Lecture 14

Note Title 2/6/2008

$n = 2^m - 1$ $\quad \alpha \in F_{2^m}$, primitive

t - error-correcting BCH code

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

Generator polynomial

$$g(x) = LCM\left(f_\alpha(x), f_{\alpha^2}(x), \ldots, f_{\alpha^{2t}}(x)\right)$$

$c(x) \in$ Code iff

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

$$g(x) = g_0 + g_1 x + \cdots + g_r x^r, \quad \deg = r$$

$g_r = 1$.

Any codeword

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} = (g_0 + g_1 x + \cdots + g_r x^r)(m_0 + m_1 x + \cdots + m_{k-1} x^{k-1})$$

$g(x)$ $\quad$ $m(x)$

$\deg \le n-1$ $\quad$ $\deg \le n-r-1$

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

$$\# \text{ of codewords} = 2^{n-r} = 2^k$$

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

Ex: 1) $n = 7$ $\quad \alpha \in GF(2^3)$, $\alpha^3 = \alpha + 1$, $\alpha^7 = 1$

$t = 1$: $\quad g(x) = \text{lcm}(f_\alpha(x), f_{\alpha^2}(x))$

$= f_\alpha(x) = x^3 + x + 1$

$c(x) = (1 + x + x^3)(m_0 + m_1 x + m_2 x^2 + m_3 x^3)$

$k = 7 - 3 = 4$ $\quad (7, 4, 3)$ Hamming code

$\uparrow$ $\deg(g(x))$

$t = 2$: $\quad g(x) = \text{lcm}(f_\alpha(x), f_{\alpha^3}(x))$

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

$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$k = 7 - 6 = 1$

$\rightarrow$ $n = 7$ repetition code

Ex: $n = 15$ $\quad \alpha \in F_{16}$, $\alpha^4 = 1 + \alpha$, $\alpha^{15} = 1$

$t = 1$: $\quad g(x) = x^4 + x + 1$

$k = 15 - 4 = 11$ $\quad$ $(15, 11, 3)$ Hamming code

$t = 2$: $\quad g(x) = \text{Lcm}\left(f_\alpha(x), f_{\alpha^3}(x)\right)$

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

$k = 15 - 8 = 7$ $\quad$ $(15, 7, \geq 5)$ Code

$g(x) = x^8 + x^7 + x^6 + x^4 + 1$

$[\,1\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,]$ ← Code

$t=3$:

$$g(x) = \mathrm{LCM}\left(f_\alpha(x), f_{\alpha^3}(x), f_{\alpha^5}(x)\right)$$

$$= f_\alpha(x)\, f_{\alpha^3}(x)\, f_{\alpha^5}(x)$$

$$= (1 + x^4 + x^6 + x^7 + x^8)(x^2 + x + 1)$$

$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

$k = 15 - 10 = 5$ $\quad (15, 5, \cancel{\cancel{7}})$ code

$t=4$:

$g(x)$: deg $= 14$

$k = 15 - 14 = 1$

$(15, 1, 15)$ repetition code

$\longrightarrow$ $(x+1)(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2^m-2}) = x^{2^m-1} + 1$

$\alpha \in F_{2^m}$, primitive

$n = 31$, $\alpha \in F_{32}$, primitive , $\alpha^{31} = 1$

$t=1$: $g(x)$: deg $= 5$ $\quad (31, 26, 3)$ ✓

$k = 26$

$t=2$: $g(x)$: deg $= 10$ $\quad (31, 21, 5)$ ✓ w/o tables

$t=3$: $g(x)$: deg $= 15$ $\quad (31, 16, 7)$ ✓

⋮

$n = 511$ $\quad t = 3$ $\quad k = ?$ $\quad (511, 484, 7)$

$f_\alpha(x)$: 1, 2, 4, 8, 16, 32, 64, 128, 256

$f_{\alpha^3}(x)$: 3, 6, 12, 24, 48, ... — 27 total

$f_{\alpha^5}(x)$: 5, 10, 20, ...

$k = 511 - 27 = 484$

Encoding:

$\underline{m} = [m_0 \; \cdots \; m_{k-1}]$

One way: $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$

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

Systematic encoder:

