BCH codes

Note Title

Bose-Chaudhuri-Hocquenghem

- define PC matrix over $GF(2^m)$

$\beta \in GF(2^m)$ $ord(\beta) \geq n$ d: design min dist

PC matrix

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

Binary BCH code:

$$C = \{ \underline{c} \in GF(2)^n : H\underline{c}^T = \underline{0} \}$$

$\underline{c} = [c_0\ c_1 \cdots c_{n-1}]$ elements over $GF(2^m)$

1st row: $c_0 \cdot \underbrace{1}_{\beta^0} + c_1 \cdot \underbrace{\beta}_{\beta^1} + c_2 \cdot \underbrace{\beta^2}_{\beta^2} + \cdots + c_{n-1} \cdot \underbrace{\beta^{n-1}}_{\beta^{n-1}} = 0$

$$GF(2^m) = \{ a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} : a_i \in GF(2) \}$$

Let $\beta^i = a_0(i) + a_1(i)\alpha + \cdots + a_{m-1}(i)\alpha^{m-1}$

$a_j(i) \in GF(2)$

$$c_0 \cdot 1 + c_1 \left(a_0(1) + a_1(1)\alpha + \cdots + a_{m-1}(1)\alpha^{m-1} \right)$$
$$+ c_2 \left(a_0(2) + a_1(2)\alpha + \cdots + a_{m-1}(2)\alpha^{m-1} \right)$$
$$+ \cdots$$
$$+ c_{n-1} \left(a_0(n-1) + a_1(n-1)\alpha + \cdots + a_{m-1}(n-1)\alpha^{m-1} \right) = 0$$

$$c_0 + c_1 a_0(1) + c_2 a_0(2) + \cdots + c_{n-1} a_0(n-1)$$
$$+ \left(c_1 a_1(1) + c_2 a_1(2) + \cdots + c_{n-1} a_1(n-1) \right)\alpha$$
$$+ \left(c_1 a_2(1) + c_2 a_2(2) + \cdots + c_{n-1} a_2(n-1) \right)\alpha^2$$
$$+ \cdots$$
$$+ \left(c_1 a_{m-1}(1) + \cdots + c_{n-1} a_{m-1}(n-1) \right)\alpha^{m-1} = 0$$

$$c_0 \cdot 1 + c_1 \cdot \beta + c_2 \cdot \beta^2 + \cdots + c_{n-1} \cdot \beta^{n-1} = 0 \quad \text{over } GF(2^m)$$

m eqns over $GF(2)$

$$\begin{bmatrix} 1 & a_0(1) & a_0(2) & \cdots & a_0(n-1) \\ 0 & a_1(1) & a_1(2) & \cdots & a_1(n-1) \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & a_{m-1}(1) & a_{m-1}(2) & \cdots & a_{m-1}(n-1) \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ 1 \\ \vdots \\ 1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Dimension of binary BCH codes

$$\underline{c} = [c_0 \; c_1 \; c_2 \cdots c_{n-1}] \in GF(2)^n$$

$$\updownarrow$$

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in GF(2)[x]$$

i-th row of H : $c_0 \cdot 1 + c_1 \beta^i + c_2 (\beta^i)^2 + \cdots + c_{n-1} (\beta^i)^{n-1} = 0$

$$\updownarrow$$

β^i is a root of $c(x) \in GF(2)[x]$

$\beta^i \in GF(2^m)$

$(x+\beta^i) \mid c(x) \Rightarrow M_{\beta^i}(x) \mid c(x)$

$\in GF(2^m)[x]$

$\beta^i \in GF(2)[x]$

roots $\{\beta^i, \beta^{2i}, \ldots\}$

Result:

$c(x) \in$ binary BCH code (length n, des. dist. d)

$\beta \in GF(2^m)$

$\Updownarrow$

$M_{\beta^i}(x) \mid c(x)$ for $i = 1, 2, \ldots, d-1$

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

↓ binary coeffs

Binary BCH code $= \{$ multiples of $g(x)$ with degree $\leq n-1 \}$

generator polynomial

Let $\deg g(x) = l$

$$= \{ m(x) g(x) : m(x) = m_0 + m_1 x + \cdots + m_{n-l-1} x^{n-l-1}, \; m_i \in GF(2) \}$$

$$\#\text{ of codewords} = 2^{n-l} \Rightarrow \dim\left(\begin{matrix}\text{binary} \\ \text{BCH code}\end{matrix}\right) = n - \deg(g(x))$$

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

$$k = \text{dimension} = n - \deg(g(x))$$

Jargon: $\beta, \beta^2, \ldots, \beta^{d-1}$: zeros of binary BCH code

Examples: $n = 15$, $\beta \in GF(16)$, primitive

$$\text{ord}(\beta) = n$$

$d = 3$: zeros: β, β^2, $g(x) = x^4 + x + 1 =$

$$LCM\left(M_{\beta}(x), M_{\beta^2}(x)\right)$$

$k = 11$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \end{bmatrix}$$

$d=5$: zeros: $\beta, \beta^2, \beta^3, \beta^4$; $g(x) = (x^4+x+1)$

$k = 7$

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

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 1 & \beta^3 & (\beta^3)^2 & \cdots & (\beta^3)^{14} \end{bmatrix}$$ $(15, 7, 5)$

$d=7$ Zeros: $\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6$

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

x^4+x+1 ↓ $M_{\beta}(x)$; $x^4+x^3+x^2+x+1$ ↓ $M_{\beta^3}(x)$; x^2+x+1 ↓ $M_{\beta^5}(x)$

$k=5$

$(15, 5, 7)$ ①

$d=9$ Zeros: $\beta, \ldots, \beta^8$ ← deg = 14

$(15, 1, 15)$ $g(x) = M_{\beta}(x) \cdot M_{\beta^3}(x) M_{\beta^5}(x) M_{\beta^7}(x)$

$= x^{14} + x^{13} + \cdots + x^1 + 1$

$n = 63$ $\quad \beta \in GF(64)$, primitive

$d = 3$; zeros $= \{\beta, \beta^2\}$; $g(x) = M_{\beta}(x)$

$t = 1$

$\{1, 2, 4, 8, 16, 32\}$ $\quad \deg g(x) = 6$

$k = 63 - 6 = 57 = n - 6 \cdot 1$

$d = 5$; zeros $= \{\beta, \beta^2, \beta^3, \beta^4\}$; $g(x) = M_{\beta}(x) M_{\beta^3}(x)$

$t = 2$

$\deg g(x) = 12$

β: $\deg 6$; β^3

$k = 51 = n - 6 \cdot 2$

$t = \frac{d-1}{2}$, $k \geq n - mt$

$\deg g(x) \leq tm$

$\beta \in GF(2^m)$

$d = 7$

$t = 3$

$k = 63 - 3 \cdot 6$

$\{5, 10, 20, 40, 17, 34\}$

$d = 9$

$t = 4$

$k = 63 - 4 \cdot 6$

$\{7, 14, 28, 56, 49, 35\}$

$d = 11$ $\quad \{9, 18, 36\}$

$t = 5 \quad k = 63 - 4 \cdot 6 - 3$

$n = 127, \; k = n - 7t$ ✓

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

$t = \frac{d-1}{2}$ rows are "usually" independent

$\therefore$