24MIS1104

P. Ashwath

Discrete Mathematics And Graph Theory

Digital Assignment - 1

Medium : (Tutorial Sheet -1)

1) Prove the logical equivalence

$$\neg(p \wedge q) \rightarrow (\neg p \vee (\neg p \vee q)) \Longleftrightarrow \neg p \vee q$$

Ans) LHS

$\Longleftrightarrow (\neg p \vee \neg q) \rightarrow (\neg p \vee (\neg p \vee q))$

$\Longleftrightarrow (\neg p \vee \neg q) \rightarrow (\neg p \vee q)$

$\Longleftrightarrow (p \wedge q) \vee (\neg p \vee q)$

$\Longleftrightarrow (p \wedge q) \vee \neg p \vee q$

$\Longleftrightarrow \neg p \vee q$ $\quad \because [(p \wedge q) \vee q \equiv q]$

$\therefore$ LHS = RHS Hence Proved.

2) Without constructing the truth table find PDNF and PCNF of $p \rightarrow ((p \rightarrow q) \wedge \neg(\neg q \vee \neg p))$

Ans) $\neg(\neg q \vee \neg p) \equiv q \wedge p \equiv p \wedge q$

$(p \rightarrow q) \wedge \neg(\neg q \vee \neg p) \equiv (p \rightarrow q) \wedge (p \wedge q)$

$\because p \rightarrow q \equiv \neg p \vee q$

$\equiv (\neg p \vee q) \wedge p \wedge q$

$\equiv (p \wedge \neg p) \vee (p \wedge q)$

$\equiv F \vee (p \wedge q)$

$\equiv p \wedge q$

24MIS1104

$\equiv P \to (P \wedge q)$

$\equiv \neg P \vee (P \wedge q)$

$\equiv (\neg P \vee q) \wedge (\neg P \vee q)$

$\equiv T \wedge (\neg P \vee q)$

$\equiv \neg P \vee q$

PCNF $\equiv \neg P \vee q$

PDNF $\equiv \neg P \neg q$

3) Find the PDNF and PCNF of $(\neg A \to C) \wedge (B \leftrightarrow A)$

Ans) $(\neg A \to C) \equiv A \vee C$

$B \leftrightarrow A \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$

$\equiv (A \vee C) \wedge ((A \wedge B) \vee (\neg A \wedge \neg B))$

$\equiv ((A \vee C) \wedge (A \wedge B)) \vee ((A \vee C) \wedge (\neg A \wedge \neg B))$

$\equiv (A \wedge B) \vee (\neg A \wedge \neg B \wedge (A \vee C))$

$(\neg A \wedge \neg B \wedge (A \wedge C)) \equiv (\neg A \wedge A \wedge \neg B) \vee (\neg A \wedge C \wedge \neg B)$

PDNF $\equiv (A \wedge B) \vee (\neg A \wedge \neg B \wedge C)$

PCNF $\equiv (B \vee \neg A) \wedge (A \vee \neg B) \wedge (A \vee C) \wedge (B \vee C)$

4) By indirect method, P.T $\forall x(P(x) \rightarrow Q(x))$, $\exists x\, P(x) \Rightarrow \exists x\, Q(x)$

S.No	Statement	Rules and formulas
1	$\forall x(P(x) \rightarrow Q(x))$	Rule P
2	$\exists x\, P(x)$	Rule P
3	$\neg(\exists x\, Q(x)) = \forall x \neg Q(x)$	Assumed Premise
4	$P(x)$	Rule ES $\{2\}$
5	$P(x) \rightarrow Q(x)$	Rule US $\{1\}$
6	$Q(x)$	Rule T $\{4, 5\}$
7	$\neg Q(x)$	Rule US $\{3\}$
8	$Q(x) \wedge \neg Q(x)$ Contradiction	Rule CP

$\neg(\neg \exists x\, Q(x)) \equiv \exists x\, Q(x)$ follows premises Hence Proved.

