Linear Codes

$C = i \cdot G$ $\quad$ $i \rightarrow$ Info. vector $\quad$ $c \rightarrow$ codeword

$G \rightarrow$ ~~generator matrix~~ generator matrix

(5,3) $\quad G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$

000 — 00000

001 — 01110

111 — 10011

$\Big\}$ matrix mult.

① In linear codes, one code word will be consist of zero vector
000 — 00000

② If there exist 2 code word c_i & c_j then $C_K = C_i + C_j$
(summation of any 2 code word generate a valid codeword)

③ Mini. hamming weight $d(Y_n)$ = min hammi wt of non zero codeword

(3,2) even parity code

C_0	0 0 0
C_1	0 1 1
C_2	1 0 1
C_3	1 1 0

	C_0	C_1	C_2	C_3
C_0	C_0	C_1	C_2	C_3
C_1	C_1	C_0	C_3	C_2
C_2	C_2	C_3	C_0	C_1
C_3	C_3	C_2	C_1	C_0

~~i.e. even parity~~

(3,2) odd parity code.

C_0	0 0 1
C_1	0 1 0
C_2	1 0 0
C_3	1 1 0

$C_0 + C_1 = 011$ (not valid)

(Consider always even parity)

(always consider parity bit for any key)

(3,2) even parity code

$d(Y_n) = \min d(c_i, c_j)$ $\quad c_i \neq j)$

$C_1 C_2 C_3$ are non zero codewords

	C_0	C_1	C_2	C_3
C_0	0	2	2	2
C_1	2	0	2	2
C_2	2	2	0	2
C_3	2	2	2	0

$d(Y_n) = 2$

$d(Y_n)$ can also be computed as → find HD of ~~C_0~~ $C_1 C_2 C_3$ then ans is min

① Construct (7,4) Hamming code

② Prove that (7,4) Hamming code is a linear code :

③ ~~Find~~ write the algorithmic steps to compute basis vector of any given set,

④ Find the basis vector of (7,4) Hamming code

Submit on Friday.

Basis vector

$u_1, u_2 \, --- \, u_n$

$\bar{u}_1, \bar{u}_2 \, --- \, \bar{u}_m \qquad m < n$

$v_1 = w_1 \bar{v}_1 + w_2 \bar{v}_2 + \cdots + w_n \bar{v}_n$

G is collection of basis vector

Systematic code ~~cor~~ word : redundant bits and ~~code word~~ info bits can be identified (in order)

$G = [I / P]$

G we can convert G to look like $[I / P]$

$e \rightarrow v$

syndrome, $s = v \cdot H^T$

$H \rightarrow$ Parity check matrix

if $s = (0, --- 0)$ then valid, no error

if $s \neq (0 --- 0)$ then invalid, error

$G \cdot H^T = 0$

$G = [I / P] \qquad H = [P^T | I]$

(5,3)

$$G_{3\times 5} = [I_3 / P] = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

canonical represen

$G_{k \times n}$

$H_{(n-k) \times n}$

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

$$H = \left[\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \middle| I_2 \right]$$

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

$G \cdot H^T = 0$

zero matrix — no error

non zero — error

6 Sep 2019

(3, 2)

c_0	00	000
c_1	01	011
c_2	10	101
c_3	11	110

Theorem 1: A block code K_n detect upto t errors if and only if its minimum distance is greater than t.

$$d(\mathcal{Y}_n) > t$$

eg. even parity $2 > t \Rightarrow 2 > 1$ ↳ single bit error

Proof. ⇒ If b is the received code word and a^* is corresponding valid codeword ~~and rest~~ of b ~~then~~

Assumption. $d(b, a_i) > 0$ (if any error is present)

$d(a^*, b) + d(b, a_i) \geq d(a^*, a_i)$ → triangle inequality.

