

Samoopravné kódy

Alexandr Kazda

Univerzita Karlova

8. dubna 2020

- p prvočíslo, 2 je kvadratický zbytek modulo p , $\alpha = \sqrt[p]{1}$
- R kv. zbytky, N nezbytky modulo p
- $r = \prod_{i \in R} (x - \alpha^i)$ generuje kód \mathcal{R}
- $n = \prod_{i \in N} (x - \alpha^i)$ generuje kód \mathcal{N}
- Tvrdili jsme, že \mathcal{R}, \mathcal{N} jsou ekvivalentní a min. vzdálenost $\geq \sqrt{p}$
- Cvičení: Bud' $u \in N$. Pak $uR = N$, $uN = R$.

- Necht' $p = 23$
- Kvadratické zbytky 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6 (celkem je jich 11)
- Polynomy r, n mají stupeň 11
- Máme $[23, 23 - 11, d] = [23, 12, d]$ kód
- Tvrdil jsem, že $d \geq \sqrt{23}$, tj. $d \geq 5$; lze to zlepšit na $d = 7$
- Vyjde kód \mathcal{G}_{23}

Lemma

Bud' $u \in N$ a bud' $c \in \mathcal{R}$. Necht'

$$c' = c[x^u] \pmod{x^p - 1}.$$

Potom $c' \in \mathcal{N}$.

Důkaz.

- Stačí ukázat, že každá α^i pro $i \in N$ je kořen c' .
- Volme $i \in N$. Víme $iu \in R$
- $c'(\alpha^i) = c((\alpha^i)^u) - r(\alpha^i)((\alpha^i)^p - 1) = c(\alpha^{iu}) = 0$



Co se to stalo?!

- Příklad $p = 7$, $c = x^4 + x + 1$ (není kódové slovo), $u = 3$
- $c' = (x^{3 \cdot 4} + x^3 + 1) \pmod{x^7 - 1} = x^5 + x^3 + 1$
- Zobrazení $c \mapsto c'$ ve skutečnosti permutuje koeficienty
- Nechť $\pi(i) = iu \pmod{p}$ a nechť $c = c_0 + c_1x + \dots + c_{p-1}x^{p-1}$
- Pak $c' = c_0 + c_1x^{\pi(1)} + c_2x^{\pi(2)} + \dots + c_{p-1}x^{\pi(p-1)}$
- Permutace pozic \Rightarrow ekvivalence \mathcal{R} a \mathcal{N}

- Pozor, bude díra...
- Bud' $c \in \mathcal{R}$ polynom minimální váhy d
- Zase použiju lemma: $c' \in \mathcal{N}$ má také váhu d
- $c \cdot c'$ (počítáno v $\mathbb{F}_2[x]$) má za kořeny α^i pro $i \in R \cup N = \{1, 2, \dots, p-1\}$
- $c \cdot c'$ počítáno modulo $x^p - 1$ je proto $1 + x + \dots + x^{p-1}$
- Díra: Potřebuji $cc' \not\equiv 0 \pmod{x^p - 1}$, tedy 1 není kořen c, c' , tedy d liché

Minimální vzdálenost II

- c, c' mají oba d nenulových koeficientů
- Modulení $x^p - 1$ nezvýší počet nenulových koeficientů, tedy $c \cdot c'$ má v $\mathbb{F}_2[x]$ aspoň p nenulových koeficientů
- Ze vzorečku pro sčítání násobení polynomů je $d^2 \geq p$
- Důkaz, že QR kód má vždy lichou minimální vzdálenost, dá zabrat (umím to trikově přes Fourierovu transformaci) a my ho vynecháme
- Důkaz $d^2 \geq p$ lze pro $p \equiv -1 \pmod{8}$ vylepšit na $d^2 - d + 1 \geq p$ (těsný odhad pro \mathcal{G}_{23})

- Bud' \mathcal{C} lineární $[24, 12, 8]$ -kód, chceme ekvivalenci s \mathcal{G}_{24}
- \mathcal{C} obsahuje slova váhy 0,8,12,16,24 (váhový polynom), tj. násobky 4
- $\langle u + v, u + v \rangle \equiv \langle u, u \rangle + 2\langle u, v \rangle + \langle v, v \rangle \pmod{4}$
- $\Rightarrow 2\langle u, v \rangle \equiv 0 \pmod{4}$
- Tedy \mathcal{C} je samoduální (dimenze sedí: $24 - 12 = 12$)

- Búno \mathcal{C} obsahuje slovo $c = \underbrace{1 \dots 1}_{12 \times} \underbrace{0 \dots 0}_{12 \times}$ a slovo $\mathbf{1} = \underbrace{1 \dots 1}_{24 \times}$
- Generující 12×24 matice (má nezávislé řádky)
$$M = \begin{pmatrix} 1 \dots 1 & 0 \dots 0 \\ R & S \end{pmatrix}$$
- S je 11×12 a tvrdíme, že má nezávislé řádky
- Kdyby S měla závislé řádky, tak lze z řádků $(R|S)$ lineárně nakombinovat nenulový vektor $g = (g_1, g_2, \dots, g_{12}, \underbrace{0 \dots 0}_{12 \times})$
- Známe váhový polynom! Váha g je nutně 8, ale pak váha $g + c$ je 4, spor

