Steganografie pomocí maticového vkládání

Andrew Kozlik

KA MFF UK

M1

Značení

- Zvolíme konečné těleso $\mathbb{F}_q$, obvykle $q = 2$ nebo $q = 3$.
- Stegoobjekt rozdělíme na bloky délky n.
- Hovoříme o posloupnosti hodnot spjatých s blokem
  - nosiče $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ a
  - stegoobjektu $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.
- Zprávu rozdělíme na bloky délky m.
- Předpokládáme, že:

  počet bloků nosiče = počet bloků zprávy.
- Blok zprávy značíme $\mathbf{z} = (z_1, \ldots, z_m) \in \mathbb{F}_q^m$.

Co jsou „spjaté hodnoty“

- Pro $q = 2$ například:
  - LSB příslušného prvku nosiče či stegoobjektu.
  - Parita ve smyslu vkládání s optimálním přiřazením parity v paletových formátech.

- Obecně:
  - Zbytek po dělení prvku číslem q.

Relativní kapacita

- Zpráva se nyní skládá z q-árních symbolů.
- Kapacitu nadále měříme v bitech!
- Proto relativní kapacita nosiče je

$$\alpha = \frac{\log_2 q^{m \cdot \#\text{bloků}}}{n \cdot \#\text{bloků}} = \frac{m}{n} \log_2 q.$$

Maticové vkládání pomocí Hammingových kódů

- **H** je paritní matice Hammingova $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m]_q$ kódu.
- Sloupce **H** jsou tvořeny všemi nenulovými vektory z $\mathbb{F}_q^m$, až na násobek.
- Pro začátek mějme $q = 2$.

  Sloupce je vhodné uspořádat lexikograficky, například:

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Vkládání a extrakce zprávy

- Extrakce zprávy ze stegoobjektu: $\mathbf{z} = \mathbf{H}\mathbf{y}$.
- Vkládání:
  - Spočítáme $\mathbf{H}\mathbf{x}$, tzv. *syndrom* vektoru $\mathbf{x}$.
  - Pokud $\mathbf{H}\mathbf{x} = \mathbf{z}$, není co řešit, $\mathbf{y} = \mathbf{x}$.
  - Pokud $\mathbf{H}\mathbf{x} \neq \mathbf{z}$:
    - Spočtu $\mathbf{z} - \mathbf{H}\mathbf{x}$.
    - V $\mathbf{H}$ najdu j-tý sloupec $\mathbf{H}_{*j} = \mathbf{z} - \mathbf{H}\mathbf{x}$.
    - Za $\mathbf{y}$ zvolím $\mathbf{x} + \mathbf{e}_j$.
- Kontrola $\mathbf{H}\mathbf{y} = \mathbf{H}(\mathbf{x} + \mathbf{e}_j) = \mathbf{H}\mathbf{x} + \mathbf{H}_{*j} = \mathbf{z}$.

Srovnání s dekódováním Hammingových kódů

- Při dekódování poškozeného slova je cílem získat nulový syndrom $\mathbf{H}y = 0$.
- $\mathbf{e}_j$ je chybový vektor.
- $x + e_j$ je opravené slovo.
- Čili dekódování $\equiv$ vkládání nulové zprávy.

Očekávaná distorze na blok

- Předpokládáme, že všechny syndromy $\mathbf{Hx} \in \mathbb{F}_q^m$ jsou stejně pravděpodobné.
- Případ $\mathbf{Hx} = \mathbf{z}$ nevnáší distorzi.
- Případ $\mathbf{Hx} \in \mathbb{F}_q^m \setminus \{\mathbf{z}\}$ vnáší distorzi 1.
- Očekávaná distorze je tedy

$$\frac{2^m - 1}{2^m} = 1 - 2^{-m}.$$

Efektivita a relativní kapacita

- Délka zprávy na jeden blok je m.
- Očekávaná distorze na blok je $1 - 2^{-m}$.
- Efektivita je

$$e = \frac{\#\text{vložených bitů}}{\text{očekávaná distorze}} = \frac{m \cdot \#\text{bloků}}{(1 - 2^{-m}) \cdot \#\text{bloků}} = \frac{m}{1 - 2^{-m}}$$

- Relativní kapacita schématu je

$$\alpha = \frac{\#\text{bitů zprávy}}{\#\text{prvků nosiče}}$$

Konkrétní čísla

- Případ $m = 1$ vede na standardní LSB embedding.
- Případ $m = 2$ odpovídá příkladu z úvodní přednášky o maticovém vkládání.

