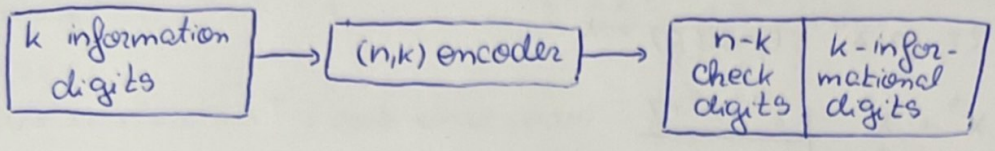
11.01.2024

Algebra - Seminar 12

Coding Theory

General scheme for an (n,k)-code, $k<n$, $k,n \in \mathbb{N}^*$



1. (i) Which of the foll. reaved words contains detectable errors when using $(3,2)$-parity check code: 110, 010, 001, 111, 101, 00

errors: 010, 001, 111, 000

(ii) $(3,1)$-repeating code: 111, 011, 101, 010, 000, 001. Correct the errors

errors	011	101	010	001
common digit	1	1	0	0

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

The polynomial f is a code-word if it is divisible by p.
The polynomial associated to a word $a_0 a_1 \dots a_{n-1}$ is
$a_0 + a_1 x + \dots + x^{n-1} a_{n-1}$

$$\begin{array}{l|l} x^7+x^6+x^4+x^3+1 & x^4+x^3+x^2+1 \\ \hline x^7+x^6+x^5+x^3 & x^3+x \\ \hline x^5+x^4+1 & \\ x^5+x^4+x^3+x & \\ \hline x^3+x+1 \neq 0 & \end{array}$$

$\rightarrow$ is not a code-word

$$\begin{array}{l|l} x^6+x^3+x^2+x & x^4+x^3+x^2+1 \\ \hline x^6+x^5+x^4+x^2 & x^2+x \\ \hline x^5+x^4+x^3+x & \\ x^5+x^4+x^3+x & \\ \hline 0 & \end{array}$$

$\rightarrow$ is a code-word

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

$n = 6$, $k = 3 \rightarrow 2^k = 8$ words: 000, 001, 010, 011, 100, 101, 110, 111

110: $\cdot\ 1 \cdot 1 + 1 \cdot x + 0 \cdot x^2 = 1 + x = m$

$\cdot\ m \cdot x^{n-k} = (1+x) \cdot x^3 = x^3 + x^4$

$\cdot\ r = m \cdot x^{n-k} \pmod p = x$

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

$\cdot\ v = r + m \cdot x^{n-k} = x + x^3 + x^4 \rightarrow$ the code-word: 010110

000 $\rightarrow$ 000000

001 $\cdot\ m = 0 \cdot 1 + 0 \cdot x + 1 \cdot x^2 = x^2$

$\cdot\ m \cdot x^{n-k} = x^2 \cdot x^3 = x^5$

$\cdot\ r = m \cdot x^{n-k} \pmod p = x + 1$

$\cdot\ v = x + 1 + x^5 = 1 + x + x^5 \rightarrow$

$\rightarrow$ the code-word: 110001

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

010 $\cdot\ m = 0 \cdot 1 + 1 \cdot x + 0 \cdot x^2 = x$

$\cdot\ m \cdot x^{n-k} = x^4$

$\cdot\ r = m \cdot x^{n-k} \pmod p = x^2 + x + 1$

$\cdot\ v = r + m \cdot x^{n-k} = 1 + x + x^2 + x^4$

$\rightarrow$ the code-word: 111010

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

011 $\cdot\ m = 0 \cdot 1 + 1 \cdot x + 1 \cdot x^2 = x + x^2$

$\cdot\ m \cdot x^{n-k} = (x + x^2) \cdot x^3 = x^4 + x^5$

$\cdot\ r = m \cdot x^{n-k} \pmod p = x^2$

$\cdot\ v = r + m \cdot x^{n-k} = x^2 + x^4 + 5 \rightarrow$ the code-word: 001011

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

100 $\cdot\ m = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 = 1$

$\cdot\ m \cdot x^{n-k} = x^3$

$\cdot\ r = m \cdot x^{n-k} \pmod p = x^2 + 1$

$\cdot\ v = x^3 + x^2 + 1 = 1 + x^2 + x^3 \rightarrow$ code-word: 101100

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

101 • $m = 1 \cdot 1 + 0 \cdot x + 1 \cdot x^0 = 1 + x^2$

• $m \cdot x^{n-k} = x^3 + x^5$

• $R = x^2 + x$

• $V = x + x^2 + x^3 + x^5 \rightarrow$ code-word: 011101

$x^5 + x^3 \;|\; x^3 + x^2 + 1$

$x^5 + x^4 + x^2 \;|\; x^2 + x$

$x^4 + x^3 + x^2$

$x^4 + x^3 + x$

$x^2 + x$

111 • $m = 1 + x + x^2$

• $m \cdot x^{n-k} = x^3 + x^4 + x^5$

• $R = 1$

• $V = 1 + x^3 + x^4 + x^5 \rightarrow$ code-word: 100111

$x^5 + x^4 + x^3 \;|\; x^3 + x^2 + 1$

$x^5 + x^4 + x^2 \;|\; x^2 + 1$

$x^3 + x^2$

$x^3 + x^2 + 1$

1

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

$P = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$. write the parity check matrix H and all the code words.

