25. Linear Block Codes

- $(n, k) = (k+r, k)$ code

- $$\underline{c} = [\underbrace{b_0\ b_1 \cdots b_{r-1}}_{r=n-k \text{ parity bits}} \vdots \underbrace{m_0\ m_1 \cdots m_{k-1}}_{k \text{ message bits}}]$$

$$= [\underline{b} \vdots \underline{m}]$$

- $\boxed{\text{systematic code}}$: the first k transmitted bits are information bits

- $$b_0 = p_{00} m_0 \oplus p_{10} m_1 \oplus \cdots \oplus p_{k-1,0}\, m_{k-1}$$

$$b_1 = p_{01} m_0 \oplus p_{11} m_1 \oplus \cdots \oplus p_{k-1,1}\, m_{k-1}$$

$$\vdots$$

$$b_{r-1} = p_{0,r-1} m_0 \oplus \cdots \oplus p_{k-1,r-1}\, m_{k-1}$$

$$p_{ij} = \begin{cases} 1 & \text{if } b_i \text{ depends on } m_j \\ 0 & \text{otherwise} \end{cases}$$

- $\underline{b} = \underline{m}\, P$

$P_{k\times r}$ coefficient matrix

$$P_{k \times r} = \underbrace{\begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,r-1} \\ p_{10} & & & p_{1,r-1} \\ \vdots & & & \\ p_{k-1,0} & & & p_{k-1,r-1} \end{bmatrix}}_{r \text{ columns}} \left.\vphantom{\begin{bmatrix}a\\a\\a\\a\end{bmatrix}}\right\} k \text{ rows}$$

- $$\boxed{\underline{c} = [\underline{b} \vdots \underline{m}] = \underline{m}\, [P \vdots I_k]}$$

where $I_k = \begin{bmatrix} 1 & 0 & 0 \cdots 0 \\ 0 & 1 & 0 \cdots 0 \\ 0 & \cdots & 1 \end{bmatrix}$

k × k identity matrix

Generator matrix

$$G = [P : I_k]$$

$$\Rightarrow \boxed{\underset{1\times n}{\underline{c}} = \underset{1\times k}{\underline{m}}\ \underset{k\times n}{G}}$$

- $\underline{b} = \underline{m}\,P$

$$\underset{1\times r}{\underline{b}} \oplus \underset{1\times k}{\underline{m}}\,\underset{k\times r}{P} = \underset{1\times r}{\underline{0}}$$

$$\underline{b}\,I_r \oplus \underline{m}P = \underline{0} \qquad \therefore I_r - r\times r \text{ identity matrix}$$

$$[\underline{b} : \underline{m}]\,H^T = \underline{0}$$

where H = parity check matrix $(r \times n)$

$$\boxed{H = [I_r : P^T]}$$

$$\Rightarrow \boxed{c\,H^T = 0} \quad \text{parity check equations}$$

- Can also show $G H^T = H G^T = 0$
- <u>Syndrome</u> <u>decoding</u>

Let $\underline{r}$ = received word $= c \oplus e$

where e = error vector

$$\underline{e} = [e_1 \ \dots \ e_n]$$

$$e_k = \begin{cases} 1 & \text{if error in } k^{th} \text{ location} \\ 0 & \text{otherwise} \end{cases}$$

i) If $\underline{r}H^T = 0 \Rightarrow \underline{r}$ is a codeword

(in max. likelihood sense)

= minimum distance

ii) If $\underline{r} H^T \neq \underline{0} \Rightarrow \underline{r}$ is <u>not</u> a codeword and at least 1 error has been made

iii) Since $\underline{r} = c \oplus e$

If we know $\underline{e}$, can reconstruct $\underline{c}$ from $\underline{r}$ and $\underline{e}$

iv) $\boxed{\underset{\substack{\Uparrow \\ 1\times r \\ \text{syndrome}}}{\underline{s}} = r H^T} = (c \oplus e) H^T = \underset{\substack{\Downarrow \\ 0}}{cH^T} \oplus e H^T$

$= e H^T$

If $\underline{s} = 0 \Rightarrow \underline{e} = 0 \Rightarrow$ no error (most likely)

If $\underline{r}$ has one error in the j^{th} position

$$\underline{e} = [0\ 0 \cdots \underset{\substack{\downarrow \\ j^{th}\text{ column}}}{1}\ 0 \cdots 0]$$

$$\underline{s} = e H^T = \underset{1\times n}{[0\ 0 \cdots 1\ \ 0 \cdots 0]} \underset{n \times r}{\boxed{\begin{bmatrix} I_r \\ \cdots \\ P \end{bmatrix}}}$$

$$= \boxed{j^{th} \text{ row of } H^T}$$

- <u>Decoding Procedure</u>

Identify the column no. 'j' of H which corresponds to $\underline{s} = \underline{r} H^T$ and correct the j^{th} position of $\underline{r}$.

