Tutorial III

23 October 2020 10:39

Cyclic codes

→ definition of cyclic codes

→ polynomials over finite fields

→ Full characterization of cyclic codes

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

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

II. $\forall x \in C, \forall a \in \{1, \dots, q-1\}$ $a.x \in C$

$q \in \mathbb{F}_q = \{0 \dots, q-1\}, +, \cdot$ if q is prime $(\bmod q)$

C is a linear code

III. $\forall x \in (x_0 x_1 \dots x_{n-1}) \in C$

$\Downarrow$

$(x_{n-1}, x_0 x_1 \dots x_{n-2}) \in C$

$\boxed{\text{Ex3.1}}$ Decide whether given codes are cyclic

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

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

I. $(2121)+(1212)=(3333)=(0000)$ ✓

II. $2\cdot(1212)=(2424)=(2121)$
$2.(2121)=(4242)=(1212)$ ✓

III. $(2121)\sim(1212)$ ✓

b) $C=\{x_0x_1x_2x_3x_4 \in \{0,1,2\}^5 \mid \underbrace{x_0+x_1+x_2+x_3}_{\text{arbitrary}}+x_4 \equiv 0 \mod 3\}$

arbitrary

$\Updownarrow$

$3.3.3.3=81$

x_4 always sets sum of $x_0+x_1+x_2+x_3$ to 0

I. $x,y\in C$

$x=(x_0x_1x_2x_3x_4)$ $\quad \sum_{i=0}^{4} x_i \equiv 0 \mod 3$

$y=(y_0y_1y_2y_3y_4)$ $\quad \sum_{i=0}^{4} y_i \equiv 0 \mod 3$

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

$$\sum_{i=0}^{4}(x_i+y_i)=\sum_{i=0}^{4}x_i+\sum_{i=0}^{4}y_i \equiv 0+0\equiv 0 \mod 3$$

II. $x\in C \Leftrightarrow \sum_{i=0}^{4} x_i \equiv 0 \mod 3$

$2x \overset{?}{\in} C$

$2x=(2x_0, 2x_1, 2x_2, 2x_3, 2x_4)$

$$\sum^{4} 2x_i \equiv 2\sum_{i=0} x_i \equiv 2\cdot 0 \equiv 0 \mod 3$$ ✓

$$\sum_{i=0}^{1} 2x_i \equiv 2\sum_{i=0}^{1} x_i \equiv 2 \cdot 0 \equiv 0 \mod 3 \quad \checkmark$$

$\underline{III}$, addition is commutative $\checkmark$

Refresher on Algebra

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

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' $(a.b).c = a.(b.c)$

→ there is a neutral element '1' s.t. $a.1 = a$

3.)

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

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

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

Every field is a ring, but additional axiom needs to hold!

Field axiom

→ for each non-zero element a there is a multiplicative inverse (a^{-1}), s.t. $a \cdot a^{-1} = 1$

Ring (not a field)

$\{0,1,2,3\}, (+,\cdot) \bmod 4$ → Ring

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

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

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

→ for n prime this is a field

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

$$\boxed{\begin{array}{c} (a_0, \dots, a_{n-1}) \in \mathbb{F}_q^n \\ \Updownarrow \\ a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots + a_{n-1} x^{n-1} \end{array}} \in \mathbb{F}_q[x]$$

Set of all polynomials over a finite field of size q.

Examples

$\mathbb{F}_2[x] \Leftrightarrow a \in \{0,1\}$

$1+x \Leftrightarrow (11)$ $\quad \deg(x+1) = 1$

$1+x^2+x^3+x^7 \Leftrightarrow (10110001)$ $\quad \deg(1+x^2+x^3+x^7) = 7$

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

Division of polynomials

Examples:

