Konečná tělesa

- těleso víte, co je :)
- každé konečné těleso má velikost p^s, kde p je prvočíslo a $s \in \mathbb{N}$. A naopak, pro každé prvočíslo p a $s \in \mathbb{N}$ existuje těleso velikosti p^s
- příklad $\mathbb{Z}_p$, tj. $(\{0,1,\dots,p-1\}, + \bmod p, \cdot \bmod p)$
- až na izomorfismus jsou všechna tělesa téže velikosti stejná

Polynomy

- tohle víte, co je
- $\mathbb{F}_q[X]$: mn. polynomů jejichž koeficienty jsou v $\mathbb{F}_q$
- nenulový polynom $f(X)$ stupně t nad tělesem $\mathbb{F}_q$ má $\leq t$ různých kořenů v $\mathbb{F}_q$
- důkaz dělením

Lagrangeova interpolace

- mějme $k+1$ různých bodů $(x_0, y_0), \dots, (x_k, y_k) \in \mathbb{R}^2$
- hledáme polynom stupně k, který jimi všemi prochází (x je def. obor, y obor hodnot)
- pro $j \in [0,k]$ značíme

$$l_j(x) = \frac{x - x_0}{x_j - x_0} \cdot \frac{x - x_1}{x_j - x_1} \cdots \frac{x - x_{j-1}}{x_j - x_{j-1}} \cdot \frac{x - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{x - x_k}{x_j - x_k}$$

$$= \prod_{\substack{0 \leq i \leq k \\ i \neq j}} \frac{x - x_i}{x_j - x_i}$$

$$l_j(x) = \begin{cases} 1 & x = x_j \\ 0 & x \in \{x_0, \dots, x_k\} \setminus \{x_j\} \\ ? & \text{jinak} \end{cases}$$

- $L(x) = \sum_{j=0}^{k} y_j \, l_j(x)$ projde v x_j bodem y_j $\quad 1 \cdot y_j = y_j$

ukážu, že je unikátní:

- uvažme poly M, který není L a interpoluje
- $M-L$ je nulový v $y_0, \dots, y_k$
- ale $\deg(M-L) \leq k$ a má $\geq k+1$ kořenů $\to$ $M-L \equiv 0$ ↯

- polynom stupně k lze reprezentovat $k+1$ koeficienty či vyhodnocením v $k+1$ bodech

Představme si, že máme v ruce (n,k,d)-kód.

a) Ukažte, že existuje $(n-1,k,d-1)$-kód. $\left(\begin{array}{l} k+1 \le n \text{ řešit?} \\ d \ge 1 \end{array}\right)$

b) Ukažte, že pokud je d liché, pak existuje $(n+1,k,d+1)$-kód.

a)

- co když utrhneme libovolný znak $C(x)$, třeba poslední?
- uvažme dvě slova x, y
- $C'(x) = C(x)$ bez posl. znaku
- $C'(y) = C(y)$ bez posl. znaku
- $\Delta(C'(x), C'(y))$?
  - stejný, pokud $C(x)$ na posl. znaku bylo stejné jako $C(y)$ na posl. znaku
  - $\ge \Delta(C(x), C(y)) - 1$ pokud naopak ✓

b)

- uvažme dvě slova x, y t.ž. $\Delta(C(x), C(y)) = d$
- $C(x), C(y)$ se liší na d znacích

$$\begin{array}{lcccccccccc} & & & & 0 & 1 & 1 & 1 & 0 & & \\ C(x) = & 0 & 1 & \dots & \times & & & & & & \\ & \shortparallel & \shortparallel & & 1 & 0 & 0 & 0 & 1 & - & - \\ & 0 & 1 & & & & & & & & \\ C(y) = & & & & & & & & & & \end{array}$$