24MIS1104

Hard (Tutorial sheet-1)

5) If Jack helps Jill then Jill will do her home work. If Jack does not help Jill then Jill will go to sleep early. If Jill goes to bed early, the teacher will punish Jill. Use CP rule to prove that above hypothesis lead to the conclusion. "If Jill does not do her home work, then the teacher will punish her. Determine whether this argument is valid.

Ans) H : Jack helps Jill
D : Jill does her homework
S : Jill goes to sleep early
P : Teacher punishes Jill

Premises : $H \to D, \neg H \to S, S \to P$, To prove : $\neg D \to P$

S.No	Statement	Rule and formulas
1	$H \to D$	Rule P
2	$\neg H \to S$	Rule P
3	$S \to P$	Rule P
4	$\neg D \to \neg H$	Rule T{1}
5	$\neg D \to S$	Rule T{4,2}
6	$\neg D \to P$	Rule T{5,3}

Hence Proved //

6) P.T $\forall x(P(x) \rightarrow Q(x))$; $\forall x(R(x) \rightarrow \neg Q(x))$
$\Rightarrow \forall x(R(x) \rightarrow \neg P(x))$

Ans)

S.No	Statement	Rules
1	$\forall x(P(x) \rightarrow Q(x))$	Rule P
2	$\forall x(R(x) \rightarrow \neg Q(x))$	Rule P
3	$P(x) \rightarrow Q(x)$	Rule US {1}
4	$R(x) \rightarrow \neg Q(x)$	Rule US {2}
5	$Q(x) \rightarrow \neg R(x)$	Rule T {4}
6	$P(x) \rightarrow R(x)$	Rule T {3, 5}
~~8~~ 7	$R(x) \rightarrow \neg P(x)$	Rule T {6}
8	$\forall x(R(x) \rightarrow \neg P(x))$	Rule UG {7}

Hence Proved //

7) a) Prove by direct method

$p \to q, (\neg q \vee r) \wedge \neg r, \neg(\neg p \wedge s) \Rightarrow \neg s$

S.No	Statement	Rules
1	$p \to q$	Rule P
2	$(\neg q \vee r) \wedge r$	Rule P
3	$\neg q \vee r$	Rule T{2}
4	$\neg r$	Rule T{2}
5	$\neg q$	Rule T{3, 4}
6	$\neg p$	Rule T{1, 5}
7	$\neg(\neg p \wedge s)$	Rule P
8	$p \vee \neg s$	Rule T{7}
9	$\neg s$	Rule {6, 8}

Hence proved //

b) $\neg(p \to q) \to \neg(r \vee s), (q \to p) \vee \neg r, r \Rightarrow p \leftrightarrow q$

S.No	Statement	Rules
1	$\neg(p \to q) \to \neg(r \vee s)$	Rule P
2	$(q \to p) \vee \neg r$	Rule P
3	r	Rule P
4	$r \vee s$	Rule T{3}
5	$(r \vee s) \to (p \to q)$	Rule T{1}
6	$p \to q$	Rule T{4, 5}
7	$q \to p$	Rule T{2, 3}
8	$p \leftrightarrow q$	Rule T{6, 7}

Hence proved //

8) Use rules of inference to show that if $\forall x (P(x) \vee Q(x))$, $\forall x (\neg Q(x) \vee S(x))$, $\forall x (R(x) \rightarrow \neg S(x))$ and $\exists x \neg P(x)$ are true, then $\exists x \neg R(x)$ is true.

Ans)

S.No	Statement	Rules
1	$\forall x (P(x) \vee Q(x))$	Rule P
2	$\forall x (\neg Q(x) \vee S(x))$	Rule P
3	$\forall x (R(x) \rightarrow \neg S(x))$	Rule P
4	$\exists x \neg P(x)$	Rule P
5	$\neg P(x)$	Rule ES $\{4\}$
6	$P(x) \vee Q(x)$	Rule US $\{1\}$
7	$Q(x)$	Rule T $\{5,6\}$
8	$\neg Q(x) \vee S(x)$	Rule US $\{2\}$
9	$S(x)$	Rule T $\{7,8\}$
10	$R(x) \rightarrow \neg S(x)$	Rule US $\{3\}$
11	$S(x) \rightarrow \neg R(x)$	Rule T $\{10\}$
12	$\neg R(x)$	Rule T $\{9,11\}$
13	$\exists x \neg R(x)$	Rule EG $\{12\}$

Hence Proved //

Medium :- Tutorial Sheet - 2

1) If G be an abelian group with identity e, then P.T all elements x of G satisfying the equation $x^2 = e$ forms sub-group H of G.