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

a.) $\mathbb{F}_2[x]$ $\quad -1 \equiv 1 \mod 2$

$$x^7+1 : \boxed{x^3+x^2+1} = x^4+x^3+x^2+1$$

$$-(x^7+x^6+x^4)$$

$$-x^6-x^4+1$$

$$x^6+x^4+1$$

$$-(x^6+x^5+x^3)$$

$$x^5+x^4+x^3+1$$

$$-(x^5+x^4+x^2)$$

$$\boxed{x^3+x^2+1}$$

$\mathbb{F}_3[x]$ $\quad (0,1,2) \sim (0,1,-1)$ $\quad 2 \equiv -1 \mod 3$

$$x^7-1 : x^3+x^2+1 = x^4-x^3+x^2+x$$

$$-(x^7+x^6+x^4)$$

$$-x^6-x^4-1$$

$$-(-x^6-x^5-x^3)$$

$$x^5-x^4+x^3-1$$

$$-(x^5+x^4+x^2)$$

$$-2x^4+x^3+x^2-1$$

$$x^4+x^3+x^2-1$$

$$-(x^4+x^3+x)$$

$$x^2-x-1 \rightarrow \text{remainder}$$

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

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

$$\deg(r(x)) \leq \deg(q(x))$$

$\mathbb{F}_q[x]/f(x)$ $\rightsquigarrow$ set of all remainders after division by $f(x)$

$\rightsquigarrow$ set of all polynomials of degree smaller than $\deg(f(x))$

$$\boxed{\mathbb{F}_2[x]/x^2+x+1} = \{0, 1, x, x+1\} \quad +, \cdot \quad \text{mod } (x^2+x+1)$$

+	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

•	0	1	x	x+1
0	0	0	0	0
1	0	$\boxed{1}$	x	x+1
x	0	x	x+1	$\boxed{1}$
x+1	0	x+1	$\boxed{1}$	x

$$\begin{aligned} &x^2 : x^2+x+1 = 1 \\ &\underline{-(x^2+x+1)} \\ &\quad x+1 \end{aligned}$$

$$\begin{aligned} &x^2+x : x^2+x+1 = 1 \\ &\underline{-(x^2+x+1)} \\ &\quad 1 \end{aligned}$$

$$\begin{aligned} &(x+1)^2 = \\ &x^2+1 : x^2+x+1 = 1 \\ &\underline{-(x^2+x+1)} \\ &\quad x \end{aligned}$$

Field! (of size 4)

$\mathbb{F}_q[x]/f(x)$ $(+, \cdot)$ mod $f(x)$ is a field iff $f(x)$ is irreducible in $\mathbb{F}_q$

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

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

x, $x+1$

$$\left.\begin{aligned} x \cdot (x+1) &= x^2+x \\ x \cdot x &= x^2 \end{aligned}\right\} \neq x^2+x+1$$

$$\left.\begin{array}{ll} x\cdot(x+1) & = x^2+x \\ x\cdot x & = x^2 \\ (x+1)\cdot(x+1) & = x^2+1 \end{array}\right\} \neq x^2+x+1$$

// all strings of size n over alphabet $\mathbb{F}_q$

$$R_n = \mathbb{F}[x] / x^n-1 = \boxed{\text{all polynomials of degree at most } n-1}$$

equipped with addition and multiplication mod x^n-1.

Multiplication by x

$$f(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$$

$$x \cdot f(x) = a_0 x + a_1 x^2 + \dots + \cancel{a_{n-1}x^n} \;:\; x^n - 1 = a_{n-1}$$

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

$$= a_{n-1} + a_0 x + a_1 x^2 + \dots + a_{n-2}x^{n-1}$$

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

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

$$\langle g(x) \rangle = \left\{ g(x) \cdot h(x) \;\middle|\; h(x) \in \mathbb{F}_2[x]/x^n-1 \right\}$$

