Cyclic Codes

Note Title

- Binary cyclic codes

Defn: A linear code is cyclic if

$$\underline{c} = [c_1\ c_2\ \cdots\ c_n] \in C \Rightarrow [c_n\ c_1\ c_2\ \cdots\ c_{n-1}] \in C$$

$R(\underline{c})$

cyclic right shift

Naive construction

$$G = \begin{bmatrix} \leftarrow & n & \rightarrow \\ — & \underline{g}_1 & — \\ — & R(\underline{g}_1) & — \\ — & R^2(\underline{g}_1) & — \\ & \vdots & \\ — & R^{n-1}(\underline{g}_1) & — \end{bmatrix}$$

- obviously cyclic
- k?

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

represents $\{0,1\}^n$

$\oplus$, $\times$: modulo $x^n + 1$

Cyclic right shift : mult. by x in R_n

Cyclic code: "ideal" in R_n

Ideal of a ring R:

A subset I of R is an ideal if

(1) I : additive subgroup.

(2) $a \in R$ & $b \in I$

$\Rightarrow ab \in I$

In R_n,

(1) $\Rightarrow$ I: linear block code

(2) $\Rightarrow$ $b(x) \in I$

$\Rightarrow x^i b(x) \in I$ $\quad i = 1, 2, \ldots, n-1$

I: cyclic code

Ex: $R_4 = \{0, 1, x, 1+x, x^2, x^2+1, x^2+x, x^2+x+1,$
$x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2+1, x^3+x^2, x^3+x^2+x,$
$x^3+x^2+x+1\}$

R_4 : ideal

$\{0\}$: ideal

Ideal generated by $a(x) \in R_n$

$\langle a(x) \rangle = \{a(x)b(x) : b(x) \in R_n\}$

Prove that this is an ideal

Principal ideals

Ex: $\langle 1 \rangle = R_4$

$\langle a(x) \rangle \overset{?}{=} R_4$ $\quad a(x)b(x) = 1$ and x^n+1

$$\gcd(a(x), x^n+1) = 1$$

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

$$a(x)b(x) + c(x)(x^n+1) = 1$$

$\langle x \rangle = R_4$

$\langle x(x+1) \rangle = ?$

When is $\langle a(x) \rangle = \langle b(x) \rangle$?

Generator polynomial: $I \subseteq R_n$, ideal

$g(x)$: least degree poly in I

Properties: (1) $g(x)$ is unique

Pf: $g'(x), g''(x)$: two least deg poly in I

$\ldots + x^i \quad \ldots + x^i$

$$g'(x) + g''(x) \in I$$

$$\| \; 0$$

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

Pf: Divide x^n+1 by $g(x)$.

$$x^n+1 = q(x)\,g(x) + r(x)$$

$q(x)$ in R_n; $\deg r(x) < \deg g(x)$ & $r(x) \in I$

$\Rightarrow r(x) = 0$

(3) $\underline{a(x) \in I}$.

$\exists\ m(x)$ s.t. $a(x) = m(x)g(x)$ in $F_2[x]$.

$\Rightarrow \boxed{I = \langle g(x) \rangle}$

Pf: Divide $a(x)$ by $g(x)$.

Ex: R_4 $\quad I = \langle x^2+1 \rangle$

$= \{0,\ x^2+1,\ x^3+x,\ x^3+x^2+x+1\}$

$a(x) \in I$, $\gcd(a(x), x^4+1)$

$\langle a(x) \rangle \subseteq I$

$\langle x^3+x \rangle = I$

$\langle x^3+x^2+x+1 \rangle = \{0,\ x^3+x^2+x+1\}$

(2) R_4 $\quad I = \langle x^3+1 \rangle$

$= \{0,\ x^3+1,\ x+1,\ x^3+x,\ x^2+x,\ x^3+x^2+x+1,$

$x^3+x^2,\ x^2+1\}$

$x \longrightarrow p$

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

generator $= a(x)$?