

Generující kořeny cyklických kódů

6. přednáška z algebraického kódování

- 1 **Generující kořeny cyklických kódů**
 - Cyklický Hammingův (7, 4)-kód
 - Generující kořeny určují cyklický kód
 - Hledání generujících kořenů

Cyklický Hammingův (7, 4)-kód

Hammingovy kódy

Hammingovy kódy jsou kódy opravující jednu chybu s co nejmenší redundancí (perfektní kódy pro jednonásobné chyby).

Binární Hammingův kód s m kontrolními znaky je kód délky $n = 2^m - 1$, v jehož kontrolní matici \mathbb{H} jsou všechny různé nenulové sloupce nad \mathbb{Z}_2 délky m .

Nad \mathbb{Z}_2 jsou totiž každé dva různé (nenulové) sloupce lineárně nezávislé, což zaručuje opravování jedné chyby.

Cyklický Hammingův (7, 4)-kód

Hammingův kód nemusí být cyklický

Binární Hammingův (7, 4)-kód s kontrolní maticí

$$\mathbb{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = ((1)_2 \quad (2)_2 \quad \dots \quad (7)_2)$$

snadno opravuje jednu chybu:

Když $\mathbb{H}\bar{w}^T = (i)_2$, tak je chyba na i -té pozici.

Tento kód ale není cyklický:

$\bar{v} = (1000011) \in K$, neboť $\mathbb{H}\bar{v}^T = S_1 + S_6 + S_7 = \bar{0}$,
ale $c(\bar{v}) = (0000111) \notin K$, $\mathbb{H}c(\bar{v})^T = S_5 + S_6 + S_7 \neq \bar{0}$.

Cyklický Hammingův (7, 4)-kód

Sestrojení cyklického Hammingova kódu

Chceme najít ekvivalentní (tudíž Hammingův) (7, 4)-kód, který bude cyklický.

Použijeme těleso $GF(8)$, $T = \mathbb{Z}_2[x]/(x^3 + x + 1)$, tedy těleso $T = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_2, \alpha^3 = \alpha + 1\}$.

Sloupce matice \mathbb{H} můžeme chápat jako prvky tělesa T :

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \leftrightarrow a\alpha^2 + b\alpha + c$$

Těleso T má primitivní prvek α . Všechny nenulové prvky tělesa T (tedy všechny sloupce matice \mathbb{H}) jsou jeho mocninami.

Cyklický Hammingův (7, 4)-kód

Tabulka pro přepsání nenulových prvků v T na mocniny prvku α :

α^1	α^2	α^3	α^4	α^5	α^6	α^7
α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

Uspořádáme sloupce v matici \mathbb{H} podle mocnin prvku α :

$$\mathbb{H} = \begin{pmatrix} \alpha^6 & \alpha^5 & \dots & \alpha & 1 \end{pmatrix} \leftrightarrow \mathbb{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Ukážeme, že Hammingův kód K určený touto kontrolní maticí \mathbb{H} už je cyklický kód.

Cyklický Hammingův (7, 4)-kód

Kódová slova délky 7 budeme chápat jako polynomy stupně nejvýše 6, jak je to u cyklických kódů obvyklé:

$$\bar{v} = (v_1, \dots, v_6, v_7) \leftrightarrow v(z) = v_1 z^6 + \dots + v_6 z + v_7$$

Cyklické otáčení se realizuje vynásobením proměnnou z podle pravidla $z^7 = 1$.

Tvrzení

Kód K určený sestavenou kontrolní maticí \mathbb{H} obsahuje právě ty polynomy, které mají kořen α v tělese T :

$$v(z) \in K \quad \text{iff} \quad v(\alpha) = v_1 \alpha^6 + \dots + v_6 \alpha + v_7 = 0 \quad \forall T$$

Cyklický Hammingův (7, 4)-kód

Zbývá ukázat, že vlastnost "mít kořen α " v tělese T je odolná vůči cyklickému posunu.

Označme cyklicky posunuté slovo $c(\bar{v}) = \bar{u}$,

tj. $u(z) = z \cdot v(z)$, kde násobíme dle pravidla $z^7 = 1$.

Prvek α také splňuje $\alpha^7 = 1$ v tělese T , tudíž $u(\alpha) = \alpha \cdot v(\alpha)$.

