Cyclic codes (13.5)

Def A linear code $C \subseteq K^n$ is cyclic if

$$(a_1, a_2, \ldots, a_n) \in C \iff (a_2, a_3, \ldots, a_{n-1}, a_n, a_1) \in C.$$

Ex The following codes are cyclic ($q = 2$)

- $C = K^n$
- $C = \{0000, 1010, 0101, 1111\}$
- $C =$ parity code in K^n
- $C =$ double repetition code e.g. $010010010 \in C$
  $100100100 \in C$.

Convenient for hardware reasons...

A polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $a_i \in K$, can be identified with the vector $(a_n, \ldots, a_0) \in K^{n+1}$.

This gives a bijection

$$\{\text{polynomials of degree} \leq n-1\} \longleftrightarrow K^n,$$

& we will write $f(x) \in K^n$.

E.g. ($q=2$), $n=3$ $\quad f(x) = x+1 = (0,1,1) \in K^3$.

Thm Let $C \subseteq K^n$ be cyclic. Then there exists a unique polynomial $g(x) = x^k + c_{k-1} x^{k-1} + \cdots + c_0$ s.t.

1. $g(x) \mid x^n - 1$
2. $C = \{f(x) \in K^n \mid g(x) \mid f(x)\}$.

Conversely, given $g(x)$ s.t. $g(x) \mid x^n - 1$, then

$C = \{ f(x) \mid g(x) \mid f(x) \} \subseteq K^n \}$ is a cyclic code.

Ex: $C = \{0000, 1010, 0101, 1111\}$

$\{0 \quad x^3+x \quad x^2+1 \quad x^3+x^2+x+1\}$

$g(x) = x^2+1$, which divides x^3+x, x^3+x^2+x+1,

& x^4-1, $(x^2+1)^2 = x^4+2x^2+1 = x^4+1 = x^4-1$.

Ex: Parity code $g(x) = x+1$. Use • $x+1$ divides $f(x)$

$\iff f(-1) = 0 \iff f(1) = 0 \iff \sum a_i = 0 \iff f(x) \in C$.

$f(x) = a_{n-1}x^{n-1} + \cdots + a_0$

Pf of thm: Let C be cyclic in K^n, want to prove $g(x)$ exists. Let $g(x) \in C$ be element of minimal degree, say $g(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$.

Then C cyclic $\Rightarrow xg(x), x^2g(x), \ldots, x^{n-d-1}g(x) \in C$.

If $f(x) \in C$, polynomial division gives

$$f(x) = q(x)g(x) + r(x)$$

with $\deg q(x) = \deg f(x) - \deg g(x), \leq n-1-d$ (1)

$r(x) = 0$ or $\deg r(x) < \deg g(x)$. (2)

(1) $\Rightarrow q(x)g(x) \in C \xrightarrow{f(x) \in C} r(x) \in C$.

Since deg $g(x)$ minimal,

must have $r(x) = 0$, so $g(x)$ divides $f(x)$.

C cyclic also means that

$$(c_{d-1}, c_{d-2}, \dots, c_0, 0, 0, \dots, 1) \in C$$

$$\| $$

$$x^{n-d} g(x) - (x^n - 1) \in C.$$

So $g(x)$ divides $x^{n-d} g(x) - (x^n - 1)$, meaning it divides $x^n - 1$.

Skip proof of 2nd half.

Polynomial $g(x)$ is called generator polynomial of C.

Every $f(x) \in C$ can be uniquely written as $q(x)\, g(x)$ for some $q(x) = \sum_{i=0}^{n-d-1} a_i x^i \rightsquigarrow f(x) = \sum_{i=0}^{n-d-1} a_i x^i g(x) \Rightarrow \{x^i g(x)\}_{i=0}^{n-d-1}$

is a basis for C.

Generator matrix if $g(x) = x^d + c_{d-1} x^{d-1} + \dots + c_0$ is

$$G = \begin{bmatrix} 0 & \cdots & & 1 & c_{d-1} & \cdots & c_0 & & & g(x) \\ \vdots & & & & & c_0 & 0 & & & x\,g(x) \\ & \ddots & & & & & \ddots & \ddots & & \vdots \\ 0 & 1 & c_{d-1} & & & & & & & \\ 1 & c_{d-1} & c_{d-2} & \cdots & c_0 & 0 & \cdots & 0 & & x^{n-d-1} g(x) \end{bmatrix}$$

To find cyclic codes in K^n, need $g(x)$ dividing $x^n - 1$ (as polynomials over K)

Ex $K = \mathbb{Z}_2$, $n = 7$, $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Find cyclic codes e.g. with $g(x) = x+1$, $g(x) = x^3 + x + 1$, $g(x) = (x+1)(x^3 + x + 1)$
$= x^4 + x^3 + x^2 + 1$.

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

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ & & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$h(x) = \frac{x^n - 1}{g(x)}$ is check polynomial.

If $h(x) = x^{n-d} + a_{n-d-1}x^{n-d-1} + \cdots + a_0$, then parity check matrix is

$$H = \begin{bmatrix} 0 & \cdots & 0 & a_0 & \cdots & a_{n-d-1} \\ \vdots & & & & & 1 \\ & & & & & 0 \\ 0 & & & & & 0 \\ a_0 & & & a_{n-d-1} & 1 & 0 \end{bmatrix}$$

(*)

Ex $(0, 0, \ldots, a_0, a_1, \ldots, a_{n-d-1}, 1) \cdot (0, 0, \ldots, 1, c_{d-1}, \ldots, c_0)$

$= c_0 + c_1 a_{n-d-1} + c_2 a_{n-d-2} + \cdots + c_{n-d} a_0$

$=$ coefficient of x^{n-d} in $g(x)h(x) = x^n - 1$

$= 0.$

Encoding: Message $f(x) \in K^{n-d-1} \longmapsto$ transmit $f(x)g(x) \in C$

Decoding: Receiving $p(x) \in C \longmapsto$ interpret as $\frac{p(x)}{g(x)} \in K^{n-d-1}$

Error detection: If $g(x)$ does not divide $p(x)$, error has occured. Check with polynomial division of $p(x)$ by $g(x)$

(*) $g(x) = x^4 + x^3 + x^2 + 1$, $h(x) = \frac{x^7 - 1}{x^4 + x^3 + x^2 + 1} = x^3 + x^2 + 1$

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