Tutorial - 2 (U20CS108)
(OZA DHAIRYA M)

1) * (i) Hamming distance :- The no. of position at which the digits are different in two different elements of is known as hamming distance.

* $x_1, x_2 \in B^5$, Let $x_1 = 10101$ and $x_2 = 01110$
$\therefore d(x_1, x_2) = \begin{matrix} 10101 \\ 01110 \end{matrix} = 4$

(ii) Hamming weight :- let $x \in B^n$, then no. of 1 in x is known as hamming weigh of x'

$x \in B^5$, $10011 \rightarrow 3 \rightarrow w(x)$

(iii) Minimum distance of a set (or Code) :- Let $a, b \in C$ then $\forall$ such a and b pair having the least distance among the set is known as minimum distance of a set

(iv) Minimum weight of a set (or code) :- Let $a \in C$ then Minimum weight is basically have least no of 1 in the set C.

(v) Generator matrix :- Let $x \in B^m$ where B^m is our message grp. then $\exists$ 'G' is such that $xG = y$, where $y \in C$ and $C \leq B^n$ where B^n is our word grp and 'C' is our code word grp. then 'G' is generator matrix.

(vi) Parity check matrix :- Let $x \in B^n$ where B^n is our word group then $\exists$ 'H' Such that $xH^T = 0$ if $x \in C$ and $xH^T \neq 0$ if $x \notin C$

Where, 'C' is our code word grp i.e, $C \leq B^n$
Then 'H' is known as parity check matrix.

(vii) Codewords :- images of a corresponding maped message through an encoding functions are codewords

(viii) Code :- The set of all the codewords.

(ix) Group code :- If set of all Code-word is group then it's called group code.

(x) Encoding function :- One-One function mapping all message to their corresponding codewords is known as encoding function.

(xi) Message :- all elements of message group are known as message.

(xii) Undetectable error :- errors which are beyond the error dectection capacity are known as undetectable errors.

(2) $G = \begin{bmatrix} 100110 \\ 010011 \\ 001101 \end{bmatrix}_{3\times 6}$, $B^3 = \{000, 001, 010, 100, 011, 101, 110, 111\}$

→ $[000]G = 000000$
$[001]G = 001101$
$[010]G = 010011$
$[100]G = 100110$
$[011]G = 011110$
$[101]G = 101011$
$[110]G = 110101$
$[111]G = 111000$

∴ $H = \begin{bmatrix} A^T \\ \hline I_{(n-m)} \end{bmatrix}_{(n-m)\times n}$, $G = \begin{bmatrix} I_m \mid A \end{bmatrix}_{m\times n}$

∴ $A = \begin{bmatrix} 1&1&0 \\ 0&1&1 \\ 1&0&1 \end{bmatrix} \rightarrow A^T = \begin{bmatrix} 1&0&1 \\ 1&1&0 \\ 0&1&1 \end{bmatrix}$

$H = \begin{bmatrix} 101100 \\ 110010 \\ 011001 \end{bmatrix}_{3\times 6} \rightarrow H^T \begin{bmatrix} 1&1&0 \\ 0&1&1 \\ 1&0&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{bmatrix}_{6\times 3}$

→ all the coset leaders:- 100000, 010000, 001000, 000100, 000010, 000001, 100001

(i) $[110101][H^T] = [000]$, ∴ 110101 is a code word.

(ii) $[001111][H^T] = [01]$

→ as we know that ~~w = v ± c~~ $w = v + c$ $\boxed{\therefore c = w - v}$

∴ $c = 001111 - 000010$
∴ 001101 is our code word.

(iii) $[110001][H^T] = [100]$

∴ $c = 110001 - 000100 = 110101$ is our code word.

(iv) $[111111][H^T] = [111]$

∴ $c = 111111 - 100001 = 011110$ is our code word.

