BCH codes

Note Title

Binary cyclic code: ideal of R_n (n: odd)

$\langle g(x) \rangle$, $g(x) \mid (x^n+1)$

$g(x)$ has linear factors over $F_{2^m}[x]$

Zeros of $g(x)$ in F_{2^m} are called zeros of the code

Check poly $h(x) = \frac{x^n+1}{g(x)}$

Result: Cyclic code $C = \langle g(x) \rangle$, $g(x) \mid (x^n+1)$.

$\langle g(x)p(x) \rangle = \langle g(x) \rangle$, if $p(x)$ has no zeros other those of $g(x)$ (among the n^{th} roots of unity)

all multiples of $g(x)p(x)$ in R_n

$\rightarrow$ Ex: $\langle g(x)^2 \rangle = \langle g(x) \rangle$

Pf: $\gcd(p(x), h(x)) = 1$

$x^n+1 = g(x)h(x)$

$\Rightarrow$ $\exists$ $a(x), b(x)$ s.t.

$$a(x)f(x) + b(x)h(x) = 1 \quad \text{in } F_2[x]$$

$$a(x)g(x)f(x) + b(x)(x^n+1) = g(x)$$

$$\Rightarrow \quad a(x)g(x)f(x) = g(x) \text{ in } R_n$$

$\underline{\Sigma_x}$: $n = 15$

$\{0\}$, $\{1,2,4,8\}$, $\{3,6,9,12\}$, $\{5,10\}$,
$\{7,11,13,14\}$

C : zeros $= \{1,2,4,8\} \cup \{5,10\}$

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

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

$$C = \langle g(x)(x^3+x+1) \rangle$$

$$C^\perp = \langle (x+1)(x^4+x+1)(x^4+x^3+x^2+x+1) \rangle$$

$\{0\} \cup \{3,6,9,12\} \cup \{5,10\} \cup \{1,2,4,8\}$

C : zeros : $C^\perp \subseteq C$

BCH bound

$C = \langle g(x) \rangle$, $g(x) \mid (x^n + 1)$.

α: primitive n^{th} root of unity

If $g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$,

then $d_{min}(C) \geq \delta$.

b: integer

PF:

Vandermonde

$$\det \begin{bmatrix} a_1 & a_2 & \cdots & a_r \\ a_1^2 & a_2^2 & \cdots & a_r^2 \\ \vdots & \vdots & & \vdots \\ a_1^r & a_2^r & \cdots & a_r^r \end{bmatrix} \neq 0 \quad a_i \neq a_j$$

Binary BCH code: b: integer

δ: design distance

$C = \langle g(x) \rangle$, where

$g(x)$: least degree divisor of $x^n + 1$ that has $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ as zeros.

$\Rightarrow g(x) = LCM\left(M_{\alpha^b}(x), \ldots, M_{\alpha^{b+\delta-2}}(x)\right)$

Binary case, narrow-sense $b=1$ $\quad \alpha \in GF(2^m)$

design distance, $\delta = 2t+1$

$$g(x) = LCM\left(M_{\alpha}(x), M_{\alpha^3}(x), \ldots, M_{\alpha^{2t-1}}(x)\right)$$

$\deg g(x) \leq tm \qquad d_{min} \geq \delta$

$\Rightarrow \quad k \geq n - mt$

Non-binary cyclic codes:

- towards Reed-Solomon codes

$$R_n = \left\{ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in GF(q) \right\}$$

$+, \times$: mod $x^n - 1$

$a(x) \in R_n, \; x\,a(x)$

$[a_0 \; a_1 \; \cdots \; a_{n-1}] \qquad [a_{n-1} \; a_0 \; a_1 \; \cdots \; a_{n-2}]$

- Ideals of R_n are cyclic codes over $GF(q)$

"q-ary cyclic codes"

- All ideals of R_n are principal.
- Unique monic polynomial of minimal degree (called generator poly)

- Generator poly: divides $x^n - 1$; ideal = {multiples of $g(x)$ with deg $\leq n-1$} (over $F_q[x]$)

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

Factoring $x^n - 1$ over GF(q):

$\gcd(n, q) = 1 \Rightarrow \exists\ \alpha \in GF(q^m)$ s.t. $\operatorname{ord}(\alpha) = n$.

Cyclotomic cosets mod n under multiplication by q

Ex: ① $n = 15$, $q = 16$

$\alpha \in GF(16)$, primitive

$$x^n - 1 = \prod_{i=0}^{14} (x - \alpha^i)$$

$\{0\}, \{1\}, \{2\}, \{3\}, \ldots, \{14\}$

② $n = 10$, $q = 9$ $\quad x^{10} - 1 = (x-1)\cdots(x-8)$

$\{0\}, \{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}$