

38

Discrete Mathematics

B.E. B.Tech. DEGREE EXAMINATION, NOV/DEC 2007.

Answer ALL questions

PART - A - (10 x 2 = 20 marks)

1. Write an equivalent formula for $P \wedge (Q \rightleftharpoons R)$ which contains neither the biconditional nor the conditional

Answer

$$P \wedge (Q \rightleftharpoons R) \Leftrightarrow P \wedge ((Q \rightarrow R) \cap (R \rightarrow Q))$$

$$\Leftrightarrow P \wedge ((7Q \vee R) \wedge (7R \vee Q))$$

2. What is duality law of logical expression? Give the dual of $(P \vee F) \wedge (Q \vee T)$

Answer

In an expression A, if we replace \vee, \wedge, T, F respectively by \wedge, \vee, F, T the resulting new formula is the dual of the expression A.

$$\text{Dual of given formula : } (P \wedge T) \vee (Q \wedge F)$$

3. Define statement function of one variable. when it will become a statement?

Answer

Statement function is an expression containing predicate symbols and an individual variable. It becomes a statement when the variable is replaced by any particular value.

Anna University Q & A

39

4. Use quantifiers to express the associative law for multiplication of real numbers.

Answer

$\forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$ where the universe of discourse for x, y and z is the set of real numbers.

5. Partition $A = \{0, 1, 2, 3, 4, 5\}$ with minsets generated by $B_1 = \{0, 2, 4\}$ and $B_2 = \{1, 5\}$

Answer

$$B_1 \cap B_2 = \emptyset, B_1 \cap B_2^c = \{0, 2, 4\}, B_1^c \cap B_2 = \{1, 5\}, B_1^c \cap B_2^c = \{3\}$$

$$\therefore \text{Partition of } A = [\{0, 2, 4\}, \{1, 5\}, \{3\}]$$

6. If a poset has a least element, then prove it is unique.

Answer

Let (L, \leq) be a poset with a_1, a_2 be two least elements. Then $a_1 \leq a_2, a_2 \leq a_1$. By antisymmetry property, $a_1 = a_2$. So the least element if exists is unique.

7. If ψ_A denotes the characteristic function of the set A, prove that $\psi_{A-B}(x) = \psi_A(x) - \psi_{A \cap B}(x)$ for all $x \in E$, the universal set.

Answer

$$\psi_{A-B}(x) = \psi_{A \cap \bar{B}}(x) = \psi_A(x) \psi_{\bar{B}}(x)$$

$$= \psi_A(x) [1 - \psi_B(x)]$$

$$= \psi_A(x) - \psi_{A \cap B}(x)$$

40

Discrete Mathematics

8. If $f(x, y) = x + y$ express $f(x, y+1)$ in terms of successor and projection functions

Answer

$$\begin{aligned} f(x, y+1) &= x + y + 1 \\ &= (x + y) + 1 = f(x, y) + 1 \\ &= S(f(x, y)) \\ &= S(U_3^3(x, y, f(x, y))) \end{aligned}$$

9. Show that semi-group homomorphism preserves the property of idempotency.

Answer

Let $f: (M, *) \rightarrow (H, \Delta)$ be a semigroup homomorphism.

x is an idempotent element of M .

$$x * x = x \quad f(x) = f(x * x) = f(x) \Delta f(x)$$

$\Rightarrow f(x)$ is an idempotent.

\therefore Idempotency preserved.

10. Let $x = 1001$, $y = 0100$, $z = 1000$. Find the minimum distance between these code words.

Answer

$$\begin{aligned} x \oplus y &= 1101, \quad y \oplus z = 1100, \quad z \oplus x = 0001, \quad H(x, y) = 3, \\ H(y, z) &= 2, \quad H(z, x) = 1. \text{ Minimum distance} = 1. \end{aligned}$$

Anna University Q & A

41

PART - B (5x16 = 80 marks)

11. (a) (i) Obtain the PCNF of the formula S given by $(7P \rightarrow R) \wedge (Q \rightleftharpoons P)$ and hence deduce The PDNF of S .

