Cyklické kódy

5. přednáška z algebraického kódování

Obsah

Cyklický kód

Definice

Cyklický kód K délky n nad $\mathbb{Z}_p$ je lineární kód, který je uzavřen na cyklický posun písmen. Pro každé $\bar{v} \in \mathbb{Z}_p^n$ platí:
Je-li $\bar{v} = (v_1 v_2 \dots v_n) \in K$, pak $c(\bar{v}) = (v_2 \dots v_n v_1) \in K$.

Příklad

- Opakovací kód délky n nad $\mathbb{Z}_p$ je cyklický.
- Binární kód kontroly parity délky n je cyklický (protože obsahuje právě všechna slova délky n o sudém počtu jedniček)
- Koktavý kód $K = \{\bar{v} = (aabbcc), a, b, c \in \mathbb{Z}_p\}$ není cyklický, ale je ekvivalentní cyklickému kódu $K' = \{\bar{v} = (abcabc), a, b, c \in \mathbb{Z}_p\}$.

Cyklický kód

Poznámka

- Cyklický kód K délky n je uzavřen na cyklické posuny o libovolných i míst doleva, pro $1 \leq i \leq n$.
  $\bar{v} \in K$ implikuje $c(\bar{v}) \in K$, implikuje $c^2(\bar{v}) = c(c(\bar{v})) \in K$ atd. $c^i(\bar{v}) \in K$.
- Cyklický kód je uzavřen na cyklické posuny písmen doleva i doprava, neboť posun o i míst doleva je vlastně posunem o $n - i$ míst doprava, pro $1 \leq i \leq n$.

Cyklický kód - slova nebo polynomy

Kódové polynomy - nový pohled na věc

U cyklických kódů se vyplatí chápat kódová slova délky n jako polynomy stupně nejvýše $(n-1)$:

$$\bar{v} = (v_1 v_2 \dots v_n) \quad \leftrightarrow \quad v(z) = v_1 z^{n-1} + v_2 z^{n-2} + \dots + v_n$$

Cyklický posun je pak realizován vynásobením proměnnou z podle pravidla $z^n = 1$:

$$\begin{aligned} c(\bar{v}) = (v_2 \dots v_n v_1) \quad \leftrightarrow \quad z \cdot v(z) &= v_1 z^n + v_2 z^{n-1} + \dots + v_n z \\ &= v_2 z^{n-1} + \dots + v_n z + v_1 \end{aligned}$$

Cyklický kód - slova nebo polynomy

Nic tím neztratíme

- Množina $\mathbb{Z}_p^n$ všech slov nad $\mathbb{Z}_p$ délky n tvoří lineární prostor nad $\mathbb{Z}_p$.
- Množina všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ také tvoří lineární prostor nad $\mathbb{Z}_p$.
  Přitom sčítání a násobení konstantou ze $\mathbb{Z}_p$ je v obou případech realizováno stejně, oba lineární prostory jsou izomorfní.
- Množinu všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ budeme značit $\mathbb{Z}_p^{(n)}$.

Cyklický kód - slova nebo polynomy

Něco tím získáme

- Na množině všech polynomů nad $\mathbb{Z}_p$ stupně nejvýše $(n-1)$ máme však navíc operaci násobení:

  Umíme vynásobit dva polynomy nad $\mathbb{Z}_p$ a použitím přepisovacího pravidla $z^n = 1$ ($z^{n+1} = z$, $z^{n+2} = z^2$ atd.) získáme opět polynom stupně nejvýše $(n-1)$.

  (Pozn: Pravidlo $z^n = 1$ jsme potřebovali při cyklickém posunu kódových polynomů!)
- Takto definované násobení odpovídá násobení ve faktorovém okruhu $\mathbb{Z}_p[x]/(x^n - 1)$, aneb $\mathbb{Z}_p^{(n)}$ tvoří komutativní okruh s jednotkou.

