

BCH kódy

7. přednáška z algebraického kódování

Obsah

- 1 **BCH kódy**
 - Minimální vzdálenost a dimenze kódu
 - Binární BCH kódy
 - Opravování chyb pomocí kořenů

BCH kódy

BCH kódy jsou cyklické kódy zadané svými generujícími kořeny. Díky šikovné volbě kořenů opravuje kód předem daný počet chyb.

Následující konstrukci vymysleli Bose a Ray-Chaudhuri (1960) a nezávisle na nich Hocquenghem (1959).

Jedná se tedy o Bose-Chaudhuri-Hocquenghemovy kódy, odtud zkratka BCH kódy.

BCH kódy

Definice

BCH kód délky n nad \mathbb{Z}_p (kde $p \nmid n$) s *plánovanou vzdáleností* d ($d \leq n$) je cyklický kód s generujícími kořeny

$$\beta^b, \beta^{b+1}, \beta^{b+2}, \dots, \beta^{b+d-2},$$

kde β je prvek řádu n v nějakém tělese $GF(p^k)$, $b \geq 1$.

Poznámky

- Kořeny tvoří $d - 1$ po sobě jdoucích mocnin prvku řádu n .
- Pokud $b = 1$, mluvíme o *BCH kódu* délky n nad \mathbb{Z}_p v *užším smyslu*. Jeho generující kořeny jsou $\beta, \beta^2, \beta^3, \dots, \beta^{d-1}$, kde β je prvek řádu n v nějakém tělese $GF(p^k)$.

BCH kódy

Poznámky - pokračování

Protože $p \nmid n$, těleso $GF(p^k)$ s prvkem β řádu n existuje.

- Volba $k = \varphi(n)$ zafunguje nad každým \mathbb{Z}_p .
- Nejmenší volba pro dané p je $k = r(p)$ v grupě \mathbb{Z}_n^* .

Příklad

Cyklický Hammingův $(7, 4)$ -kód má v tělese $GF(8)$,

$T = \mathbb{Z}_2[x]/(x^3 + x + 1) = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_2, \alpha^3 = \alpha + 1\}$,
generující kořeny α , α^2 a $\alpha^4 = \alpha^2 + \alpha$, přitom $r(\alpha) = 7$.

Jedná se o BCH kód s plánovanou vzdáleností $d = 3$.

Minimální vzdálenost BCH kódu

Věta

BCH kód K délky n nad \mathbb{Z}_p s plánovanou vzdáleností d má minimální Hammingovu vzdálenost kódu $d_H(K) \geq d$.

Aneb: BCH kód s plánovanou vzdáleností d (tj. s $d - 1$ kořeny) objevuje $d - 1$ chyb a opravuje $\lfloor \frac{d-1}{2} \rfloor$ chyb.

Důkaz

Kontrolní matice \mathbb{H} nad $GF(p^k)$ má $d - 1$ řádků. Lze dokázat, že libovolných $d - 1$ sloupců v \mathbb{H} je lineárně nezávislých.

Determinant každé čtvercové podmatice řádu $d - 1$ v matici \mathbb{H} lze totiž převést na Vandermondův determinant pro mocniny prvku β . Jelikož $\beta^i \neq \beta^j$ pro $0 \leq i \neq j \leq n - 1$ (neboť $r(\beta) = n$), je Vandermondův determinant nenulový.

Minimální vzdálenost BCH kódu

Lemma

Pro prvky a_1, \dots, a_n v tělese T platí:

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{pmatrix} = \prod_{i>j} (a_i - a_j)$$

Determinant se nazývá *Vandermondův determinant* řádu n pro prvky a_1, \dots, a_n a je nenulový právě, když jsou tyto prvky různé.

Minimální vzdálenost BCH kódu

Příklad

Použijeme naše $GF(8) = \mathbb{Z}_2[x]/(x^3 + x + 1)$ k vytvoření binárního BCH kódu K délky 7 opravujícího dvě chyby, tedy BCH kódu s plánovanou vzdáleností $d = 5$.

Kód K má generující kořeny $\alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha$. Kódové polynomy jsou polynomy nad \mathbb{Z}_2 , stačí tedy požadovat kořeny $\alpha, \alpha + 1$. Generující polynom kódu bude:

$$\begin{aligned} g(z) &= m_\alpha(z)m_{\alpha+1}(z) = (z^3 + z + 1)(z^3 + z^2 + 1) \\ &= z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 \end{aligned}$$

Jedná se o opakování kód délky 7 a skutečná $d_H(K) = 7$. Kód opravuje dokonce tři chyby.