Answer

$$\begin{aligned} S &\Leftrightarrow (P \vee R) \wedge (Q \rightarrow P) \wedge (P \rightarrow Q) \\ &\Leftrightarrow (P \vee R) \wedge (7Q \vee P) \wedge (7P \vee Q) \\ &\Leftrightarrow ((P \vee R) \vee (Q \wedge 7Q)) \wedge ((7Q \vee P) \vee (R \wedge 7R)) \\ &\quad ((7P \vee Q) \vee (R \wedge 7R)) \end{aligned}$$

$$\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee 7Q \vee R) \wedge (P \vee 7Q \vee 7R) \wedge (7P \vee Q \vee R) \wedge (7P \vee Q \vee 7R)$$

$$\therefore \text{PCNF of } S \Leftrightarrow (P \vee Q \vee R) \wedge (P \vee 7Q \vee R) \wedge (P \vee 7Q \vee 7R) \wedge (7P \vee Q \vee R) \wedge (7P \vee Q \vee 7R)$$

$$7S \Leftrightarrow (P \vee Q \vee 7R) \wedge (7P \vee 7Q \vee R) \wedge (7P \vee 7Q \vee 7R)$$

$$\text{PDNF of } S \Leftrightarrow (7P \wedge 7Q \wedge R) \vee (P \wedge Q \wedge 7R) \vee (P \wedge Q \wedge R)$$

11. (a) (ii) Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \rightarrow R$, $(P \rightarrow M)$, $7M$

Answer

- | | | |
|----|-------------------|----------------------|
| 1. | $P \rightarrow M$ | P, rule |
| 2. | $7M$ | P rule |
| 3. | $7P$ | T rule from (1), (2) |

42

Discrete Mathematics

4. $P \vee Q$ P rule
5. $\neg P \rightarrow Q$ T rule from (4)
6. Q T rule from (3), (5)
7. $Q \rightarrow R$ P rule
8. R T rule from (6), (7)
9. $R \wedge (P \vee Q)$ T rule from (4), (8) $P, Q \Rightarrow P \wedge Q$

11. b. (i) Without using truth tables, prove the equivalences
 $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$ and $P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)$

Answer

$$\begin{aligned}
 P \rightarrow (Q \rightarrow R) &\Leftrightarrow P \rightarrow (\neg Q \vee R) \\
 &\Leftrightarrow \neg P \vee (\neg Q \vee R) \\
 &\Leftrightarrow (\neg P \vee \neg Q) \vee R \\
 &\Leftrightarrow \neg(P \wedge Q) \vee R \\
 &\Leftrightarrow (P \wedge Q) \rightarrow R \\
 P \rightarrow (Q \rightarrow P) &\Leftrightarrow \neg P \vee (Q \rightarrow P) \\
 &\Leftrightarrow \neg P \vee (\neg Q \vee P) \\
 &\Leftrightarrow \neg P \vee (P \vee \neg Q) \\
 &\Leftrightarrow (\neg P \vee P) \vee \neg Q
 \end{aligned}$$

Anna University Q & A

43

$$\begin{aligned}
 &\Leftrightarrow T \vee \neg Q \Leftrightarrow T \\
 \neg P \rightarrow (P \rightarrow Q) &\Leftrightarrow P \vee (\neg P \vee Q) \\
 &\Leftrightarrow (P \vee \neg P) \vee Q \\
 &\Leftrightarrow T \vee Q \\
 &\Leftrightarrow T \\
 \therefore P \rightarrow (Q \rightarrow P) &\Leftrightarrow \neg P \rightarrow (P \rightarrow Q)
 \end{aligned}$$

11. (b) (ii) Show that the premise $R \rightarrow \neg Q$, $R \vee S$, $S \rightarrow \neg Q$, $P \rightarrow Q$,
 P are inconsistent.

Answer

1. P Rule P.
2. $P \rightarrow Q$ Rule P
3. Q Rule T from (1), (2)
4. $S \rightarrow \neg Q$ Rule P.
5. $Q \rightarrow \neg S$ Rule T from
6. $\neg S$ Rule T from (3), (5)
7. $R \vee S$ Rule P
8. R Rule T from (6), (7)
9. $R \rightarrow \neg Q$ Rule P
10. $\neg Q$ Rule T from (8), (9)
11. $Q \wedge \neg Q \equiv F$ Rule T from (3), (10)

\therefore The Premises are inconsistent.

