Tutorial III group 2

03 October 2019 15:58

CYCLIC CODES

- ⟶ definition of C. Codes
- ⟶ polynomials over Finite fields
- ⟶ Full characterization of C. Codes

$C \subseteq \{0, \dots, q-1\}^n$ is a cyclic code if following holds:

C is a linear code

I. $\forall x, y \in C, \quad x+y \in C$

II. $\forall x \in C, \quad a \cdot x \in C$ $\quad a \in \mathbb{F}_q = \{0, \dots, q-1\}$, $+, \cdot \mod q$ $\quad$ q - prime

III. $\forall x \in (x_0 \dots x_{n-1}) \in C$

$$\Updownarrow$$

$(x_{n-1}\, x_0 \dots x_{n-2}) \in C$

$\boxed{\text{Ex } 3.1}$ Decide whether given codes are cyclic

a.) $C = \{0000, 1212, 2121\} \subseteq (\mathbb{F}_3)^4$ $\quad$ $(+, \cdot) \mod 3$

I. $(2121) + (1212) = (3333) = (0000)$ ✓

II. $2 \cdot (1212) = (2424) = (2121)$

C is cyclic

III. 1212 - 2121 ✓

b.) $C_3 = \{ x_0x_1x_2x_3x_4 \in \{0,1,2\}^5 \mid x_0 + x_1 + x_2 + x_3 + x_4 \equiv 0 \bmod 3 \}$

$\underbrace{3 \quad 3 \quad 3 \quad 3}_{81 = 3^4}$

the last one can always set sum to 0.

I. $x, y \in C$

$\sum_{i=0}^{4} x_i \equiv 0 \bmod 3 \qquad \sum_{i=0}^{4} y_i \equiv 0 \bmod 3$

$x + y = (x_0 + y_0, x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4)$

$x + y \in C \Leftrightarrow \sum_{i=0}^{4} x_i + y_i \equiv 0$ ✓

$\| $

$\sum_{i=0}^{4} x_i + \sum_{i=0}^{4} y_i = 0 + 0 = 0 \bmod 3$

$a \cdot x \in C$

II. $a \cdot x = (ax_0, ax_1, ax_2, ax_3, ax_4)$

$\sum_{i=0}^{4} ax_i \equiv 0$

$|||$

$a \sum^{4} x_i = a \cdot 0 \equiv 0 \bmod 3$

$i=0$

$\underline{\text{III}}$. addition is commutative ✓

$(a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n$

$\Updownarrow$

$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]$ Set of all polynomials over a finite field of size q.

$a_i \in \{0, \dots, q-1\}$ (for q prime)

$\boxed{\text{Rings}}$ $(S = \{0, \dots, n-1\}, +, \cdot)$

1.) $(S, +)$ is a commutative group

- → addition is 'associative' $(a+b)+c = a+(b+c)$
- → addition is 'commutative' $a+b = b+a$
- → there is a neutral element '0' s.t. $a+0=a$
- → for each element 'a' there is an additive inverse '$-a$' s.t. $a+(-a) = 0$.

2.) $(S, \cdot)$ is 'monoid'

- → multiplication is 'associative' $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- → there is a neutral element '1' s.t. $a \cdot 1 = a$

→ '$\cdot$' is distributive towards '+'

$$a\cdot(b+c) = ab + ac$$
$$(b+c)\cdot a = ba + ca$$

Field axiom

→ for each non-zero element a there is a multiplicative inverse 'a^{-1}', s.t. $a \cdot a^{-1} = 1$

$\boxed{\{0,1,2,3\} \quad (+,\cdot) \bmod 4}$

2^{-1} does not exist (division by 2 is not defined)

1133 1123
3311 3321

$\{0,2,0,2\}$

$(\{0,\ldots,n-1\}, \cdot, + \bmod n)$ → generally a ring

→ for n prime it is a field

Finite fields exist for $n = p^k$ where p is a prime

POLYNOMIALS OVER FINITE FIELDS

$\mathbb{F}[x]$ - a set of all polynomials over a finite field $\mathbb{F}$

$f(x) = \sum_{i=0}^{\infty} a_i x^i \qquad a_i \in \mathbb{F}$ ~~4~~ $(+,\cdot)$

$\mathbb{R}$

$\mathbb{F}_2[x]$ examples

$1+x \qquad \deg(x+1)=1$

$1+x^2+x^3+x^7 \qquad \deg(1+x^2+x^3+x^7)=7$

$\deg(f(x))$ is it's highest exponent

Division of polynomials

Examples

$x^7-1 : x^3+x^2+1$

a.) in $\mathbb{F}_2$

$$
\begin{aligned}
&x^7+1 : x^3+x^2+1 = x^4+x^3+x^2+1\\
&-(x^7+x^6+x^4)\\
&\overline{x^6+x^4+1}\\
&-(x^6+x^5+x^3)\\
&\overline{x^5+x^4+x^3+1}\\
&-(x^5+x^4+x^2)\\
&\overline{x^3+x^2+1}
\end{aligned}
$$

