U20CS110 [Krishna Pandey]

Date / /
Page No.

29/8/21

Tutorial - 2

1 (i) Hamming distance: the number of positions at which the digits are different in 2 different elements of B^n is k/a Hamming distance

★ Example:- $x_1, x_2 \in B^5$
∴ let $x_1 = 10101$ and $x_2 = 01110$
∴ $d(x_1, x_2) = 4$

(ii) Hamming weight:- Let $x \in B^n$, then the no. 1's in x is known as Hamming weight of x.
Ex- $x \in B^{10}$
Let $x = 1001011101$
∴ $w(x) = 6$

(iii) Minimum distance of a set (or a code)
Let $x_1, x_2 \in C$ then $\forall$ x_1 and x_2 pair having the least distance among the set (or code) is known as minimum distance of a set or code.

(iv) Minimum weight of a set (or a code)
Min weight of a set (or code) is equal to the weight of an element $x \in C$ which is having the least no. of 1's in the set 'C'.

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

then G is a generator matrix

(vi) Parity check matrix :- Let $x \in B^n$ when B^n is our word group, then $\exists$ 'H' such,
$$xH^T = 0 \text{ if } x \in C \text{ and } xH^T \neq 0$$
if $x \notin C$
where 'C' is our code word group i.e. $C \subseteq B^n$
then 'H' is known as parity check matrix.

(vii) Codewords :-
images of a corresponding messages mapped through an encoding function are known as code words

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

(ix) Group Code :- If the set of all the code words is a group then it is called as group code.

(x) Encoding function
An 1-1 function mapping all the message to their corresponding code words is known as an encoding function.

(xi) Message :- all the elements of our message grp are known as message

(xii) Undetectable error :- errors which are beyond the error detectn capacity.

Date / /
Page No.

Sol-2 $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{3\times 6}$

also $B^3 = [000, 001, 010, 100, 011, 101, 110, 111]$

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

$\therefore$ Code $C = \{000000, 100110, 010011, 001101, 011110, 101011, 110101, 111000\}$

as we know that $H = [A^T / I_{(n-m)}]_{(n-m)\times n}$
and $G = [I_m / A]_{m\times n}$

$\therefore A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, $A^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

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

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

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

(1) 110101

$[110101]H^T = 000$
110101 is a code word

(2) 001111
$[001111]H^T = [010]$

$\therefore$ as we know that $w = v + c$

$\Rightarrow c = w + v$

$\therefore c = 001111 + 000010$
$= 001101$ is our code word

(3) 110001
$[110001]H^T = [100]$

$c = 110001 + 000100$
$= 110101$ is our code word

(4) 111111
$[111111]H^T = [111]$

$c = 111111 + 100001$
$= 011110$ is our code word
the last word is not decoded uniquely due to possibility of having more than 1 coset leaders

Sol - 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 $\in C \subseteq B^6$

$$x_1, x_2, x_3 - - - x_6 \in C$$

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

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

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

3 variable must be free variable
let x_2, x_3, x_4 are free variables

then
$$x_1 = x_2 + x_3 + x_4 \quad - (1)$$
$$x_5 = x_2 + x_4 \quad - (2)$$

$$x_6 = x_2 + x_3 \quad - (3)$$

$\therefore$ we have $[x_2 + x_3 + x_4,\ x_2,\ x_3,\ x_4,\ x_2 + x_4,\ x_2 + x_3]$

$\Rightarrow$ $x_2 = 0, \quad x_3 = 0, \quad x_4 = 0$
$[0,0,0,0,0,0] \Rightarrow 000000$

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

$\Rightarrow$ $x_2 = 0, x_3 = 1, x_4 = 0$
$[1,0,1,0,0,1] \Rightarrow 101001$

$\Rightarrow$ $x_2 = 0 \quad x_3 = 1, x_4 = 1$
$[0,0,1,1,1,1]$ 001111

$\Rightarrow$ $x_2 = 1, x_3 = 0, x_4 = 0$
$[1,1,0,0,1,1]$ 110011

$\Rightarrow$ $x_2 = 1, x_3 = 0 \quad x_4 = 1$
$[0,1,0,1,0,1]$ 010101

$\Rightarrow$ $x_2 = 1, \quad x_3 = 1, \quad x_4 = 0$
$[0,1,1,0,1,0]$ 011010

$x_2 = 1, \quad x_3 = 1, \quad x_4 = 1$
$[1,1,1,1,0,0]$ 111100

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

also $w(100110) = 3$ $\quad w(010101) = 3$
$w(101001) = 3$ $\quad w(011010) = 3$
$w(001111) = 4$ $\quad w(111100) = 4$
$w(110011) = 4$

