Součtově a rozdílově pokrývací množiny

Andrew Kozlik

KA MFF UK

Motivační příklad

- Nosič rozdělíme na dvouprvkové bloky $(x_1, x_2) \in \mathbb{Z}^2$.
- Do každého bloku vkládáme kvaternární symbol $z \in \mathbb{Z}_4$.
- **Extrakce**: Definována jako $\mathrm{Ext}(y_1, y_2) = (y_1 + 2y_2) \bmod 4$.
- **Vkládání**: Mějme např. $(x_1, x_2) = (15, 16)$ a $z = 2$.
  - Zkusíme extrakci: $\mathrm{Ext}(15, 16) = 3 \neq 2$ ☹.
  - To se dá snadno napravit: Snížíme x_1 o 1.
  - Zápis: $(y_1, y_2) = (15, 16) + (-1, 0) = (14, 16)$.
  - Obecně:

	zpráva z			
$x_1 + 2x_2$	0	1	2	3
0	$(0, 0)$	$(+1, 0)$	$(0, \pm 1)$	$(-1, 0)$
1	$(-1, 0)$	$(0, 0)$	$(+1, 0)$	$(0, \pm 1)$
2	$(0, \pm 1)$	$(-1, 0)$	$(0, 0)$	$(+1, 0)$
3	$(+1, 0)$	$(0, \pm 1)$	$(-1, 0)$	$(0, 0)$

Parametry motivačního příkladu

- Relativní kapacita

$$\alpha = \frac{2 \text{ bity}}{2 \text{ prvky}} = 1.$$

- Efektivita

$$e = \frac{2 \text{ bity}}{\frac{3}{4} \text{ jednotek distorze}} = \frac{8}{3} = 2{,}66\overline{6}$$

- To je nejlepší schéma s takto vysokou kapacitou, které jsme dosud viděli.
- Standardní LSB vkládání: $\alpha = 1$ a $e = 2$.
- Bezmaticové ternární vkládání: $\alpha = \log_2 3 \approx 1{,}58$ a $e = \frac{3}{2} \log_2 3 \approx 2{,}38$.

Definice SDCS a SDCS váhy

Nechť:

- n a r jsou přirozená čísla,
- $(G, +)$ je konečná abelovská grupa,
- $\mathcal{A} = \{a_1, \ldots, a_n\}$ posloupnost po dvou různých hodnot z G.

Pokud pro každé $g \in G$ existují $s_1, \ldots, s_n \in \{-1, 0, 1\}$ takové, že

$$\sum_{i=1}^{n} |s_i| \leq r \quad \text{a} \quad \sum_{i=1}^{n} s_i a_i = g,$$

pak říkáme, že $\mathcal{A}$ je *součtově a rozdílově pokrývací množina* (sum and difference covering set, SDCS) s parametry (n, r, G).

Pro každé $g \in G$ definujeme *SDCS váhu* prvku g

$$w_{\mathcal{A}}(g) := \min \left\{ \sum_{i=1}^{n} |s_i| \;\middle|\; s_1, \ldots, s_n \in \{-1, 0, 1\}, \; \sum_{i=1}^{n} s_i a_i = g \right\}.$$

Příklad

- Motivační příklad můžeme popsat jako SDCS $\{1, 2\}$ s parametry $(2, 1, \mathbb{Z}_4)$.
- SDCS zobecňují maticové vkládání ternárními kódy:
  - Z každého $[n, k]_3$ kódu s pokrývacím poloměrem r_c lze sestrojit SDCS s parametry $(n, r_c, \mathbb{F}_3^{n-k})$.
  - Za $\mathcal{A}$ stačí zvolit sloupce paritní matice kódu.

Definice

Nechť:

- $\mathcal{A} = (a_1, \ldots, a_n)$ je SDCS,
- $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ je blok stegoobjektu.

Definujeme *SDCS extrakci* z bloku $(y_1, \ldots, y_n)$ jako

$$\mathrm{Ext}_{\mathcal{A}}(y_1, \ldots, y_n) := \sum_{i=1}^{n} y_i a_i.$$

Algoritmus (SDCS vkládání)

vstup: SDCS $\mathcal{A} = (a_1, \ldots, a_n) \in G^n$,
blok nosiče $(x_1, \ldots, x_n) \in \mathbb{Z}^n$,
zpráva $z \in G$

výstup: blok $(y_1, \ldots, y_n) \in \mathbb{Z}^n$ takový, že $\mathrm{Ext}_{\mathcal{A}}(y_1, \ldots, y_n) = z$

1. $g := z - \sum_{i=1}^{n} x_i a_i$
2. najdi $s_1, \ldots, s_n$ takové, že
   $g = \sum_{i=1}^{n} s_i a_i$ a zároveň $\sum_{i=1}^{n} |s_i| = w_{\mathcal{A}}(g)$
3. **return** $(x_1 + s_1, \ldots, x_n + s_n)$

Důkaz.