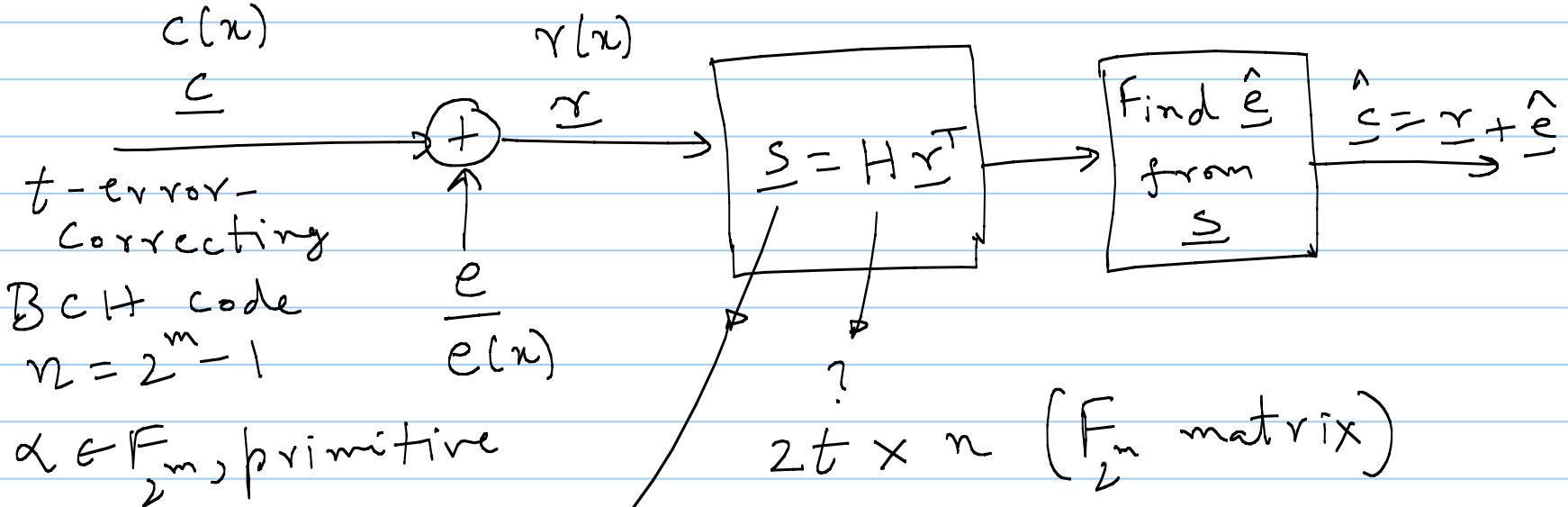
Divide $x^{n-k} m(x)$ by $g(x)$. → (can be done by LFSR circuits)

$$\underbrace{x^{n-k} m(x)}_{x^{n-1} \text{ to } x^{n-k} \text{ terms only}} = q(x) g(x) + r(x)$$

$\deg \le n-k-1$

$$\underbrace{x^{n-k} m(x) + r(x)}_{\text{systematic}} = q(x) g(x) \rightarrow \text{a codeword!!}$$

Decoding:



$$\underline{s} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{2t} \end{bmatrix} \Rightarrow \quad \begin{aligned} s_1 &= r(\alpha) \\ s_2 &= r(\alpha^2) \\ &\vdots \\ s_{2t} &= r(\alpha^{2t}) \end{aligned}$$

$$r(x) = c(x) + e(x)$$

Syndromes, $S_i = r(\alpha^i) = e(\alpha^i)$

$$1 \le i \le 2t$$

Suppose 1^s in $\underline{e}$ are at positions $i_1, i_2, \ldots, i_w$, $wt(\underline{e}) = w$ $\Rightarrow$

$$e(x) = e_0 + e_1 x + e_2 x^2 + \cdots + e_{n-1} x^{n-1}$$
$$= x^{i_1} + x^{i_2} + \cdots + x^{i_w}.$$

$$S_j = e(\alpha^j) = (\alpha^j)^{i_1} + (\alpha^j)^{i_2} + \cdots + (\alpha^j)^{i_w}$$

$$1 \le j \le 2t$$

$$S_j = (\alpha^{i_1})^j + (\alpha^{i_2})^j + \cdots + (\alpha^{i_w})^j$$

Error locators $X_l = \alpha^{i_l}$, $1 \le l \le w$

Syndromes $S_j = X_1^j + X_2^j + \cdots + X_w^j$

$1 \le j \le 2t$

Solve

$$S_1 = X_1 + X_2 + \cdots + X_w$$
$$S_2 = X_1^2 + X_2^2 + \cdots + X_w^2$$
$$S_3 = X_1^3 + X_2^3 + \cdots + X_w^3$$
$$\vdots$$
$$S_{2t} = X_1^{2t} + X_2^{2t} + \cdots + X_w^{2t}$$

for $X_1, X_2, \ldots, X_w$

Σ_x: $n = 15$ $\alpha \in F_{16}$, $\alpha^{15} = 1$, $\alpha^4 = 1 + \alpha$

$t = 1$: 1) $r(x) = x + x^4$

$w = 0, 1, 2, \ldots, t$

$S_1 = 1 = X_1$ $(w = 1)$

$\Rightarrow i_1 = 0$ & $\hat{e}(x) = 1$

& $\hat{c}(x) = 1 + x + x^4$

2) $r(x) = x^{10} + x^7$

$S_1 = \alpha^6 = X_1$ $(w = 1)$

$\Rightarrow i_1 = 6$ & $\hat{e}(x) = x^6$

& $\hat{c}(x) = x^6 + x^7 + x^{10}$

$t=2$:

$$r(x) = x^9 + x^5 + x$$

$$S_1 = \alpha^{11} = X_1 + X_2$$

$$S_2 = \alpha^{7} = X_1^2 + X_2^2$$

$$S_3 = \alpha^{5} = X_1^3 + X_2^3$$

$$S_4 = \alpha^{14} = X_1^4 + X_2^4$$

$\Rightarrow X$

$$X_1 + X_2 = \alpha^{11} \qquad X_2 = \alpha^{11} + X_1$$

$$X_1^3 + X_2^3 = \alpha^5$$

$$X_1^3 + (\alpha^{11} + X_1)^2 (\alpha^{11} + X_1) = \alpha^5$$

$$\alpha^{11} X_1^2 + \alpha^7 X_1 + \alpha^{11} = 0$$

$$X_1^2 + \alpha^{11} X_1 + 1 = 0$$

$$X_1 = \alpha^7, \alpha^8$$

$$X_2 = \alpha^8, \alpha^7$$

$$\hat{e}(x) = x^7 + x^8$$

$$\hat{c}(x) = x^9 + x^8 + x^7 + x^5 + x$$