$G = \begin{pmatrix} P \\ I_3 \end{pmatrix} \in M_{n,k}(\mathbb{Z}_2)$

$H = (I_{n-k} \; P) \in M_{n-k \text{ in}}(\mathbb{Z}_2)$

• $u \in \mathbb{Z}_2^n$ is a code-word $\Leftrightarrow H \cdot [u]_{\mathcal{E}'} = [0]_{\mathcal{E}'}$

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$u_1 + u_5 = 0 \rightarrow u_5 = -u_1 = u_1 \quad (\mathbb{Z}_2)$

$u_2 + u_3 + u_4 + u_5 = 0 \rightarrow u_2 = -u_3 - u_4 - u_5 = u_1 + u_3 + u_4$

$S = \{(u_1, u_1 + u_3 + u_4, u_3, u_4, u_1)\} = \langle (1,1,0,0,1), (0,1,1,0,0), (0,1,0,1,0) \rangle =$

$= \{(0,0,0,0,0), (1,1,0,0,1), (0,1,1,0,0), (0,1,0,1,0), (1,0,1,0,1), (1,0,0,1,1), (0,0,1,1,0), (1,1,1,1,1)\}$

5. Det. the minimum Hamming distance between the code words of the cod with generator matrix $G = \begin{pmatrix} P \\ I_4 \end{pmatrix}$, where $P = \begin{pmatrix} 0&0&1&0 \\ 0&1&0&1 \\ 1&0&1&1 \\ 0&1&0&0 \\ 1&0&0&1 \end{pmatrix}$

Remark1: Consider H - the parity check matrix. Then if:

1. H has one zero column $\rightarrow d = 1$
2. H has 2 equal col. $\rightarrow d \leq 2$
3. H has all the columns non-zero & distinct $\rightarrow d \geq 3$

Remark3: It is equal to the minimum linearly-dependent columns of H.

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

$$C_2 + C_6 + C_9 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow d = 3$$

- Discuss the error-detecting and error correcting capabilities of this code.

- A code [detects all sets of t or fewer errors $\leftrightarrow d \geq t+1$ (Hamming dist)
  corrects ——— // ——— $\leftrightarrow d \geq 2t+1$

- detects max 2 errors ($d = 3 = 2+1$)
- corects max 1 errors ($d = 3 = 2 \cdot 1 + 1$)

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

A message $m \in M_{k,1}(\mathbb{Z}_2)$ encoded as $G \cdot m$

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

- 1101 → 001011101
- 0111 → 100110111
- 0000 → 000000000
- 1000 → 001011000

Determine the generator matrix and the parity check matrix for:

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

• The encoder is a $\mathbb{Z}_2$ - linear map $g: \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ and $G[g]_{EE'}$, E, E' - canonical basis of $\mathbb{Z}_2^k$, $\mathbb{Z}_2^n$ resp.

$n = 4, k = 1$

Canonical basis of $\mathbb{Z}_2$ is 1

$m = 1$

$m \cdot x^3 = x^3$

$r = x^2 + x + 1$

$v = 1 + x + x^2 + x^3$ → code-word: 1111

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

$x^3 + x^2 + x + 1$

$x^2 + x + 1$

$g(1) = 1111$ → $G = \left(\begin{array}{c} 1 \\ \hline 1 \end{array}\right)$ (P) → $H = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

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

The canonical basis of $\mathbb{Z}_2^3$: $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$

• 100 → $m = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 = 1$

$m \cdot x^{n-k} = x^4$

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

$v = 1 + x^2 + x^3 + x^4$ → code-word: 1011100

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

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

$x^3 + x^2 + 1$

• 010 → $m = x$

$m \cdot x^{n-k} = x^5$

$r = x^2 + x + 1$

$v = 1 + x + x^2 + x^5$

→ code-word: 1110010

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

$x^5 + x^4 + x^3 + x$

$x^4 + x^3 + x$

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

$x^2 + x + 1$

• 001 → $m = x^2$

$m \cdot x^{n-k} = x^6$

$r = x^3 + x^2 + x$

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

→ code-word: 0111001

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

$x^6 + x^5 + x^4 + x^2$

$x^5 + x^4 + x^2$

$x^5 + x^4 + x^3 + x$

$x^3 + x^2 + x$

(P) → $G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$