in $\mathbb{F}_3 \qquad (0,1,2)\sim(0,1,-1)$

$$
\begin{aligned}
&x^7-1 : x^3+x^2+1 = x^4-x^3+x^2+x\\
&-(x^7+x^6+x^4)\\
&\overline{-x^6-x^4-1}\\
&-(-x^6-x^5-x^3)\\
&\overline{x^5-x^4+x^3-1}\\
&-(x^5+x^4+x^2)\\
&\overline{x^4+x^3+x^2-1}\\
&-(x^4+x^3+x)\\
&\overline{x^2+x-1}
\end{aligned}
$$

$x^7-1 = (x^3+x^2+1)(x^4-x^3+x^2+x) + x^2+x+1$

$f(x) = q(x)\cdot h(x) + r(x)$

$\deg(r(x)) < \deg(h(x))$

Example

all remainders after division by x^2+x+1

$0+0\cdot x \quad 1+0\cdot x \quad 0+1\cdot x \quad 1+x$

$00 \quad 10 \quad 01 \quad 11$

$\mathbb{F}_2[x]/\underline{x^2+x+1} = \{0, 1, x, x+1\}$

$\mathbb{F}_q[x]/f(x)$ contains all polynomials of degree smaller than $\deg(f(x))$ $\Leftrightarrow$ corresponds to strings of size n

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Commutative group

$\cdot$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$x^2 : x^2+x+1 = 1$

$\underline{x^2+x+1}$

$x+1$

$x\cdot(x+1)$

$x^2+x : x^2+x+1$

$\underline{x^2+x+1} = 1$

1

$\mathbb{F}[x]/f(x)$ is a field iff $f(x)$ is a primitive polynomial over $\mathbb{F}$.

$f(x)$ is a primitive polynomial over $\mathbb{F}$, if it cannot be written as a product of two polynomials of a smaller degree

is x^2+x+1 primitive over $\mathbb{F}_2$?

x

$(x+1)$

$x(x+1) = x^2+x \neq x^2+x+1$

$x \cdot x = x^2 \neq x^2+x+1$

$(x+1)\cdot(x+1) = x^2+1 \neq x^2+x+1$

$R_n = \mathbb{F}[x]/x^n-1$ = all polynomials of degree at most $n-1$, thus corresponds to all strings of $\mathbb{F}$ of size n.

multiplication by x:

$f(x) = a_0 + a_1x + \dots a_{n-1}x^{n-1}$

$x \cdot f(x) = a_0x + a_1x^2 + \dots + a_{\cancel{n-1}}x^n \,:\, x^n-1 = a_{n-1}$

$-(a_{\cancel{n-1}}x^n - a_{n-1})$

$= a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1}$

$(a_0, \dots a_{n-1}) \sim (a_{n-1}\; a_0 \dots a_{n-2})$

Ideals $I \subseteq \mathbb{F}[x]/x^n-1$ closed under multiplication

$\langle g(x) \rangle = \{ g(x) \cdot h(x) \mid h(x) \in \mathbb{F}[x]/x^n-1 \}$

$x^2(x+1)$

Example

Example

$$\mathbb{F}_2[x]/x^3-1 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^2+x\}$$

110, 011, 101

$x^2(x+1)$

$(x+1) \to x^2+x \to x^2+1$

$x^2+1 = 1\cdot 0 + 0\cdot x + 1\cdot x^2$

$$\langle x+1\rangle = \{\overset{000}{0}, \overset{110}{x+1}, \overset{011}{x^2+x}, \overset{101}{x^2+1}\}$$

$$= \{h(x)\cdot(x+1) \mid h(x)\in \mathbb{F}[x]/x^3-1\}$$

$$\langle x^2+1\rangle = \langle x^2\cdot(x+1)\rangle$$

$$= \{\underbrace{h(x)\cdot x^2}_{h'(x)}\cdot(x+1) \mid h(x)\in \mathbb{F}[x]/x^3-1\}$$