Ex:

$$H = \begin{array}{c} \begin{array}{ccccccc} b_0 & b_1 & b_2 & m_0 & m_1 & m_2 & m_3 \end{array} \\ \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right] \end{array}$$

$r \times n$ $\Rightarrow k = 4$:
3×7

2^4 equi. probable messages $[m_0 m_1 m_2 m_3]$

- $\underline{c} H^T = \underline{0}$

$b_0 = m_0 \oplus m_1 \oplus m_2$

$b_1 = m_0 \oplus m_1 \oplus m_3$

$b_2 = m_0 \oplus m_2 \oplus m_3$

e.g. If $\underline{m} = [m_0\ m_1\ m_2\ m_3] = [1\ 0\ 0\ 0]$

$b_0 = b_1 = b_2 = 1$

$\Rightarrow \underline{c} = [1\ 1\ 1\ 1\ 0\ 0\ 0]$

Let $\underline{r} = [1\ 1\ 1\ 1\ 0\ 1\ 0]$
↑ error in 6^{th} position

$\underline{s} = r H^T = [1\ 0\ 1] \Rightarrow 6^{th}$ row of H^T
or 6^{th} column of H

$\Rightarrow$ error in 6^{th} position of $\underline{r}$

$\Rightarrow$ corrected word is $1111\,0\,\underline{\underline{0}}\,0$

- What is the special advantage of binary code, in error correction?

- Note : $2^r - 1 = n$ in example.

- For syndrome to give unambiguous determination, each column of H must be distinct and no column consists of all zeros.
- Why is "all-zero" column not allowed?
- (n, k) code $\quad r = n - k$

H matrix : r rows : 2^r possibilities

$$\underbrace{\boxed{2^r - 1 \geq n}}_{\text{all-zero case}} \quad \text{to be distinct}$$

$$2^{(n-k)} - 1 \geq n \quad \text{or} \quad (n-k) \geq \log_2 (n+1)$$

$$n \geq k + \log_2 (n+1)$$

Given 'k' $\rightarrow$ can determine min. 'n'

<u>Ex</u>: Construct an H matrix for a single-error correcting $(6, 3)$ systematic parity check code. Write out parity check equations, allowed code words.
What happens when there are 2 errors?

- $2^3 - 1 \geq 6 \Rightarrow$ can have distinct columns of H
- $$H = \begin{bmatrix} \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{r} & \underbrace{\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{matrix}}_{k} \end{bmatrix} \Bigg\} r$$

- $\underline{c} = [b_0\ b_1\ b_2\ m_0\ m_1\ m_2]$
- $\underline{c} H^T = \underline{0} \Rightarrow b_0 = m_1 \oplus m_2$;

  $b_1 = m_0 \oplus m_2$; $b_2 = m_0 \oplus m_1$
- <u>Code words</u> :

b_0	b_1	b_2	m_0	m_1	m_2
0	0	0	0	0	0
1	1	0	0	0	1
1	0	1	0	1	0
0	1	1	0	1	1
0	1	1	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
0	0	0	1	1	1

- $d \geq 3$ for single error correction.
  d_{min} = min. no. of columns of H that add up to zero vector

- $\underline{c} = [000\ 000]$; let $\underline{r} = [000\ 110]$

  $\underline{s} = \underline{r} H^T = [1\ 1\ 0] \rightarrow 6^{th}$ column of H

  indicates 6^{th} digit of $\underline{r}$ to be wrong

  corrected word $\Rightarrow [000\ 111]$

  $\Rightarrow$ 3 errors made !
- Note $\begin{bmatrix}1\\1\\0\end{bmatrix} = \oplus$ sum of 4 & 5^{th} columns of H
- $\underline{s}^T$ will be $\oplus$ sum of 2 corresponding columns of H which generally equals another column of H, so a correct digit is changed giving a net result of 3 errors.

- 2 errors bring $\underline{r}$ closer to another codeword.
- To correct more than 1 error, not only every column of H be distinct and non-zero, but certain vector sums of columns must be distinct.
- To correct 't' or fewer errors,
  i) all sums of t or fewer columns must be distinct from all other sums of 't' or fewer columns.
  ii) all sums of t or fewer columns do not sum to zero.

- $\underline{\text{Hamming}}$ $\underline{\text{codes}}$ (n, k) block codes with $d_{min} = 3$.
  - H matrix is $\underset{(n-k)}{r} \times 2^r - 1$

e.g. (7, 4) Hamming code

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

$\underbrace{\qquad\qquad}_{I_r}$ $\qquad P^T$

$k = 4 \Rightarrow 2^k = 16$ messages

- If $\underline{r} = [1100010]$, what is the decoded word?
- $r H^T = [0 0 1] \rightarrow 3^{rd}$ column of H
  $\Rightarrow$ decoded word is $[1110010]$