Example

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

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

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

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

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

$$\|$$

$$\{h(x)(x^2+1) \mid h(x)\in \mathbb{F}_2[x]/x^3-1\}$$

$$\|$$

$$\{\underbrace{h(x)\cdot x^2}_{h'(x)}(x+1) \mid h(x)\in \mathbb{F}_2[x]/x^3-1\}$$

$$\|$$

$$\{h'(x)\cdot(x+1) \mid h'(x)\} \subseteq \langle x+1\rangle = \{h(x)\cdot(x+1) \mid h(x)\in\mathbb{F}_2[x]/x^3-1\}$$

$$\boxed{\langle x^2+1\rangle \subseteq \langle x+1\rangle}$$

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

$$\|$$

$$\{\underbrace{h(x)\cdot x}_{h'(x)}\cdot(x^2+1) \mid h(x)\in\mathbb{F}_2[x]/x^3-1\}$$

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

$$\boxed{\langle x+1\rangle \subseteq \langle x^2+1\rangle}$$

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

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

x^2+1

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

$(x+1)\cdot x^3 \Leftrightarrow (101) \Leftrightarrow (x^2+1)$

(110)

$(x+1)\cdot x \Leftrightarrow (011) \Leftrightarrow (x^2+x)$

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

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

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

$$(101) \overset{\cdot x}{\sim} (110) \sim (x+1)$$

How do we characterize different ideals?

Each ideal is characterized by a unique divisor of $\underline{x^n-1}$

Example

$$x^3-1 = \underbrace{(x+1)}_{\text{irreducible}}\,\underbrace{(x^2+x+1)}_{\text{irreducible}}$$

$$
\begin{array}{lll}
x+1 & \langle x+1\rangle = \{\overset{0}{000},\ \overset{1+x}{110},\ \overset{1+x^2}{101},\ \overset{x+x^2}{011}\} & \leftarrow \\
x^2+x+1 & \langle x^2+x+1\rangle = \{000,\ 111\} & \leftarrow \\
x^3-1 & \langle x^3-1\rangle = \{000\} & \leftarrow \\
1 & \langle 1\rangle = \{0,1\}^3 & \leftarrow
\end{array}
$$

To find $\underline{\text{all}}$ cyclic codes over $\mathbb{F}_q[x]$ of length n, you need to find decomposition of x^n-1 into irreducible polynomials in $\mathbb{F}_q$

Ideals of $\mathbb{F}_q[x]/x^n-1$ are the cyclic codes of length n.

To each cyclic code we can associate a divisor $g(x)$ and we call it the generator polynomial

$\deg(g(x)) = k$ $\qquad g(x) = g_0 + g_1x + g_2x^2 + \cdots g_kx^k$

$$G = \begin{pmatrix} \overbrace{g_0 \ g_1 \ g_2 \cdots g_k}^{k-1} & \overbrace{0 \ 0 \ 0 \ 0}^{n-k-1} \\ 0 \ g_0 \ g_1 \ g_2 \cdots & g_k \ 0 \ 0 \ 0 \\ & \vdots \\ \underbrace{0 \ 0 \ 0 \ 0}_{n-k-1} & g_0 \ g_1 \cdots \ g_k \end{pmatrix}$$

$$x^n-1 = g(x)\cdot h(x)$$

$$h(x) = h_0 + h_1x + \cdots + h_{n-k}x^{n-k}$$

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

$$H = \begin{array}{c} \overbrace{\qquad\qquad}^{n-(n-k-1)} \\ \begin{pmatrix} h_{n-k} & h_{n-k-1} & \cdots & h_0 & 0 & 0 & 0 & 0 \\ 0 & h_{n-k} & \cdots & \cdots & h_0 & 0 & 0 & 0 \\ & & & & & & & \\ 0 & 0 & 0 & 0 & & \cdots & h_1 & h_0 \end{pmatrix} \end{array}$$

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

$G = k \times n$ matrix

$m \in \{0, 1, \dots, q-1\}^k$

$m \approx m(x)$ - polynomial of degree at most $k-1$

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

$$m(x) \cdot g(x) = (m_0 + m_1 x + \dots + m_{k-1} x^{k-1}) \cdot (g_0 + g_1 x + \dots + g_{n-1} x^{n-1})$$

$$= m_0 g_0 + (m_0 g_1 + m_1 g_0) \cdot x + \dots$$