$\mathrm{Ext}_{\mathcal{A}}(y_1, \ldots, y_n) = \sum_{i=1}^{n} (x_i + s_i) a_i = g + \sum_{i=1}^{n} x_i a_i = z.$ □

Omezený obor hodnot

- **Problém**

  Mají-li prvky stegoobjektu omezený obor hodnot $\mathcal{X} \subseteq \mathbb{Z}$, může se stát, že

  $$y_i = x_i - 1 \notin \mathcal{X} \quad \text{nebo} \quad y_i = x_i + 1 \notin \mathcal{X}.$$

- **Řešení**

  1. případ: Zvolíme $y_i = x_i + 2$.
  2. případ: Zvolíme $y_i = x_i - 2$.

- Tyto speciální případy z následujících úvah vynecháváme.

Relativní kapacita a efektivita

- Relativní kapacita $\alpha = (\log_2|G|)/n$.
- Z algoritmu vidíme, že

$$w_{\mathcal{A}}(z - \sum_{i=1}^{n} x_i a_i) = \text{počet změn v bloku},$$

$$r = \text{horní mez na počet změn v bloku}.$$

- Střední hodnota distorze je

$$\frac{1}{|G|} \sum_{g \in G} w_{\mathcal{A}}(g),$$

jsou-li zprávy voleny z G náhodně s rovnoměrným rozdělením.

- Efektivita

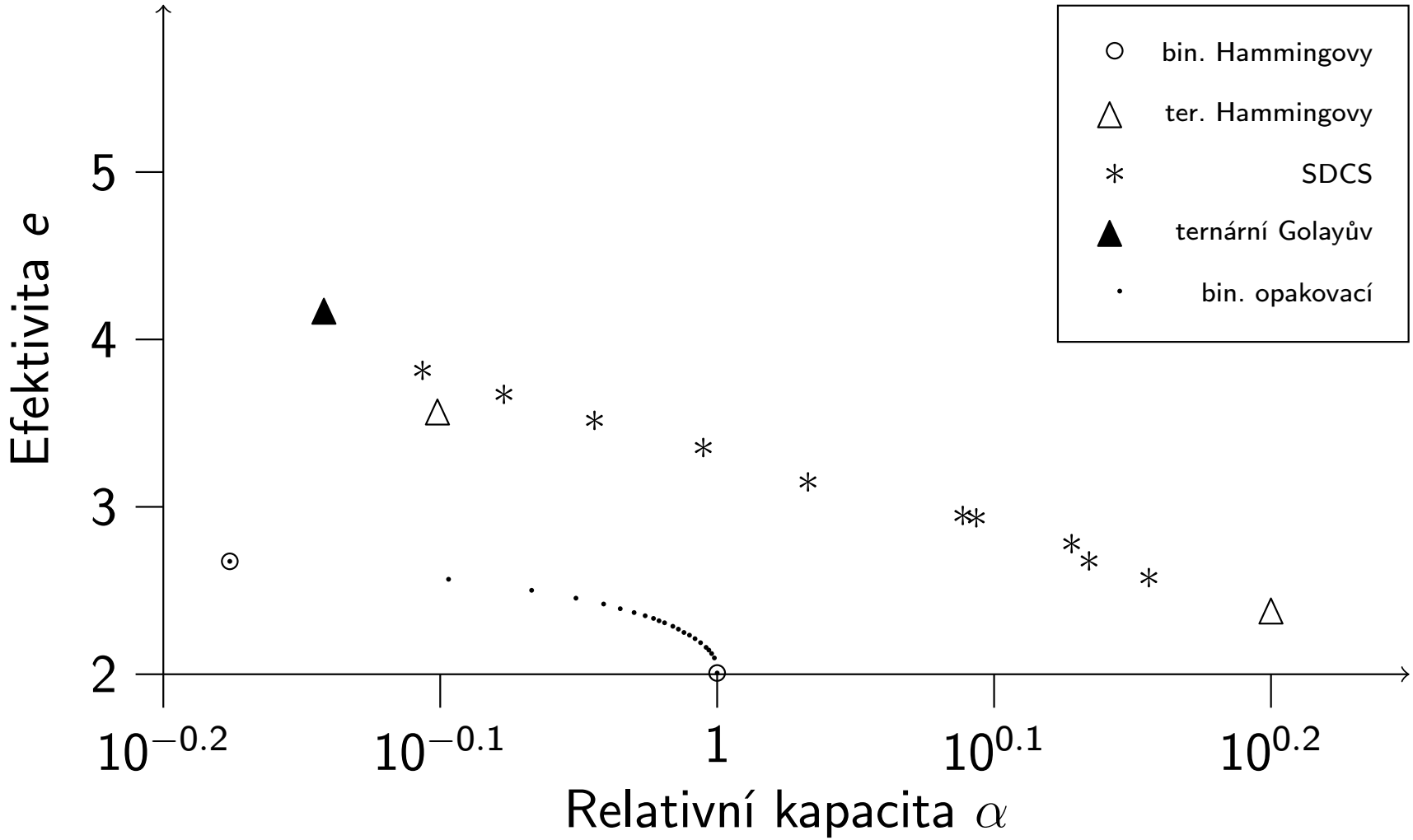
$$e = \frac{\log_2|G|}{\sum_{g \in G} w_{\mathcal{A}}(g)/|G|} = \frac{|G|\alpha n}{\sum_{g \in G} w_{\mathcal{A}}(g)}.$$