Ans) (i) Non-empty :

$e * e = e$ Hence $e \in H$ and $H \neq \phi$.

(ii) Closure :

Let $a, b \in H$. then $a * a = e$ and $b * b = e$ using commutativity of G

$$(ab)^2 = abab = aabb = a^2b^2 = e.e = e$$

Thus $ab \in H$.

(iii) Inverse:

Let $a \in H$, then $a^2 = e$. Multiply left by a^{-1} to get $a = a^{-1}$

Hence $a^{-1} \in H$.

By subgroup test, H is a subgroup of G Hence Proved,,

2) If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ are two elements of symetric group. S_6, find $\alpha\beta$, $\beta\alpha$, α^2, β^2, α^{-1} and β^{-1}.

Ans) $\alpha : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 5, 4 \mapsto 4, 5 \mapsto 6, 6 \mapsto 2$

$\beta : 1 \mapsto 5, 2 \mapsto 3, 3 \mapsto 1, 4 \mapsto 6, 5 \mapsto 2, 6 \mapsto 4$

(i) $\alpha\beta$

$1 \xrightarrow{\beta} 5 \xrightarrow{\alpha} 6 \Rightarrow \alpha\beta(1) = 6$

$2 \xrightarrow{\beta} 3 \xrightarrow{\alpha} 5 \Rightarrow \alpha\beta(2) = 5$

$3 \xrightarrow{\beta} 1 \xrightarrow{\alpha} 3 \Rightarrow \alpha\beta(3) = 3$

$4 \xrightarrow{\beta} 6 \xrightarrow{\alpha} 2 \Rightarrow \alpha\beta(4) = 2$

$5 \xrightarrow{\beta} 2 \xrightarrow{\alpha} 1 \Rightarrow \alpha\beta(5) = 1$

$6 \xrightarrow{\beta} 4 \xrightarrow{\alpha} 4 \Rightarrow \alpha\beta(6) = 4$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

(ii) $\beta\alpha$

$1 \xrightarrow{\alpha} 3 \xrightarrow{\beta} 1 \Rightarrow \beta\alpha(1) = 1$

$2 \xrightarrow{\alpha} 1 \xrightarrow{\beta} 5 \Rightarrow \beta\alpha(2) = 5$

$3 \xrightarrow{\alpha} 5 \xrightarrow{\beta} 2 \Rightarrow \beta\alpha(3) = 2$

$4 \xrightarrow{\alpha} 4 \xrightarrow{\beta} 6 \Rightarrow \beta\alpha(4) = 6$

$5 \xrightarrow{\alpha} 6 \xrightarrow{\beta} 4 \Rightarrow \beta\alpha(5) = 4$

$6 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3 \Rightarrow \beta\alpha(6) = 3$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix}$$

(iii) α^2

$1 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 5 \Rightarrow \alpha^2(1) = 5$