44

Discrete Mathematics

12. (a) (i) Prove that

$$(\exists x)(P(x) \wedge S(x)), \forall x(P(x) \rightarrow R(x)) \Rightarrow (\exists x)(R(x) \wedge S(x))$$

Answer

1. $(\exists x)(P(x) \wedge S(x))$ Rule P
2. $P(y) \wedge S(y)$ from (1), ES rule
3. $\forall x(P(x) \rightarrow R(x))$ Rule P
4. $P(y) \rightarrow R(y)$ from (3), US rule
5. $P(y)$ from (2) $P \wedge Q \Rightarrow P$
6. $R(y)$ from (4), (5) Rule T
7. $S(y)$ from (2), $P \wedge Q \Rightarrow Q$
8. $R(y) \wedge S(y)$ from (6), (7)
9. $(\exists x)(R(x) \wedge S(x))$ EG rule from (8)

12. (a) (ii) By indirect method, prove that $\forall x(P(x) \rightarrow Q(x)),$
 $(\exists x)P(x) \Rightarrow (\exists x)Q(x)$

Answer

The negated conclusion $\neg(\exists x)Q(x)$ is taken as an additional premise
 and a contradiction concluded finally

1. $\neg(\exists x)Q(x)$ Additional premise

Anna University Q & A

45

2. $(\forall x) \neg Q(x)$ from (1)
3. $\neg Q(y)$ US rule from (2)
4. $\forall x(P(x) \rightarrow Q(x))$ Rule P
5. $P(y) \rightarrow Q(y)$ US rule from (4)
6. $(\exists x)P(x)$ Rule P
7. $P(y)$ ES rule from
8. $Q(y)$ T rule from (5), (7)
9. $Q(y) \wedge \neg Q(y) \equiv F$ from (3) (8)

\therefore The conclusion is valid

12. (b) (i) Find the scope of the quantifiers and the nature of the occurrence of the variables in the formula $\forall x(P(x) \rightarrow (\exists y)R(x, y))$

Answer

Scope of $\forall x$: $P(x) \rightarrow (\exists y)R(x, y)$

Scope of $\exists y$: $R(x, y)$

Occurrence of x : Bound

Occurrence of y : Bound

46

Discrete Mathematics

12. (b) (ii) Is the following argument valid? All lecturers are determined. Any one who is determined and intelligent will give satisfactory service. Clare is an intelligent lecturer. Therefore Clare will give satisfactory service (Use Predicates)

Answer

$L(x)$: x is a lecturer

$D(x)$: x is determined

$I(x)$: x is intelligent

$S(x)$: x will give satisfactory service

C : Clare

Premises are $(\forall x)(L(x) \rightarrow D(x))$, $(\forall x)(D(x) \wedge I(x) \rightarrow S(x))$

$L(c) \wedge I(c)$. Conclusion: $S(c)$.

To Prove: $(\forall x)(L(x) \rightarrow D(x))$, $(\forall x)(D(x) \wedge I(x) \rightarrow S(x))$

$L(c) \wedge I(c) \Rightarrow S(c)$

1. $(\forall x)(L(x) \rightarrow D(x))$ Rule P
2. $L(c) \rightarrow D(c)$ US rule from (1)
3. $L(c) \wedge I(c)$ Rule P
4. $L(c)$ Rule T, from (3)
5. $D(c)$ Rule T, from (2), (5)

Anna University Q & A

47

6. $I(c)$ Rule T from (3)
7. $D(c) \wedge I(c)$ Rule T from (5), (6) $P, Q \Rightarrow P \wedge Q$
8. $(\forall x)(D(x) \wedge I(x) \rightarrow S(x))$ Rule P
9. $(D(c) \wedge I(c)) \rightarrow S(c)$ US rule, from (8)
10. $S(c)$ Rule T, from (7), (9)

\therefore The argument is valid.