m	α	e
1	1,000	2,000
2	0,667	2,667
3	0,429	3,429
4	0,267	4,267
5	0,161	5,161
6	0,095	6,095
7	0,055	7,055
8	0,031	8,031
9	0,018	9,018

Praktický postup

- Máme dánu zprávu a nosič.
- Najdeme největší m takové, že

$$\frac{m}{2^m - 1} \geq \frac{\#\text{bitů zprávy}}{\#\text{prvků nosiče}}.$$

- Potom použijeme Hammingův $[2^m - 1, 2^m - 1 - m]_2$ kód.
- Do stegoobjektu uložíme informaci o zvolené hodnotě m.
- Tento postup používá stegosystém F5.
- Připomenutí vkládání v F5:
  - F5 pracuje s nenulovými AC koeficienty obrázku JPEG.
  - Změna parity se provádí dekrementací v absolutní hodnotě.
  - Parita je definovaná obráceně pro záporné AC koeficienty.

Použití těles $\mathbb{F}_q$, kde $q \geq 3$

- Prvky nosiče budou asociovány s prvky tělesa operací $x \mapsto x \bmod q$.
- Např. pro $q = 3$ to znamená, že libovolnou hodnotu $\{0, 1, 2\}$ lze docílit změnou velikosti 1.
- I bez maticového vkládání tím získáváme lepší výsledky!
- Očekávaná distorze na blok je

$$\frac{m}{3} \cdot 0^2 + \frac{m}{3} \cdot 1^2 + \frac{m}{3} \cdot (-1)^2 = \frac{2}{3}m.$$

- Délka zprávy v bitech je $\log_2 3^m = m \log_2 3 \approx 1{,}585m$.
- Efektivita

$$e = \frac{m \log_2 3}{\frac{2}{3}m} \approx 2{,}377.$$

- Pro vyšší hodnoty q už ovšem efektivita této metody klesá.

Vkládání a extrakce pro q-ární Hammingovy kódy

- Extrakce opět $\mathbf{z} = \mathbf{H}\mathbf{y}$.

- Vkládání:
  vstup: nosič $\mathbf{x} \in \mathbb{F}_q^n$, zpráva $\mathbf{z} \in \mathbb{F}_q^m$,
  paritní matice $\mathbf{H}$ Hammingova $[n, n-m]_q$ kódu
  výstup: stegoobjekt $\mathbf{y} \in \mathbb{F}_q^n$ takový, že $\mathbf{H}\mathbf{y} = \mathbf{z}$

```
1  if Hx = z then
2      return x
3  else
4      najdi j a a ∈ F_q takové, že z − Hx = aH_{*j}
5      return x + ae_j
```

Důkaz.
$\mathbf{H}\mathbf{y} = \mathbf{H}\mathbf{x} + a\mathbf{H}\mathbf{e}_j = \mathbf{H}\mathbf{x} + a\mathbf{H}_{*j} = \mathbf{z}$. □

Příklad pro $q = 3$ a $m = 3$

- Máme paritní matici Hammingova $[13, 10]_3$ kódu.

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

- Zpráva $\mathbf{z} = (1, 2, 0)^{\mathrm{T}} \in \mathbb{F}_3^3$.
- Vektor $\mathbf{x}$ získáme z prvků nosiče jako zbytky po dělení 3.

Blok nosiče: 20 21 19 19 18 16 19 20 24 23 20 20 19

$$\mathbf{x} = (\,2 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 2 \quad 0 \quad 2 \quad 2 \quad 2 \quad 1\,)^{\mathrm{T}}$$

- $\mathbf{z} - \mathbf{H}\mathbf{x} = (1, 2, 0)^{\mathrm{T}} - (2, 1, 1)^{\mathrm{T}} = 2 \cdot (1, 2, 1)^{\mathrm{T}} = 2 \cdot \mathbf{H}_{*\,12}$.
- Odtud $\mathbf{y} = \mathbf{x} + 2\mathbf{e}_{12}$

$$\mathbf{y} = (\,2 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 2 \quad 0 \quad 2 \quad 2 \quad \mathbf{1} \quad 1\,)^{\mathrm{T}}$$

Blok stegoobjektu: 20 21 19 19 18 16 19 20 24 23 20 **19** 19

- Jedinou změnou jsme vložili $3 \cdot \log_2 3 = 4{,}75$ bitů informace!