Cyklický kód - slova nebo polynomy

Shrnutí

Množina $\mathbb{Z}_p^{(n)}$ všech polynomů nad $\mathbb{Z}_p$ v proměnné z stupně nejvýše $(n-1)$ tvoří

- lineární prostor nad $\mathbb{Z}_p$
- komutativní okruh, v němž násobíme dle pravidla $z^n = 1$

Cyklický kód K délky n nad $\mathbb{Z}_p$ je

- podprostor v lineárním prostoru $\mathbb{Z}_p^{(n)}$
- uzavřený na násobení proměnnou z

Cyklický kód - slova nebo polynomy

Definice

Nechť $(R, +, \cdot)$ je komutativní okruh. Podmnožina $I \subset R$ se nazývá *ideál* okruhu R, jestliže

1. $(I, +)$ je podgrupa grupy $(R, +)$,
2. pro všechny $r \in R$ a všechny $i \in I$ je $r \cdot i \in I$.

Tvrzení

Cyklický kód K délky n nad $\mathbb{Z}_p$ je ideál okruhu $\mathbb{Z}_p^{(n)}$.

Generující polynom

Tvrzení

Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$. Pak existuje kódový polynom $g(z) \in K$ tak, že platí

$$v(z) \in K \quad \text{iff} \quad v(z) = a(z) \cdot g(z) \quad \text{pro nějaký } a(z) \in \mathbb{Z}_p^{(n)}.$$

Definice

Výše uvedený polynom $g(z)$ se nazývá *generující polynom* cyklického kódu K.

Generujícím polynomem je jakýkoliv nenulový kódový polynom nejmenšího stupně.

Takových polynomů je $(p-1)$ a jsou navzájem asociované, obvykle se generující polynom volí monický.

Kódování

Navíc platí:

Pro každý $v(z) \in K$ existuje jediný $a(z)$ stupně nejvýše $(k-1)$, kde $k = n - \mathrm{st}(g)$, pro nějž $v(z) = a(z) \cdot g(z)$.

Máme zde vzájemně jednoznačné zobrazení mezi kódovými polynomy $v(z) \in K$ a polynomy $a(z) \in \mathbb{Z}_p^{(k)}$.

Kódování pomocí generujícího polynomu

Nechť K je cyklický (n, k)-kód s generujícím polynomem $g(z)$, tedy $\mathrm{st}(g) = n - k$.
Kódování informace délky k pomocí $g(z)$ probíhá takto:

$$\bar{a} \leftrightarrow a(z) \quad \xrightarrow{\varphi} \quad v(z) = a(z) \cdot g(z) \leftrightarrow \bar{v}$$

Generující matice

Tvrzení

Buď $g(z)$ generující polynom cyklického (n, k)-kódu K nad $\mathbb{Z}_p$.

- Množina $\{g(z), z\,g(z), z^2\,g(z), \ldots, z^{k-1}\,g(z)\}$ tvoří bázi podprostoru K lineárního prostoru $\mathbb{Z}_p^{(n)}$.
- Aneb bázi v podprostoru K lineárního prostoru slov $\mathbb{Z}_p^n$ získáme cyklickým otáčením slova $\bar{g} \leftrightarrow g(z)$.
- Generující matice $\mathbb{G} = \begin{pmatrix} c^{k-1}(\bar{g}) \\ \vdots \\ c(\bar{g}) \\ \bar{g} \end{pmatrix}$ určuje stejné kódování jako generující polynom $g(z)$.

Kódování

Příklad

Binární kód kontroly parity délky 3
$K = \{(0\,0\,0), (0\,1\,1), (1\,0\,1), (1\,1\,0)\} \leftrightarrow \{0, z+1, z^2+1, z^2+z\}$.
Generujícím polynomem je $g(z) = z + 1$ a určuje toto kódování:

$$\begin{array}{lcll} \bar{a} = (0\,0) & \longrightarrow & v(z) = 0 \cdot g(z) = 0 & \leftrightarrow \quad \bar{v} = (0\,0\,0) \\ \bar{a} = (0\,1) & \longrightarrow & v(z) = 1 \cdot g(z) = z + 1 & \leftrightarrow \quad \bar{v} = (0\,1\,1) \\ \bar{a} = (1\,0) & \longrightarrow & v(z) = z \cdot g(z) = z^2 + z & \leftrightarrow \quad \bar{v} = (1\,1\,0) \\ \bar{a} = (1\,1) & \longrightarrow & v(z) = (z+1) \cdot g(z) = z^2 + 1 & \leftrightarrow \quad \bar{v} = (1\,0\,1) \end{array}$$

Stejné kódování určuje matice $\mathbb{G} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} z \cdot g(z) \\ g(z) \end{pmatrix}$.

