Lecture 43

Linear block codes:

$$\underset{k \text{ bits}}{\xrightarrow{\underline{m}}} \boxed{\begin{matrix}\text{Linear} \\ \text{Encoder}\end{matrix}} \underset{n \text{ bits}}{\xrightarrow{\underline{c}}}$$

$\underline{m} = [m_1 \; m_2 \; \cdots \; m_k]$

$\underline{c} = [c_1 \; c_2 \; \cdots \; c_n]$

c_i = XOR of bits of $\underline{m}$

$= m_{i_1} \oplus m_{i_2} \oplus \cdots \oplus m_{i_d}$

$\longrightarrow$ Linear code

Systematic encoder

$1 \leq i \leq k$

$c_i = m_i$

$k+1 \leq i \leq n$

$c_i = m_{i_1} \oplus \cdots \oplus m_{i_d}$

Ex: (1) Repetition code $= \{000, 111\}$

$k=1, \; n=3$

$$c_1 = m_1$$
$$c_2 = m_1$$
$$c_3 = m_1$$

(2) Even parity code

$k = 7 \qquad n = 8$

$$c_i = m_i \qquad 1 \le i \le 7$$

$\underline{c}$: even # of 1s

$$c_8 = m_1 \oplus m_2 \oplus \cdots \oplus m_7$$

Notation: (n, k) Code

Size of code $=$ # of codewords $= 2^k$

$R = k/n$

(3) (7, 4) Hamming Code

$$c_i = m_i \qquad 1 \le i \le 4$$

$$c_5 = m_1 \oplus m_2 \oplus m_3$$

$$c_6 = m_1 \oplus m_2 \oplus m_4$$

$$c_7 = m_2 \oplus m_3 \oplus m_4$$

Generator matrix:

$$\underbrace{\underline{c}}_{1 \times n} = \underbrace{\underline{m}}_{1 \times k} \underbrace{G}_{k \times n}$$

Ex:

$$c_1 = m_1$$
$$c_2 = m_2$$
$$c_3 = m_3$$
$$c_4 = m_4$$

$$\underline{c} = \underline{m} \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Ex: (3, 1) repetition code

$$G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Ex: (8, 7) even parity code

$$G = \left[\begin{array}{c|c} I_7 & 1_7 \end{array} \right]$$

Parity-check matrix:

$$c_i = m_i \qquad 1 \leq i \leq k$$

$$k+1 \leq i \leq n \qquad c_i = c_{i_1} \oplus c_{i_2} \oplus \cdots \oplus c_{i_d}$$

$$c_i \oplus c_{i_1} \oplus c_{i_2} \oplus \cdots \oplus c_{i_d} = 0$$

$n-k$ equations

Ex: (7,4) Hamming

$$c_5 = c_1 \oplus c_2 \oplus c_3$$
$$c_6 = c_1 \oplus c_2 \oplus c_4$$
$$c_7 = c_2 \oplus c_3 \oplus c_4$$

H : parity-check matrix

$$\left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right] \underline{c}^T = \underline{0}_3^T$$

Dim: $n-k \times n$

null space (H) = rowspace (G) = Code

$n-k \times n$ $\qquad$ $k \times n$

$$H = [P^T \mid I_{n-k}] \longleftrightarrow G = [I_k \mid P]$$

P: $k \times n-k$

Ex: (3,1) repetition code

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

Ex: (8,1) repetition code

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad H = \left[\begin{array}{c|c} 1_7^T & I_7 \end{array}\right]$$

Ex: (8,7) even parity code

$$G = \left[\begin{array}{c|c} I_7 & 1_7^T \end{array}\right] \qquad H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

__Ex:__ (7,4) Hamming Code

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

$$\left.\begin{array}{ll} \text{Code:} & \text{can be computed.} \\ \text{Encoder:} & \text{can be implemented} \end{array}\right\} ?$$

__Minimum distance:__

(n,k) linear code $C = \{\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_M\}$

$M = 2^k$

$$d = \min_{\substack{1 \le i,j \le M \\ i \ne j}} \underline{\underline{d_H}}(\underline{c}_i, \underline{c}_j)$$

$\underline{u} = [u_1 \cdots u_n]$ $\underline{v} = [v_1 \cdots v_n]$

$d_H(\underline{u}, \underline{v}) =$ # of positions where $\underline{u}$ and $\underline{v}$ differ

$$= \left| \{ 1 \le i \le n : u_i \ne v_i \} \right|$$

$w_H(\underline{u}) =$ # of 1s in $\underline{u}$

$$d_H(\underline{u}, \underline{v}) = w_H(\underline{u} \oplus \underline{v})$$

$$d = \min_{\substack{1 \le i,j \le M \\ i \ne j}} d_H(\underline{c}_i, \underline{c}_j) = w_H(\underbrace{\underline{c}_i \oplus \underline{c}_j}_{\substack{\parallel \\ \underline{c}_\ell \text{ for} \\ \text{some } 1 \le \ell \le M}})$$

$$= \min_{\underline{c} \in \mathcal{C}} w_H(\underline{c})$$

Ex: $(n, 1)$ repetition code

$$d = n$$

Ex: $(n, n-1)$ even-weight code

$$d = 2$$

$$H = [\underbrace{1\,1 \cdots\cdots 1\,1}_{n \text{ 1s}}]$$