- pozic, na kterých se liší, je lichý
- a jelikož „lišit se" znamená, že jeden z x,y má na patřičné pozici jedničku a druhý nulu,

tak jeden z x,y má lichý # jedniček a druhý sudý # jedniček

$\to$ paritní bit způsobí, že budou ještě dál od sebe o jedničku

Chceme definovat Hammingův kód nad q-ární abecedou. (Budeme potřebovat konečná tělesa, takže q bude mocnina prvočísla). To uděláme tak, že zavedeme následující kontrolní matici $H_{q,r}$:

- $H_{q,r}$ má ve sloupcích všechny nenulové vektory t.ž. první nenulová shora (či zleva, čte-li ten vektor po řádku) je 1

příklad
$$H_{3,2} = \left(\begin{array}{cccccccc} 0 & \boxed{0} & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & \boxed{2} & 0 & 1 & 2 & 0 & 1 & 2 \\ & (2)_3 & (3)_3 & (4)_3 & (5)_3 & \text{NE} & \text{NE} & \text{NE} \end{array}\right) \to \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

NE, první nenulová je 2, ale my chceme 1

1 v ternární soustavě $= (1)_3$

a) Ukažte $n = \frac{q^r - 1}{q-1}$

b) Ukažte, že dim prostoru zpráv je $n-r$

c) Ukažte, že min vzdálenost mezi kódovými slovy je 3.

---

a)

- pro každý sloupec může první jednička být v jednom z r řádků a pod ní je cokoliv z q prvků tělesa

→ výsledek je $\sum_{i=0}^{r-1} q^i = \frac{q^r - 1}{q-1}$

kolik je řádků pod první jedničkou

b)

- rank matice = rank její transpozice
- každý jednotkový vektor se vyskytuje jako sloupec $H_{q,r}$

→ rank $\geq r$, a # řádků r → rank $= r$

· teorie kódování říká, že generující matice má dim $n - \text{rank}(H_{q,r})$ → hotovo

c)

· stejné jako pro bin Hammingův kód

· tedy každé dva sloupce jsou LN

· pokud dva sloupečky mají první jedničku na jiném řádku, tak rozhodně jeden není násobkem druhého

· a pokud dva sloupečky mají první jedničku na tomtéž řádku, tak musí být 1-násobkem jeden druhého kvůli, ale zbytek je různý

· a určitě existuje sloupec pro $(1)_q$ $(q)_q$ $(q+1)_q = (00\ldots 11)$

$$= (0\ldots 010)$$

Jak z kontrolní matice dostat generující a naopak

a) Ukažte, že pro libovolnou generující matici G existuje ekvivalentní lin. kód t.ž. má generující matici G' ve tvaru $G' = (I_k \mid A)$

zavorná $k \times k$ jednotkovou matici

cokoli velikosti $k \times (n-k)$

· lin kódům v tomto tvaru říkáme <u>systematický kód</u>, neboť prvních k znaků kódového slova je původní zpráva

$$k \updownarrow \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix}, \quad \underset{k}{\longleftrightarrow}$$

· G má plnou hodnost → Gaussova eliminační metoda převede G do požadovaného tvaru

· a operace GEMu lze vidět jako násobení maticemi plného ranku

· např. přinásobení k násobku j-tého řádku k i-tému je přenásobení zleva maticí

$$\begin{array}{cc} & \qquad\quad j \\ i & \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & k \\ & & & \ddots \end{pmatrix} \end{array}$$, prohození i-tého a j-tého řádku $$\begin{array}{cc} & \qquad\quad i \quad\; j \\ \begin{array}{c} i \\ j \end{array} & \begin{pmatrix} 1 & & & \\ & \ddots & 0 & 1 \\ & & 1 & 0 & \ddots \\ & & & & 1 \end{pmatrix} \end{array}$$

- takže posl. těchto operací je dohromady lin. zobrazení, které je bijekcí

b) Najděte kontrolní matici H ke generující matici ve tvaru $G = (I_k \; \underbrace{A}_{n-k}) \,]k$

- chceme $G \cdot H = 0$

$\rightarrow \quad H = \begin{pmatrix} -A^T \\ I_k \end{pmatrix}$