DISCRETE MATHEMATICS

DIGITAL ASSIGNMENT II

OM ASHISH MISHRA
16BCE0789

1(a) State and prove Lagrange's theorem

Ans: **Statement**

Let G be a finite group of order n and H be any subgroup of G then the order of H divides the order of G, i.e, O(H)/O(G).

(OR)

The order of subgroup of a finite group is a divisor of the order of the group.

Proof

Let (G, *) be a finite group of order n is O(G) = n and let (H, *) be a finite group of order m is O(H) = m.

Let $h_1, h_2 \ldots h_m$ are m different elements of H.

The right coset H * a of H in a is defined by $H * a = \{ h_1 * a, h_2 * a, \ldots h_m * a \}$ for $a \in G$. Since there is one to one correspondence between the elements of H and H * a, the elements of H * a are distinct.

Hence each right coset of H in G has m distinct element. We know that any right cosets of H in G are earlier disjoint or identical.

The number of distinct right cosets of H in G is finite (say k) the union of these k distinct elements of H in G is equal to G.

Let these k distinct right cosets are $H*a_1$, $H*a_2$, ... $H*a_n$ then

$$G = (H*a_1) \cup (H*a_2) \cup \ldots \cup (H*a_k)$$

$$O(G) = O(H*a_1) + O(H*a_2) + \ldots + O(H*a_k)$$

$$n = m + m + \ldots + m \text{ (k times)}$$

$$n = km$$

$$k = \frac{n}{m} \text{ or } m/n$$

$$k = O(H)/O(G).$$

Since k is an integer $O(H)$ divides $O(G)$.

Hence the theorem is proved.

(b) Determine the group code (3,6) using the parity check matrix H is given by.

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Ans: Given that $m = 3$, $n = 6$. Rewriting the given matrix:

$$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T | I_{n-m}]$$

A^T $\quad$ I_{n-m}

The generator matrix $G = [I_m | A]$

$$= \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$B^3 = \{000, 001, 010, 100, 011, 101, 110, 111\}$

and $e(w) = wG$

$$e[000] = [000] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$= [0\ 00\ 000]$$

$$e[001] = [0\ 0\ 1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [0\ 0\ 1\ 0\ 1\ 1]$$

$$e[100] = [1\ 0\ 0]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [1\ 0\ 0\ 1\ 1\ 1]$$

$$e[010] = [0\ 1\ 0]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [0\ 1\ 0\ 1\ 0\ 1]$$

$$e[011] = [0\ 1\ 1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [0\ 1\ 1\ 1\ 1\ 0]$$

$$e[101] = [1\ 0\ 1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [1\ 0\ 1\ 1\ 0\ 0]$$

$$e[110] = [1\ 1\ 0]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [1\ 1\ 0\ 0\ 1\ 0]$$

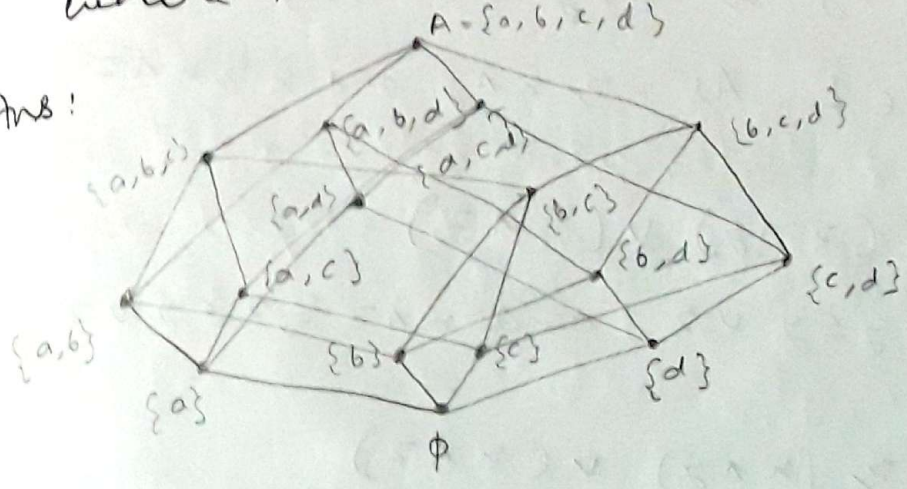
$$e[111] = [1\ 1\ 1]\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&0&1&1\end{bmatrix} = [1\ 1\ 1\ 0\ 0\ 1]$$

Thus, the code words generated are

000000, 001011, 010101, 100111, 011110,
101100, 110010, 111001.