Efektivita vkládání s q-árními Hammingovými kódy

- Jaká je velikost změn, které mohou nastat při vkládání?
- Např. pro $q = 3$ máme $\Delta_3 = \{-1, 0, 1\}$.
- Obecně:
  - Pro q liché $\Delta_q := \{\frac{-q+1}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2}\}$.
  - Pro q sudé $\Delta_q := \{\frac{-q}{2} + 1, \ldots, -1, 0, 1, \ldots, \frac{q}{2}\}$.
- Očekávaný příspěvek jedné změny k distorzi je
$$\frac{1}{q-1} \sum_{\delta \in \Delta_q} \delta^2.$$
- Očekávaný počet změn za předpokladu, že všechny vektory $\mathbf{z} - \mathbf{Hx} \in \mathbb{F}_q^m$ jsou stejně pravděpodobné, je
$$\frac{q^m - 1}{q^m} = 1 - q^{-m}.$$

Efektivita vkládání s q-árními Hammingovými kódy

- Délka zprávy:

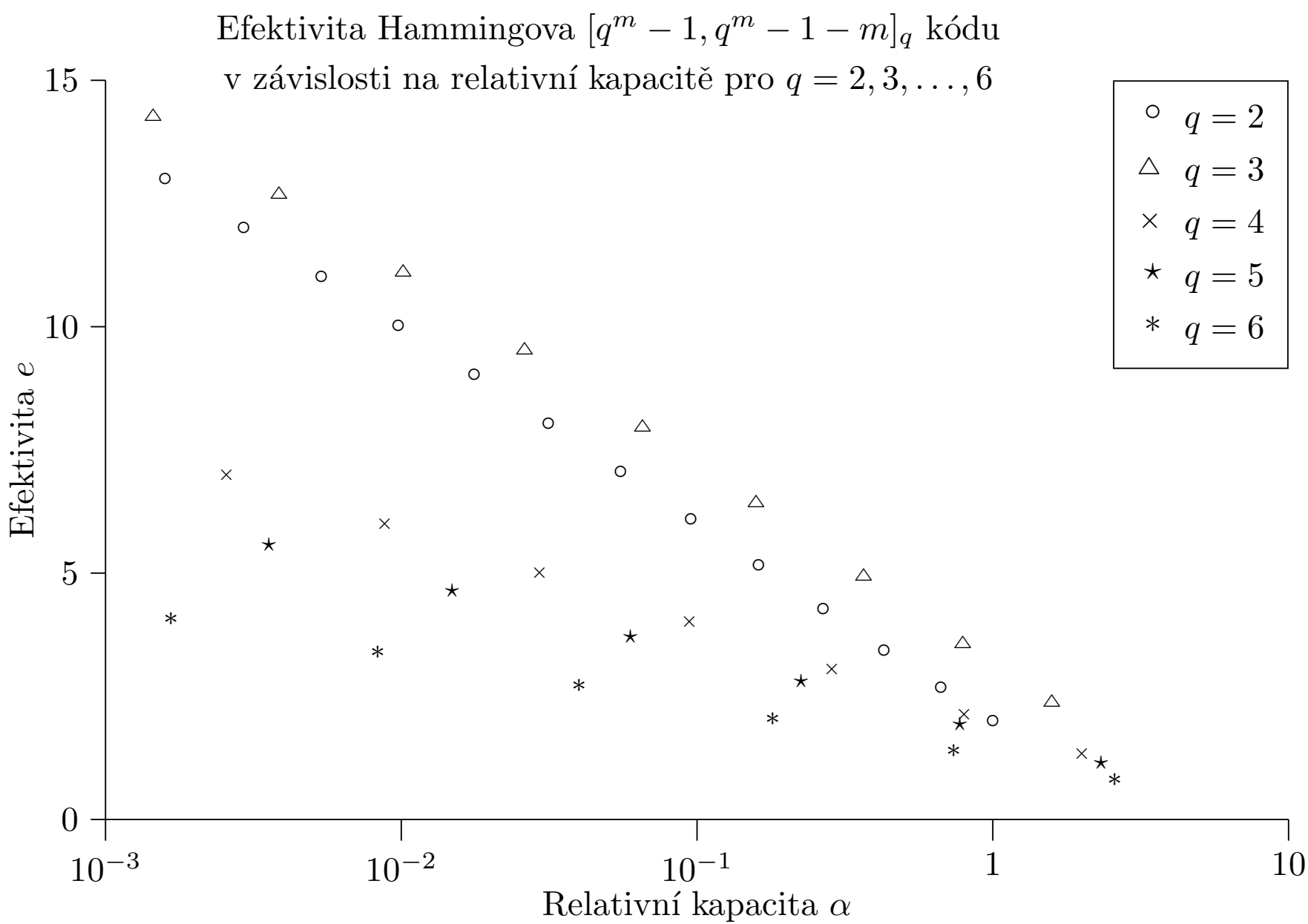
$$\log_2 q^m = m \log_2 q \quad \text{[bitů]}.$$