BCH kódy

Otevřené problémy

- BCH kód s plánovanou vzdáleností d může mít minimální vzdálenost $d_H(K) > d$. Je otevřeným problémem, jak určit skutečnou minimální vzdálenost BCH kódu.

Neví se ani, jak poznat, pro které dvojice n a d (nad \mathbb{Z}_p) nastane rovnost $d_H(K) = d$.

- Další otevřený problém je určení počtu informačních a kontrolních znaků pro BCH kódy.
Tento problém je částečně vyřešen pro kódy délek $n = p^k - 1$.

Dimenze BCH kódu

Situace

- Máme BCH kód K délky n nad \mathbb{Z}_p (v užším smyslu) s plánovanou vzdáleností d s generujícími kořeny $\beta, \beta^2, \beta^3, \dots, \beta^{d-1}$, kde β je prvek řádu n v nějakém tělese T charakteristiky p .
- Chceme zjistit, kolik informačních a kolik kontrolních znaků má BCH kód K .
Počet informačních znaků (aneb dimenze kódu K) se značí k , počet kontrolních znaků se značí m .
- V této části budeme značit těleso T jako $GF(p^s)$.
 $T = \mathbb{Z}_p[x]/q(x)$, kde $q(x)$ je ireducibilní nad \mathbb{Z}_p stupně s ,
 $T = \{a(\alpha) \in \mathbb{Z}_p[x], \text{st}(a(\alpha)) \leq s - 1, q(\alpha) = 0\}$.

Dimenze BCH kódu

Situace - pokračování

- Známe-li generující kořeny cyklického kódu, umíme z nich najít generující polynom $g(z)$ a kontrolní matici \mathbb{H} .
K výpočtu dimenze kódu využijeme dvou známých vztahů:
 - $\text{st}(g(z)) = n - k = m$
 - \mathbb{H} nad \mathbb{Z}_p má $n - k = m$ (lineárně nezávislých) řádků
- Kontrolní matice \mathbb{H} nad T má $d - 1$ řádků obsahujících mocniny kořenů. Každý prvek z T (polynom stupně $\leq s - 1$) nahradíme sloupcem jeho koeficientů, vyškrtáme řádky, které jsou lineární kombinací ostatních, a získáme \mathbb{H} nad \mathbb{Z}_p .
Odtud počet kontrolních znaků $m \leq s(d - 1)$, kde s je dáno volbou tělesa $GF(p^s)$.

Dimenze BCH kódu

Tvrzení

Nechť K je BCH kód délky n nad \mathbb{Z}_p s plánovanou vzdáleností d , pak pro počet informačních znaků $k = \dim K$ platí odhad:

$$k \geq n - s(d - 1), \quad \text{kde } s = r(p) \text{ v grupě } \mathbb{Z}_n^*$$

Poznámka

Tento odhad může být poměrně hrubý.

Kódové polynomy jsou celočíselné nad \mathbb{Z}_p , mají tudíž s kořenem $c \in T$ také kořeny $c^p, c^{(p^2)}, \text{ atd.}$ Tudíž se může stát, že v BCH kódu nemusíme některé z kořenů $\beta, \beta^2, \beta^3, \dots, \beta^{d-1}$ požadovat (budou tam automaticky).

Kontrolní matice \mathbb{H} nad T pak bude mít méně než $d - 1$ řádků.

Binární BCH kódy

Tvrzení

Binární cyklický kód délky n , kde $2 \nmid n$, s generujícími kořeny

$$\beta, \beta^3, \beta^5, \dots, \beta^{2t-1},$$

kde β je prvek řádu n v nějakém $GF(2^s)$, je binární BCH kód s plánovanou vzdáleností $d = 2t + 1$.

Každé sudé číslo je tvaru $2^j i$, kde i je liché. Charakteristika tělesa je 2, tudíž stačí požadovat liché mocniny prvku β .

Tvrzení

Binární BCH kód s t kořeny (= t po sobě jdoucími lichými mocninami prvku β) opravuje aspoň t chyb.