(3) $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3 \times 6}$

$\therefore$ Code word $\in C \leq B^6$

→ Let $x_1\, x_2\, x_3\, x_4\, x_5\, x_6 \in C$

$\therefore [x_1\, x_2\, x_3\, x_4\, x_5\, x_6] H^T = [0]$

→ $[x_1\, x_2\, x_3\, x_4\, x_5\, x_6] \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0]$

→ $x_1 + x_2 + x_3 + x_4 = 0$
$x_1 + x_3 + x_5 = 0$
$x_2 + x_3 + x_6 = 0$

→ Here, 3 variables must be free variables then Let's suppose x_2, x_3, x_4.

→ $x_1 = x_2 + x_3 + x_4$ — (1)
→ $x_5 + x_1 = x_3$
→ $x_5 = x_2 + x_4$ — (2)
→ $x_6 = x_2 + x_3$ — (3)

We have, $[x_2 + x_3 + x_4,\ x_2,\ x_3,\ x_4,\ x_2 + x_4,\ x_2 + x_3]$

→ $x_2 = 0,\ x_3 = 0,\ x_4 = 0$
$[0, 0, 0, 0, 0, 0] \to 000000$

→ $x_2 = 0,\ x_3 = 0,\ x_4 = 1$
$[1, 0, 0, 1, 1, 0] \to 100110$

→ $x_2 = 0,\ x_3 = 1,\ x_4 = 0$

$[1, 0, 1, 0, 0, 1] \to 101001$

→ $x_2 = 0,\ x_3 = 1,\ x_4 = 1$

$[0, 0, 1, 1, 1, 1] \to 001111$

→ $x_2 = 1,\ x_3 = 0,\ x_4 = 0$

$[1, 1, 0, 0, 1, 1] \to 110011$

→ $x_2 = 1,\ x_3 = 0,\ x_4 = 1$

$[0, 1, 0, 1, 0, 1] \to 010101$

Same $\therefore C = \{000000, 100110, 101001, 001111, 110011, 010101, 011010, 111100\}$

$\therefore W : \{0, 3, 3, 4, 4, 3, 3, 4\}$

→ Min. distance in the above code is $\boxed{3}$

$\therefore$ error detecting capacity $= d_{min} - 1 = \boxed{2}$

$\therefore$ error correcting capacity $= \frac{d_{min} - 1}{2} = \boxed{1}$

(5) $e : B^2 \to B^5$

$00 \to 00000$
$01 \to 01110$
$10 \to 10101$
$11 \to 11011$

+	000000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	10011	10101
10101	10101	11011	0000	01110
11011	11011	10101	01110	00000

→ from table, ~~Group~~ Code follows closure property so $e : B^2 \to B^5$ is a group code.

(5) $H = \{0, 3, 6, 9, 12\}$ $G = \{0, 1, 2, 3 \ldots, 14\}$

no. of distinct cosets $= \frac{o(G)}{o(H)} = \frac{15}{5} = 3$

$\therefore$ $0 +_{15} H = \{0, 3, 6, 9, 12\}$

$\therefore$ $1 +_{15} H = \{1, 4, 7, 10, 13\}$

$\therefore$ $2 +_{15} H = \{2, 5, 8, 11, 14\}$

(6) $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / \forall\, a, b, c, d \in R \right\}$

$\therefore$ We have a map $D : M \to R$

Let $M_1, M_2 \in M$

$\rightarrow M_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$D(M_1) = (a_1 d_1 - b_1 c_1)$ and $D(M_2) = (a_2 d_2 - b_2 c_2)$

also, we know that M is a grp under addition.

$\therefore$ $M_1 + M_2 = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in M$

$\therefore$ $D(M_1 + M_2) = (a_1 + a_2)(d_1 + d_2) - (b_1 + b_2)(c_1 + c_2)$

$\therefore$ $D(M_1 + M_2) = D(M_1) + D(M_2) + (a_1 d_2 + a_2 d_1 - c_1 b_2 - c_2 b_1)$

$\therefore$ $D(M_1 + M_2) \neq D(M_1) + D(M_2)$.

$\rightarrow$ So $D : M \to R$ is not a homomorphism.