$2 \xrightarrow{\alpha} 1 \xrightarrow{\alpha} 3 \Rightarrow \alpha^2(2) = 3$

$3 \xrightarrow{\alpha} 5 \xrightarrow{\alpha} 6 \Rightarrow \alpha^2(3) = 6$

$4 \xrightarrow{\alpha} 4 \xrightarrow{\alpha} 4 \Rightarrow \alpha^2(4) = 4$

$5 \xrightarrow{\alpha} 6 \xrightarrow{\alpha} 2 \Rightarrow \alpha^2(5) = 2$

$6 \xrightarrow{\alpha} 2 \xrightarrow{\alpha} 1 \Rightarrow \alpha^2(6) = 1$

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

(iv) β^2

$1 \xrightarrow{\beta} 5 \xrightarrow{\beta} 2 \Rightarrow \beta^2(1) = 2$

$2 \xrightarrow{\beta} 3 \xrightarrow{\beta} 1 \Rightarrow \beta^2(2) = 1$

$3 \xrightarrow{\beta} 1 \xrightarrow{\beta} 5 \Rightarrow \beta^2(3) = 5$

$4 \xrightarrow{\beta} 6 \xrightarrow{\beta} 4 \Rightarrow \beta^2(4) = 4$

$5 \xrightarrow{\beta} 2 \xrightarrow{\beta} 3 \Rightarrow \beta^2(5) = 3$

$6 \xrightarrow{\beta} 4 \xrightarrow{\beta} 6 \Rightarrow \beta^2(6) = 6$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 3 & 6 \end{pmatrix}$$

v) α^{-1}

1 is image of 2 $\Rightarrow \alpha^{-1}(1) = 2$

2 is image of 6 $\Rightarrow \alpha^{-1}(2) = 6$

3 is image of 1 $\Rightarrow \alpha^{-1}(3) = 1$

4 is image of 4 $\Rightarrow \alpha^{-1}(4) = 4$

5 is image of 3 $\Rightarrow \alpha^{-1}(5) = 3$

6 is image of 5 $\Rightarrow \alpha^{-1}(6) = 5$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

(vi) β^{-1}

1 is image of 3 $\Rightarrow \beta^{-1}(1) = 3$

2 is image of 5 $\Rightarrow \beta^{-1}(2) = 5$

3 is image of 2 $\Rightarrow \beta^{-1}(3) = 2$

4 is image of 6 $\Rightarrow \beta^{-1}(4) = 6$

5 is image of 1 $\Rightarrow \beta^{-1}(5) = 1$

6 is image of 4 $\Rightarrow \beta^{-1}(6) = 4$

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix} //$$

3) The generating matrix of an encoding fn $E = Z_2^3 \to Z_2^6$

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

(i) Find code words assigned 110 and 010
(ii) Obtain associated parity check matrix
(iii) Decode message 111111 by using H

Ans) (i) m = 110

$c = (1,1,0)\ G = [1+0, 0+1, 0+0, 1+0, 1+1, 0+1] \bmod 2$

$= [1,1,0,1,0,1]$

$E(110) = 110101$

m = 010

$c = (0,1,0)\ G = [0,1,0,0,1,1]$

$E(010) = 010011$

(ii) $G = [I_3 | P]$

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$H = [P^T | I_3]$

$$P^T = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(iii) $r = 111111,\ S = Hr^T \pmod 2$

$S_1 = 1+0+1+1+0+0 = 3 \equiv 1$

$S_2 = 1+1+0+0+1+0 = 3 \equiv 1$

$S_3 = 0+1+1+0+0+1 = 3 \equiv 1$

$S = (1,1,1)^T$

$C_1 = (1,1,0)^T$, $C_2 = (0,1,1)^T$, $C_3 = (1,0,1)^T$
$C_4 = (1,0,0)^T$, $C_5 = (0,1,0)^T$, $C_6 = (0,0,1)^T$

none equals $S = (1,1,1)^T$ so it is not a single-bit error

000000 (m = 000)
001101 (m = 001)
010011 (m = 010)
011110 (m = 011)
100110 (m = 100)
101011 (m = 101)
110101 (m = 110)
111000 (m = 111)

The closest codewords are
011110 (m = 011), 101011 (m = 101), 110101 (m = 110)

---

4) Let $f: R^+ \to C^*$ be defined by $f(x) = e^{ix}$, S.T f is a homomorphism ~~(R, +) to~~ Also find kernal of f

Ans) $f: (R, +) \to (C^\times, \cdot)$, $f(x) = e^{ix}$

we must show $f(x+y) = f(x) f(y)$ for all $x, y \in R$

$$f(x+y) = e^{i(x+y)} = e^{ix} e^{iy} = f(x) f(y)$$

So f is a group homomorphism from $(R, +)$ to $(C^\times, \cdot)$.

To find kernal:

$$\ker f = \{x \in R : f(x) = 1\} = \{x \in R : e^{ix} = 1\}.$$

Using Euler's formula $e^{ix} = \cos x + i \sin x$, we have $e^{ix} = 1$ if $\cos x = 1$ and $\sin x = 0 \iff x = 2\pi k, k \in Z$.