Systematické kódování

Buď K cyklický (n, k)-kód s generujícím polynomem $g(z)$.
Popíšeme systematické kódování informace $\bar{a} = (a_1, \ldots, a_k)$.

1. Napíšeme info-znaky na začátek polynomu stupně $(n-1)$:
$$u(z) = z^{n-k} a(z) = a_1 z^{n-1} + \ldots + a_k z^{n-k}$$
2. Polynom $u(z)$ vydělíme generujícím polynomem $g(z)$:
$$u(z) = f(z)\, g(z) + r(z), \quad st(r) < st(g) = n - k$$
3. Odečteme zbytek po dělení. Odečítání nezasáhne informační znaky a vzniklý polynom bude kódový:
$$\begin{array}{rl} v(z) = & u(z) - r(z) = f(z)\, g(z) \\ \leftrightarrow & \bar{v} = (a_1, \ldots, a_k, -r_{n-k-1}, \ldots, -r_0) \end{array}$$

Systematické kódování

Příklad

Binární kód kontroly parity délky 3 má $g(z) = z + 1$.
Zakódujeme systematicky informaci $\bar{a} = (10) \leftrightarrow a(z) = 1z + 0$

1. $u(z) = z\, a(z) = z^2$
2. $z^2 = (z+1)g(z) + 1$
3. $v(z) = u(z) - 1 = z^2 + 1 \leftrightarrow \bar{v} = (101)$

Kolik je cyklických kódů délky n nad $\mathbb{Z}_p$?

Tvrzení

Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím pol. $g(z)$.
Pak $g(x) \mid x^n - 1$ v $\mathbb{Z}_p[x]$.

Důsledek

Je tolik cyklických kódů délky n nad $\mathbb{Z}_p$, kolik je monických dělitelů polynomu $x^n - 1$ v $\mathbb{Z}_p[x]$.

Příklad

$x^3 - 1 = (x+1)(x^2 + x + 1)$ je ireducibilní rozklad v $\mathbb{Z}_2[x]$,
existují tedy pouze dva (netriviální) binární cyklické kódy délky 3:

- opakovací kód s $g(z) = z^2 + z + 1$
- kód kontroly parity s $g(z) = z + 1$

Kontrolní polynom

Tvrzení

Nechť K je cyklický kód délky n nad $\mathbb{Z}_p$ s generujícím pol. $g(z)$ a nechť $x^n - 1 = h(x)g(x)$ v $\mathbb{Z}_p[x]$.
Pak pro každý polynom $v(z) \in \mathbb{Z}_p^{(n)}$ platí:

$$v(z) \in K \quad \text{iff} \quad v(z) \cdot h(z) = 0 \quad \text{v} \quad \mathbb{Z}_p^{(n)} \, (\text{kde } z^n = 1).$$

Definice

Výše uvedený polynom $h(z)$ se nazývá *kontrolní polynom* cyklického kódu K.

Kontrolní polynom budeme volit monický, každý jeho konstantní nenulový násobek je též kontrolním polynomem kódu K.

Kontrolní polynom

Příklad

Binární kód kontroly parity délky 3 má $g(z) = z + 1$.
$x^3 - 1 = (x + 1)(x^2 + x + 1)$ v $\mathbb{Z}_2[x]$, tedy $h(z) = z^2 + z + 1$.

Zkontrolujeme kódové slovo $z^2 + 1$:
$h(z)\,(z^2 + 1) = z^4 + z^3 + z + 1 = z + 1 + z + 1 = 0$,
počítáme dle pravidla $z^3 = 1$.

Tvrzení

Pro cyklický (n, k)-kód K nad $\mathbb{Z}_p$ platí:

- $\text{st}(h(z)) = k$, protože $\text{st}(g(z)) = n - k$;
- $g(z)$ i $h(z)$ mají nenulový absolutní člen

Objevování chyb

Detekce chybného slova

Nechť K je cyklický (n, k)-kód nad $\mathbb{Z}_p$ s generujícím polynomem $g(z)$ a kontrolním polynomem $h(z)$.

