Binary Cyclic Codes

Note Title

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

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

Ideal I of R_n $\longleftrightarrow$ Cyclic code

- subspace of R_n
- $a(x) \in I$, $b(x) \in R_n$
  $\Rightarrow b(x)\, a(x) \in I$

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

$\Downarrow$

$[c_{n-1}\ c_0 \cdots c_{n-2}] \in C$

Generator poly: minimal degree poly in I.

$g(x)$

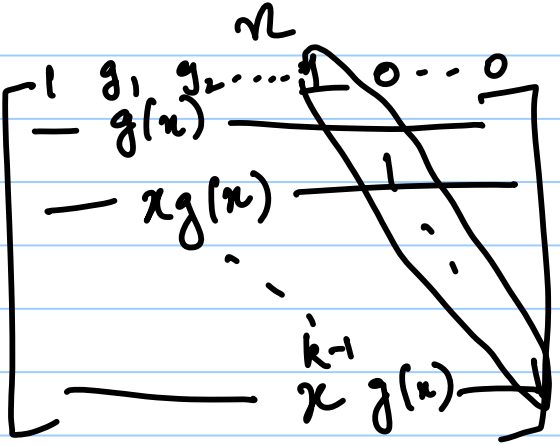
- $g(x) \mid c(x) \in I$
- $\boxed{g(x) \mid (x^n + 1)}$

(n,k) cyclic code

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

$g(x) = 1 + g_1 x + \cdots + x^{n-k}$

Generator matrix:



Parity-check polynomial

$$h(x) \triangleq \frac{x^n+1}{g(x)} = 1 + h_1 x + \cdots + h_{k-1} x^{k-1} + x^k$$

Claim:

$c(x) \in \text{Code}$

$\Updownarrow$

$c(x)\,h(x) = 0 \quad \text{in } R_n.$

makes error detection easy.

$$\left(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}\right)\left(h_0 + h_1 x + \cdots + h_k x^k\right) =$$

$$0 \quad \text{in } R_n.$$

$$x^0: \quad c_0 h_0 + h_1 c_{n-1} + h_2 c_{n-2} + \cdots + h_k c_{n-k} = 0$$

$$(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1})(h_0 + h_1 x + \cdots + h_k x^k) = 0 \quad \text{in } R_n$$

$$x^{n-1}: \; h_0 c_{n-1} + h_1 c_{n-2} + \cdots + h_k c_{n-k-1} = 0$$

$$x^{n-2}: \; h_0 c_{n-2} + h_1 c_{n-3} + \cdots + h_k c_{n-k-2} = 0$$

$$\vdots$$

$$x^{k}: \; h_0 c_k + h_1 c_{k-1} + \cdots + h_k c_0 = 0$$

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

$$\begin{matrix} \\ n-k \end{matrix} \overbrace{\begin{bmatrix} 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 & 0 \\ & & & & \ddots & & & \\ h_k & \cdots & \cdots & h_0 & 0 & \cdots & 0 \end{bmatrix}}^{n} \Leftrightarrow \begin{bmatrix} h^{\perp}(x) \\ x h^{\perp}(x) \\ \ddots \\ x^{n-k-1} h^{\perp}(x) \end{bmatrix}$$

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

Pf: $x^n+1 = g(x)\, h(x)$

$$1+x^n = x^n\, g(x^{-1})\, h(x^{-1})$$

$$= \underbrace{x^{n-k} g(x^{-1})}\ \underbrace{x^k h(x^{-1})}$$

$$h^{\perp}(x)$$

Result: Dual of cyclic code is also cyclic.

$\langle g(x) \rangle$ $\quad h(x) = (x^n+1)/g(x)$

$\langle h^{\perp}(x) \rangle$ $\quad h^{\perp}(x) = x^{\deg h(x)}\, h(x^{-1})$.

Cyclic codes: Encoding + error detection are easy to implement.

Encoding → $m(x)g(x)$ "multiply" by $g(x)$

error detection → divide by $g(x)$

Zeros of a cyclic code: roots of $g(x)$.

Ex: Zeros of t-error-correcting BCH code

$= \{\beta^{b+1}, \beta^{b+2}, \beta^{b+3}, \ldots, \beta^{b+2t}\}$

any b

Zeros are consecutive $\Rightarrow$ guaranteed d_{min}, implementable algebraic BDDs

BCH code connection $n = \text{ord}(\beta)$, BCH is cyclic

Ex:

$t=1$: $H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \end{bmatrix}$

Set $n = 2^m - 1$. Set $\beta \in GF(2^m)$, primitive.

$\longrightarrow$ Hamming code is cyclic in above order

$g(x) = M_\beta(x)$

$m=3$, $n=7$, $\beta \in GF(8)$, primitive, $\beta^3 = 1+\beta$

Hamming code

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$: Not cyclic

	Vector
0	000
1	001
β	010
β^2	100
$\beta^3 = 1+\beta$	011
$\beta^4 = \beta^2+\beta$	110
$\beta^5 = \beta^2+\beta+1$	111
$\beta^6 = 1+\beta^2$	101

$$H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$: cyclic

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

t-error-correcting BCH code:

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

Open + interesting issues

- Decoders beyond t errors?
- "Soft" decoder.