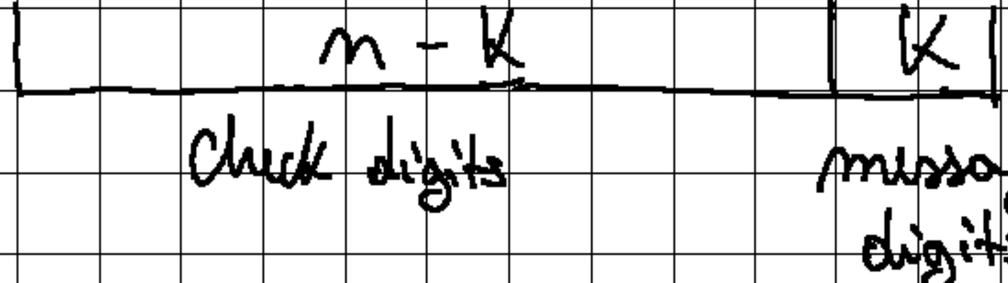
Message : k bits long

Encoded message : n bits long $\quad n > k$

$\gamma : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ - encoder

$\mathbb{Z}_2 = \{0,1\}$



Linear code if γ is a linear map

$$\gamma(m_1 + m_2) = \gamma(m_1) + \gamma(m_2)$$

$C = \operatorname{Im}\gamma \leq \mathbb{Z}_2^n$

↳ the of codewords

$G = [\gamma]_{E,E'}$

generator matrix

- we use it to encode messages

$$[\gamma(m)]_{E'} = [\gamma]_{E,E'} \cdot [m]_E$$

$$G = \begin{pmatrix} P \\ I_k \end{pmatrix}$$

$H = (\, i_{n-k} \mid P \,)$

↳ parity check matrix

$v \in \mathbb{Z}_2^n$ is a codeword $\iff H \cdot [v]_{E'} = 0$

$v, v' \in \mathbb{Z}_2^n$, $d_H(v, v') =$

= number of positions where v, v' disagree =

$= w(v - v') =$ number of 1's in $v - v'$

↳ weight

$d_H(101001, 111010) = 3$

$d(C) = \min d_H(v, v')$, $v, v' \in C$

↳ minimum Hamming distance

A linear code can detect at most $d(C) - 1$ errors and at most $\left\lfloor \frac{d(C)-1}{2} \right\rfloor$ can be corrected

(⌊ ⌋ floor)

To find $d(C)$:

$d(C)$ = minimal number of columns of H that add up to a zero column.

5&6. Determine the minimum Hamming distance between the codewords of the code with generator matrix $G = \begin{pmatrix} P \\ I_4 \end{pmatrix} \in M_{9,4}(\mathbb{Z}_2)$ where

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

Discuss the error-detecting and error-correcting capabilities of this code and encode 1101, 0111, 0000, 1000.

$$H = \left(\begin{array}{ccccc:cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right)$$

there is no zero column $\Rightarrow$ $d(C) > 1$

no identical column $\Rightarrow$ $d(C) > 2$

$C_3 + C_5 + C_6 = 0 \Rightarrow d(C) = 3$

the code can detect

$3-1=2$ errors

and it can correct

$\left\lfloor \frac{3-1}{2} \right\rfloor = 1$ error

$$G \cdot [m_1]_E = \left(\frac{P}{I_4}\right) \cdot [m_1]_E = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\gamma(0111)_{E'} = G \cdot (0111) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

$$[\gamma(1010)]_{E'} = G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$[\gamma(1000)]_{E'} = G \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The (n,k) polynomial code generated by

$p \in \mathbb{Z}_2[x]$ if $\deg p = n-k \Rightarrow$ the code is linear

Ex: $n=5$, $k=3$

$p = x^2+x$

Step 1: Write the polynomial f_m associated to the message m

$m = \overline{a_0 a_1 \dots a_{k-1}} \rightsquigarrow f_m = a_0 + a_1 x + \dots + a_{k-1} x^{k-1}$

$m = 101 \rightsquigarrow f_m = 1 + x^2$

Step 2: multiply f_m by x^{n-k}

$g_m = f_m \cdot x^{n-k}$

$g_m = (1+x^2)x^2 = x^4 + x^2$

Step 3: divide g_m by p (euclidian division)

$g_m = p \cdot q + r_m$

$x^4+x^2 \mid x^2+x$

$x^4+x^3 \mid x^2+x$

x^3+x^2

0

$r_m = 0$

Step 4: Add R_m to g_m and convert it back to a vector

$$R_m + g_m = x^4 + x^2$$

$$\longrightarrow v = 00\underline{101}$$

Step 5: already

$$m = 101$$

8. Find G and H for the (7,3) code generated by $p = 1 + x^2 + x^3 + x^4 \in \mathbb{Z}_2[x]$

$m = 100 = 1$

Step 2: $1 \cdot x^4 = x^4$

Step 3:

$$\begin{array}{r|l} x^4 & x^4 + x^3 + x^2 + 1 \\ \hline x^4 + x^3 + x^2 + 1 & 1 \\ \hline R_m = x^3 + x^2 + 1 & \end{array}$$

Step 4: $R_m + g_m = x^4 + x^3 + x^2 + 1$

Step 5: 1011100

$$G = [\gamma]_{\mathcal{E},\mathcal{B}'} = \left([\gamma(e_1)]_{\mathcal{E}'}, [\gamma(e_2)]_{\mathcal{E}'}, [\gamma(e_3)]_{\mathcal{E}'} \right)$$

$m = \overline{010} \Rightarrow g_m = X$

$g_m = X \cdot X^4 = X^5$

$X^5 : X^4+X^3+X^2+1 = X+1$

$X^5+X^4+X^3+X$

$X^4+X^3+X^2+1$

X^2+X+1

$r_m + g_m = X^5 + X^2 + X + 1$

$v = 1110010$

$m = 001 = X$

Step 2 $X^2 \cdot X^4 = X^6$

Step 3:

$X^6 : X^4+X^3+X^2+1 = X^2+X$

$X^6+X^5+X^4+X^2$

$X^5+X^4+X^2$

X^3+X^2+X

$R_m = X$

$R_m + g_m = X^6 + X^3 + X^2 + X$

01110001

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$H = (I_4 \mid P) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

There are no zero columns, no identical columns and no two columns sum up to a third therefore $d(C) \geq 3$

$C_1 + C_3 + C_4 + C_7 = 0 \Rightarrow d(C) = 4 \Rightarrow$

$\Rightarrow$ it can detect 3 errors and correct $\frac{3}{2} = 1$ err.