- Protože $\underbrace{0 \dots 0}_{12 \times} \underbrace{1 \dots 1}_{12 \times} \in \mathcal{C}$, tak všechny řádky matice S mají sudý počet jedniček
- Řádků S je 11, tedy řádky matice S generují $[12, 11, 2]$ -kód (paritní)
- Řádkové úpravy nám dají

$$M = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ & & & 0 & 1 & 0 & 0 & \dots & 0 & 1 \\ & RD & & 0 & 0 & 1 & 0 & \dots & 0 & 1 \\ & & & \vdots & & & & \ddots & & 1 \\ & & & 0 & 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

- Přerovnáme prvních 11 sloupců úplně doprava...

Hezká generující matice [lépe viz začátek přednášky 15.4]

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 1 & \dots & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 & & & \\ 0 & 0 & 1 & \dots & 0 & 1 & & D & \\ & & & \ddots & 0 & 1 & & & \\ 0 & 0 & 0 & \dots & 1 & 1 & & & \end{pmatrix}$$

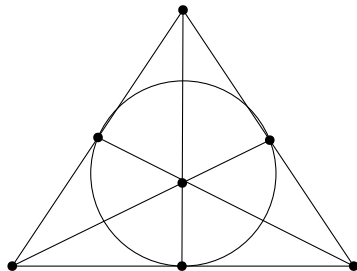
- Povolené váhy řádků M : 8,12,16
- D je 11×11 , váhy řádků 6 nebo 10
- Kdyby řádek D měl váhu 10, ~~tak ho přičtu k jinému~~ [toto nefunuje],
tak přičtu daný řádek M k prvnímu řádku M a dostanu kódové slovo
váhy 4, spor
- Tedy řádek D má váhu 6
- Váha součtu dvou různých řádků D je také 6 \Rightarrow každé dva řádky D mají právě 3 jedničky na společných pozicích
- To je velmi pravidelná matice!

- D je 11×11 matice, jejíž každý řádek má 6 jedniček a dva řádky mají „průnik“ přesně 3
- Řádky $D \equiv$ podmnožiny $\{1, 2, \dots, 11\}$, říkejme jim **bloky** B_1, \dots, B_{11}
- Tvrdíme, že každá dvojice $\{i, j\}$ leží v přesně 3 blocích
- Potom systém B_1, \dots, B_{11} bude $2 - (11, 6, 3)$ design
- Ukážeme jednoznačnost takového designu \Rightarrow jednoznačnost D

- Spočteme průměrný počet bloků, ve kterých jsou dvojice z $\binom{11}{2}$
- Máme $\binom{11}{2} = 55$ dvojic, každý blok obsahuje $\binom{6}{2} = 15$ dvojic;
 $15 \cdot 11 / 55 = 3$
- Pokud není rozložení rovnoměrné, tak (búno) $\{1, 2\}$ leží v B_1, B_2, B_3, B_4
- Odeberme $\{1, 2\}$. Pak nové bloky $B'_1, B'_2, B'_3, B'_4 \subset \{3, \dots, 11\}$ mají velikost 4 a jednoprvkové průniky
- PIE: $B'_1 \cup B'_2 \cup B'_3 \cup B'_4 \geq 4 \times 4 - \binom{4}{2} = 10$, spor

- Říkejme prvkům $V = \{1, 2, \dots, 11\}$ **vrcholy**
- (Jednoduchý) $2 - (v, k, \lambda)$ design je systém k -prvkových podmnožin (bloků) B_1, B_2, \dots množiny $V = \{1, 2, \dots, v\}$ takový, že každá dvojice vrcholů leží v přesně λ blocích
- Náš systém B_1, \dots, B_{11} je $2 - (11, 6, 3)$ design
- Víme více: Počet našich bloků = počet vrcholů; tomu se říká čtvercový design
- Design je **regulární** pokud každý vrchol leží ve stejném počtu bloků

Příklad: Fanova rovina



- Čtvercový 2 – $(7, 3, 2)$ design
- 7 vrcholů, 7 bloků, regulární
- Každé dva body určují blok (přímku)
- Fanova rovina je častý (proti)příklad v kombinatorice a geometrii
- Navíc: Každý bod leží přesně ve třech blocích, tj. je to regulární

- Pokud máme v bloků velikosti k a každý vrchol leží v právě r blocích, tak

$$rv = vk,$$

tedy $r = k$

- Je náš design B_1, B_2, \dots, B_{11} regulární?
- Tj. obsahuje každý sloupec matice D přesně $k = 6$ jedniček?
- „V průměru“ ano, ale mohlo by se nám třeba stát, že první sloupec má 7 jedniček, poslední sloupec 5 jedniček a ostatní sloupce mají 6 jedniček. . .
- Pokračování příště. . .
- Veselé Velikonoce!