13. (a) (i) Define the relation P on $\{1, 2, 3, 4\}$ by $P = \{(a, b) / |a - b| = 1\}$. Determine the adjacency matrix of P^2

Answer

$$P = \{(1, 2) (2, 1) (2, 3) (3, 2) (3, 4) (4, 3)\}$$

$$P^2 = \{(1, 1) (1, 3) (2, 2) (2, 4) (3, 1) (3, 3) (4, 2) (4, 4)\}$$

$$M_{P^2} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

13. (a) (ii) Let (L, \leq) be a lattice. For any $a, b, c \in L$, if $b \leq c$, Prove that $a * b \leq a * c$ and $a \oplus b \leq a \oplus c$

Answer

$$b \leq c \Rightarrow b * c = b \quad \text{and} \quad b \oplus c = c$$

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

48

Discrete Mathematics

$$\Rightarrow a * b \leq a * c$$

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

$$\Rightarrow a \oplus b \leq a \oplus c$$

13. (a) (iii) In a distributive lattice, show that

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

Answer

$$(a * b) \oplus [(b * c) \oplus (c * a)]$$

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

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

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

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

13. b. (i) If r_1 and r_2 are equivalence relations in a set A , then prove

$r_1 \cap r_2$ is an equivalence relation in A .

Answer

r_1 and r_2 are reflexive.

For every $a \in A, (a, a) \in r_1$ and $(a, a) \in r_2$ is reflexive

$(a, a) \in r_1 \cap r_2 \Rightarrow r_1 \cap r_2$ is reflexive

Let us assume that $(a, b) \in r_1 \cap r_2$

If $(a, b) \in r_1$ and $(a, b) \in r_2$ then $(b, a) \in r_1$ and $(b, a) \in r_2$ since r_1 are

Anna University Q & A

49

r_2 are symmetric

$\therefore (b, a) \in r_1 \cap r_2 \Rightarrow r_1 \cap r_2$ is symmetric

Let $(a, b) \in r_1 \cap r_2$ and $(b, c) \in r_1 \cap r_2$

If $(a, b), (b, c) \in r_1$ and $(a, b), (b, c) \in r_2, (a, c) \in r_1$ and $(a, c) \in r_2$ since r_1 and r_2 are transitive $\therefore (a, c) \in r_1 \cap r_2$

$\therefore (a, b) \in r_1 \cap r_2, (b, c) \in r_1 \cap r_2 \Rightarrow (a, c) \in r_1 \cap r_2$

$r_1 \cap r_2$ is transitive.

Hence $r_1 \cap r_2$ is an equivalence relation.

13. b. (ii) Simplify the Boolean expression

$$((x_1 + x_2) + (x_1 + x_3)) \cdot x_1 \cdot \bar{x}_2$$

Answer

$$((x_1 + x_2) + (x_1 + x_3)) \cdot x_1 \cdot \bar{x}_2$$

$$= (x_1 + x_2 + x_3) \cdot x_1 \cdot \bar{x}_2$$

$$= x_1 \cdot x_1 \cdot \bar{x}_2 + x_2 \cdot x_1 \cdot \bar{x}_2 + x_1 \cdot \bar{x}_2 \cdot x_3$$

$$= x_1 \cdot \bar{x}_2 + 0 + x_1 \cdot \bar{x}_2 \cdot x_3$$

$$= (1 + x_3) x_1 \cdot \bar{x}_2 = x_1 \cdot \bar{x}_2 \cdot 1$$

$$= x_1 \cdot \bar{x}_2$$

50

Discrete Mathematics

13. b. (iii) State and prove the distributive inequalities of a lattice.

Answer

Statement

Let (L, \leq) be a lattice. Then for $a, b, c \in L$, $a \oplus (b * c) \leq (a \oplus b) * (a \oplus c)$ and $a * (b \oplus c) \geq (a * b) \oplus (a * c)$

Proof

(L, \leq) is a lattice. For $a, b, c \in L$, $a \leq a \oplus b$ and $a \leq a \oplus c$

$$\therefore a \leq (a \oplus b) * (a \oplus c) \quad \text{----- (1)}$$

$$b * c \leq b \leq (a \oplus b) \quad \therefore \quad b * c \leq (a \oplus b)$$

$$b * c \leq c \leq (a \oplus c) \quad \therefore \quad b * c \leq (a \oplus c)$$

$$\therefore b * c \leq (a \oplus b) * (a \oplus c) \quad \text{----- (2)}$$

$a \oplus (b * c)$ is the LUB of a and $b * c$

From (1) and (2), $a \oplus b * c \leq (a \oplus b) * (a \oplus c)$

By duality, $a * (b \oplus c) \geq (a * b) \oplus (a * c)$

14. (a) (i) Show that $f : R - \{3\} \rightarrow R - \{1\}$ given by $f(x) = \frac{x-2}{x-3}$ is a bijection.

