Seminar 12

1. (i) Which of the following received words contain detectable errors when using the (3,2)-parity check code: 110, 010, 001, 111, 101, 000?

(ii) Decode the following words using the (3,1)-repeating code to correct errors: 111, 011, 101, 010, 000, 001. Which of them contain detectable errors?

2. Are $1 + X^3 + X^4 + X^6 + X^7$ and $X + X^2 + X^3 + X^6$ code words in the polynomial (8,4)-code generated by $p = 1 + X^2 + X^3 + X^4 \in \mathbb{Z}_2[X]$?

3. Write down all the words in the (6,3)-code generated by $p = 1 + X^2 + X^3 \in \mathbb{Z}_2[X]$.

4. A code is defined by the generator matrix $G = \begin{pmatrix} P \\ I_3 \end{pmatrix} \in M_{5,3}(\mathbb{Z}_2)$, where:

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

Write down the parity check matrix and all the code words.

5. Determine the minimum Hamming distance between the code words 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 write down the parity check matrix.

6. Encode the following messages using the generator matrix of the (9,4)-code of Exercise **5.**: 1101, 0111, 0000, 1000.

Determine the generator matrix and the parity check matrix for:

7. The (4,1)-code generated by $p = 1 + X + X^2 + X^3 \in \mathbb{Z}_2[X]$.

8. The (7,3)-code generated by $p = 1 + X^2 + X^3 + X^4 \in \mathbb{Z}_2[X]$.

$n-k$ bits	k bits
check digits	message

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

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

Linear code

↳ $\gamma : \mathbb{Z}_2^k \longrightarrow \mathbb{Z}_2^n$

linear

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

↳ use it to encode:

$[\gamma(m)]_{\epsilon'} = G \cdot [m]_\epsilon$

$G = \begin{pmatrix} P \\ \hline I_k \end{pmatrix} \in \mathcal{M}_{n,k}(\mathbb{Z}_2)$

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

↳ parity check matrix

↳ $v \in \mathcal{C} \iff H \cdot [v]_\epsilon = 0$

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

$d_H(v, v') =$ # of positions that v and v' disagree on

↳ Humming distance

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

ex: $d_H(\underline{1}1\,0\,\underline{1}\,\underline{0}, \underline{0}\,1\,0\,0\,\underline{1}) = 3$

$= w(1\,0\,0\,1\,1) = 3$

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

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

$d(\mathcal{C}) =$ min # of columns in H that add up to 0

5. Determine the minimum Hamming distance between the code words of the code with generator matrix $G = \left(\frac{P}{I_4}\right) \in M_{9,4}(\mathbb{Z}_2)$, where:

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Discuss the error-detecting and error-correcting capabilities of this code, and write down the parity check matrix.

6. Encode the following messages using the generator matrix of the (9,4)-code of Exercise **5.**: 1101, 0111, 0000, 1000.

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

We can detect the min. nr of columns that add up to $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

~~$\exists$~~ a 0 column $\Rightarrow d(\mathcal{C}) > 1$

there are no identical columns $\Rightarrow d(\mathcal{C}) > 2$

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

$\Rightarrow d(\mathcal{C}) = 3$

* go for the columns in P that has the least amount of 1's

$\Rightarrow$ we can detect $d(\mathcal{C})-1$ errors and can correct $\left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor = 1$ error

encode 1101, 0000

$[\gamma(w)]_{\mathcal{C}'} = G \cdot [m]_{\mathcal{C}}$

for 1101: $G \cdot [(1101)]_{\mathcal{C}'} = G \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ p_1 \end{pmatrix}$

for 0000: $G \cdot [(0000)]_{\mathcal{C}'} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

for (0111) : $G \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

for (1000) : $G \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

(n,k) polynomial code generated by $P \in \mathbb{Z}_2[X]$

$m = \overline{a_0 a_1 \dots a_{k-1}}$

ex: $n=5$, $k=3$ $P = X^2+1$

message 101

If $\deg P = n-k$ then the code is linear

Step 1: Encode m as a poly.

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

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

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

$F_m = f_m \cdot X^{n-k}$

$F_m = (1+X^2) \cdot X^2 = X^2 + X^4$

Step 3: We divide F_m by P (Euclidean division)

$$\begin{array}{r|l} X^4 + X^2 & X^2+1 \\ \hline -X^4 - X^2 & X^2 \\ \hline 0 & \end{array}$$

Step 4: Compute $g_m = F_m + R_m$

$g_m = X^4 + X^2 + 0 = X^4 + X^2$

Step 5: Convert to a vector

$g_m = X^2 + X^4 \rightsquigarrow v = 00\underbrace{101}_{\text{message}}$

12.8 The $(7,3)$ code generated by $1+x^2+x^3+x^4 \in \mathbb{Z}_2[x]$

↳ Find G

↳ Find H, $d(\mathcal{C})$ and discuss the correctability

* encode the canonical messages

$e_1 = 100$

$e_2 = 010$

$e_3 = 001$

$$G = \left(\frac{I_3}{A}\right)$$

- $m = 100 \Rightarrow f_m = 1$

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

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

x^3+x^2+1 remainder $\quad R_m = x^3+x^2+1$

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

$g_m = 1+x^2+x^3+x^4 \rightsquigarrow v = 1011\underbrace{100}_{\text{message}}$

- $m = 010$ – tabla

- $m = 001 \Rightarrow f_m = x^2$

$F_m = f_m \cdot x^{n-k} = x^2 \cdot x^4 = x^6$

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

$g_m = R_m + F_m = x^6+x^3+x^2+x \rightsquigarrow v = 0111\underbrace{001}_{m}$

* v should always have n digits. add 0's at the end if you don't have enough

$$G = \begin{pmatrix} P \\ \hline I_k \end{pmatrix} \quad , \quad H = \left(I_{n-k} \mid P \right)$$

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

$d(\mathcal{C}) = ?$

$C_1 + C_3 + C_4 + C_5 = 0 \Rightarrow d(\mathcal{C}) \leq 4 \quad (1)$

there are no 0 columns and no identity columns $\Rightarrow d(\mathcal{C}) > 2$

* there are no 2 columns that add up to the 3rd

$$C_5 + C_6 + C_7 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \neq 0$$

$$\left.\begin{array}{l} d_H(C_5, C_6) = d_H(C_6, C_7) = d_H(C_5, C_7) = 2 \\ w(C_5) = w(C_6) = w(C_7) = 3 > 2 \end{array}\right\} \Rightarrow d(\mathcal{C}) > 3 \quad (2)$$

$(1), (2) \Rightarrow \quad d(\mathcal{C}) = 4$

we can detect $d(\mathcal{C}) - 1 = 3$ errors

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