Nyní je zřejmé, že pokud $v(\alpha) = 0$, pak také $u(\alpha) = 0 \in T$.

Tvrzení

Nechť T je výše používané těleso $GF(8)$ s primitivním prvkem α . Kód

$$K = \{v(z) \in \mathbb{Z}_2^{(7)}, v(z) \text{ má kořen } \alpha \text{ v } T\}$$

je cyklický Hammingův (7, 4)-kód.

Cyklický Hammingův (7, 4)-kód

Generující polynom

Chceme pro sestrojený cyklický Hammingův (7, 4)-kód K najít generující polynom.

Víme, že $g(z)$ je nenulový kódový polynom nejmenšího stupně, což zde znamená nenulový polynom nad \mathbb{Z}_2 nejmenšího stupně mající kořen α v tělese T .

To je ale minimální polynom pro kořen α . Tím je zde polynom $q(x) = x^3 + x + 1$, modulo který se počítá v tělese T .

$$g(z) = m_\alpha(z) = z^3 + z + 1$$

Binární cyklické kódy délky 7

Příklad

Cyklický kód K délky 7 nad \mathbb{Z}_2 s $g(z) = (z + 1)(z^3 + z + 1)$.

Všimněme si, že $g(z) = m_1(z)m_\alpha(z)$. Přitom víme, že minimální polynomy jsou ireducibilní.

Odtud $v(z) \in K$ právě, když $g(z) \mid v(z)$, což nastane právě, když $v(z)$ má kořeny 1 a α v tělese T .

$$K = \{v(z) \in \mathbb{Z}_2^{(7)}, v(z) \text{ má kořeny } 1, \alpha \text{ v } T\}$$

Kontrolní matice pro kód K bude určena rovnicemi $v(\alpha) = 0$ a také $v(1) = 0$ v tělese T :

$$H = \begin{pmatrix} \alpha^6 & \alpha^5 & \dots & \alpha & 1 \\ 1^6 & 1^5 & \dots & 1 & 1 \end{pmatrix} \text{ nad } T$$

Binární cyklické kódy délky 7

Uvažujme stále těleso $GF(8)$, $T = \mathbb{Z}_2[x]/(x^3 + x + 1)$, aneb těleso $T = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_2, \alpha^3 = \alpha + 1\}$ s primitivním prvkem α .

Generující polynom každého binárního cyklického kódu délky 7 dělí $x^7 - 1$ nad \mathbb{Z}_2 . Víme, že polynom $x^7 - 1$ se nad \mathbb{Z}_2 rozkládá na ireducibilní polynomy takto:

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

Dále víme, že každý nenulový prvek osmiprvkového tělesa T je kořenem polynomu $x^7 - 1$.

To znamená, že každý binární cyklický kód délky 7 můžeme zadat pomocí jeho kořenů v osmiprvkovém tělese T .

Binární cyklické kódy délky 7

Příklad-pokračování

Použitím tabulky pro mocniny primitivního prvku α v tělese T získáme:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ nad } \mathbb{Z}_2$$

Kód K obsahuje právě všechna slova Hammingova kódu, která mají sudou paritu.

Generující kořeny

Definice

Generující kořeny cyklického kódu K délky n nad \mathbb{Z}_p jsou takové prvky c_1, c_2, \dots, c_m nějakého tělesa $GF(p^k)$, že pro každý $v(z) \in \mathbb{Z}_p^{(n)}$ platí:

$$v(z) \in K \quad \text{právě, když} \quad v(z) \text{ má kořeny } c_1, c_2, \dots, c_m$$

Poznámka

Generující kořeny cyklického kódu K nejsou určeny jednoznačně, protože $v(z)$ má s kořenem c také kořeny $c^p, c^{(p^2)}, \dots$, atd.

Např. cyklický Hammingův $(7, 4)$ -kód K s $g(z) = z^3 + z + 1$ má v tělese $T = \mathbb{Z}_2[x]/x^3 + x + 1$ generující kořen α .

Také má generující kořen α^2 , anebo kořeny $\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha$.

Generující kořeny

Cyklický kód K délky n nad \mathbb{Z}_p je svými generujícími kořeny v tělese $GF(p^k)$ jednoznačně určen.

Odvodíme, jak z generujících kořenů spočteme generující polynom a kontrolní matici kódu K .