- Relativní kapacita:

$$\alpha = \frac{m \log_2 q}{(q^m - 1)/(q - 1)} \quad \text{[bitů na prvek]}.$$

- Efektivita vkládání je

$$e = \frac{(q-1) m \log_2 q}{(1 - q^{-m}) \sum_{\delta \in \Delta_q} \delta^2} \quad \text{[bitů na jednotku distorze]}.$$


Efektivita Hammingova $[q^m - 1, q^m - 1 - m]_q$ kódu
v závislosti na relativní kapacitě pro $q = 2, 3, \ldots, 6$
$q = 2$
$q = 3$
$q = 4$
$q = 5$
$q = 6$
Efektivita e
15
10
5
0
10^{-3}
10^{-2}
10^{-1}
1
10
Relativní kapacita α

Maticové vkládání obecně

- Značení:
  - n je délka kódu $\mathcal{C}$.
  - k je dimenze kódu $\mathcal{C}$.
  - q je velikost tělesa.
- Pro $\mathcal{X} \subseteq \mathbb{F}_q^n$ a $u \in \mathbb{F}_q^n$ definujeme

$$d_{\mathrm{H}}(\mathbf{u}, \mathcal{X}) = \min_{\mathbf{v} \in \mathcal{X}} w(\mathbf{v} - \mathbf{u}).$$

- Matici $\mathbf{H}$ typu $(n-k) \times n$ s lineárně nezávislými řádky nazýváme *paritní maticí* kódu $\mathcal{C}$ jestliže

$$\mathcal{C} = \{\, \mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{Hu} = \mathbf{0} \,\}.$$

- Prostor $\mathbb{F}_q^n$ můžeme faktorizovat podle podprostoru $\mathcal{C}$.
- Definujeme *rozkladovou třídu příslušnou syndromu* $\mathbf{s} \in \mathbb{F}_q^{n-k}$

$$\mathcal{C}(\mathbf{s}) := \{\, \mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{Hu} = \mathbf{s} \,\}.$$

Maticové vkládání a extrakce

Definice

- Nechť $\mathbf{H}$ je paritní matice $[n, k]_q$ kódu $\mathcal{C}$.
- Nechť $\mathbf{e} : \mathbb{F}_q^{n-k} \to \mathbb{F}_q^n$ je zobrazení takové, že pro všechna $\mathbf{s} \in \mathbb{F}_q^{n-k}$ je $\mathbf{He}(\mathbf{s}) = \mathbf{s}$ a $w(\mathbf{e}(\mathbf{s})) = \min_{\mathbf{u} \in \mathcal{C}(\mathbf{s})} w(\mathbf{u})$.
- Potom definujeme *maticovou extrakci* a *maticové vkládání*

$$\mathrm{Ext}_{\mathbf{H}}(\mathbf{y}) := \mathbf{Hy} \quad \text{a} \quad \mathrm{Emb}_{\mathbf{H},\mathbf{e}}(\mathbf{x}, \mathbf{z}) := \mathbf{x} + \mathbf{e}(\mathbf{z} - \mathbf{Hx}),$$

kde $\mathbf{x}$, $\mathbf{y} \in \mathbb{F}_q^n$ a $\mathbf{z} \in \mathbb{F}_q^{n-k}$.

Ověření korektnosti definice:

$$\mathrm{Ext}_{\mathbf{H}}(\mathrm{Emb}_{\mathbf{H},\mathbf{e}}(\mathbf{x}, \mathbf{z})) = \mathbf{H}(\mathbf{x} + \mathbf{e}(\mathbf{z} - \mathbf{Hx})) = \mathbf{Hx} + \mathbf{z} - \mathbf{Hx} = \mathbf{z}$$

pro každé $\mathbf{x} \in \mathbb{F}_q^n$ a $\mathbf{z} \in \mathbb{F}_q^{n-k}$.

