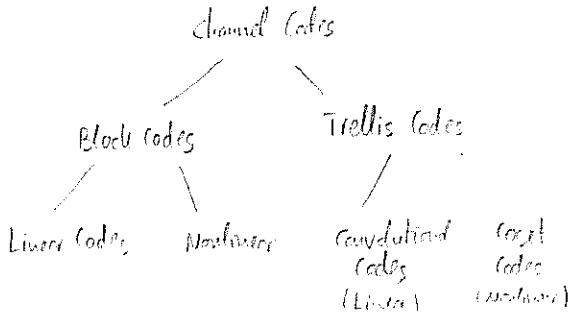
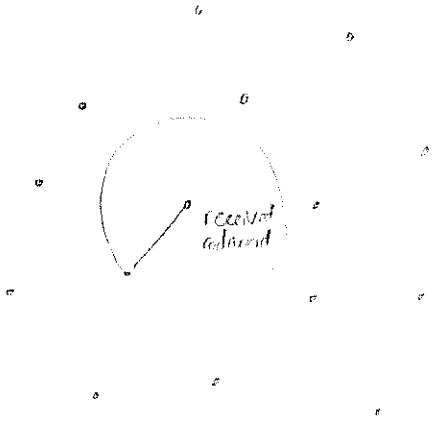
Error Control Coding





Hamming code

$$P_1\ P_2\ m_3\ P_4\ m_5\ m_6\ m_7$$

$$P_1 = m_3 + m_5 + m_7$$
$$P_2 = m_3 + m_6 + m_7$$
$$P_4 = m_5 + m_6 + m_7$$

$$(c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7) = (m_3\ m_5\ m_6\ m_7)\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Suppose that an error occured at bit 6

$$P_1 = 0$$
$$P_2 = 1$$
$$P_4 = 1$$

$$P_4\ P_2\ P_1 \rightarrow (1\ 1\ 0)_2 \rightarrow (6)_{10}$$

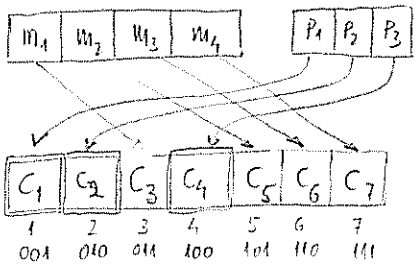
$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} = \begin{bmatrix} \not{1} & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} m_3 \\ m_5 \\ m_6 \\ m_7 \end{bmatrix}$$

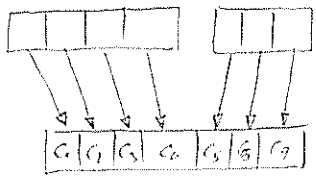
$$\begin{bmatrix} P_1 & P_2 & P_3 \end{bmatrix} = \begin{bmatrix} m_3 & m_5 & m_6 & m_7 \end{bmatrix} \begin{bmatrix} \not{1} & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$p = m\ P$$

$$c = m \cdot G = [I : P]$$

Hamming Code





$C_1 = P_1 = C_3 + C_5 + C_7$

$C_2 = P_2 = C_3 + C_6 + C_7$

$C_4 = P_3 = C_5 + C_6 + C_7$

$S = (C_4 \cdot 4 + C_2 \cdot 2 + C_1 \cdot 1)$

error at position 6 $\quad C_4 = 0 \quad C_2 = 1 \quad C_1 = 1$

$S = 6 \rightarrow$

$C_5 = C_1 + C_2 + C_3$

$C_6 = C_2 + C_3 + C_4$

$C_7 = C_1 + C_2 + C_4$

$C_1 + C_2 + C_3 + C_5 = 0$

$C_2 + C_3 + C_4 + C_6 = 0$

$C_1 + C_3 + C_4 + C_7 = 0$

$$\left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right] \cdot \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_7 \end{bmatrix} = 0$$

$C_1 + C_3 + C_5 + C_7 = 0$

$C_2 + C_3 + C_6 + C_7 = 0$

$C_4 + C_5 + C_6 + C_7 = 0$

$C = (C_1\ C_2 \dots C_7)$

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

$$\left[P^T ; I_{n-k}\right] \cdot \begin{bmatrix} m^T \\ P^T \end{bmatrix} = 0$$

$P^T \cdot m + P = 0$

$P^T \cdot m^T = P^T$

$P = mP$

$C = [m \quad P]$

$C = [mI_k \quad mP] = m[I_k ; P]$

$C = m\,G \qquad G = [I_k ; P]$

$H = [P^T ; I_{n-k}]$

$C \cdot H^T = 0$

$r = C + e$

$S = r \cdot H^T = C \cdot H^T + e H^T$

$S = e H^T$

There are $2^{n-k} - 1$ different syndromes can reveal any single error

$k = 2^{n-k} - 1 - (n-k)$

Parity Check Matrix and Generator Matrix

Hamming code — it can correct a single error
because all the columns are different

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} P^T_{n-k \times k} & I_{n-k} \end{bmatrix}$$

