

Samoopravné kódy

Alexandr Kazda

Univerzita Karlova

6. dubna 2020

BCH kódy (primitivní, v užším smyslu)

- $\text{BCH}_{q,m,\delta}$ je cyklický nad tělesem \mathbb{F}_q , délky $q^m - 1$, dimenze aspoň $q^m - m(\delta - 1) - 1$ a min. vzdálenosti aspoň δ
- Zvolme α generátor $\mathbb{F}_{q^m}^*$ (primitivní prvek, proto „primitivní“ kódy)
- Kódová slova jsou $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$, že polynom $\sum_{j=0}^{q^m-2} a_j x^j$ má nuly v bodech α^i pro $i \in \{1, 2, \dots, \delta - 1\}$
- Vzdálenost aspoň δ , dimenze aspoň $q^m - 1 - m(\delta - 1)$
- Používané pro kanály s málo chybami
- Efektivní kódování a dekódování vynecháme

- **Pozor! Opačná inkluze než ve skriptech**
- Skripta: Popis, jak vyrobit BCH kód tak, že vyjdeme z R-S kódu a děláme úpravy
- My: $RS_{q,k} = BCH_{q,1,q-k}$ (modulo ekvivalence)
- Připomenutí: $RS_{q,k}$ má kódová slova hodnoty polynomů stupně $< k$ nad \mathbb{F}_q
- Bud' $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$. Volme pořadí písmen

$$(f(1), f(\alpha), f(\alpha^2), \dots, f(\alpha^{q-2}))$$

- **Oprava po přednášce:** Cyklický posun \equiv vynásob koeficient u x^j v f pomocí α^j
- Z půlky března známe paritní matici $RS_{q,k}$ (Tvrzení 6.2.4)!

- Paritní matice $RS_{q,k}$ při cyklickém pořadí písmen

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(q-2)} \\ & & & \ddots & \\ 1 & \alpha^{q-k-1} & \alpha^{2(q-k-1)} & \dots & \alpha^{(q-2)(q-k-1)} \end{pmatrix}$$

- Kdy je $(a_0, a_1, a_2, \dots, a_{q-2}) \in RS_{q,k}$? Právě když pro každé $e \in \{1, 2, \dots, q-k-1\}$ platí $\sum_{i=0}^{q-2} a_i \cdot (\alpha^e)^i = 0$
- To je právě když polynom $a_0 + a_1x + \dots + a_{q-2}x^{q-2}$ má nuly v bodech $\alpha, \alpha^2, \dots, \alpha^{q-k-1}, \dots$
- ... neboli $(a_0, a_1, \dots, a_{q-2}) \in BCH_{q,1,q-k}$.
- Pozor!** Tato čísla a_i nejsou koeficienty, ale hodnoty polynomu z definice R-S kódu! Platí $a_i = f(\alpha^i)$ pro f z předchozího slajdu

R-S kódy \subset BCH kódy – příklad

- Necht' $q = 7, k = 2, \alpha = 3$
- Mocniny 3 v \mathbb{F}_7 : 3, 2, 6, 4, 5, 1
- $RS_{7,2}$ má kódová slova délky 6

$$\{(b + c, 3b + c, 2b + c, 6b + c, 4b + c, 5b + c) : b, c \in \mathbb{F}_7\}$$

- $BCH_{7,1,5}$ má kódová slova (a_0, a_1, \dots, a_5) , že $a_0 + a_1x + \dots + a_5x^5$ má nuly v bodech 3, 2, 6, 4
- Obě množiny kódových slov jsou stejné, například

$$(b+c) + (3b+c)3 + (2b+c)3^2 + (6b+c)3^3 + (4b+c)3^4 + (5b+c)3^5 =$$

$$(b+c) + (3b+c)3 + (2b+c)2 + (6b+c)6 + (4b+c)4 + (5b+c)5 =$$

$$91b + 21c = 0$$

- Motivace: Chceme cyklický zhruba $[n, n/2, \sqrt{n}]$ -kód



- **Nebudou** to „Quick Response“ kódy jako je tento...

QR kód pro <http://en.m.wikipedia.org>, zdroj: <https://commons.wikimedia.org/w/index.php?title=File:>

[QR_code_for_mobile_English_Wikipedia.svg&oldid=234508292](https://commons.wikimedia.org/w/index.php?title=File:QR_code_for_mobile_English_Wikipedia.svg&oldid=234508292)

- „QR“ znamená „quadratic residue“, tj. kvadratický zbytek
- $a \neq 0$ je kvadratický zbytek \Leftrightarrow existuje b , že $a = b^2 \pmod{p}$
- Připomenutí z Teorie čísel: V \mathbb{F}_p^* je polovina prvků kvadratický zbytek R a druhá polovina kvadratický nezbytek N
- Příklad: V \mathbb{Z}_7 jsou zbytky $R = \{1, 4, 2\}$ a nezbytky $N = \{3, 5, 6\}$

- Zvolme $p = 7$
- $R = \{1, 4, 2\}$ a nezbytky $N = \{3, 5, 6\}$, obě množiny jsou uzavřené na násobení 2
- Bud' α primitivní 7. odmocnina z 1 v rozšíření \mathbb{Z}_2 ; volme třeba $\mathbb{Z}_2[\alpha]/(1 + \alpha^2 + \alpha^3)$
- Pamatujete na polynomy ze středy?

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

- Tyto polynomy nám určují dva ekvivalentní cyklické kódy nad \mathbb{Z}_2

- Vyrábíme binární kód délky p
- Zvolme p prvočíslo takové, že 2 je kvadratický zbytek modulo p (tj. $p \equiv \pm 1 \pmod{8}$)
- R resp. N jsou kvadratické zbytky resp nezbytky modulo p
- Buď α primitivní p -tá odmocnina z 1 ve vhodném rozšíření \mathbb{Z}_2 . Volme

$$r(x) = \prod_{i \in R} (x - \alpha^i)$$

$$n(x) = \prod_{i \in N} (x - \alpha^i)$$

- Jsou $r, n \in \mathbb{Z}_2[x]$?

- $R \subset \{1, 2, \dots, p-1\}$ jsou kvadratické zbytky modulo p
- Volíme p tak, aby $2 \in R$
- Je $r(x) = \prod_{i \in R} (x - \alpha^i) \in \mathbb{Z}_2[x]$?
- Teorie z minula (cyklotomické polynomy): Potřebujeme, aby R byla uzavřená na násobení 2 modulo p
- Bud' $2 = c^2$, $e = f^2$. Pak $2e = (cf)^2$. Tedy $e \in R \Rightarrow 2e \in R$
- Tedy R je sjednocení cyklotomických tříd a $r \in \mathbb{Z}_2[x]$
- Nutně také $n \in \mathbb{Z}_2[x]$

- Délka p (prvočíslo, $p \equiv \pm 1 \pmod{8}$)
- Máme dva kódy generované r a n ; tyto kódy jsou vždy ekvivalentní
- Dimenze $p - (p - 1)/2 = (p + 1)/2$
- Minimální vzdálenost $\geq \sqrt{p}$
- Hustota zhruba $1/2$ a relativně velká vzdálenost
- Příklady: H_3 , G_{23}