Assignment: BCH & RS Codes

Note Title

① k & $g(x)$ for all "narrow-sense" binary BCH codes with $n = 31$

Zeros: $\alpha, \alpha^2, \ldots, \alpha^{2t}$ where $\text{ord}(\alpha) = n$

$x+1$ $\quad M_1(x)$

$\{0\}, \{1, 2, 4, 8, 16\}$ $\quad M_1(x)$

$M_3(x)\{3, 6, 12, 24, 17\}$ $\quad M_{11}(x)\{11, 22, 13, 26, 21\}$

$M_5(x)\{5, 10, 20, 9, 18\}$

$M_7(x)\{7, 14, 28, 25, 19\}$

for t-error-correcting code

t	k	$g(x)$
1	26	$M_1(x)$
2	21	$M_1(x)\,M_3(x)$
⋮		

(3) $n = 65 = 2^6 + 1$

$\alpha \in GF(2^m)$ s.t. $ord(\alpha) = 65$

$m = 12$

$\alpha \in GF(2^{12})$ primitive

$\{0\}$,

$\{1, 2, 4, 8, 16, 32, 64, 63, 61, 57, 49, 33\}$

$\Downarrow$

$ord(\alpha) = 2^{12} - 1 = (2^6 - 1)(2^6 + 1)$

$= (63)(65)$

$\Rightarrow ord(\alpha^{63}) = 65$

(4) $n = 31$, $t = 2$ BCH code

(a) $r(x) = x^7 + x^{30} \longrightarrow \hat{c}(x) = 0$

(b) $r(x) = 1 + x^{17} + x^{28}$?

(7) $(15, 5)$ BCH code, $t = 3$

$\underline{r} = [0\,000\;\; 0110\;\; 1000\;\; 100]$

Find $\hat{\underline{c}}$.

(8) $n = 7$ RS code over $GF(8)$, $t = 2$

$k = 3$

(a) $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$

Encode $[1 \;\; \alpha \;\; \alpha^2]$ systematically

(b) $GF(8)$: $(7, 3, 5)$

↓ binary expansion

$(21, 9, \geq 5)$

(c) Decode $[0 \;\; 1 \;\; \alpha \;\; \alpha^2 \;\; \alpha^3 \;\; 1 \;\; 0]$

(9) $n = 15$, RS code over GF(16), $t = 2$

(a) $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$

Check poly $h(x) = \dfrac{x^n+1}{g(x)} = (x+\alpha^5)(x+\alpha^6) \cdots (x+\alpha^{14})(x+1)$

(b) $4\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \\ 1 & \alpha^4 & \alpha^8 & \cdots & \end{bmatrix}$ 15

(10) $(\text{RS code})^{\perp}$: another RS code $(\text{ord}(\alpha) = n)$

$$g(x) = (x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t})$$

$(k = n-2t)$

$$h(x) = (x+\alpha^{2t+1})\cdots(x+\alpha^{n-1})(x+1)$$

Dual's gen. poly. $= x^k h(x^{-1})$

$$= x^k (x^{-1}+\alpha^{2t+1})\cdots(x^{-1}+\alpha^{n-1})(x^{-1}+1)$$

$$= (1+\alpha^{2t+1}x)\cdots(1+\alpha^{n-1}x)(1+x)$$

Zeros of dual: $1, \alpha, \alpha^2, \ldots, \alpha^{n-2t-1}$

Dual: $(n, 2t, n-2t+1)$

(12) C_{RS}: $n = 2^m - 1$ RS code over $GF(2^m)$ Zeros $\{\alpha, \alpha^2, \ldots, \alpha^{2t}\}$ t-error-correcting

$g_{RS}(x) = (x+\alpha)\cdots(x+\alpha^{2t})$

C_{BCH}: $n = 2^m - 1$ binary BCH, t-error-correcting

$g_{BCH}(x) = LCM\left(M_\alpha(x), M_{\alpha^2}(x), \ldots, M_{\alpha^{2t}}(x)\right)$

Show $C_{BCH} \subseteq C_{RS}$

$\Downarrow$

$g_{RS}(x) \mid g_{BCH}(x)$

(13) $\alpha \in GF(16)$, primitive — over $GF(16)$

(a)

$d=3$

$$H=\left[\begin{array}{cc|cccc} 1 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 \cdots \alpha^{14} \\ 0 & 1 & 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 \cdots (\alpha^2)^{14} \end{array}\right]$$

$x \quad x \quad | \quad \longleftarrow$

$1 \quad 1 \quad | \quad 0 \quad - \quad 0$

(b)

$$H=\left[\begin{array}{ccc|cccc} 0 & x & x & & & & \\ 1 & 0 & 0 & 1 & \alpha & \alpha^2 & \cdots \alpha^{14} \\ 0 & 1 & 0 & 1 & \alpha^2 & (\alpha^2)^2 & \cdots (\alpha^2)^{14} \\ 0 & 0 & 1 & 1 & \alpha^3 & (\alpha^3)^2 & \cdots (\alpha^3)^{14} \end{array}\right]$$

(15) H: pc matrix of $(n, k, n-k+1)$ RS code

$d = n-k+1$

$$\begin{matrix} & \\ n-k & \end{matrix}\begin{bmatrix} 1 & 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 0 & 0 & 1 & \alpha^2 & - & - & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 1 & \alpha^{n-k} & (\alpha^{n-k})^2 & \cdots & (\alpha^{n-k})^{n-1} \\ 0 & I & 1 & \alpha & (\alpha^{n-k})^2 & \cdots & (\alpha^{n-k})^{n-1} \end{bmatrix}$$

$X \quad X$

$\longleftarrow \quad n+2 \quad \longrightarrow$

$(n+2, k+2, d)$

(14) C : RS code ; zeros : $\{\alpha, \alpha^2, \ldots, \alpha^{d-1}\}$

$$C^{(e)} = \{ [u_1\ u_2 \ldots u_n\ u_{n+1}] :$$

$$[u_1\ u_2 \ldots u_n] \in C,$$

$$u_{n+1} = u_1 + u_2 + \cdots + u_n \}$$

$(n+1, k, d+1)$

$$\begin{bmatrix} 0 & 1 & \alpha & \cdots & \alpha^{n-1} \\ 0 & 1 & \alpha^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & & & \\ 0 & 1 & \alpha^{d-1} & \cdots & (\alpha^{d-1})^{n-1} \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$