Answer

$$f(x) = f(y) \Rightarrow \frac{x-2}{x-3} = \frac{y-2}{y-3}$$

Anna University Q & A

51

$$\Rightarrow xy - 3x - 2y + 6 = xy - 3y - 2x + 6$$

$$\Rightarrow x = y$$

$\therefore f$ is 1-1

$$\text{Let } y = \frac{x-2}{x-3} \Rightarrow \frac{2-3y}{1-y}$$

$\therefore \frac{2-3y}{1-y}$ is the preimage of $y \in R - \{1\}$

$\Rightarrow f$ is onto. Hence f is a bijection.

14. a. (ii) Let $f(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in R$. Find $g \circ f$ and $f \circ h \circ g$

Answer

$$(g \circ f)(x) = g[f(x)]$$

$$= g(x+2) = x+2-2 = x$$

$$\therefore (g \circ f)(x) = x \quad \forall x \in R$$

$$f \circ (h \circ g)(x) = f \circ [(h \circ g)(x)]$$

$$= f \circ [h(g(x))]$$

$$= f \circ [h(x-2)] = f(h(x-2))$$

$$= f[3x-6] = 3x-6+2$$

$$= 3x-4$$

52

Discrete Mathematics

14. a. (iii) Let $D(x)$ denote the number of divisors of x . show that $D(x)$ is a primitive recursive function.

Answer

$$r_m(1, x) = 0. [r_m(1, x) \text{ is the remainder when } x \text{ is divided by } 1]$$

$$r_m(2, x) = 0 \text{ or non-zero}$$

$$\Rightarrow r_m(y, x) = 0 \text{ when } y = x$$

$$\text{The number of divisors } D(x) = \sum_{y=1}^x \bar{S}_g r_m(y, x). \text{ Zero test function } \bar{S}_g$$

is primitive recursive

$\therefore D(x)$ is primitive recursive.

14. b. (i) Prove that the set $2P$ of even positive integers has the same cardinality as the set P of positive integers

Answer

Define a mapping $f: P \rightarrow 2P$ by $f(x) = 2x \quad \forall x \in P$

$$f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y \quad \therefore f \text{ is } 1-1$$

$$\text{Let } y \in 2P \quad \therefore y = 2x \Rightarrow x = \frac{y}{2}$$

$$\text{Now } f\left(\frac{y}{2}\right) = y. \quad \therefore \text{For any } y \in 2P, \text{ There is a preimage } \frac{y}{2} \in P$$

$\therefore f$ is onto

$$\text{Hence } f \text{ is a bijection} \Rightarrow N(P) = N(2P)$$

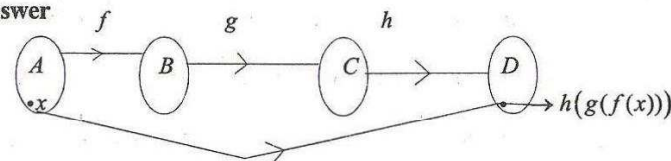
$\therefore P$ and $2P$ have the same cardinality.

Anna University Q & A

53

14. b. (ii) If $f: A \rightarrow B$, $g: B \rightarrow C$ and $h: C \rightarrow D$ are functions, then Prove that $h \circ (g \circ f) = (h \circ g) \circ f$

Answer



$$h \circ (g \circ f) = (h \circ g) \circ f$$

$h \circ (g \circ f)$ and $(h \circ g) \circ f$ are both from A to D

$$\text{Let } x \in A \quad [h \circ (g \circ f)](x) = h \circ (g f(x)) = h(g f(x))$$

$$\text{Similarly } [(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g f(x))$$

$$\therefore h \circ (g \circ f) = (h \circ g) \circ f$$

14. b. (iii) Define even and odd permutations. Show that the

$$\text{permutations } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix} \text{ and}$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \text{ are respectively even and odd.}$$

