero is an abelian group under the multiplication.

7) **Coset**:

If H is a subgroup of a group G under the operation *, then the set aH, where $a \in G$, define by $aH = \{a*h / h \in H\}$ is called the left coset of H in G generated by the element $a \in G$. Similarly the set Ha is called the right coset of H in G generated by the element $a \in G$.

Example: $G=\{1,-1,i,-i\}$ be a group under multiplication and $H=\{1,-1\}$ is a subgroup of G. The right cosets are $1H=\{1,-1\}$, $-1H=\{-1,1\}$, $iH=\{i,-i\}$ and $-iH=\{-i,i\}$.

8) **Lagrange's theorem**:
The order of each subgroups of a finite group is a divisor of a order of a group.

9) **Cyclic group**:
A group $(G,*)$ is said to be cyclic, if $\exists$ and element $a\in G$ such that every element of G generated by a. (i.e) $G=<a>=\{1,a,a^2,...a^n=e\}$.
Example: $G=\{1,-1,i,-i\}$ is a cyclic group under the multiplication. The generator is i, because $i^4=1,\ i^2=-1,\ i,\ i^3=-i$.

10) **Normal subgroup**:
A subgroup H of the group G is said to be normal subgroup under the operation *, if for any $a\in G$, $aH=Ha$.

11) **Kernel of a homomorphism**:
If f is a group homomorphism from $(G,*)$ and (G',Δ), then the set of element of G, which are mapped into e', the identity element of G', is called the kernel of the homomorphism f and denoted by $\ker(f)$.

12) **Fundamental theorem of homomorphism**:
If f is a homomorphism of G on to G' with kernel K, then G/K is isomorphic to G'.

13) **Cayley's theorem**:
Every finite group of order n is isomorphic to a permutation group of degree n.

14) **Ring**:
An algebraic system $(S,+,\bullet)$ is called a ring if the binary operations $+$ and $\bullet$ on S satisfy the following properties.
    (i) $(S,+)$ is an abelian group
    (ii) $(S,\bullet)$ is a semi group
    (iii) The operation $\bullet$ is distributive over $+$.
Example: The set of all integers Z, and the set of all rational numbers R are rings under the usual addition and usual multiplication.

15) **Integral domain**:
A commutative ring without zero divisor is called Integral domain.
Example: (i) $(R,+,\bullet)$ is an integral domain, since $a,b\in R$ such that $a\neq 0,\ b\neq 0$ then $ab\neq 0$. (ii) $(Z_{10},+_{10},\times_{10})$ is not an integral domain, because $2,3\in Z_{10}$ and $2\times_{10}5=0$. Therefore 2 and 5 are zero divisors.

16) **Field**:

A commutative reing $(S,+,\bullet)$ which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a field.

Example: The ring of rational numbers $(Q,+,\bullet)$ is a field since it is a commutative ring and each non-zero element is inversible.

Unit – V (Lattices and Boolean algebra)

1) **Partially ordered set (Poset)**:

A relation R on a set A is called a partial order relation, if R is reflexive, antisymmetric and transitive. The set A together with partial order relation R is called partially ordered set or poset.

Example: The greater than or equal to $(\geq)$ relation is a partial ordering on the set of integers Z .

2) **Lattice**:

A lattice is a partially ordered set $(L,\leq)$ in which every pair of elements $a,b\in L$ has a glb and lub.

3) **General formula**:

i) $\text{glb}\{a,b\} = a*b = a\wedge b$

ii) $\text{lub}\{a,b\} = a\oplus b = a\vee b$

iii) $a*b\leq a$ & $a*b\leq b$; $a\oplus b\geq a$ & $a\oplus b\geq b$

iv) If $a\leq b \Rightarrow a*b=a$, $a\oplus b=b$

4) **Properties**:

Name of Law	Primal form	Dual form
Idempotent law	$a*a=a$	$a\oplus a=a$
Commutative law	$a*b=b*a$	$a\oplus b=b\oplus a$
Associative law	$(a*b)*c=a*(b*c)$	$(a\oplus b)\oplus c=a\oplus(b\oplus c)$
Distributive law	$p*(q\oplus r)\equiv(p*q)\oplus(p*r)$	$p\oplus(q*r)\equiv(p\oplus q)*(p\oplus r)$
Absorption law	$a*(a\oplus b)=a$	$a\oplus(a*b)=a$
Complement	$a*a'=0$	$a\oplus a'=1$

Demorgan's law	$(a*b)' = a' \oplus b'$	$(a \oplus b)' = a' * b'$
Double Negation law	$\sim\sim p \equiv p$	

5) **Complemented Lattices**:
   A Lattice $(L,*,\oplus)$ is said to be complemented if for any $a \in L$, there exist $a' \in L$, such that $a*a' = 0$ and $a \oplus a' = 1$.
6) **Demorgan's laws**:
   Let $(L,*,\oplus)$ be the complemented lattice, then $(a*b)' = a' \oplus b'$ and $(a \oplus b)' = a' * b'$.
7) **Complete Lattice**:
   A lattice $(L,*,\oplus)$ is complete if for all non-empty subsets of L, there exists a glb and lub.
8) **Lattice Homomorphism**:
   Let $(L,*,\oplus)$ and $(S,\wedge,\vee)$ be two lattices. A mapping $g : L \to S$ is called lattices homomorphism if $g(a*b) = g(a) \wedge g(b)$ and $g(a \oplus b) = g(a) \vee g(b)$.
9) **Modular Lattice**:
   A lattice $(L,*,\oplus)$ is said to be modular if for any $a,b,c \in L$
   i) $a \le c \;\Rightarrow\; a \oplus (b*c) = (a \oplus b)*c$
   ii) $a \ge c \;\Rightarrow\; a*(b \oplus c) = (a*b) \oplus c$
10) **Chain in Lattice**:
   Let $(L,\le)$ be a Chain if
   i) $a \le b \text{ or } a \le c$ and
   ii) $a \ge b \text{ and } a \ge c$
11) **Condition for the algebraic lattice**:
   A lattice $(L,*,\oplus)$ is said to be algebraic if it satisfies Commutative Law, Associative Law, Absorption Law and Existence of Idempotent element.
12) **Isotone property**:
   Let $(L,*,\oplus)$ be a lattice. The binary operations $*$ and $\oplus$ are said to possess isotone property if $\begin{array}{l} b \le c \;\Rightarrow\; a*b \le a*c \\ \qquad\qquad a \oplus b \le a \oplus c \end{array}$.

13) **Boolean Algebra**:

A Boolean algebra is a lattice which is both complemented and distributive. It is denoted by $(\boldsymbol{B},*,\oplus)$.

---- *All the Best* ----