Start 11:35

Věta (Hamming): Pokud P je (M, n, d) kód nad abecedou s (q) znaky a $t := \lfloor \frac{d-1}{2} \rfloor$, tak

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq \frac{q^n}{M}$$

Rovnost „P je perfektní"

$t := \lfloor \frac{d-1}{2} \rfloor$

q^{n-r} lineární kód s kontrolní maticí hodnosti k

Věta (Gilbert-Varsham): q mocnina prvočísla, $n \in \mathbb{N}$, $r \in \mathbb{N}$, $d \in \mathbb{N}$. Pokud

$$\sum_{j=0}^{d-2} \binom{n-1}{j} \cdot (q-1)^j < q^r$$

pak $\exists$ kontrolní matice $H \in T^{r \times n}$ pro nějaký lineární (q^{n-r}, n, d)-kód

Dk: H je kontrolní matice pro kód s vzdáleností d

$\Updownarrow$

$\leq d-1$ sloupců H je LN

$$H = \begin{array}{c} \overset{\uparrow}{n} \\ \boxed{1111\ldots1} \\ \underset{\downarrow}{r} \end{array} \quad \overset{i}{\rightarrow}$$

Indukčně:

1. sloupec – libovolný nenulový vektor z F^r

mějme i sloupců, $i < n$, spočtěme kolik sloupců nelze přidat jako $(i+1)$-sloupec

$$\leq \underbrace{1}_{\text{0 sloupců}} + \underbrace{i\cdot(q-1)}_{\text{1 sloupec}} + \underbrace{\binom{i}{2}(q-1)^2}_{\text{2 sloupce}} + \dots + \underbrace{\binom{i}{d-2}(q-1)^{d-2}}_{(d-2)\text{-sloupců}}$$

pokud $\sum_{j=0}^{d-2}\binom{i}{j}(q-1)^j < q^r$

$\exists$ sloupec co jde přidat, přidejme lib. z nich

Chceme pro $i \leq n-1$ aby platilo

$\Leftarrow$ stačí $i = n-1$

$$\sum_{j=0}^{d-2}\binom{n-1}{j}(q-1)^j < q^r$$

VI

Def: $\forall k \in \mathbb{N}$, $d \in \mathbb{N}$, $\mathbb{F} = \mathbb{Z}_2$

dim e

$$N(k,d) := \min\{n \in \mathbb{N} : \exists \text{ lin. binární kód délky } n, \text{ dimenze } k, \text{ vzdálenosti } d\}$$

Př: $N(4,3) = 7$ protože Hammingův kód

$d-1 <$ **$N(1,d) = d$** ; $N(k,1) = k$

$C = \{\overbrace{0\ldots0}^{d}, \overbrace{1\ldots1}^{d}\}$ $\quad C = \{0,1\}^k$

$d = 21$ $\Leftrightarrow$ dvě kódová slova $d_H(x,y) \geq 21$ $\quad \left(\begin{matrix}\text{nad} \\ \mathbb{Z}_2\end{matrix}\right)$

$\Leftrightarrow$ oprava až 10 chybně přenesených bitů

$00\ldots0,\ 11\ldots11$

$w_1,\ \overline{w_1}$

Věta: $\forall d \in \mathbb{N},\ \forall k \geq 2 \quad N(k,d) \geq d + N\left(k-1, \left\lceil \frac{d}{2} \right\rceil\right)$

Důsledek (Griesmerův odhad): $N(k,d) \geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{2^j} \right\rceil$

Dk.: indukcí dle k

$k = 1$ $\quad N(1,d) \geq d$

$k \geq 2$, z věty $N(k,d) \geq d + \underbrace{N\left(k-1, \left\lceil \frac{d}{2} \right\rceil\right)}_{\text{IP}}$

$$\geq d + \sum_{j=0}^{k-2} \left\lceil \frac{\left\lceil \frac{d}{2} \right\rceil}{2^j} \right\rceil \geq d + \sum_{j=1}^{k-1} \left\lceil \frac{d}{2^j} \right\rceil$$

$\left\lceil \frac{\lceil x \rceil}{b} \right\rceil \geq \left\lceil \frac{x}{b} \right\rceil \quad \forall x, b \geq 0$ $\square$

Věta: $\forall d \in \mathbb{N}, \forall k \geq 2 \quad N(k,d) \geq d + N\left(k-1, \lceil \frac{d}{2} \rceil\right)$

Dk: Mějme lin. kód $\mathcal{C}$ délky $n = N(k,d)$ t.ž. $\mathcal{C}$ je $(2^k, n, d)$-kód

(1) $\mathcal{C}$ je lineární, tak $\forall u, w \in \mathcal{C}$ platí $(u-w) \in \mathcal{C}$

Tudíž $\exists w_0 \in \mathcal{C}$ t.ž. w_0 má d 1, a $n-d$ 0

$$G_{\mathcal{C}} = \begin{pmatrix} \overbrace{w_0}^{n} \\ w_1 \\ \vdots \\ w_{k-1} \end{pmatrix} \Big\} k$$

kde $w_0, \dots, w_{k-1}$ je báze $\mathcal{C}$

BÚNO $w_0 = \overbrace{0 \dots 0}^{n-d} \overbrace{1 \dots 1}^{d}$

Tudíž:

$$G_{\mathcal{C}} = \left(\begin{array}{c|c} \overbrace{0 \dots 0}^{n-d} & \overbrace{1 \dots 1}^{d} \\ \hline G_1 & \sim \end{array} \right) k$$

