Tutorial 3 SK

29 September 2021 17:58

CYKLICKÉ KÓDY

Lekcia 1 | Lekcia 2 | Lekcia 3

$C \subseteq \{0,1\}^n$ $\supseteq$ C je lineárny podpriestor $\supseteq$ C je ideál R_n

Kódovanie: tabuľka | Kódovanie: Generujúca matica | Kódovanie: generujúci polynóm

Dekódovanie: nájdi najbližšie kódové slovo | Dekódovanie: Ktorý kód? | Dekódovanie: parity check polynóm

$\Downarrow$

Parity check matica

Definícia

Kód $C \subseteq \{0, \dots, q-1\}^n$ je cyklický ak má 3 nasledujúce vlastnosti:

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

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

C je lineárny

$a \in \mathbb{F}_q = \{0, \dots, q-1\}, +, \cdot$ [ak q je prvočíslo mod q]

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

$\Updownarrow$

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

Ex 3.1 b.) $C = \{x_0 x_1 x_2 x_3 x_4 \in \{0,1,2\}^5 \mid x_0 + x_1 + x_2 + x_3 + x_4 \equiv 0 \mod 3\}$

3^4 sbv

I. $x, y \in C$

$\forall\, x = (x_0 x_1 x_2 x_3 x_4) \mid \sum_{i=0}^{4} x_i \equiv 0 \mod 3$

$\forall\, y = (y_0 y_1 y_2 y_3 y_4) \mid \sum_{i=0}^{4} y_i \equiv 0 \mod 3$

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

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

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

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

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

$k.x \overset{?}{\in} C \iff \sum_{i=0}^{4} k.x_i \equiv 0 \mod 3$

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

$\iff k.0 \equiv 0 \mod 3$ ✓

III. $x \in \mathbb{C} \Leftrightarrow r_4 x_0 \lambda_1 r_2 \lambda_3 \in \mathbb{C}$ Sčítanie je komutatívne

---

Algebra

$S \times S \to S$

Okruh $(S = \{0_1 \ldots n-1\}, +, \cdot)$

1.) $(S, +)$ je komutatívna grupa

a.) → sčítanie je asociatívne $(a+b)+c = a+(b+c)$

b.) → sčítanie je komutatívne $(a+b) = (b+a)$

c.) → existuje prvok 0 neutrálny voči sčítaniu $(a+0) = a$

d.) → pre každý element $a \in S$ existuje prvok inverzný voči sčítaniu $'-a'$ $\boxed{a + '-a' = 0}$

2.) $(S, \cdot)$ je monoid

a.) asociativita $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

b.) neutrálny prvok voči násobeniu '1' : $\forall a \in S \quad a \cdot 1 = a$
$1 \cdot a = a$

3.) '$\cdot$' je distributívne voči '+'

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

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

Pole je okruh + inverzia voč. násobeniu

2.1 d.) Pre všetky $a \in S$ | $\exists$ existuje (a^{-1}):

$$a \cdot a^{-1} = 1$$

$$\frac{1}{a}$$

Okruhy:

$S = \{0,1,2,3\}$, $(+, \cdot)$ mod 4 → Okruh ale nie pole

2^{-1} neexistuje

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

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

$\{0,\dots,n-1\}$, $+, \cdot$ mod n ⇒ Okruh

pre prvočíselné n je to aj pole.

Konečné polia existujú pre veľkosti $|S| = n, n = p^z$ a p je prvočíslo.

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

$\Updownarrow$

$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots + a_{n-1} x^{n-1}$

množina všetkých polynómov nad konečným poľom $\mathbb{F}_q$

$\in \mathbb{F}_q[x]$

$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots + a_{n-1} x^{n-1}$ $\in \mathbb{F}_q[x]$ ... nad konečným polem $\mathbb{F}_q$

Příklady

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

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

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

Stupeň polynómu je jeho nejvyšší exponent.

Dělení polynómů

Příklad:

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

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

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

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

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

$x^6 + x^4 + 1$

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

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

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

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

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

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

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

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

$(x^5 \dots)$

$$\begin{array}{r|l} x^5+x^4+x^3+1 & x^3-x^4+x^3-1 \\ -(x^5+x^4+x^2) & \hline -2x^4+x^3-x^2-1 \\ \hline x^3+x^2+1 & x^5+x^3-x^2-1 \\ & -(x^4+x^3+1) \\ & \hline & -x^2-x-1 \leftarrow \text{zvyšok} \end{array}$$

$\forall f(x)$ a $g(x)$

$\deg(f(x)) \geq \deg(g(x))$

$\exists r(x) : \deg(g(x)) \geq \deg(r(x))$

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

$$(x^5 - x^3 + x^2 + x) \cdot (x^3 + x^2 + 1) + (-x^2 - x - 1)$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \|$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad x^2 + 1$$

$\mathbb{F}_q[x]/f(x)$ ~ množina všetkých zvyškov po delení polynómom $f(x)$

1) množina všetkých polynómov stupňa menšieho ako $\deg(f(x))$ spolu so sčítaním a násobením modulo $f(x)$.