Příklady různých SDCS

(n, r, G)	α	e	$\mathcal{A}$
$(4, 3, \mathbb{Z}_{53})$	1,4320	2,5727	$\{1, 2, 6, 18\}$
$(3, 2, \mathbb{Z}_{17})$	1,3625	2,6726	$\{1, 2, 6\}$
$(5, 3, \mathbb{Z}_{105})$	1,3428	2,7756	$\{1, 3, 14, 36, 42\}$
$(6, 3, \mathbb{Z}_{174})$	1,2405	2,9300	$\{1, 3, 9, 21, 51, 86\}$
$(4, 2, \mathbb{Z}_{30})$	1,2267	2,9441	$\{1, 3, 9, 14\}$
$(5, 2, \mathbb{Z}_{42})$	1,0785	3,1445	$\{1, 2, 7, 14, 18\}$
$(6, 2, \mathbb{Z}_{61})$	0,9885	3,3498	$\{1, 2, 5, 11, 19, 27\}$
$(7, 2, \mathbb{Z}_{80})$	0,9031	3,5122	$\{1, 22, 26, 30, 34, 36, 39\}$
$(8, 2, \mathbb{Z}_{104})$	0,8376	3,6676	$\{2, 4, 6, 13, 16, 34, 39, 40\}$
$(9, 2, \mathbb{Z}_{132})$	0,7827	3,8109	$\{2, 11, 33, 34, 44, 50, 55, 58, 62\}$

Převzato z: X. Li, T. Zeng a B. Yang, Improvement of the embedding efficiency of LSB matching by sum and difference covering set.

Srovnání SDCS z tabulky s perfektními kódy



Pozorování

- Každý prvek z G lze sestrojit sčítáním a odečítáním nejvýše r prvků z $\mathcal{A}$.
- Sčítáním a odečítáním i prvků z $\mathcal{A}$ lze sestrojit nejvýše $2^i \binom{n}{i}$ prvků z G.
- Pro každou (n, r, G)-SDCS tedy platí

$$|G| \leq \sum_{i=0}^{r} 2^i \binom{n}{i} = V_3(n, r).$$

Věta

Pro každou (n, r, G)-SDCS platí $r \geq nH_3^{-1}(\alpha/\log_2 3)$.

Důkaz.

- Pro $\frac{r}{n} \geq \frac{2}{3}$ věta platí triviálně (H_3^{-1} má obor hodnot $[0, \frac{2}{3}]$).
- Dále předpokládejme $\frac{r}{n} < \frac{2}{3}$.
- Víme, že $\log_3|G| \leq \log_3 V_3(n, r) \leq nH_3(\frac{r}{n})$.
- H_3 je na $[0, \frac{2}{3}]$ rostoucí, proto

$$H_3^{-1}\left(\frac{\log_3|G|}{n}\right) \leq \frac{r}{n}.$$

- Zbývá dosadit

$$\log_3|G| = \frac{\log_2|G|}{\log_2 3} = \frac{n\alpha}{\log_2 3}.$$

□