Těleso $GF(p^k)$, v němž má kód K generující kořeny, označíme T . Jak takové těleso najít a za jaké podmínky existuje, ukážeme posléze.

Generující kořeny určují $g(z)$

Jeden generující kořen

Cyklický kód K délky n nad \mathbb{Z}_p má generující kořen $c \in T$, kde T je rozšíření tělesa \mathbb{Z}_p .

Chceme najít generující polynom kódu K . Víme, že je jím nenulový kódový polynom nejmenšího stupně.

Potřebujeme tedy najít nenulový polynom nad \mathbb{Z}_p nejmenšího stupně s kořenem c v tělese T . To je minimální polynom pro prvek c a ten najít umíme:

$$g(z) = m_c(z) = (x - c)(x - c^p) \cdots (x - c^{(p^l)}),$$

kde $c, c^p, c^{(p^2)}, \dots, c^{(p^l)}$ jsou všechny různé prvky tělesa T vzniklé postupným umocňováním prvku c na p -tou.

Generující kořeny určují $g(z)$

Více generujících kořenů

Cyklický kód K délky n nad \mathbb{Z}_p má generující kořeny $c_1, c_2, \dots, c_m \in T$, kde T je rozšíření tělesa \mathbb{Z}_p .

Pro každý prvek c_i najdeme minimální polynom. Pokud je prvek $c_j = c_i^{(p^s)}$, pak tyto prvky mají stejný minimální polynom.

Generující polynom kódu K je nenulový polynom nad \mathbb{Z}_p nejmenšího stupně, který je dělitelný všemi minimálními polynomy pro dané kořeny. Protože minimální polynomy jsou ireducibilní, tak různé minimální polynomy jsou nesoudělné a jejich nejmenší společný násobek je jejich součinem.

$$g(z) = \text{lcm}(m_{c_1}(z), \dots, m_{c_i}(z)) = \prod_{\text{přes různé}} m_{c_i}(z)$$

Generující kořeny určují H

Jeden generující kořen

Cyklický kód K délky n nad \mathbb{Z}_p má generující kořen $c \in T$, kde T je rozšíření tělesa \mathbb{Z}_p , tj. nějaké $GF(p^k)$.

Kontrolní matice kódu K je odvozena ze vztahu $v(c) = 0$.

Vztah je vlastně homogenní soustavou nad tělesem T s maticí

$$\mathbb{H} = \begin{pmatrix} c^{n-1} & c^{n-2} & \dots & c & 1 \end{pmatrix}$$

Nahradíme-li každé $c^i =$ "polynom stupně nejvýše $(k-1)$ v T " sloupcem jeho koeficientů, získáme matici \mathbb{H} o k řádcích nad \mathbb{Z}_p .

Jsou-li v této matici některé řádky lineární kombinací ostatních, můžeme je vyškrtnout (pak získáme vlastní matici \mathbb{H} , která má v řádcích bázi duálního kódu K^T).

Generující kořeny určují H

Více generujících kořenů

Kontrolní matice cyklického kódu K délky n s generujícími kořeny c_1, c_2, \dots, c_m v tělese T , kde T je $GF(p^k)$, se získá analogicky z matice

$$\mathbb{H} = \begin{pmatrix} c_1^{n-1} & c_1^{n-2} & \dots & c_1 & 1 \\ c_2^{n-1} & c_2^{n-2} & \dots & c_2 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ c_m^{n-1} & c_m^{n-2} & \dots & c_m & 1 \end{pmatrix} \text{ nad } T.$$

Nahradíme-li každé $(c_j)^i =$ "polynom stupně nejvýše $(k-1)$ v T " sloupcem jeho koeficientů, získáme o (mk) řádcích nad \mathbb{Z}_p .

Z této matice vyškrtneme řádky, které jsou lineární kombinací ostatních řádků, a vznikne matice \mathbb{H} nad \mathbb{Z}_p .

Generující kořeny a délka kódu

Dvojitý pohled na věc

Nechť cyklický kód K délky n nad \mathbb{Z}_p má generující kořeny c_1, c_2, \dots, c_m v tělese T , kde T je $GF(p^k)$.

