Seminar 12

Error correcting codes

(n, k) code

n ‖ encoded message

k : the lenght of the message

$m \in \mathbb{Z}_2^k \xrightarrow{\text{encode}}$ encoded vector $v \in \mathbb{Z}_2^n$

$\underbrace{(x_0, x_1, \dots x_{k-1})}_{\text{binary digits}}$ $\qquad (y_0, y_1, \dots, y_{n-k-1}, x_0, x_1, \dots x_{k-1})$

$\downarrow$ channel

decode $\nwarrow$ $\quad v \xleftarrow[\text{correction}]{\text{error}} v'$ (output vector)

the (n, k) code is linear if its encoding function $\gamma : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ is linear, i.e:

$\forall m_1, m_2 \in \mathbb{Z}_2^k : \gamma(m_1 + m_2) = \gamma(m_1) + \gamma(m_2)$

$(\forall) \alpha \in \mathbb{Z}_2, (\forall) m \in \mathbb{Z}_2^k : \gamma(\alpha m) = \alpha \cdot \gamma(m)$

$G := [\gamma]_{E,E'} = ([\gamma(e_1)]_{E'} \dots [\gamma(e_k)]_{E'})$

$\downarrow$

generator matrix of the code

$\Rightarrow$ the encoding can be done by $[v]_{E'} = G \cdot [m]_E$

$G = \left(\dfrac{M}{I_k}\right) \in \mathcal{M}_{n,k}(\mathbb{Z}_2)$

$H = (I_{n-k} \mid M) \in \mathcal{M}_{n-k,k}(\mathbb{Z}_2)$

$\downarrow$

the parity check matrix (role in correcting)

Polynomial codes. The (n,k) – p. code generated by a polynomial $p \in \mathbb{Z}_2[x]$

Here's how we encode:

Step 1: $m = (a_0, \dots a_{k-1}) \rightsquigarrow P_m = \underbrace{a_0 + a_1 x + \dots + a_{k-1} x^{k-1}}$

we identify it with the initial message

Step 2: $Q_m = P_m \cdot x^{n-k}$

Step 3: We devide Q_m by p : $\underset{\text{divident}}{Q_m} = \underset{\text{divisor}}{p} \cdot \underset{\text{quotient}}{q} + R_m$ – remainder

Step 4: The encoded polynomial is $T_m = Q_m - R_m \underset{=}{=} Q_m + R_m$

Step 5: $T_m = b_0 + \dots + b_{n-1} x^{n-1}$

we get the encoded vector $v = (b_0, \dots b_{n-1})$

ex: Let us encode the message $m = (1,1,0)$ by using the $(6,3)$ code generated by the poly $p = 1 + x^2 + x^3 \in \mathbb{Z}_2[x]$

1. $m = (1,1,0) \longrightarrow P_m = 1 + x$

2. $Q_m = P_m \cdot x^3 = x^4 + x^3$

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

$\Rightarrow R_m = x$

4. $T_m = x + x^4 + x^3$

5. $v = (0,1,0,1,1,0)$ – 6 digits because of $(\underline{\underline{6}},3)$ code

ex 12.2 Determine the G and the H for the (7,5) code generated by the poly $P = 1+x^2+x^3+x^4 \in \mathbb{Z}_2[x]$

I for $u = (1,0,0) \to P_u = 1$

$\theta_u = P_u \cdot x^{n-k} = 1 \cdot x^4 = x^4$

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

$\Rightarrow R_u = x^3+x^2+1 \Rightarrow T_u = \theta_u + R_u = x^4+x^3+x^2+1 \Rightarrow v = (1,0,1,1,1,0,0)$

II for $u = (0,1,0) \to P_u = x$

$\theta_u = P_u \cdot x^{n-k} = x \cdot x^4 = x^5$

$$\begin{array}{r|l} x^5 & x^4+x^3+x^2+1 \\ \cline{2-2} x^5+x^4+x^3+x & x+1 \\ \hline x^4+x^3+x & \\ x^4+x^3+x^2+1 & \\ \hline x^2+x+1 & \end{array}$$

$\Rightarrow R_u = x^2+x+1 \Rightarrow T_u = x^5+x^2+x+1 \Rightarrow v = (1,1,1,0,0,1,0)$

III for $u = (0,0,1) \Rightarrow P_u = x^2$

$\theta_u = P_u \cdot x^{n-k} = x^2 \cdot x^4 = x^6$

$$\begin{array}{r|l} x^6 & x^4+x^3+x^2+1 \\ \cline{2-2} x^6+x^5+x^4+x^2 & x^2+x \\ \hline x^5+x^4+x^2 & \\ x^5+x^4+x^3+x & \\ \hline x^3+x^2+x & \end{array}$$

$\Rightarrow R_u = x^3+x^2+x \Rightarrow T_u = \theta_u + R_u = x^6+x^3+x^2+x \Rightarrow v = (0,1,1,1,0,0,1)$

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to I_3$$

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

G linear map, $\mathcal{C}$ = set of codewords in our code, $\mathcal{C} \leq_{\mathbb{Z}_2} \mathbb{Z}_2^n$

$d_H(v,v')$ = no of positions where v and v' disagree, $(\forall)\, v,v' \in \mathbb{Z}_2^n$

the Hamming distance

$= w(v+v')$

the no of 1's

$d(\mathcal{C}) = \min\limits_{v,v' \in \mathcal{C}} d_H(v,v')$

the minimum Hamming distance

$d(\mathcal{C})$ = minimal no of coulumns in H that add up to 0

Th: For a linear code $\mathcal{C}$ we can detect at most $d(\mathcal{C})-1$ errors and we can correct at most $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor$ errors

ex 12.5 Determine $d(\mathcal{C})$ if $G=\left(\frac{P}{I_n}\right) \in \mathcal{M}_{9,4}(\mathbb{Z}_2)$ where

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

. Find H and discuss the error-detecting and error-correcting capabilities of this code

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

no 0 columns $\Rightarrow d(\mathcal{C})>1$

no identical columns

$\Rightarrow d(\mathcal{C})>2$

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

$d(\mathcal{C})-1 = 3-1 = 2$ detectable errors

$\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$ correctable error