Zobrazení $\mathbf{e}$

- Zobrazení $\mathbf{e}$ zajišťuje, že počet změn vyvolaných vkládáním je minimalizován.
- Zobrazení $\mathbf{e}$ nemusí být jednoznačně určeno.
- Místo $\mathrm{Emb}_{\mathbf{H},\mathbf{e}}$ budeme psát jen $\mathrm{Emb}_{\mathbf{H}}$.
  (Zobrazení $\mathbf{e}$ nás samo o sobě obvykle nezajímá.)
- U Hammingových kódů $\mathbf{e}(\mathbf{s})$ vrací sloupec paritní matice, který je násobkem $\mathbf{s}$.
- U jiných kódů nemusí být výpočet $\mathbf{e}(\mathbf{s})$ tak jednoduchý.
- Obecně se jedná o NP-úplný problém.

Další probraná témata (viz skripta)

Definice minimum-distance dekodéru.

Algoritmus maticového vkládání pomocí minimum-distance dekodéru.

Pokrývací poloměr a průměrná vzdálenost od kódu.

Věta o maticovém vkládání a její důsledek týkající se efektivity.

q-ární entropická funkce.

Lemma o vztahu mezi entropickou funkcí a objemem koule.

Spodní mez na pokrývací poloměr.

Spodní efektivita

Definice

Pro $[n, k]_q$ kód s pokrývacím poloměrem r_c definujeme *spodní efektivitu* vkládání

$$\underline{e} := \frac{n\alpha(q-1)}{r_\mathrm{c} \sum_{\delta \in \Delta_q} \delta^2},$$

kde $\alpha = (1 - \frac{k}{n}) \log_2 q$.

- Místo očekávaného počtu změn r_a počítáme u spodní efektivity s maximálním počtem změn r_c.
- Alespoň v případě „většiny“ binárních kódů mají hodnoty r_c a r_a k sobě asymptoticky blízko.

Věta (Fridrich et al.)

Nechť $0 < \alpha < 1$ *a* $\varepsilon > 0$. *Podíl všech* $[n, (1-\alpha)n]_2$ *kódů, pro něž platí* $|r_\mathrm{c} - r_\mathrm{a}|/n \leq \varepsilon$, *konverguje k* 1 *pro* $n \to \infty$.

Věta

Pro každý $[n, k]_q$ *kód s pokrývacím poloměrem* r_c *platí*

$$r_c \geq n\, H_q^{-1}\left(\frac{\alpha}{\log_2 q}\right),$$

kde $\alpha = (1 - \frac{k}{n}) \log_2 q$.

