Binary BCH codes

Note Title

length : n, $d_{min} \geq d$ ← design distance, $d = 2t+1$ ← design error-correcting capability

Let $\beta \in GF(2^m)$ s.t. $ord(\beta) \geq n$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & \vdots & & \\ 1 & \beta^{d-1} & (\beta^{d-1})^2 & \cdots & (\beta^{d-1})^{n-1} \end{bmatrix}$$

$$g(x) = LCM\left(M_{\beta}(x), M_{\beta^2}(x), \ldots, M_{\beta^{d-1}}(x)\right)$$

$$n - k = \deg(g(x))$$

$$\deg(g(x)) \leq mt$$

→ Small t, this is tight

$$k \geq n - mt$$

Binary BCH code $= \{ c \in GF(2)^n : H c^T = 0 \}$

↓ contained in

Another code $= \{ c \in GF(2^m)^n : H c^T = 0 \}$

Reed-Solomon code

$\dim = n - \text{rank}(H)$

how? Gaussian elimination

$\underline{\underline{\text{Ex}}}$: $n = 4095 = 2^{12} - 1$ $\quad \beta \in GF(2^{12})$, primitive

$m = 12$

$t = 1$, $\underline{d} = 3$: $k = 4083$

$t = 2$, $\underline{d} = 5$: $k = 4071$

$\vdots$

$t = 10$, $d = 21$: $k = 3975$ $\quad \underline{g(x)}$

2^{3975} codewords in $\{0,1\}^{4095}$

Encoder: $(n, k, \geq d = 2t+1)$ binary BCH code.

d: design distance

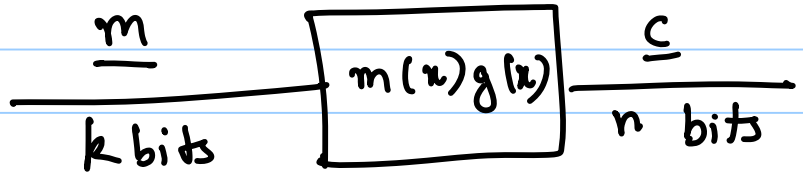
Suppose $g(x)$: generator poly, deg $= n-k$

$c(x) = m(x)\,g(x)$

$c(x)$: codeword

$m(x)$: message poly, $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$

$m_i \in \{0, 1\}$



Systematic encoder:

$$m(x) \longrightarrow x^{n-k} m(x) = m_{k-1} x^{n-1} + \cdots + m_1 x^{n-k+1} + m_0 x^{n-k}$$

put $r(x)$ here

$$[\underbrace{0 \cdots 0}_{n-k} \underbrace{m_0 m_1 \cdots m_{k-1}}_{\text{message}}]$$

Divide $x^{n-k} m(x)$ by $g(x)$

$$x^{n-k} m(x) = \underline{q(x)}\, g(x) + \underline{\underline{r(x)}}$$

$\deg \leq n-k-1$

R

Generator matrix: $(n, k, d = 2t+1)$

binary BCH code: defined using a

$2t \times n$ pc matrix over $GF(2^m)$

?

$mt \times n$ binary pc matrix

$k \times n$ generator matrix: ?
(binary)

$$g(x) = g_0 + g_1 x + \cdots + \underset{\neq 0}{g_{n-k}} x^{n-k}$$

$\Rightarrow$ $[g_0\ g_1 \cdots g_{n-k}^{\downarrow=1}\ 0 \cdots 0]$ is a codeword.

Other codewords: easily found by shifting

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & & 1 & & \\ 0 & 0 & g_0 & \cdots & & 1 & \\ \vdots & & & \ddots & & & \ddots \\ 0 & \cdots & & g_0 & \cdots & & 1 \end{bmatrix}$$

(g_{n-k} above the 1 in column $n-k$; $k-1$ above the run of zeros; k rows; n columns)

Quiz 1:

(1) GF(16) table 6 marks

(2) (n, k, d) over GF(16)

6

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ ! & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \end{bmatrix}$$

↓ Gaussian elimination

$k = 4$

$n - k = 2$

$d = 1$ ✗

$$\begin{bmatrix} \alpha^i \\ \alpha^{2i} \end{bmatrix} = c \begin{bmatrix} \alpha^j \\ \alpha^{2j} \end{bmatrix}$$

$$\alpha^i = c\,\alpha^j \longrightarrow \alpha^{2i} = c^2\,\alpha^{2j}$$

$$\alpha^{2i} = c\,\alpha^{2j}$$

$c^2 = c$

$c = 0, 1$ ✗

$d = 3$

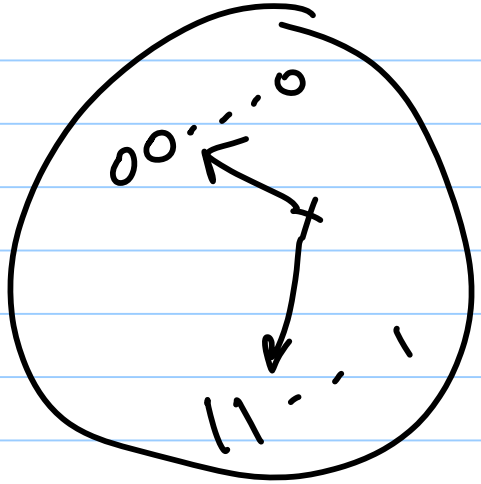
3 (a) $(n, n-1, 2)$ even-wt code

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

$\underline{s}$	$\underline{\hat{e}}$
0	$0\ 0 \cdots 0$
1	$1\ 0 \cdots 0$

$\Pr(\text{error}) = 1 - (1-p)^n - (1-p)^{n-1} p$

(b) $(n, 1, n)$ repetition code



n: odd

$wt(\underline{e}) \leq \frac{n-1}{2}$

correctable

$wt(\underline{e}) > \frac{n-1}{2}$

not correctable

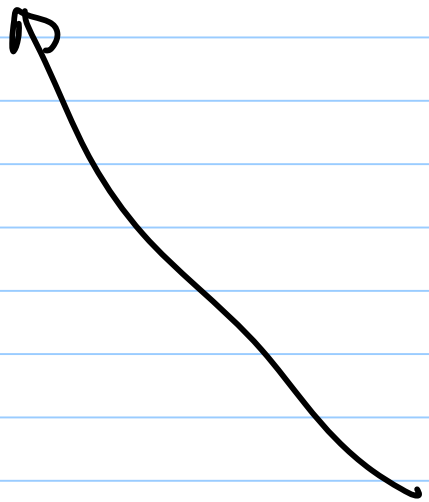
n: even

$wt(\underline{e}) < \frac{n}{2}$ correctable

$wt(\underline{e}) > \frac{n}{2}$ fails

$wt(\underline{e}) = \frac{n}{2}$ correct $\frac{1}{2}$ of the errors

2^{n-k} syndromes



$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} + 2$$