Tutorial III (1)

03 October 2019 09:55

CYCLIC CODES

- → definition
- → polynomials over finite fields
- → cyclic code characterization

Cyclic codes definition

$C \subseteq \{0, \dots, q-1\}^n$ is cyclic if

1.) $\forall x, y \in C \quad x + y \in C$

2.) $\forall x \in C \quad a \cdot x \in C \quad \boxed{a \in \mathbb{F}_q}$

Finite field of size q

→ C is linear

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

$\Updownarrow$

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

$\boxed{\text{Ex.3.1}}$ Are the following codes cyclic?

a.) $\{0000, 1212, 2121\} \quad C \leq (\mathbb{F}_3)^4 \quad (\{0,1,2\}, (+, \cdot) \bmod 3)$

LINEARITY ✓

$(1212) + (2121) = (3333) = (0000)$

$2 \cdot (1212) = (2424) = (2121)$ ✓

$2121 \to 1212$ ✓

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

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

$\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \quad \downarrow$

$3 \quad 3 \quad 3 \quad 3 \quad \approx 3^4$ codewords

$x = (x_0 \dots x_4)$
$y = (y_0 \dots y_4)$ $\in C$

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

I. $x+y \overset{?}{\in} C$

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

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

II. for each $c \in \mathbb{F}_3$ $\forall x \in C$

$c \cdot x \overset{?}{\in} C$

$c \cdot x = (c \cdot x_0, c \cdot x_1, c \cdot x_2, c \cdot x_3, c \cdot x_4)$

$$\sum_{i=0}^{4} c \cdot x_i \equiv c \cdot \sum_{i=0}^{4} x_i = c \cdot 0 = 0 \quad \bmod 3$$

III. if $(x_0, \dots, x_4) \in C$ is also $(x_4, x_0, \dots, x_3) \overset{?}{\in} C$

$$(x_0+x_1+x_2+x_3+x_4) = 0 \overset{?}{\Rightarrow} (x_4+x_0+x_1+x_2+x_3) = 0$$

$\checkmark$

$c \in \mathbb{F}_q^n \qquad (c_0, c_1, \dots, c_{n-1}) \in \{0, \dots, q-1\}^n$ Set of all polynomials over $\mathbb{F}_q$

$\Updownarrow$

$$(c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}) \in \mathbb{F}_q[x]$$

Rings $\left(S=\{0,\ldots,n-1\}, +, \circ\right)$ n - prime
$+,\circ$ mod n

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

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

2.) - multiplication is associative $(a\circ b)\circ c = a(b\circ c)$
- there is a neutral element '1' s.t. $a\circ 1 = a$
- '$\circ$' is distributive toward '$+$' (left distributive)
$a\circ(b+c) = a\circ b + a\circ c$

RING

+ FIELD AXIOM

- for each $a \neq 0$ there is an inverse (a^{-1})
s.t. $a\cdot a^{-1} = 1$.

- $\{0,1,2,3\}$ mod 4

2^{-1} does not exist

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

$\left(\{0,\ldots,n-1\}, +,\circ \text{ mod } n\right)$ ⇝ is generally a ring not a field.

if n is a prime ↑ is a field

Finite fields exist for any number of elements p^k, where p is a prime.

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

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \qquad a_i \in \mathbb{F} \quad f(x) \approx (a_0, a_1, \dots,)$$

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

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

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

$1+x+x^2+\overset{0}{2}x^3 = 1+x+x^2 \qquad \deg(1+x+x^2) = 2$

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

Division of polynomials

Example:

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

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

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

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

b.) in $\mathbb{F}_3$ – $(0,1,2) \approx (0,1,-1)$

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

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

$-x^6 - x^4 \quad 1$

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

$\cancel{x^7}-\cancel{x^7}-x^6-x^4+1$

x^6+x^4+1

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

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

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

x^3+x^2+1

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

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

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

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

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

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

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

$-x^2-x-1$

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

$-x^2-x-1$

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

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

$\rightarrow$ polynomials can be divided with a remainder

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

Example

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

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

$x+1$

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

·	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

$\Downarrow$

Commutative group

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

$\overline{\quad 1 \quad}$

$\Rightarrow$ all ring axioms and a field axiom

$\Uparrow$

if all ring axioms
and a field axiom
hold.

$$\Updownarrow$$

$$\left(\{0, 1, x, x+1\}, \cdot, + \mod x^2+x+1 \right)$$ is a field!