Bylo posláno slovo $\bar{v} \in K$ a přijato slovo $\bar{w} = \bar{v} + \bar{e} \in \mathbb{Z}_p^n$.
Kontrolu správnosti můžeme provést dvěma způsoby:

- Pokud $g(z) \nmid w(z)$ v $\mathbb{Z}_p[z]$, pak $w(z) \notin K$, tedy přijaté slovo je chybné.
- Pokud $h(z)\,w(z) \neq 0$ v $\mathbb{Z}_p^{(n)}$ (kde $z^n = 1$), pak $w(z) \notin K$, tedy přijaté slovo je chybné.
- V opačném případě považujeme $w(z) = v(z)$ za slovo poslané, neboť pravděpodobnější je menší počet chyb.

Objevování chyb a dekódování

Objevování shluků chyb

Cyklický kód K objevuje všechna chybová slova, která obsahují shluky chyb o délce $d \leq \text{st}(g(z)) = n - k$.

Chybový polynom má tvar $e(z) = z^i f(z)$, kde $\text{st}(f(z)) \leq d - 1$, a $\gcd(g(z), z^i) = 1$, tudíž $g(z) \nmid e(z)$ v $\mathbb{Z}_p[z]$.

Vlastní dekódování

Vlastní dekódování kódového polynomu $v(z) \in K$ při nesystematickém kódování provedeme vydělením generujícím polynomem $g(z)$ nad $\mathbb{Z}_p$:

$$v(z) : g(z) = a(z) \quad \text{v} \quad \mathbb{Z}_p[z]$$

Opravování chyb

Opravování jedné chyby

Pokud je v přijatém polynomu jedna chyba, pak
$w(z) = v(z) + a\,z^i$, kde $v(z) \in K$.
Při vynásobení kontrolním polynomem vznikne syndrom:

$$s(z) = w(z) \cdot h(z) = 0 + a\,z^i \cdot h(z)$$

Určíme-li jednoznačně konstantu a a z^i, pak můžeme chybu opravit: $v(z) = w(z) - a\,z^i$.
Pozor, násobení jsme prováděli podle pravidla $z^n = 1$, nelze tedy jednoduše podělit $s(z) : h(z)$ jakožto polynomy nad $\mathbb{Z}_p$.

K opravování chyb budeme raději používat kontrolní matici.

Duální kód

Řádky matice $\mathbb{H}$ tvoří bázi duálního kódu K^T.

Tyto řádky vznikly cyklickým otáčením slova $(0 \ldots 0\, h_0\, h_1 \ldots h_k)$, které odpovídá reciprokému polynomu k polynomu h(z) (reciproký polynom má koeficienty v opačném pořadí):

$$\begin{aligned} h(z) &= h_k\,z^k + h_{k-1}\,z^{k-1} + \cdots + h_1\,z + h_0 \\ h_r(z) &= h_0\,z^k + h_1\,z^{k-1} + \cdots + h_{k-1}\,z + h_k \end{aligned}$$

Tvrzení

Duální kód K^T cyklického kódu K je také cyklický.
Jeho generujícím polynomem je $h_r(z)$, reciproký polynom ke kontrolnímu polynomu kódu K.

Kontrolní matice

Tvrzení

Nechť $h(z) = h_k\,z^k + \cdots + h_1\,z + h_0$ je kontrolní polynom cyklického (n, k)-kódu K nad $\mathbb{Z}_p$.
Pak kontrolní matice kódu K má tvar

$$\mathbb{H} = \begin{pmatrix} 0 & \ldots & & 0 & h_0 & h_1 & \ldots & h_k \\ & & & \vdots & & & & \\ 0 & h_0 & h_1 & \ldots & h_k & 0 & \ldots & 0 \\ h_0 & h_1 & \ldots & h_k & 0 & & \ldots & 0 \end{pmatrix}$$

Matice má $(n - k)$ lineárně nezávislých řádků, stačí tedy ověřit jejich kolmost na kódová slova. ($\dim K = k$, $\dim K^T = n - k$.)
V syndromu $\bar{s}^T = \mathbb{H}\,\bar{v}^T$ jsou koeficienty polynomu $s(z) = h(z) \cdot v(z)$, tudíž pro kódová slova je syndrom nulový.