- Každý kořen podléhá pravidlu $z^n = 1$ pro násobení v $\mathbb{Z}_p^{(n)}$. Tudíž řád každého generujícího kořene musí dělit délku n .
- Víme: $g(x) \mid x^n - 1$ nad \mathbb{Z}_p , $g(z) = \text{lcm}(m_{c_1}(z), \dots, m_{c_m}(z))$. Tudíž pro minimální polynomy generujících kořenů platí:

$$m_{c_i}(x) \mid x^n - 1 \text{ nad } \mathbb{Z}_p$$

To nastane, když c_i je kořen $x^n - 1$, aneb když $(c_i)^n = 1$.

Řád každého generujícího kořene musí dělit délku n .

Generující kořeny a délka kódu

Důsledek

Nechť T je těleso $GF(p^k)$ a necht' $c_1, c_2, \dots, c_m \in T$.

Chceme sestavit cyklický kód nad \mathbb{Z}_p , který má tyto prvky jako generující kořeny. Pro jakou délku n kódových slov je to možné?

Protože $r(c_i) \mid n$ pro každé $1 \leq i \leq m$, je nejkratší možná délka cyklického kódu s generujícími kořeny c_1, c_2, \dots, c_m :

$$n = \text{lcm}(r(c_1), \dots, r(c_m))$$

Další možné délky jsou kladné celočíselné násobky tohoto n .

Hledání generujících kořenů

Cyklický kód je svými generujícími kořeny jednoznačně určen. Zatím jsme se nezabývali otázkou, zda každý cyklický kód má generující kořeny.

Pokusíme se k danému cyklickému kódu najít těleso, ve kterém kód má generující kořeny. Odvodíme také podmínku pro existenci takového tělesa.

Hledání generujících kořenů

Tvrzení

Cyklický kód K délky n nad \mathbb{Z}_p má v tělese T , kde T je $GF(p^k)$, generující kořeny právě, když generující polynom $g(z)$ kódu K má v tělese T tolik navzájem různých kořenů, kolik je jeho stupeň.

Aneb $g(z)$ se rozkládá nad T na navzájem různé kořenové činitele, všechny kořeny polynomu $g(z)$ jsou jednonásobné.

Cyklické kódy, které nemají generující kořeny

Důsledek

Nechť K je cyklický kód délky n nad \mathbb{Z}_p . Má-li jeho generující polynom $g(z)$ vícenásobný kořen v \mathbb{Z}_p , pak kód K nemá generující kořeny v žádném rozšíření T tělesa \mathbb{Z}_p .

Příklad

$x^5 - 1 = (x - 1)^5$ nad \mathbb{Z}_5 ,
můžeme udělat cyklický kód K délky 5 nad \mathbb{Z}_5 s $g(z) = (z - 1)^2$.
Tento kód nemá generující kořeny v žádném rozšíření T tělesa \mathbb{Z}_5 ,
neboť ne každý polynom s kořenem 1 je kódový.
(Fakt, že kořen má být dvojnásobný, není podchycen.)

Cyklické kódy, které nemají generující kořeny

Tvrzení

Nechť $p \mid n$, pak existují cyklické kódy délky n nad \mathbb{Z}_p , které nemají generující kořeny v žádném rozšíření T tělesa \mathbb{Z}_p .

Důvod: $x^n - 1 = x^{mp} - 1 = (x^m - 1)^p$ nad \mathbb{Z}_p

Příklad

$x^{14} - 1 = (x^7 - 1)^2 = [(x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)]^2$ nad \mathbb{Z}_2 .
Binární cyklický kód K délky 14 s $g(z) = (z^3 + z + 1)^2$ má
všechny kořeny dvojnásobné (pokud tedy nějaké kořeny v T má).

Poznámka

Někdy se pojem generující kořeny definuje pouze pro cyklické kódy nad \mathbb{Z}_p , jejichž délka n není násobkem p .

Hledání generujících kořenů

Hledání tělesa s generujícími kořeny cyklického kódu

Nechť K je cyklický kód délky n nad \mathbb{Z}_p a necht' $p \nmid n$.

Pokusíme se najít rozšíření T tělesa \mathbb{Z}_p , ve kterém by měl generující polynom $g(x)$ stupně m celkem m různých kořenů.

Víme, že $g(x) \mid x^n - 1$ nad \mathbb{Z}_p .

Pokud nalezneme těleso T charakteristiky p , ve kterém bude mít polynom $x^n - 1$ celkem n různých kořenů, tak bude hotovo - kořeny polynomu $g(x)$ jsou mezi nimi.

