Tutorial 3 ENG

29 September 2021 13:52

CYCLIC CODES

Tutorial 1		Tutorial 2		Tutorial 3
General codes	$\supseteq$	Linear codes	$\supseteq$	Cyclic codes
$C \subseteq \{0,1\}^n$		C is a subspace of $\{0,1\}^n$		C is an ideal in R_n
encode: store whole code		encode: generation matrix		encode: generation polynomial
decode: find closest codeword		decode: parity check matrix which coset?		decode: parity check polynomial

Definition of cyclic codes

$C \in \{0, \dots, q-1\}^n$ is a cyclic code (q is a power prime)

if following holds:

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

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

C is a linear code

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

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

$$\Downarrow$$

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

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

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

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

II.) $2.(1212) = (2424) = (2121) \in C$

$2.(2121) = (4242) = (1212) \in C$

$2.(0000) = (0000) \in C$

III $1212 \rightsquigarrow 2121 \in C$

$2121 \rightsquigarrow 1212 \in C$

✓ CYCLIC CODE

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

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

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

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

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

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

$k \in \{0,1,2\}$

$k.x \overset{?}{\in} C$

$k.x = (k.x_0, k.x_1, kx_2, kx_3, kx_4)$

$$\sum_{i=0}^{4} k.x_i = k.\boxed{\sum_{i=0}^{4} x_i} \equiv k.0 \equiv 0 \mod 3$$

III addition is commutative

Refresher on algebra

Refresher on algebra

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 $a \in S$ there is an additive inverse '$-a$'

  s.t. $a + (-a) = 0$

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

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

3.) '$\cdot$' is distributive towards '$+$'

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

Every field is a ring with an additional axiom

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

Ring (not a field)

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

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

2^{-1} does not exist

$2.\ \{0,1,2,3\}$

$\|$

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

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

$\rightarrow$ for n prime this is also a field

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

$$\boxed{\begin{gathered}(a_0,\dots,a_{n-1}) \in \mathbb{F}_q^n \\ \Updownarrow \\ (a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{n-1}x^{n-1}) \in\end{gathered}}\ \mathbb{F}_q[x]$$

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

Examples

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

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

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

$\deg(f(x))$ is the highest exponent of $f(x)$.

Division of polynomials

Examples:

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

$2 \equiv -1 \mod 3$

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

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

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

$x^6 + x^4 + 1$

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

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

$x^5 + x^4 + x^2$

$x^3 + x^2 + 1$

b.) $\mathbb{F}_3[x]$ $\quad (0,1,2) \sim (0,1,-1)$

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

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

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

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

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

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

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

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

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

$-x^2 - x - 1$ → remainder

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

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

↙ remainder ↙ divisor

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

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

⇝ Set of all polynomials of degree smaller than $\deg(f(x))$

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

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

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

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

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

Finite field of size 4!

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

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

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

x, x+1, 1, 0

$$\left.\begin{array}{ll} x\cdot(x+1) & = x^2+x \\ (x+1)\cdot(x+1) & = x^2+1 \\ x\cdot x & = x^3 \end{array}\right\} \neq x^2+x+1$$

↗ all strings of length n over $\mathbb{F}_q$.

$R^q = \mathbb{F}]x[\ /$ $=$

≙ all strings of length n over $\mathbb{F}_q$.

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

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

Multiplication by x in R_n

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

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

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

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

$(a_0, \dots, a_{n-1}) \rightsquigarrow (a_{n-1}, a_0, \dots, a_{n-2})$ → cyclic shift!

Ideal

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

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

Example

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

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

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

$\{ h(x) \cdot (x^2+1) \mid h(x) \in$?

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

$\Rightarrow x^3 + x^2 : x^3 - 1 = 1$

$-(x^3 - 1)$

$(110) \sim (011) \sim (101) \quad 0$

$(1 + x^2) \quad \emptyset$

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

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

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

$$\|$$

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

$$\|$$

$$\{h'(x)\cdot(x+1) \mid h'(x)\} \subseteq \langle x+1\rangle$$

$$\Big| = (x+1)\cdot x^2 + (x+1)$$
$$= x^2+1 \quad + x+1$$
$$= \boxed{x^2+x}$$

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

$h(x).\ x+1$

$\underbrace{h(x).\ x}_{h'(x)}\cdot(x^2+1)$

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

How do we find all ideals of R_n^q?

$\|$

all cyclic codes of lenght n over $\mathbb{F}_q$.

Each ideal is uniquely characterized by an unique divisor of $\underline{x^n-1}$ in $\mathbb{F}_q[x]$.

↗ irreducible ↗ irreducible

$|.\ 2$

$$\boxed{x^3-1} = \underset{\nearrow}{(x+1)}\overset{\nearrow \text{irreducible}}{}(x^2+x+1) \quad \nearrow \text{irreducible}$$

$\mathbb{F}_2[x]$

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

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

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

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

$$(x^2+x+1)\circ(a_2x^2+a_1x+1)$$

$$(x^2+x+1) + a_1x(x^2+x+1) + a_2x^2(x^2+x+1) = 0$$

$$\Rightarrow x^2+x+1$$

To each cyclic code we can associate generator polynomial $\langle g(x)\rangle$ (divisor of x^n-1)

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

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & \overbrace{0\;0\;0\;0}^{n-k} \\ 0 & g_0 & g_1 & \cdots & g_{k-1} & g_k & 0\;0 \\ & & & \vdots & & & \ddots \\ 0\;0\;0\;0 & g_0 & \cdots & g_k \end{pmatrix}$$

$m, n, 1$

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

$\nearrow$ parity check polynomial

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

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

$$H = \begin{pmatrix} h_{n-k} & h_{n-k-1} & \dots & h_0 & \overbrace{0 \quad 0 \quad 0 \quad 0}^{n-(n-k-1)} \\ 0 & h_{n-k} & h_{n-k-1} & \dots & h_0 \quad 0 \quad 0 \quad 0 \\ & & \vdots & & \\ & & h_{n-k} & \dots & h_1 \quad h_0 \end{pmatrix}$$

$$m \circ G = C$$

$$\Updownarrow$$

$m(x) \circ \boxed{g(x)}$ → LFSR (linear feedback shift registers)

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

$$m(x) \circ g(x) = (m_0 + m_1 x + \dots + m_{k-1} x^{k-1}) \circ (g_0 + g_1 x + g_2 x^2 + \dots + g_{n-1} x^{n-1})$$

$$= m_0 \cdot g_0 + (m_1 \cdot g_0 + m_0 \cdot g_1) \cdot X$$