Primitive polynomials

A primitive polynomial over $\mathbb{F}_q$ cannot be written as a product of two other polynomials.

$F[x]/f(x)$ is a field iff $f(x)$ is primitive

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

$$\left.\begin{array}{l} x \cdot x = x^2 \neq x^2+x+1 \\ x(x+1) = x^2+x \neq x^2+x+1 \\ (x+1)(x+1) = x^2+1 \neq x^2+x+1 \end{array}\right| \rightarrow \text{Q.E.D}$$

x^2+x+1 is primitive

$R_n = \mathbb{F}[x]/x^n-1$ = all polynomials with $\deg < n$ together with multiplication and addition "mod x^n-1"

$\approx$ All strings of length n

MULTIPLICATION BY x

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

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

$$\approx (a_{n-1} a_0 \dots a_{n-1})$$

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

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

$$a_{n-2} x^{n-1} + a_{n-3} x^{n-2} + \dots + a_1 x^2 + a_0 x + a_{n-1}$$

Ideals $\boxed{I \subseteq \mathbb{F}[x]/x^n - 1}$ a subset of polynomials closed under multiplication.

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

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

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

$$\{000, 110, 011, 101\}$$

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

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

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

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

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

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

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

$h'(x) = h(x) \cdot x^2$

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

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

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

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

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

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

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

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

(x^2+1)

$(x+1) =$

$x^2(h(x) \quad x^3-1$

What is missing is a way to characterize different ideals:

Each ideal is characterized by a unique divisor of x^n-1

Primitive — this is primitive

$x^3-1 = \boxed{(x+1)(x^2+x+1)}$ — This is the hard part!

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

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

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

$\langle 1\rangle \to \{0,1\}^3$

To each code we associate a divisor $g(x)$ of x^n-1 in $\mathbb{F}_q$. It is called a <u>generator polynomial</u>.

if C has a generator polynomial $g(x)$ $\deg(g(x))=\ell$

$$\begin{array}{c} \\ (m_0 \dots m_\ell) \end{array} \quad G = \overbrace{\begin{pmatrix} g_0 & g_1 & \dots & g_\ell & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \dots & g_{\ell-1} & g_\ell & \\ & & \dots & & & & \\ 0 & 0 & \dots & g_0 & \dots & g_{\ell-1} & g_\ell \end{pmatrix}}^{n}$$

$m \cdot G = c = (g_0 m_0, g_1 m_0 + g_0 m_1, g_2 m_0 + g_1 m_1 + g_0 m_2, \dots)$

$m(x) = m_0 + m_1 x + \dots + m_\ell x^\ell$

$\boxed{m(x) \cdot g(x)} = c(x)$ $\qquad (g_1 m_0 + m_1 g_0)\, x$

$= g_0 m_0,$

H

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

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

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

$$\bar{h}(x) = h_{n-k} + \dots + h_1 x^{n-k-1} + h_0 x^{n-k} \leftarrow (h_{n-k}\ h_{n-k-1} \dots h_0) \sim$$

$$H = \begin{pmatrix} h_{n-k} & h_{n-k-1} & \dots & h_0 & 0 & 0 & 0 \\ 0 & h_{n-k} & \dots & & h_0 & 0 & 0 \\ & \vdots & & & & & \\ 0 & 0 & 0 & \dots & h_2 & h_1 & h_0 \end{pmatrix}$$