$$= \langle h'(x)\cdot(x+1) \mid h'(x)\rangle$$

φ

$$\langle x^2+1\rangle \subseteq \langle x+1\rangle$$

$$\langle x+1\rangle = \langle x(x^2+1)\rangle$$

$$\| $$

$$\langle \underbrace{h(x)\cdot x}_{h'(x)}(x^2+1) \mid h(x)\, \mathbb{F}[x]/x^3-1\rangle$$

$$\subseteq \langle x^2+1\rangle$$

$(x+1)(x+1)$

$\|$

$(x+1)x + (x+1)1$

$x^2+x \quad +x+1$

x^2+1

$(x+1)\cdot(x^2+1)$

$= (x+1)\cdot x^2 + (x+1)$

$x^2+1 \quad +x+1 = x^2+x$

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

$(x+1)\cdot x^2 + (x+1)x + x+1$

$x^2+1 \quad + x^2+x \quad + x+1 = 0$

$(x+1)\cdot(x^2+x) =$

$(x+1)\cdot x^2 + (x+1)x$

$x^2+1 + x^2+x = x+1$

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

110   101

110

$x^2\cdot(x+1) = x^3+x^2 ; x^3+1=1$

x^3+1

$$\frac{x^3+1}{(x^2+1)}$$

$$(1\,1\,0)$$

$$\underbrace{x\cdot x\cdot(x+1)}_{0\,1\,1}$$

$$1\cdot x^0 + 1\cdot x + 0\cdot x^3$$

$$x\cdot(x+x^2)$$

$$(0\,1\,1)$$

$$(1\,0\,1)$$

$$1+0\cdot x+1\cdot x^2$$

$$\shortparallel$$

$$(x^2+1)$$

$$\underline{x^2+1 = x^2(x+1)}$$

$$\langle x^2+1\rangle = \{(x^2+1)\cdot h(x) \mid h(x)\in R_n\}$$

$$\langle x+1\rangle = \{(x+1)\,h(x) \mid h(x)\in R_n\}$$

$$\langle x^2+1\rangle = \langle x^2(x+1)\rangle$$

$$= \{\underbrace{h(x)\cdot x^2}_{h'(x)}\cdot(x+1) \mid h(x)\in R_n\}$$

$$= \{h'(x)\cdot(x+1) \mid h'(x) \text{ are some (possibly not all polynomials)}\}$$

$$\subseteq \langle x+1\rangle$$

$$\langle x+1\rangle \subseteq \langle x^2+1\rangle \qquad x+1 = x\,(x^2+1)$$

How do we characterize different ideals?

Each ideal is characterized by a unique divisor of x^n-1 in $\mathbb{F}[x]$

primitive   primitive

$$x^3-1 = (x+1)(x^2+x+1)$$

$x+1$ $\quad \langle x+1 \rangle = \{000, 110, 101, 011\}$

x^2+x+1 $\quad \langle x^2+x+1 \rangle = \{000, 111\}$

x^3-1 $\quad \langle x^3-1 \rangle = \{000\}$

1 $\quad \langle 1 \rangle = \{0,1\}^3$

To find all cyclic codes you need to find decomposition of $f(x)$ into primitive polynomials.

$$f(x) = h(x)\, g(x)\, a(x)$$

To each C. Code we can associate a divisor $g(x)$, and we call it the generator polynomial

$\deg(g(x)) = t$

$$G = \overbrace{\begin{pmatrix} g_0 & g_1 & \cdots & g_t & 0 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_{t-1} & g_t & 0 & 0 & 0 \\ & & & \vdots & & & & \\ 0 & 0 & 0 & \cdots & \cdots & g_{t-2} & g_{t-1} & g_t \end{pmatrix}}^{n}$$

$$f(x) = g(x) \cdot h(x)$$

$$h(x) = h_0 + h_1 x + \dots + h_{n-k} x^{n-k}$$

$$H = \begin{pmatrix} \overbrace{h_{n-k} & h_{n-k-1} & \dots & h_0 & 0 & \cdots 0 & 0}^{n} \\ 0 & h_{n-k} & & & h_0 & 0 & 0 \\ & & & \vdots & & & \end{pmatrix}$$

$$mG = c$$

$$\Updownarrow$$

$$m(x) \cdot g(x) = c(x)$$

$$m \cdot G$$

$$m = (m_0 \dots m_{n-1})G = (m_0 g_0, \; m_0 g_1 + m_1 g_0, \; m_0 g_2 + m_1 g_1 + m_2 g_0, \dots$$

$$(m_0 + m_1 x + \dots + m_{n-1} x^{n-1})(g_0 + g_1 x + \dots x^2 \dots + g_{n-1} x^{n-1})$$

$$= m_0 g_0 + (m_0 g_1 + g_0 m_1) X + \qquad x^2$$