Binární BCH kódy

Tvrzení

Binární BCH kód délky n s plánovanou vzdáleností $d = 2t + 1$ má odhad pro počet informačních znaků:

$$k \geq n - s \frac{d-1}{2} = n - st, \quad \text{kde } s = r(2) \text{ v grupě } \mathbb{Z}_n^*$$

To už je poměrně dobrý odhad počtu informačních znaků, někdy dokonce naprosto přesný (viz níže).

Tvrzení

Binární BCH kód délky $n = 2^s - 1$ s plánovanou vzdáleností $d = 2t + 1$, kde $d < 2^{\lceil \frac{s}{2} \rceil} + 2$ ($\lceil x \rceil$ značí horní celou část z x), má právě $k = n - s \frac{d-1}{2} = n - st$ informačních znaků.

Binární BCH kódy

Poznámka k důkazu

Nechť β je primitivní prvek tělesa $GF(2^s)$. Lze dokázat, že minimální polynomy prvků $\beta, \beta^3, \beta^5, \dots, \beta^{2t-1}$ jsou navzájem různé a že mají stupeň s , pokud ovšem $2t - 1 = d - 2 < 2^{\lceil \frac{s}{2} \rceil}$. Tudíž $g(z) = \prod_{i=1}^t m_{\beta^{2i-1}}(z)$ má stupeň $m = s \cdot t$.

Příklad

Popište parametry binárních BCH kódů délky $31 = 2^5 - 1$.
Pro $d < 2^{\lceil \frac{5}{2} \rceil} + 2 = 10$, aneb pro kódy opravující až čtyři chyby, bude cena za opravování každé chyby $s = 5$ kontrolních znaků.
Např. kód opravující dvě chyby má informační poměr
 $k : n = 21 : 31$.

Primitivní BCH kódy

Definice

BCH kódy nad \mathbb{Z}_p délky $n = p^s - 1$ se nazývají *primitivní BCH kódy*. Za jejich kořeny totiž můžeme volit mocniny primitivního prvku v tělese $GF(p^s)$.

Poznámka

Vždy lze zvolit ireducibilní polynom $q(x)$ nad \mathbb{Z}_p stupně s tak, aby jeho kořen α byl primitivním prvkem tělesa $T = \mathbb{Z}_p[x]/q(x)$ (jehož prvky zapisujeme jako polynomy stupně nejvýše $s - 1$ v proměnné α).

Provedeme-li tuto konstrukci tělesa $GF(p^s)$, pak generující kořeny budou mocninami prvku α .

Primitivní BCH kódy

Pokračování

Primitivní BCH kódy s jediným generujícím kořenem α v tělese T :

Generující polynom $g(z) = m_\alpha(z) = q(z)$

Kontrolní matice $\mathbb{H} = \begin{pmatrix} \alpha^{n-1} & \alpha^{n-2} & \dots & \alpha & 1 \end{pmatrix}$ nad T obsahuje všechny nenulové prvky tělesa T .

Tudíž kontrolní matice \mathbb{H} nad \mathbb{Z}_p má ve sloupcích všechny nenulové s -tice nad \mathbb{Z}_p .

Poznámka

Každé dva sloupce matice \mathbb{H} nad \mathbb{Z}_p jsou lineárně nezávislé právě, když pracujeme nad \mathbb{Z}_2 .

Primitivní binární BCH kódy

Tvrzení

Binární BCH kód délky $n = 2^s - 1$ s jedním kořenem je cyklický Hammingův kód o s kontrolních znacích (tedy perfektní kód pro jednonásobné opravy).

Binární BCH kódy délky $n = 2^s - 1$ zobecňují Hammingovy kódy. Mají-li t generujících kořenů (= t po sobě jdoucích lichých mocnin primitivního prvku), pak:

- opravují t chyb
- mají velmi dobrý informační poměr (malou redundanci)
- mají vypracované dekódovací metody, jak opravovat vícenásobné chyby pomocí kořenů
- jsou to jedny z nejlepších kódů pro délky do $n \doteq 10^5$

Opravení chyb pomocí kořenů

Opravení jedné chyby nad \mathbb{Z}_2

K je binární BCH kód délky n s generujícím kořenem β v $GF(2^s)$.

Bylo vysláno slovo $\bar{v} \in K$ a přijato slovo $\bar{w} = \bar{v} + \bar{e}$.

Když $w(\beta) \neq 0$, pak při přenosu došlo k chybě.

Pokud došlo k jedné chybě, tak $w(z) = v(z) + z^i$ a $w(\beta) = 0 + \beta^i$.