$\mathbb{F}_2[x]/x^2+x+1 = \{0, 1, x, 1+x\}$ f_1 a 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

$x^3 : x^2+x+1 = 1$ $\quad x^2+x : x^2+x+1 = 1$

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

Pole velkosti 4. $\quad (x+1)^2 = x^2+1 : x^2+x+1 =$

x

$\mathbb{F}_q[x]/f(x)$ $\quad (+, \cdot)$ mod $f(x)$ je pole práve vtedy keď

$f(x)$ je **ireducibilný** v $\mathbb{F}_q[x]$

$f(x)$ je ireducibilný nad $\mathbb{F}_q$ až sa napísať ako súčin dvoch polynómov menšieho stupňa.

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

x^2+x+1 je ireducibilný nad $\mathbb{F}_2$.

$x, \; x+1$

$x \cdot x = x^2$

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

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

$\neq \; x^2+x+1$

$R_n^q = \mathbb{F}_q[x]/x^n-1$

Všetky reťazce nad $\mathbb{F}_q$ dĺžky n

- obsah všetkých polynómov stupňa maximálne $n-1$

Spolu s násobením a sčítaním mod x^n-1

Násobenie $f(x) = x$

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

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

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

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

$$(a_0\ a_1 \dots a_{n-1}) \rightsquigarrow (a_{n-1}\ a_0\ a_1 \dots a_{n-2})$$

Ideály $I \leq \mathbb{F}[x] / x^n - 1$ uzavretá voči násobeniu

$$\langle g(x) \rangle = \{ g(x) \cdot h(x) \mid h(x) \in R_n \}$$

Príklad

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

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

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

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

$$(x+1) \cdot (x^2+1)$$
$$\parallel$$
$$(x+1) \cdot x^2 + (x+1)$$
$$(110) + (110)$$
$$\rangle$$

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

(011)

$(101) + (110) = (011)$

$1+x^2 \qquad 1+x \qquad x+x^3$

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

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

Ako nájsť všetky vôbec ideály?

Každý ideál je unicátne charakterizovaný deliteľom $x^n - 1$ v $\mathbb{F}_q$

ireducibilné

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

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

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

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

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

$\langle 0 \rangle = \langle x^3-1 \rangle = \{000\}$

$0 = x^3 - 1$

$h(x) = a_0 + a_1 x + a_2 x^2$

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

$(x^2+x+1)\cdot a_0 + (x^2+x+1)\cdot a_1 x + (x^2+x+1)\cdot a_2 x^2$

$= a_0 \cdot (x^2+x+1) + a_1 (x^2+x+1) + a_2 (x^2+x+1)$

$= (a_0 + a_1 + a_2)(x^2+x+1)$

Každý ideál charakterizuje cyklický kód a ku každému cyklickému kódu vieme priradiť práve jeden ideál.

Každému cyklickému kódu môžeme priradiť jeho generujúci polynóm $g(x)$. $\deg(g(x)) = k$

$$g(x) = g_0 + g_1 x + \dots + g_k x^k$$

$$G = \begin{matrix} m \\ \cdot \end{matrix} \begin{pmatrix} \overbrace{g_0\ g_1\ g_2 \dots g_k}^{k+1}\ \overbrace{0\ 0\ 0\ 0\ 0}^{n-k-1} \\ 0\ g_0\ g_1\ g_2 \dots g_k\ 0\ 0\ 0 \\ \vdots \\ \underbrace{0\ 0\ 0\ 0\ 0}_{n-k-1}\ g_0\ g_1 \dots g_k \end{pmatrix} \quad n \times (n-k-1)$$

$$m \cdot G = c$$

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

$$m(x) \cdot g(x) = (m_0 + m_1 x + m_2 x^2 \dots m_{n-k-1} x^{n-k-1}) \cdot (g_0 + g_1 x + \dots + g_k x^k)$$

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

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

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

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

$n - (n-k-1)$