Binary cyclic codes

Note Title

$$R_n = \{ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in [0,1] \}$$
$$+, \times : \bmod x^n + 1$$

Cyclic codes: - ideals in R_n

- all ideals are principal ideals in R_n

$$I = \langle g(x) \rangle$$

$g(x)$: the least deg poly in I

has binary coefficients ← $g(x) \mid (x^n+1)$

$$I = \langle a(x) \rangle, \quad a(x) \mid (x^n+1)$$

We know $x^n + 1 = a(x)e(x)$ in $F_2[x]$

$\Rightarrow$ $a(x)$: generator poly of I

Pf: Suppose $g(x) = m(x)a(x)$ in R_n

$$g(x) = \underbrace{m(x)a(x)}_{\text{in } F_2[x]} \bmod x^n + 1$$

$$g(x) = m(x)a(x) + b(x)(x^n+1)$$
$$= a(x)\big(m(x) + b(x)e(x)\big) \quad \text{in } F_2[x]$$

$\Rightarrow$ $a(x) \mid g(x)$ in $F_2[x]$.

$I = \langle g(x) \rangle$, $g(x)$: generator poly

$\deg g(x) = r$

$g(x) = g_0 + g_1 x + \cdots + g_r x^r$ ($g_0 \neq 0$, $g_r \neq 0$)

$I = \{ m(x) g(x) : \deg m(x) \leq n-r-1 \}$ ($\deg \leq n-1$)

$|I| = ?$

$|I| = 2^{n-r}$

I: cyclic code

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{r-1} & g_r & \cdots & 0 \\ & & \ddots & & & \ddots & \\ & & & g_0 & \cdots & & g_r \end{bmatrix}$$

$g(x)$, $x g(x)$, $x^{n-r-1} g(x)$; n columns

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

$c(x) = m(x) g(x) = m_0 (g(x)) + m_1 (x g(x)) + \cdots + m_{n-r-1} (x^{n-r-1} g(x))$

$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

$[c_0 \; c_1 \; \cdots \; c_{n-1}]$

Factoring x^n+1 $\quad n$: odd

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

For n: odd, $\exists\ m$ s.t. $n \mid (2^m - 1)$.

(Smallest such m is usually chosen)

$\beta \in GF(2^m)$, primitive.

Set $\alpha = \beta^{(2^m-1)/n}$

α : root of x^n+1

$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}, 1$: distinct roots of x^n+1 in $GF(2^m)$

$$x^n+1 = \underbrace{(x+1)}_{\text{binary factor}}(x+\alpha)(x+\alpha^2)\ldots(x+\alpha^{n-1})$$

- Find Cyclotomic cosets of $\{0, 1, 2, \ldots, n-1\}$ mod n under mult by 2
- Group linear factors according to cyclotomic cosets to get binary factors

Ex: $n = 9$ $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

Cyclotomic cosets: $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 7, 5\}$,

$C_3 = \{3, 6\}$

$$x^9 + 1 = \underbrace{M_0(x)}\ \underbrace{M_1(x)}\ \underbrace{M_3(x)}$$

$x+1$ deg 6 x^2+x+1

$M_1(x) = \frac{x^9+1}{x^3+1} = 1 + x^3 + x^6$

binary cyclic codes of length $n = 9$

$g(x)$	k	
1	9	identity code
$x+1$	8	even-weight code
x^2+x+1	7	
$(x+1)(x^2+x+1)$	6	
$M_1(x) = 1+x^3+x^6$	3	3 repetition of (3,1,3) $\subseteq = [m_0\ m_1\ m_2\ m_0\ m_1\ m_2\ m_0\ m_1\ m_2]$
$(x+1)\,M_1(x)$	2	
$(x^2+x+1)M_1(x)$	1	repetition code
$\|$		
$1 + x + x^2 + \cdots + x^8$		

Ex: $n = 21$

$M_1(x)$ $M_3(x)$ $M_5(x)$

$\{0\}$, $\{1, 2, 4, 8, 16, 11\}$, $\{3, 6, 12\}$, $\{5, 10, 20, 19, 17, 13\}$,

$(x+1)$

$\{7, 14\}$, $\{9, 18, 15\}$

x^2+x+1 $M_9(x)$

$g(x)$	k
1	21
$x+1$	20
x^2+x+1	19
$M_3(x), M_9(x), (x+1)(x^2+x+1)$	18

all k's are possible.

Ex: $n = 17$

$M_1(x)$

$\{0\}, \{1, 2, 4, 8, 16, 15, 13, 9\},$

$x+1$ $\{3, 6, 12, 7, 14, 11, 5, 10\}$

$M_3(x)$

possible k: $17, 16, 9, 8, 1, 0$

Ex: $n = 19$

$\{0\}, \{1, 2, 4, 8, 16, 13, 7, 14, 9, 18, \_ \_ \_ \_ \_ \_ \_ \_ \_\}$

Zeros of a cyclic code: x^n+1 factors into linear factors in $GF(2^m)$

n: odd

Cyclic code: defined by a generator poly

$g(x)$, deg $= r$

$g(x) \mid (x^n+1)$

$\Rightarrow$ $g(x)$: - factor into linear factors in $GF(2^m)$
- has r distinct roots in $GF(2^m)$

Zeros of cyclic code = { distinct roots of $g(x)$ }

- Zeros are elements of order $| n$ in $GF(2^m)$
- Zeros are unions of cyclotomic cosets

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

$c(x) \in$ cyclic code if and only if $c(x)h(x) = 0$ in R_n.

Pf: $c(x) = m(x)g(x)$

Zeros of check poly = $\{0, 1, 2, \ldots, n-1\} \setminus \{\text{zeros of code}\}$

$\langle h(x) \rangle$

Dual of a cyclic code:

C: Cyclic code, $C = \langle g(x) \rangle$

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

$h^\perp(x) = x^{\deg h(x)} h(x^{-1})$

Results: (1) $h^{\perp}(x) \mid (x^n+1)$

(2) $C^{\perp} = \langle h^{\perp}(x) \rangle$

(3) Z : zero set of C

zero set of dual $C^{\perp}$:

$$Z^c = \{0, 1, 2, \ldots, n-1\} \setminus Z$$

$-Z^c \bmod n$