~~d(b,~~ $d(b, a_i) \geq d(a^*, a_i) - d(a^*, b)$

$\therefore$ $d(a^*, a_i) - d(a^*, b) > 0$

$d(a^*, b) = t$ if t is the error

~~d(a*, a~~ $d(\mathcal{Y}_n) > d(a^*, b)$

$d(\mathcal{Y}_n) > t$

Error Correction Property

1. A block code A_n correct upto t bits of error if and only if $d(\mathcal{Y}_n) > 2t$

$d(b, a^*) = t$

$d(b, a^*) < d(b, a_i) \quad \forall i$

~~$d(a^*, b) + d(b, a_i) \geq d(a^*, a_i)$~~

~~$\Rightarrow d(a^*, b) \geq d(a^*, a_i) - d(b, a_i)$~~

~~$d(a^*, a_i) - d(b, a_i) \leq d(a^*, b)$~~

~~$d(a^*, a_i) - d(b, a_i) < d(b, a_i)$~~

$d(b, a_i) > d(b, a^*)$

$d(a^*, b) + d(b, a_i) \geq d(a^*, a_i)$

$\cancel{d(b, a_i) \geq d(a^*, a_i) - d(a^*, b)}$ (1)

$\cancel{d(a^*, a_i) - d(a^*, b) > d(a^*, a_i)}$

$\cancel{d(a^*, a_i) > 2d(a^*, b)}$

$\cancel{d(C_n) > 2t}$

$d(a^*, b) + d(b, a_i) \geq d(a^*, a_i)$

$d(b, a_i) \geq d(a^*, a_i) - d(a^*, b)$

incomplete

⇒ $C = i \cdot G$

$G = [I | P]$

$H = [P^T | I]$

$G \cdot H^T = 0$

if H.D = 2 then error corrected upto 1 bit.

The Standard Array : 2D array.

combination ~~that if~~ of valid & invalid codewords.

Size (n, k)

$c_0 \quad c_1 \quad c_2 \quad c_3 \; --- \; c_{n-1}$ ← valid codeword.

$w_0 \quad c_0 + w_0 \quad c_1 + w_0$

w_1

w_2

error vectors

if $v \cdot H^T = 0$ then $v \to$ valid code word.

⇒ $v \cdot H^T = i \cdot G H^T = i \cdot 0 = 0$

if $v \to$ not valid:

$= (c + e) \cdot H^T$ $e \to$ error pattern

$= c \cdot H^T + e H^T$

$= e H^T$ (depends on error pattern)

dis: if n,k very large then huge table ⇒ huge memory
So not a good mechanism for ~~find~~ decoding

Syndrom Error Table

$S = v \cdot H^T = e \cdot H^T$

(7,4) Hamming code ⇒ single bit error

So, error pattern possible =

$$\left.\begin{array}{l} 0000001 \cdot H^T = \\ 0000010 \cdot H^T = \\ 0000100 \cdot H^T = \\ 0001000 \cdot H^T = \\ 0010000 \cdot H^T = \\ 0100000 \cdot H^T = \\ 1000000 \cdot H^T = \end{array}\right\} \text{syndrom value}$$

for decoding :
→ find $S = v \cdot H^T$
→ then find s value in syndrom table.
→ If syndrom is matched then its corresponding is the error

$v = c + e$
$c = v + e$ } modulo 2 ~~expo~~ add.

→ then find $c = v + e$.

eg. (6,3) $G = \begin{bmatrix} 100 & 101 \\ 010 & 011 \\ 001 & 110 \end{bmatrix}$

i	codeword	H.D
000	000000	0
001	001110	3
010	010011	3
011	011101	4
100	100101	3
101	101011	4
110	110110	4
111	111000	3

X

codeword = sum of those row whose bit position is 1 in X

$C = i \cdot G$

$H = \begin{bmatrix} 101 & 100 \\ 011 & 010 \\ 110 & 001 \end{bmatrix}$

$u = 100110$

$e.$

Syndrom table: $000001 \cdot H^T = 001$

$000010 \quad 010$

$000100 \quad 100$

$001000 \quad 110$

$010000 \quad 011$

$100000 \quad 101$

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

$S = v \cdot H^T = 011$

$= \cancel{011}$

$= 010000$ (error)

$c = 100110 + 010000$

$= 110110$