(2)(a) Draw the Hasse diagram of $(P(A), \subseteq)$ where $A = \{a, b, c, d\}$.

Ans:



(b) State and prove distributive inequality of lattice.

Ans: Statement

A lattice $(L, *, \oplus)$ is called a distributive lattice if for any $a, b, c \in L$. $a * (b \oplus c) = (a * b) \oplus (a * c)$ and $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$

Proof

Distributive inequalities:

(i) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

(ii) $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

(i) Let $x, y, z \in L$. As $x \leq x \vee y$ and $x \leq x \vee z$ we have,

$x \leq (x \vee y) \wedge (x \vee z)$

As $y \wedge z \leq y \leq x \vee y$ and $y \wedge z \leq z \leq x \vee z$ we have,

$(y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

So $(x \vee y) \wedge (x \vee z)$ is an upper bound for x and $y \wedge z$.

Hence $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

Hence (i) is proved.

(ii) Let $x \wedge (y \vee z) \geq x \wedge y \vee (x \wedge z)$

Let $x, y, z \in L$. As $x \geq x \wedge y$ and $x \geq x \wedge z$ we have,

$$x \geq (x \wedge y) \vee (x \wedge z)$$

As $x \wedge y \leq y \leq y \vee z$ and $x \wedge z \leq z \leq y \vee z$ we have,

$$(y \vee z) \geq (x \wedge y) \vee (x \wedge z)$$

So $(x \wedge y) \vee (x \wedge z)$ is an lower bound for x and $y \vee z$.

Hence $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

(3)(a) In a complemented distributive lattice, show that $a \le b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b = 1 \Leftrightarrow b' \le a'$

Ans: Proof

We know that $a \le b \Leftrightarrow a \oplus b = b$

Multiplying on both sides by b'

$\Rightarrow (a \oplus b) * b' = b * b'$

$\Rightarrow (a * b') \oplus (b * b') = b * b'$ [By distributive law]

$\Rightarrow (a * b') \oplus 0 = 0$ [By $a * a' = 0$]

$\Rightarrow a * b' = 0 \rightarrow (1)$

$\Rightarrow (a * b')' = 0'$ [Taking complement on both sides.]

$\Rightarrow a' \oplus b = 1 \rightarrow (2)$

Again we know that $a \le b \Leftrightarrow a * b = a$

$\Rightarrow (a * b)' = a'$ [Taking complement on both sides.]

$\Rightarrow a' \oplus b' = a'$ [By Demorgan's law]

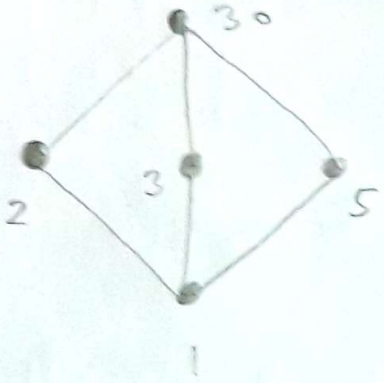
$\Rightarrow b' \le a' \rightarrow (3)$

$\therefore$ From (1), (2) and (3)

$a \le b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b' = 1 \Leftrightarrow b' \le a'$

(3)(b) In a lattice $L = \{1, 2, 3, 5, 30\}$ then L is a poset under the relation divides. Prove that $(L, *, \oplus)$ is a distributive lattice.

Ans:



$*$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

$\oplus$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$

Let $a = 2$, $b = 3$, $c = 5$

$2 \oplus (3 * 5) = (2 \oplus 3) * (2 \oplus 5)$

$2 \oplus 1 = 30 * 30$

$2 \neq 30$

$\therefore$ The $(L, *, \oplus)$ is NOT distributive lattice.

④ In any Boolean algebra prove that

$(a+b')(b+c')(c+a') = (a'+b)(b'+c)(c+a)$

Ans: Consider $(a+b')(b+c')$

$= ((a+b')b) + ((a+b')c')$ [By distributive law].