Dosadíme tedy generující kořen:

$w(\beta) =$ "syndromový polynom v β stupně nejvýše $s - 1$ " = s_1

Podíváme se do tabulky mocnin prvku β , pro jaké i je $s_1 = \beta^i$
(exponent i je určen jednoznačně, neboť $r(\beta) = n$ a $0 \leq i \leq n - 1$).

Tudíž chyba je v i -té mocnině, opravíme $v(z) = w(z) - z^i$.

Opravení chyb pomocí kořenů

Příklad

Cyklický Hammingův $(7, 4)$ -kód má generující kořen α v $GF(8)$,
 $T = \mathbb{Z}_2[x]/(x^3 + x + 1) = \{a\alpha^2 + b\alpha + c, a, b, c \in \mathbb{Z}_2, \alpha^3 = \alpha + 1\}$.

Opravíme přijaté slovo $\bar{w} = (0110111)$.

$$w(\alpha) = \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1 = \dots = \alpha^2 + \alpha = \alpha^4,$$

k výpočtu potřebujeme tabulku pro mocniny α v tělese T .

Poslané slovo je $\bar{v} = (0100111)$.

Opravení chyb pomocí kořenů

Opravení jedné chyby nad \mathbb{Z}_p

Buď nyní $p \geq 3$. K je BCH kód délky n nad \mathbb{Z}_p s generujícími kořeny β a β^2 v $GF(p^s)$.

Pokud došlo k jedné chybě, tak $w(z) = v(z) + a z^i$ pro $v(z) \in K$, $a \in \mathbb{Z}_p$. Potřebujeme zjistit a , i .

Dosadíme tedy oba generující kořeny:

$w(\beta) =$ "1. syndromový polynom v β stupně nejvýše $s - 1$ " = s_1
 $w(\beta^2) =$ "2. syndromový polynom v β stupně nejvýše $s - 1$ " = s_2

Podíváme se do tabulek mocnin prvků β a β^2 a najdeme všechny možnosti, jak napsat syndromy ve tvaru $s_1 = a_1 \beta^{i_1}$, $s_2 = a_2 (\beta^2)^{i_2}$. Teorie zaručuje, že bude jediná možnost společná oběma kořenům. Tato možnost určuje chybový polynom $e(z) = a z^i$, opravíme $v(z) = w(z) - a z^i$.

Opravení chyb pomocí kořenů

Příklad

BCH kód nad \mathbb{Z}_3 délky 8 s generujícími kořeny $i, i+1$ v $GF(9)$, kde $T = \mathbb{Z}_3[x]/(x^2 + 1) = \{ai + b, a, b \in \mathbb{Z}_3, i^2 = -1\}$, objevuje tři chyby a jednu chybu opravuje.

Jeho kořeny jsou $\pm i, \pm i + 1$, což jsou tyto mocniny primitivního prvku $i + 1$: $(i + 1)^1 = i + 1$, $(i + 1)^2 = -i$, $(i + 1)^3 = -i + 1$ a ještě $(i + 1)^6 = i$.

Opravíme přijaté slovo $\bar{w} = (00211012)$.

$$\begin{aligned} w(i+1) &= 2(i+1)^5 + (i+1)^4 + (i+1)^3 + (i+1) + 2 = \dots = \\ &= i+1 = 1(i+1)^1 = 2(i+1)^5 \end{aligned}$$

$$w(i) = 2i^5 + i^4 + i^3 + i + 2 = \dots = 2i = 2i^1 = 2i^5 = 1i^3 = 1i^7$$

K výpočtu potřebujeme tabulky mocnin prvků $i + 1$ a i v tělese T .

Jediná společná možnost určuje chybový polynom $e(z) = 2z^5$.

Poslané slovo je $\bar{v} = (00011012)$.

Opravení chyb pomocí kořenů

Opravení dvou chyb nad \mathbb{Z}_2

K je binární BCH kód délky n s generujícími kořeny β a β^3 v $GF(2^s)$, tudíž opravuje dvě chyby.

Došlo-li ke dvěma chybám, tak $w(z) = v(z) + z^i + z^j$, kde $i \neq j$.

Dosadíme tedy oba generující kořeny a spočteme syndrom(y):

$$w(\beta) = s_1 = \beta^i + \beta^j$$

$$w(\beta^3) = s_3 = (\beta^3)^i + (\beta^3)^j = \beta^{3i} + \beta^{3j}$$

Potřebujeme ze znalosti prvků $s_1, s_3 \in T$ určit čísla i, j .