V tělese T o p^k prvcích má polynom $x^n - 1$ celkem n různých kořenů právě, když n dělí $|T^*|$, kde $|T^*| = p^k - 1$.

Kořeny jsou tvaru β^i pro nějaký prvek β řádu n .

Hledání generujících kořenů

Pokračování

Hledáme tedy k tak, aby pro dané n a p platilo: $n \mid p^k - 1$.

$$n \mid p^k - 1 \quad \text{iff} \quad p^k - 1 = 0 \quad \text{v} \quad \mathbb{Z}_n \quad \text{iff} \quad p^k = 1 \quad \text{v} \quad \mathbb{Z}_n$$

Pokud $p \nmid n$, pak můžeme použít Euler-Fermatovu větu:

$$\text{Když } p \nmid n, \text{ pak } p^{\varphi(n)} = 1 \quad \text{v} \quad \mathbb{Z}_n.$$

Můžeme tedy volit $k = \varphi(n)$ a těleso T bude $GF(p^{\varphi(n)})$.

Pokud $p \mid n$, pak naše úloha nemá řešení.

Kdyby totiž existovalo k tak, že $p^k = 1$, pak by existoval p^{-1} v \mathbb{Z}_n . Ten však neexistuje (p je soudělné s n). Neřešitelnost úlohy pro případ $p \mid n$ nás ale nepřekvapuje (viz str. 24).

Hledání generujících kořenů

Pokračování

Mohou existovat i menší tělesa, která řeší naši úlohu.

Nejmenší k , které splňuje $p^k = 1$ v grupě invertibilních prvků \mathbb{Z}_n^* , je řád prvku p v této grupě. Dokonce víme:

$$p^k = 1 \quad \text{v} \quad \mathbb{Z}_n^* \quad \text{právě, když} \quad r(p) \mid k$$

Těles $GF(p^k)$, v nichž má polynom $x^n - 1$ celkem n různých kořenů, je tedy nekonečně mnoho (za předpokladu, že $p \nmid n$).

Chceme-li zadat cyklický kód pomocí jeho generujících kořenů, pak naštěstí nezáleží na tom, které z těchto těles použijeme.

Cyklické kódy, které mají generující kořeny

Věta

Nechť K je cyklický kód délky n nad \mathbb{Z}_p a necht' $p \nmid n$.

Položme $k = \varphi(n)$ (anebo $k = r(p)$ v grupě \mathbb{Z}_n^*).

Pak v tělese $GF(p^k)$ má cyklický kód K generující kořeny.

Generující kořeny jsou tvaru $\beta^{i_1}, \beta^{i_2}, \dots, \beta^{i_m}$ pro nějaký prvek β řádu n v tělese $GF(p^k)$.

Cyklické kódy, které mají generující kořeny

Příklad

Cyklický kód K délky 13 nad \mathbb{Z}_3 má $g(z) = z^4 + 2z^3 + 2z^2 + 1$.

Najděte jeho generující kořeny v nějakém $GF(3^k)$.

Řád $r(3) = 3$ v grupě \mathbb{Z}_{13}^* , postačí těleso $GF(3^3) = GF(27)$.

$g(z) = (z - 1)(z^3 + 2z + 2)$ je ireducibilní rozklad nad \mathbb{Z}_3 .

Použijeme tudíž těleso

$$T = \mathbb{Z}_3[x]/(z^3 + 2z + 2) = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_3, \alpha^3 = \alpha + 1\}.$$

Generujícími kořeny kódu K jsou zde prvky 1 a α

(popřípadě také $\alpha^3 = \alpha + 1$, $\alpha^9 = \alpha + 2$).

Cyklické kódy, které mají generující kořeny

Příklad - pokračování

Cyklický kód K délky 13 nad \mathbb{Z}_3 s $g(z) = z^3 + z^2 + 2$

má také generující kořeny v našem tělese T .

Rovnici $x^{13} = 1$ řeší v T všechny prvky α^i , neboť $r(\alpha) = 13$.

Postupným dosazováním zjistíme, že $\alpha^4 = \alpha^2 + \alpha$ je kořenem $g(z)$ (a tudíž i $\alpha^{12} = \alpha^2 + 2$, $\alpha^{36} = \alpha^{10} = \alpha^2 + 2\alpha$).