Hence, $\ker f = 2\pi n = \{2\pi k : k \in \mathbb{Z}\}$.

Hard : (Tutorial Sheet-2)

5) Prove the code words generated by parity check matrix

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

with $e : B^2 \to B^5$ to parity check check matrix form a group with respect to operation $\oplus$.

Ans) $H_c T = 0$ over F_2

$$\begin{array}{l|l} c_1 + c_4 = 0 & c_3 = c_6 \\ c_1 + c_3 + c_5 = 0 & c_4 = c_2 \\ c_3 + c_6 = 0 & c_7 = c_1 \\ c_1 + c_7 = 0 & c_5 = c_1 + c_3 \end{array}$$

$(0,0,0,0,0,0,0) - (0,0,0)$

$(0,0,1,0,1,1,0) - (0,0,1)$

$(0,1,0,1,0,0,0) - (0,1,0)$

$(0,1,1,1,1,1,0) - (0,1,1)$

$(1,0,0,0,1,0,1) = (1,0,0)$

$(1,0,1,0,0,1,1) - (1,0,1)$

$(1,1,0,1,1,0,1) - (1,1,0)$

$(1,1,1,1,0,1,1) - (1,1,1)$

(i) Closure:-

if $u, v \in C$, then $H(u \oplus v)^T = Hu^T \oplus Hv^T = 0 \oplus 0 = 0$ Thus $u \oplus v \in C$

2) Associativity :-

Bitwise XOR is associative on $\{0,1\}^7$: $(u \oplus v) \oplus w = u \oplus (v \oplus w)$

3) Identity :-

it satisfies $H \cdot 0 = 0$ and $u \oplus 0 = u$ for all u.

4) Inverses :-

For each $u \in C$, $u \oplus u = 0$, so every element is its own inverse. Thus inverse exist in C.

5) Commutative :-

XOR is commutative : $u \oplus v = v \oplus u$, so C is abelian group

6) If G is a multiplicative group of all $(n \times n)$ whose elements are real numbers and G' is multiplicative group of all non-zero numbers, S.T mapping $f: G \to G'$, $f(A) = |A|$, $A \in G$ is a homomorphism

Ans) $f(AB) = f(A) f(B)$ for all $A, B \in G$

$$\det(AB) = \det(A) \det(B)$$

$f(AB) = \det(AB) = \det(A)\det(B) = f(A) f(B)$ hence f is a homomorphism

$$\ker f = \{A \in G \mid f(A) = 1\}$$

$$\ker |f| = \{A \in G\,L_n(R) \mid \det(A) = 1\}$$

It is a subgroup of G

$$Im(f) = \{\det(A) : A \in G\,L_n(R)\}$$

so $Im(f) = R^{\times}$. Thus f is surjective

Hence f is homomorphism, $Ker|f| = SL_n(R)$ and f is surjective onto $R^\times$.

7) Let $(H, *)$ be a subgroup of group $(G, *)$. Let $N = \{x \mid x \in G, xHx^{-1} = H\}$ S.T $(N, *)$ is a subgroup of $(G, *)$.

Ans) Non-empty:

The identity element $e \in G$ satisfies $eHe^{-1} = H$, so $e \in N$

N is non-empty

closure:

$x, y \in N$, $xHx^{-1} = H$ and $yHy^{-1} = H$

$(xy)H(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$

$yHy^{-1} = H$ and $x(\cdot)x^{-1}$ sends H to H. Thus $xy \in N$.

So N is closure

Inverse:

$x \in N$ $\quad xHx^{-1} = H$ $\quad$ conjugate. BT by x^{-1}

$x^{-1}(xHx^{-1})x = x^{-1}Hx = H$

$(x^{-1}x)H(x^{-1}x) = H$

$H = x^{-1}Hx$; $xHx^{-1} = H$

Hence $x^{-1}Hx = H$ says $x^{-1} \in N$. So N contains inverse.

$\therefore$ It is a subgroup of G.

X – X – X