$= ab + b'b + ac' + b'c'$ [By distributive law]

$= ab + 0 + ac' + b'c'$

$= ab + ac' + b'c' \rightarrow (1)$

Now, $(ab + ac' + b'c')(c+a') =$

$= (ab + ac' + b'c')c + (ab + ac' + b'c')a'$

[By distributive law]

$= abc + acc' + b'cc' + aba' + aa'c' + a'b'c'$

$= abc + 0 + 0 + 0 + 0 + a'b'c'$

$= abc + a'b'c' \rightarrow (2)$

L.H.S

$(a+b')(b'+c')(c+a') = abc + a'b'c'$

Now consider $(a'+b)(b'+c)$

$= ((a'+b)b') + ((a'+b)c)$

[By distributive law]

$= a'b' + bb' + a'c + bc$

[By distributive law]

$= a'b' + 0 + a'c + bc$

$= a'b' + a'c + bc \rightarrow (1)$

Now $(a'b' + a'c + bc)(c'+a)$

$= (a'b' + a'c + bc)c' + (a'b' + a'c + bc)a$

[By distributive law]

$= a'b'c' + a'cc' + bcc' + aa'b' + aa'c + abc$

[By distributive law]

$= a'b'c' + 0 + 0 + 0 + 0 + abc$

$= a'b'c' + abc \rightarrow (2)$

R.H.S

$(a'+b)(b'+c)(c'+a) = a'b'c' + abc$

$\therefore$ L.H.S = R.H.S

$\therefore (a'+b)(b'+c)(c'+a) = (a+b')(b+c')(c+a')$

Hence proved.

(5) State and prove De-Morgan's laws for lattice.

Ans: Proof

Let L be a distributive lattice. Let $a, b \in L$ have complements a' and b' respectively thus $a * a' = 0$ and $a \oplus a' = 1$, $b * b' = 0$ and $b \oplus b' = 1$.

We shall show that $a' \oplus b'$ is the complement of $a * b$ and $a' * b'$ is the complement of $a \oplus b$.

Now consider $(a * b) * (a' \oplus b')$

$= [(a * b) * a'] \oplus [(a * b) * b']$

[By distributive law]

$= [a' * (a * b)] \oplus [(a * b) * b']$

[By commutative law]

$= [(a' * a) * (b)] \oplus [(a) * (b * b')]$

[By associative law]

$= [0 * b] \oplus [a * 0]$

[By negation law]

[By given]

$= 0 \oplus 0$

$= 0$

Next consider $(a * b) \oplus (a' \oplus b')$

$= [a \oplus (a' \oplus b')] * [b \oplus (a' \oplus b')]$

[By distributive law]

$= [a \oplus (a' \oplus b')] * [(a' \oplus b') \oplus b]$

[By commutative law]

$= [(a \oplus a') \oplus b'] * [a' \oplus (b \oplus b')]$

[By associative law]

$= [1 \oplus b'] * [a' \oplus 1]$ [By given]

$= 1 * 1$

$= 1$

$(a \overset{x}{*} b) * (a' \overset{y}{\oplus} b') = 0$

$(a * b) \oplus (a' \oplus b') = 1$

$x * y = 0 \Rightarrow y = x'$

$x \oplus y = 1 \Rightarrow x = y'$

$\therefore (a * b)' = a' \oplus b'$

Here we conclude that $a' \oplus b'$ is the complement of $a * b$.

Next we prove that $a' * b'$ is complement of $a \oplus b$.

Consider $(a \oplus b) * (a' * b')$

$= [a * (a' * b')] \oplus [b * (a' * b')]$

[By distributive law]

$= [a * (a' * b')] \oplus [(a' * b') * b]$

[By commutative law]

$= [(a * a') * b'] \oplus [(b * b') * a']$

[By associative law]

$= [0 * b'] \oplus [0 * a']$ [By given]

$= 0 \oplus 0$

$= 0$

Next consider $(a \oplus b) \oplus (a' * b')$

$= [(a \oplus b) \oplus a'] * [(a \oplus b) \oplus b']$

[By distributive law]

$= [a' \oplus (a \oplus b)] * [(a \oplus b) \oplus b']$

[By commutative law]

$= [(a' \oplus a) \oplus b] * [a \oplus (b \oplus b')]$

[By associative law]

$= [1 \oplus b] * [a \oplus 1]$ [By given]

$= 1 * 1$

$= 1$

$\therefore (a \overset{x}{\oplus} b) * (a' \overset{y}{*} b') = 0$ | $x * y = 0 \Rightarrow y = x'$

$(a \oplus b) \oplus (a' * b') = 1$ | $x \oplus y = 1 \Rightarrow x = y'$

$\therefore (a \oplus b)' = a' * b'$

$a' * b'$ is the complement of $a \oplus b$.

Hence the De-morgan's laws for lattice is proved.

Statement:

A lattice $(L, \oplus, *)$ is said to satisfy De-morgan's law if for any $a, b \in L$.

$(a \oplus b)' = a' * b'$ and $(a * b)' = a' \oplus b'$