↙ a systematic form

$$c = [c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7]_{1\times n}$$

$$H_{n-k \times n}\, c^T_{n\times 1} = 0_{n-k\times 1}$$

$$c_{1\times n}\, H^T_{n\times n-k} = 0_{1\times n-k}$$

$$[P^T\ I] \cdot c^T = 0 \qquad c = [m\ \ p]$$

$$[P^T\ I] \cdot \begin{bmatrix} m^T \\ p^T \end{bmatrix} = 0$$

$$P^T m^T + I p^T = 0$$

$$p^T = P^T \cdot m^T$$

$$p = m P$$

$$c = [m\ \ mP] = m_{1\times k}[I\ P]$$

$$c = mG \qquad G = [I_k\ P_{k\times n-k}]$$

m_1	m_2	m_3	m_4	p_1	p_2	p_3
0	0	0	0	0	0	0
0	0	0	1	1		
0	0	1	0	1		
0	0	1	1	0		
0	1	0	0			
0	1	0	1			
0	1	1	0			≥ 3
0	1	1	1			
1	0	0	0			
1	0	0	1			
1	0	1	0			≥ 3
1	0	1	1			
1	1	0	0			
1	1	0	1			
1	1	1	0			
1	1	1	1			

d_{min}

$c_{min}\, H^T = 0$

- -

- -

$$rank(H) = d_{min} - 1$$

$$rank(H) \leq n-k$$

Minimum distance of a linear code

— A linear code always have a all-zero codeword
— A sum of two codewords is also a codeword

$$d_{min} = \min \{ d(u,v) : u, v \in C, u \neq v \}$$

minimum distance

$$w_{min} = \min \{ w(v) : v \in C, v \neq 0 \}$$

minimum weight

$$d_{min} = \min \{ d(u,v) : u, v \in C, u \neq v \}$$

$$= \min \{ w(u+v) ; u, v \in C, u \neq v \}$$

$$= \min \{ w(x) ; x \in C, x \neq 0 \}$$

$$= w_{min}$$

C_w - minimum weight codeword

$C_w \cdot H^T = 0$ — C_w is a codeword

$C_w H^T = 0 \Rightarrow$ d_{min} columns of H are linearly dependent

$$d_{min} = rank(H) + 1$$

$$d_{min} \leq n - k + 1$$

↖ Singleton bound

Let A_i be the number of codewords in C with Hamming weight i

The set $\{ d_0, d_1, \ldots, d_n \}$ is called the weight distribution or spectrum of C

$$A_0 = 1$$

$$A_0 + A_1 + \ldots + A_n = 2^k$$

Cyclic Codes

$$c = m\,G$$

$$c = m_{1\times k}\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k-1} & & \\ & g_0 & \cdots & & g_{n-k-1} & \\ & & & \ddots & & \\ & & & g_0 & g_1 & \cdots & g_{n-k-1} \end{bmatrix}_{k\times n}$$

$$m(X) = m_0 + m_1 X + \dots + m_{k-1}X^{k-1}$$

$$c(X) = c_0 + c_1 X + \dots + c_{n-1}X^{n-1}$$

$$g(X) = g_0 + g_1 X + \dots + g_{n-k-1}X^{n-k-1}$$

$$c(X) = \begin{bmatrix} m_0 & m_1 & \cdots & m_{n-k-1} \end{bmatrix}\begin{bmatrix} g(X) \\ X\,g(X) \\ \\ X^{n-k-1}g(X) \end{bmatrix}$$

$$c(X) = m_0 g(X) + m_1 X g(X) + \dots + m_{n-k-1}X^{n-k-1}g(X)$$

$$c(X) = (m_0 + m_1 X + \dots + m_{n-k-1}X^{n-k-1})\,g(X)$$

$$c(X) = m(X)\,g(X)$$

$$H\,G^T = 0 \quad \Rightarrow \quad h(X)g(X) = X^n + 1$$

An (n,k) linear block code is said to be cyclic if for every codeword c there is a codeword c' so that

$$c = (c_0, c_1, \dots, c_{n-1})$$
$$c' = (c_{n-1}, c_0, \dots, c_{n-2})$$

$$Xc(X) = c_0 X + c_1 X^2 + \dots + c_{n-1}X^n + c_{n-1} + c_{n-1}$$

$$Xc(X) = c_{n-1} + c_0 X + c_1 X^2 + \dots + c_{n-2}X^{n-1} + c_{n-1}(1+X^n)$$

$$Xc(X) = c'(X) + c_{n-1}(1+X^n)$$

$$\frac{Xc(X)}{1+X^n} = c_{n-1} + \frac{c'(X)}{1+X^n}$$

$$c'(X) = Xc(X) \mod (X^n+1)$$

$$c\,H^T = 0$$

$$c(X)h(X) = 0 \mod (X^n+1)$$

$$h(X)g(X) = X^n + 1$$

Example

cyclic code of length 7

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}_{k \times n}$$

$$x^7 + 1 = x + 1$$

$$H = \begin{bmatrix} & & \\ & & \end{bmatrix}$$

GCD $(x^7+1,\ x+1)$

$$x^7 + 1 \quad x + 1 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$x^7 + x^6$

$x^6 + 1$

$-x^6 + x^5$

$x^5 + 1$

$x^5 + x^4$

$x^4 + 1$

$x^4 + x^3$

$x^3 + 1$

$x^3 + x^2$

$x^2 + 1$

$x^2 + x$

$x + 1$

$x + 1$

0

$0\ g(x) = c_0(x) = 0$

$1\ g(x) =$

$$x^7 + 1 = (x+1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \ ; \ x^3 + x^2 + 1 = x^3 + x + 1$$

$x^6 + x^5 + x^3$

$x^4 + x^3 + x + 1$

$x^4 + x^3 + x$

$x^2 + x^2 + 1$

$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x + 1)$$

$$g(x) = (x+1)(x^3 + x + 1) = x^4 + x^2 + x + x^3 + x + 1$$

$$= x^4 + x^3 + x^2 + 1$$

$$h(x) = x^3 + x^2 + 1$$