$\therefore$ min distance in above code is $\boxed{3}$

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

and error correcting capacity $= \dfrac{d_{min} - 1}{2}$
$= 1$

(4) $e : B^2 \longrightarrow B^5$

B^2	B^5
00	00000
01	01110
10	10101
11	11011

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

clearly our code follows closure property

$\therefore e : B^2 \rightarrow B^5$ is a group code.

Sol - 5 $H = \{0, 3, 6, 9, 12\}$, $G = \{0, 1, 2, 3, --- 14\}$

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

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

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

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

Sol - 6

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

$\therefore$ we have a map $D : M \longrightarrow R$

let $M_1, M_2 \in M$

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

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

also, we know that 'M' is grp under addition

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

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

$= [(a_1 d_1 + a_1 d_2 + a_2 d_1 + a_2 d_2) - (c_1 b_1 + c_1 b_2 + c_2 b_1 + c_2 b_2)]$

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

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

$\therefore$ $D: M \longrightarrow R$ is not a homomorphism.

Sol-7 we have $\phi: G \rightarrow G'$
where $G \rightarrow$ set of all non-zero real no.
$G' = \{1, -1\}$

$$\phi = \begin{Bmatrix} R^+ \rightarrow 1 \\ R^- \rightarrow -1 \end{Bmatrix}$$

let take 3 cases, for $R_1, R_2 \in \mathbb{R} - \{0\}$

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

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

(3) $R_1 \in R^+$ and $R_2 \in R^-$ or vice versa

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

~~$\phi \in R$~~ 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 $R_1 \times R_2 \in R^+$

$\phi(R_1 \times R_2) = +1 = \phi(R_1) \times \phi(R_2)$
for this case ϕ is a homomorphism

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

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

$R_1 \times R_2 \in R^-$

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

for above case ϕ is homomosphism,

Hence for all case ϕ is a Homomorphism
proved

Sol-8 We have $\phi : G \longrightarrow G'$

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

$\Rightarrow$ Let $a, b \in G$

$\therefore$ as 'ϕ' is a Homomorphism

$$\boxed{\phi(a *_1 b) = \phi(a) *_2 \phi(b)} \quad \text{— ①}$$

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

$\therefore$ due to eqn -①, $Im(\phi)$ is closed under '$*_2$'
It follows closure property

$\Rightarrow$ also, $a, a^{-1} \in G$ such that $a *_1 a^{-1} = e$
where e is identity of G

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

$\therefore$ due to eq^n - (2) for all elements of Im (ϕ), there exist inverse member for it.

$\therefore$ as Im (ϕ) follows 'Closure' and 'inverse' property under $*_2$, it is a subgroup of 'G''.

$$\therefore \boxed{Im(\phi) \leq G'}$$

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

$\Rightarrow$ Here 'G' represent our Cartesian cood. and 'H' represent $y = 3x$ line on it

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

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

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

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

$$Y = 3X$$

$$y + 7 = 3(x + 3)$$

$$\boxed{y = 3x + 2}$$

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

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

$\Rightarrow$ $y = 3x$ is parallel to $y = 3x + 2$

Sol-10 We have

$$C = \{0000000, 1110100, 0111010, 0011101, \\ 1001110, 0100111, 1101001\}$$

as the above code follows the closure property, it is a group code.

also, $w(1110100) = 4$
$w(0111010) = 4$
$w(0011101) = 4$
$w(1001110) = 4$
$w(0100111) = 4$
$w(1010011) = 4$
$w(1101001) = 4$

$\therefore$ ~~min~~ distance $= 4$

$\therefore$ error - detecting capacity of $C = 4 - 1 = 3$

and the error - correcting capacity of $C = \frac{4}{2} = 2$