Answer

Even permutation

A permutation expressed as a product of even number of transpositions

Odd permutation

A permutation expressed as an odd number of transpositions

54

Discrete Mathematics

$$\begin{aligned}
 f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix} \\
 &= (3 \ 7 \ 4 \ 8) \ (1 \ 2 \ 5 \ 6) \\
 &= (3, 8) (3, 7) (3, 4) (1, 6) (1, 5) (1, 2) \\
 &= \text{even no. of transpositions} \Rightarrow f \text{ is even}
 \end{aligned}$$

$$\begin{aligned}
 g &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \\
 &= (1 \ 4 \ 2 \ 3) \\
 &= (1, 3) (1, 2) (1, 4) \\
 &= \text{odd no. of transpositions} \Rightarrow g \text{ is odd}
 \end{aligned}$$

15. a. (i) Show that monoid homomorphism preserves the property of invertibility

Answer

Let $f: (M, *) \rightarrow (H, \Delta)$ be monoid homomorphism.

Let e_1 and e_2 be the identities of M and H

$$f(e_1 * e_1) = f(e_1) \Delta f(e_1) \Rightarrow f(e_1) \Delta f(e_1) = f(e_1)$$

$$f(e_1) \Delta e_2 = f(e_1) \text{ since } e_2 \text{ is the identity}$$

$$\therefore f(e_1) \Delta f(e_1) = f(e_1) \Delta e_2$$

By left cancellation law $f(e_1) = e_2$, For $a \in M$, $a * a^{-1} = e_1$

Anna University Q & A

55

$$\therefore f(a * a^{-1}) = f(e_1)$$

$$f(a) \Delta f(a^{-1}) = e_2$$

$$f(a^{-1}) = [f(a)]^{-1}$$

\therefore The property of invertibility is preserved.

15. a. (ii) Let

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

be a parity check matrix. Determine the

group code $e_H: B^2 \rightarrow B^5$

Answer

$B^2 = \{00, 01, 10, 11\}$ Any element of B^5 is $x_1 \ x_2 \ x_3 \ x_4 \ x_5$

x_1 and x_2 are bits an element of B^2

$$\begin{aligned}
 H = \begin{bmatrix} x_1 & 1 & 1 & 0 \\ x_2 & 0 & 1 & 1 \\ x_3 & 1 & 0 & 0 \\ x_4 & 0 & 1 & 0 \\ x_5 & 0 & 0 & 1 \end{bmatrix} &\Rightarrow \begin{aligned} x_3 &= x_1 \\ x_4 &= x_1 + x_2 \pmod{2} \\ x_5 &= x_2 \end{aligned}
 \end{aligned}$$

$$\therefore e(00) = x_1 x_2 x_3 x_4 x_5 \text{ where } x_1 = 0, x_2 = 0$$

$$\therefore x_3 = 0, x_4 = 0 + 0 = 0, x_5 = 0$$

$$\Rightarrow e(00) = 00000$$

56

Discrete Mathematics

Similarly $e(01) = 01011$

$e(10) = 10110$ and

$e(11) = 11101$

Hence the group code $e_H: B^2 \rightarrow B^5$ is defined by $e(00) = 00000$
 $e(01) = 01011$, $e(10) = 10110$ and $e(11) = 11101$.

15. b. (i) Prove that the intersection of two normal subgroup of a group will be a normal subgroup

Answer

Let H and K be two normal subgroups of a group $(G, *)$.

Let $h \in H \cap K$ and $g \in G$

Then for $g \in G$, $h \in H$, $g^{-1} * h * g \in H$ since H is a normal subgroup

Also for $g \in G$, $h \in K$, $g^{-1} * h * g \in K$

Then $g^{-1} * h * g \in H \cap K$

$\therefore H \cap K$ is a normal subgroup

15. b. (ii) State and prove Lagrange's Theorem.

Statement

Let G be a finite group of order n and H be any subgroup of G . Then $O(H)$ divides $O(G)$.

Proof

Since G is finite and H is a finite subgroup of G , the number of distinct left cosets of H in $G = r$

Anna University Q & A

57

let $O(H) = m$ and $O(G) = n$

Then every left coset has m distinct elements

The left cosets of H are mutually disjoint and their union is the group G .

$\therefore G = (a_1 * H) \cup (a_2 * H) \cup \dots \cup (a_r * H)$

$\Rightarrow O(G) = O(H) + O(H) + \dots + O(H) \text{ (r times)}$

$\therefore n = mr \Rightarrow \frac{n}{m} = r$

$\therefore O(H)$ divides $O(G)$