Stačí určit β^i, β^j , neboť $r(\beta) = n$ a $0 \leq i, j \leq n - 1$, takže čísla i, j jednoznačně dohledáme v tabulce pro mocniny prvku β .

Opravení chyb pomocí kořenů

Opravení dvou chyb nad \mathbb{Z}_2 - pokračování

$$\begin{aligned} s_1^3 &= (\beta^i + \beta^j)^3 \\ &= \beta^{3i} + \beta^{2i}\beta^j + \beta^i\beta^{2j} + \beta^{3j} \\ &= s_3 + \beta^i\beta^j s_1 \\ \beta^i\beta^j &= (s_1^3 - s_3) s_1^{-1} \end{aligned}$$

Známe součet a součin obou prvků, pak tyto prvky jsou kořeny polynomu $L(x) = x^2 - \sum x + \prod = (x - \beta^i)(x - \beta^j)$.

Ze syndromů spočteme koeficienty: $\sum = s_1$, $\prod = (s_1^3 - s_3) s_1^{-1}$

Dosazováním prvků z tělesa T nalezneme kořeny $L(x)$.

(Pozn.: Vzorec na kořeny kvadrátu nad tělesem charakteristiky 2 nefunguje, protože tam $(a + b)^2 = a^2 + b^2$.)

Polynom $L(x)$ se nazývá *lokátor chyb*.

Opravení chyb pomocí kořenů

Opravení dvou chyb nad \mathbb{Z}_2 - pokračování

V praxi nevíme dopředu, kolik je chyb v přijatém slově \bar{w} .
U binárního BCH kódu opravujícího dvě chyby postupujeme takto:
Spočteme syndrom $\bar{s}^T = \mathbb{H}\bar{w}^T$ nad tělesem T dosazením kořenů:

$$\bar{s}^T = \begin{pmatrix} w(\beta) \\ w(\beta^3) \end{pmatrix} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix}$$

Pokud $\bar{s} = (00)$, pak prohlásíme \bar{w} za bezchybné.

Pokud $\bar{s} = (s_1 s_1^3)$, kde $s_1 \neq 0$, pak je ve \bar{w} jedna chyba.

Pokud $\bar{s} = (s_1 s_3)$, kde $s_1 \neq 0$ a $s_3 \neq s_1^3$, pak určíme lokátor $L(x)$.

Má-li $L(x)$ dva různé kořeny, pak jsou ve \bar{w} dvě chyby.

Nemá-li $L(x)$ dva kořeny, pak je ve \bar{w} více chyb (v tomto případě chyby neopravíme).

Opravení chyb pomocí kořenů

Opravení více chyb nad \mathbb{Z}_2

K je binární BCH kód délky n s generujícími kořeny $\beta, \beta^3, \dots, \beta^{2^t-1}$ v $GF(2^s)$, tudíž opravuje t chyb.

Došlo-li k $r \leq t$ chybám, tak $w(z) = v(z) + z^{i_1} + \dots + z^{i_r}$.

Spočteme syndrom $\bar{s}^T = \mathbb{H}\bar{w}^T$ nad tělesem T dosazením kořenů:

$$\bar{s}^T = \begin{pmatrix} w(\beta) \\ w(\beta^3) \\ \vdots \\ w(\beta^{2^t-1}) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^r \beta^{ij} \\ \sum_{j=1}^r \beta^{3ij} \\ \vdots \\ \sum_{j=1}^r \beta^{(2^t-1)ij} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_3 \\ \vdots \\ s_{2^t-1} \end{pmatrix}$$

Hledáme prvky β^{ij} , pro $1 \leq j \leq r$, a známe součty jejich lichých mocnin. Pomocí Newtonových vzorců lze nalézt lokátor $L_r(x)$ stupně r , jehož kořeny jsou právě hledané prvky.

Opravování chyb pomocí kořenů

Opravování více chyb nad \mathbb{Z}_2 - pokračování

Problémem je, že nevíme dopředu, kolik je chyb ve slově \bar{w} .

Musíme tedy počítat lokátory $L_r(x)$ postupně pro všechna $1 \leq r \leq t$, dokud nenajdeme takový, který má r různých kořenů.

Pokud takový lokátor nenajdeme, pak je ve slově \bar{w} více než t chyb a opravovat ho nebudeme. (Popsali jsme částečné dekódování.)