$N(k-1, \lceil d/2 \rceil)$

(1): ukázat že G_1 generuje lin. kód $\mathcal{D}$ dimenze $k-1$

$\forall$ dva $u, w \in \mathcal{D}$ mají vzdálenost $\geq d/2$

(2) $N(k, d_1) < N(k, d_2)$ pro $d_1 < d_2$

P_1 odstraní $d_2 - d_1$ sloupců $\rightsquigarrow P_2$

1) $hodnost(G_1) = k-1$

pro spor, $\exists$ netriviální lineární komb. řádků G_1

$$\sum_{i=1}^{k-1} \alpha_i w_i^* = \underbrace{(0, \dots, 0)}_{n-d}$$

w_i^* = zúžení w_i na prvních $n-d$ souřadnic

$$\sum_{i=1}^{k-1} \alpha_i \cdot w_i = (\underbrace{0 \dots 0}_{n-d} \boxed{b_1 \dots b_d})$$

$\exists i : b_i = 1$ jinak by $\{w_0, \dots, w_{k-1}\}$ netvořila báz. $\neq i$ $\in C$

$C \ni w_0 = (0 \dots 0 1 1 1 1)$

$C \ni \sum_{i=1}^{m-1} \alpha_i w_i = (0 \dots 0 \dots 1 \dots)$ } vzdálenost $\leq d-1$

2) $\forall u^*, w^* \in \mathcal{D}$ platilo $dist(u^*, w^*) \geq d/2$

$\Rightarrow dist(u^*, w^*) \geq \lceil d/2 \rceil$

$d_1 :=$ minimální vzdálenost v kódu $\mathcal{D}$

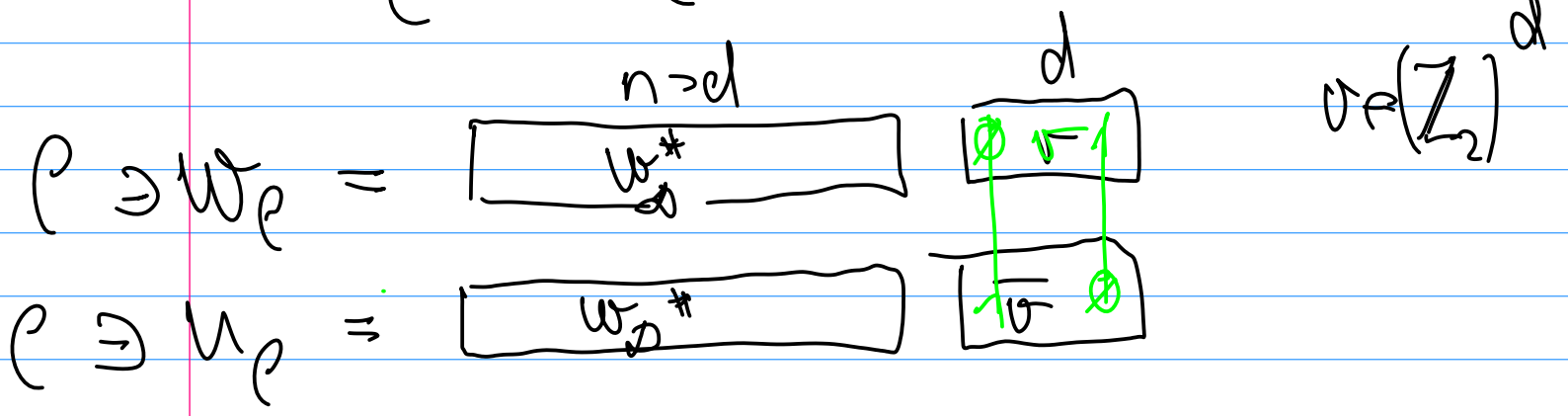
$\Rightarrow \exists w_2^* \in \mathcal{D}$ které má d_1 1

$(n-d)-d_1$ 0

$$w_{\mathcal{D}}^* = \sum_{i=1}^{k-1} \alpha_i w_i^* \in (\mathbb{Z}_2)^{n-d}$$

$$\mathcal{C} \ni w_{\mathcal{C}} := \sum_{i=1}^{k-1} \alpha_i w_i \in (\mathbb{Z}_2)^n$$

$$u_{\mathcal{C}} := w_{\mathcal{C}} + w_0$$



speciálně $u_{\mathcal{C}}$ i $w_{\mathcal{C}}$ mají $\geq d$ 1ek

$$2d \leq \underbrace{\#1 \text{ v } u_{\mathcal{C}}}_{\geq d} + \underbrace{\#1 \text{ v } w_{\mathcal{C}}}_{\geq d} = 2d_1 + d$$

$$\Rightarrow \quad d_1 \geq d/2$$

∎