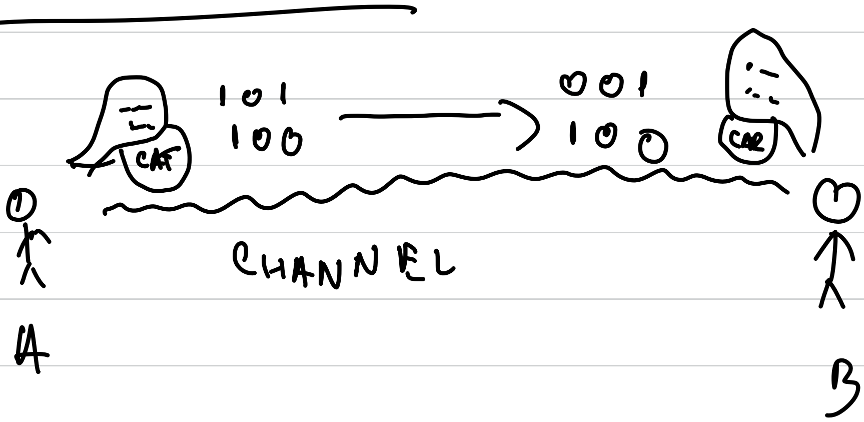
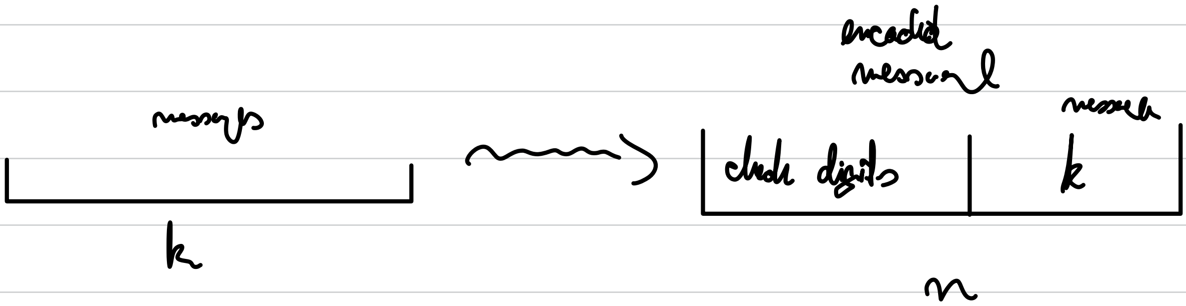
Seminar 12

Linear codes



(n, k) codes

$$\underset{\text{message}}{m \in \mathbb{F}_2^k} \rightsquigarrow \underset{\text{encoded message}}{v \in \mathbb{F}_2^n}$$



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

The encoding is done by means of an encoder function:

$$\gamma : \mathbb{F}_2^K \to \mathbb{F}_2^n$$

Linear code = codes where we have γ a linear map

$$\underbrace{\operatorname{Im} \gamma}_{\text{L}} \leq_{\mathbb{F}_2} \mathbb{F}_2^n$$

L = C = space of codewords for the code

We define the generator matrix

$$G = [\gamma]_{EE'} =$$

$$= \left([\gamma(e_1)]_{E'} \middle| \dots \middle| [\gamma(e_k)]_{E'} \right)$$

The encoding is done through:

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

$$= G \cdot [m]_E$$

Due to how we encode:

$$G = \left(\frac{P}{I_k} \right) \in M_{n,k}(\mathbb{F}_2)$$

This allows us to define the parity check matrix

$$H = \left(I_{n-k} \mid P \right)$$

We use it to check for codeword, so if $v \in \mathbb{F}_2^n$:

$$v \in C \iff H \cdot [v]_{E} = 0$$

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

$d_H(v, v') = \#$ of positions where v and v' disagree

Ex: $d_H(11001, 01101) = 2$

$d(C)$ = lowest # of cols in H that add up to 0

---

4) A code is defined by the generator matrix

$$G = \begin{pmatrix} P \\ I_3 \end{pmatrix} \in M_{5,3}(\mathbb{F}_2)$$

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

Write down H and all the codewords.