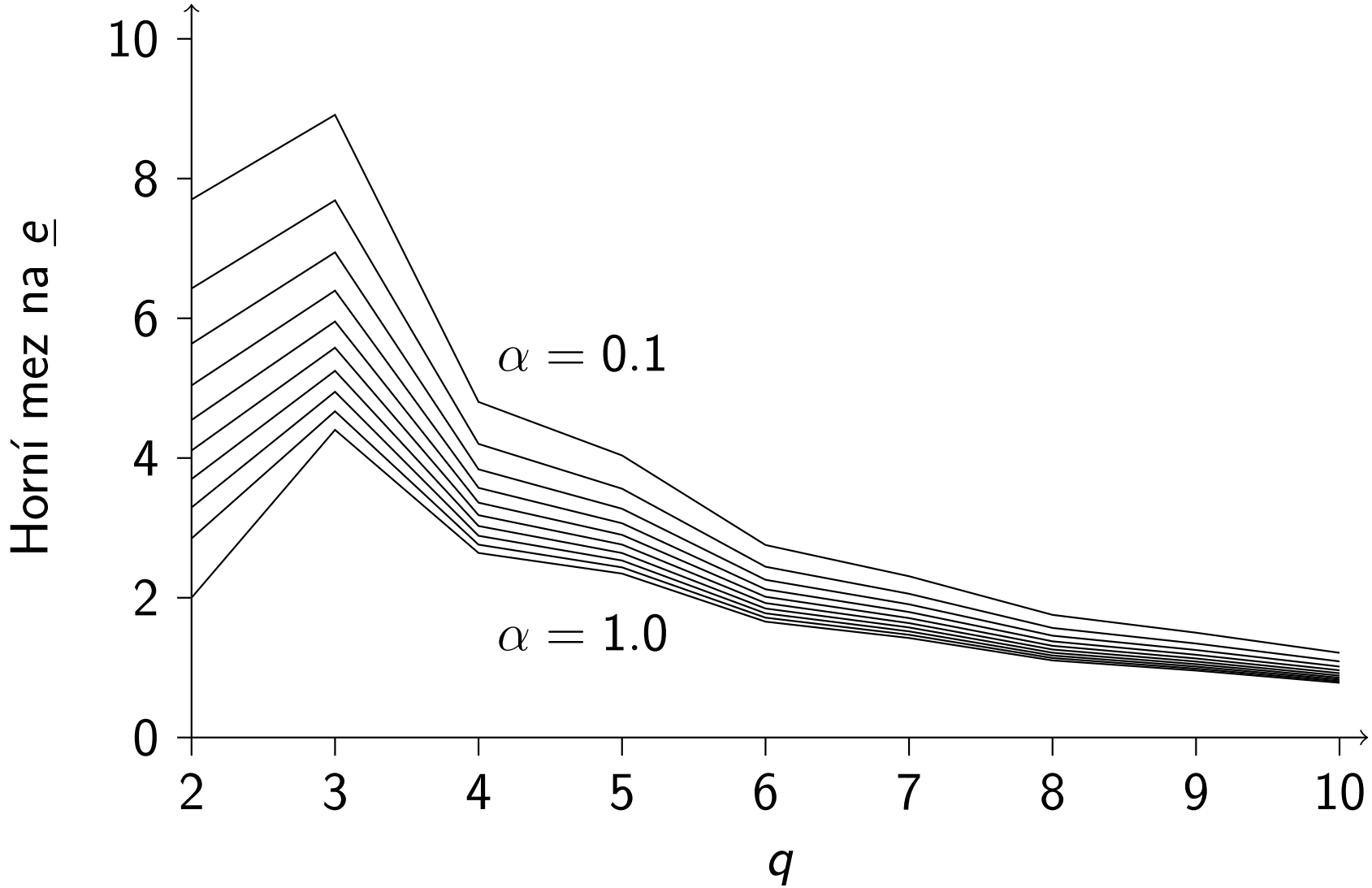
Důkaz.

Viz minulá přednáška. □

Z věty plyne horní mez na spodní efektivitu maticového vkládání v závislosti na relativní kapacitě α

$$\overline{e}(q, \alpha) := \frac{\alpha(q-1)}{H_q^{-1}(\alpha/\log_2 q) \sum_{\delta \in \Delta_q} \delta^2} \geq \underline{e}.$$

Horní mez $\overline{e}(q, \alpha)$ na spodní efektivitu vkládání v závislosti na q pro $\alpha = 0{,}1, 0{,}2, \ldots, 1{,}0$.



Tvrzení

Nechť $\mathcal{C}$ je $[n,k]_q$ kód s průměrnou vzdáleností r_{a} a nechť r je největší celé číslo takové, že $V_q(n,r) \leq q^{n-k}$. Potom

$$r_{\mathrm{a}} \geq q^{k-n} \sum_{i=1}^{r} i(q-1)^i \binom{n}{i},$$

přičemž rovnost nastává právě tehdy, když $\mathcal{C}$ je perfektní kód.

Důsledek

Nechť $\mathcal{C}$ je $[n,k]_q$ kód, kde $q \in \{2,3\}$, a nechť r je největší celé číslo takové, že $V_q(n,r) \leq q^{n-k}$. Potom efektivita maticového vkládání pro kód $\mathcal{C}$ je

$$e \leq \frac{q^{n-k}(n-k)\log_2 q}{\sum_{i=1}^{r} i(q-1)^i \binom{n}{i}},$$

přičemž rovnost nastává právě tehdy, když $\mathcal{C}$ je perfektní kód.

Golayovy kódy

- Stačí za r dosadit $(d-1)/2$, kde d je minimální váha kódu.
- Pro binární Golayův $[23, 12, 7]_2$ kód máme
  - $\alpha = 11/23$ a
  - $e = 11 \cdot 2^{11} / \sum_{i=1}^{3} i\binom{23}{i} = 11264/2921 \approx 3{,}856.$
- Pro ternární Golayův $[11, 6, 5]_3$ kód máme
  - $\alpha = 5(\log_2 3)/11 \approx 0{,}720$ a
  - $e = 5 \cdot 3^5(\log_2 3) / \sum_{i=1}^{2} i \cdot 2^i \binom{11}{i} = 1215(\log_2 3)/462 \approx 4{,}168.$

Efektivita perfektních kódů a horní mez efektivity