(7) $\phi : G \to G'$

where, $G \to$ Set of all non-zero real nos

$G' \to \{1, -1\}$

$\phi = \left\{ \begin{matrix} R^+ \to 1 \\ R^- \to -1 \end{matrix} \right\}$

- Let take three cases, for $R_1, R_2 \in R-\{0\}$

(i) $R_1 \in R^+$ and $R_2 \in R^+$

(ii) $R_1 \in R^-$ and $R_2 \in R^-$

(iii) $R_1 \in R^+$ and $R_2 \in R^-$ or $R_1 \in R^-$ and $R_2 \in R^+$

(i) $\phi(R_1) = 1$ and $\phi(R_2) = 1$

also, $R_1 \times R_2 \in R^+$

$\therefore$ $\phi(R_1 \times R_2) = 1 = \phi(R_1) \times \phi(R_2)$

$\therefore$ for this case ϕ is a homomorphism

(ii) $\phi(R_1) = -1$ and $\phi(R_2) = -1$

also, $R_1 \times R_2 \in R^+$

$\therefore$ $\phi(R_1 \times R_2) = +1 = \phi(R_1) \times \phi R_2$

$\therefore$ for this case ϕ is a homomorphism

(iii) $R_1 \in R^+$ and $R_2 \in R^-$

$\therefore$ $\phi(R_1) = 1$
$\phi(R_2) = -1$

also $R_1 \times R_2 \in R^{-1}$

$\therefore$ $\phi(R_1 \times R_2) = -1 = \phi(R_1) \times \phi(R_2)$

$\therefore$ ϕ is homomorphism.

→ For all cases, ϕ is homomorphism.

(8) $\phi : G \to G'$

$Im(\phi) = \{ \phi(x) \mid x \in G \} \leq G'$

Let $a, b \in G$

∴ as ϕ is homomorphism,

$$\phi(a *_1 b) = \phi(a) *_2 \phi(b) \quad - (1)$$

where, $\phi(a)$, $\phi(b)$ and $\phi(a *_1 b) \in Im(\phi)$

→ due to eq-(1), $Im(\phi)$ is closed under $*_2$ → It follows closure property.

$$[\phi(a)]^{-1} = \phi(a^{-1}) \quad - (2)$$

→ due to eq-(2), for all element of $Im(\phi)$, there exist inverse member for it.

∴ as $Im(\phi)$ follows 'closure and Inverse' for $*_2$ it's subgroup of 'G'. $\boxed{\therefore Im(\phi) \leq G'}$

(9) We have $H = \{(x, 3x) \mid x \in R\}$ and $G = R^2$

→ $G \rightarrow$ Cartesian co-ordinate
$H \rightarrow y = 3x$

$\therefore H = \{(x, y) \mid x \in R,\ y = 3x\}$

$\therefore$ the coset $(3, 7) + H = \{(x+3), (y+7) \mid x \in R, y = 3x\}$

here $X = x + 3$
$Y = y + 7 \rightarrow y = Y - 7$

$\therefore (3, 7) + H = \{(x, y) \mid x \in R,\ y = 3x\}$

$Y = 3X$
$y + 7 = 3(x + 3)$
$\therefore y = 3x + 2$

$\therefore$ the coset $(3, 7) + H$ represents $y = 3x + 2$ line

$\therefore$ as we can see that the slope of the line is equal.

→ $y = 3x \parallel y = 3x + 2$

(10) $C = \{0000000, 1110100, 0111010, 0011101, 1001110, 0100111, 1010011, 1101001\}$

→ It's group code because it follows closure property.

$w(1110100) = 4$

$w(0111010) = 4$

$w(0011101) = 4$

$w(1001110) = 4$

$w(0100111) = 4$

$w(1010011) = 4$

$w(1101001) = 4$

→ min distance = 4 (the one which have least!)

$\therefore$ error detecting capacity of $C = 4 - 1$ (dmn)

$= \boxed{3}$

$\therefore$ error correcting capacity of $C = \frac{4}{2} = \boxed{2}$