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \Rightarrow d(C) = 2$$

Th. For a linear code we C we can detect $d(C)-1$ errors and we can correct $\boxed{\left[\frac{d(C)-1}{2}\right]}$

We find the codeword by encoding all possible messages:

$\{000, 001, 010, 011,$
$100, 101, 110, 111\}$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & & \dots & a_{2n} \\ \dots & & & \\ a_{m1} & & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = x_1 (a_{11}, \dots, a_{m1}) + \dots + x_n (a_{1n}, \dots, a_{mn})$$

m	v
000	00000
001	11001
010	01010
011	10011
100	01100
101	10101
110	00110
111	11111

$m = 101$

$$\left[\varphi(m)\right]_{\mathcal{E}} = G \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

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

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

---

5. +6.

Determine the minimum Hamming distance between the codewords of the code with generator matrix

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

Discuss the error-det. and error. cor.

Write H.

Encode the following:
1101, 0111, 0000, 1000, 1111, 0011

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

Na zona calun, Na identical dens

$d(C) \geq 3$

$C_1 + C_3 + C_7 = 0 \Rightarrow d(C) = 3$

Form. det. $= 3 - 1 = 2$

corected $= \frac{2}{2} = 1$

m_K	v_{m_K}
1 1 0 1	0 0 1 1 0 1 1 0 1
0 1 1 1	1 0 0 1 1 0 1 1 1
0 0 0 0	0 0 0 0 0 0 0 0 0
1 0 0 0	0 0 1 0 1 1 0 0 0
1 1 1 1	1 0 1 1 0 1 1 1 1
0 0 1 1	1 1 0 0 1 0 0 1 1

Polynomial codes :

$P \in \mathbb{F}_2[x]$ the generator polynomial

1. Convert the message m to a polynomial

$m = a_0 \; a_1 \; \dots \; a_{n-1} \Rightarrow f_m = a_0 + \dots + a_{n-1} x^{n-1}$

2. Multiply f_m by x^{n-k}

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

3. Perform Euclidean division on g_m and P, obtain R_m, the remainder

4. The encoded poly. is $h_m = g_m + R_m$

5. Convert h_m to a vector

$h_m = h_0 + h_1 x + \dots + h_{n-1} x^{n-1} \rightsquigarrow$

$\rightsquigarrow v = h_0 h_1 \dots h_{n-1}$

Ex: (6, 3) - poly code generated by

$P = x^{3} + 1$ $\rightsquigarrow n-k$

We encode $m = 011$

$t_m = x + x^2$

$g_m = x^5 + x^4$

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

$$h_m = x^5 + x^4 + x^2 + x$$

$$v_m = \underset{0}{0}\,\underset{1}{1}\,\underset{2}{1}\,\underset{3}{0}\,\underset{4}{1}\,\underset{5}{1}$$

8. Determine G, H, $d(C)$, the capabilities for the $(7,3)$ code generated by

$$p = 1 + x^2 + x^3 + x^4 \in \mathbb{F}_2[x]$$

$$G = [\gamma]_{E E'} = \left([\gamma(e_1)]_{E'} | \dots | [\gamma(e_3)] \right)$$

$$e_1 = (1,0,0) \Rightarrow f_m = 1$$

$$d_m = f_m \cdot x^4 = x^4$$

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

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

$$v_m = 1011100$$

$l_2 = (0,1,0) \to l_m = x$

$g_m = l_m \cdot x^4 = x^5$

$r_m = x^2 + x + 1$

$u_m = g_m + r_m = x^5 + x^2 + x + 1$

$v_{a_2} = 1110010$

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

$l_3 = (0;0,1)$

$l_m = x^2$

$g_m = x^2 \cdot x^4 = x^6$

$r_m = x^3 + x^2 + x$

$u_m = x^6 + x^3 + x^2 + x$

$v_{l_3} = 0111001$

$$G = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

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

$d(C) = 4$

Errors detected: 3

errors corrected: 1

Encode $m = 111$ | $P = x^4 + x^3 + x^2 + 1$

$f_m = 1 + x + x^2$

$g_m = x^6 + x^5 + x^4$

$R_m = x^2$

$h_m = x^{\cancel{8}6} + x^5 + x^4 + x^2$

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

$v = 0010111$