Dvouúrovňové ± 1 vkládání

Jednoduché ± 1 vkládání zprávy $\mathbf{z} \in \{0,1\}^m$ do nosiče $\mathbf{x} \in \mathbb{Z}^n$:

- Jestliže $\mathrm{LSB}(x_i) = z_i$, pak $y_i := x_i$.
- Jestliže $\mathrm{LSB}(x_i) \neq z_i$, pak $y_i := x_i + a$, kde $a \in_{\mathcal{R}} \{-1, 1\}$.
- Obrana proti kvantitativním útokům na LSB embedding.

Rozhodnutí přičíst anebo odečíst 1 nám dává plnou kontrolu nad hodnotou druhého nejnižšího bitu:

	Poslední dvě cifry binárního rozvoje			
x_i	$(\ldots 00)_2$	$(\ldots 01)_2$	$(\ldots 10)_2$	$(\ldots 11)_2$
$x_i + 1$	$(\ldots 01)_2$	$(\ldots 10)_2$	$(\ldots 11)_2$	$(\ldots 00)_2$
$x_i - 1$	$(\ldots 11)_2$	$(\ldots 00)_2$	$(\ldots 01)_2$	$(\ldots 10)_2$

Dvouúrovňové ± 1 vkládání

Značení:

- $\mathbf{H}$ je paritní matice $[n, n - m_1]_2$ kódu $\mathcal{C}$ s průměrnou vzdáleností r_a, relativní kapacitou α a efektivitou e.
- $\mathcal{B}$ je kódová kniha, která umožňuje vkládat m_2 bitů do nosiče délky n bitů, z nichž r_a je suchých.
- $\mathbf{x}'$ a $\mathbf{y}'$ vektor nejnižších bitů nosiče a stegoobjektu.
- $\mathbf{x}''$ a $\mathbf{y}''$ vektor druhých nejnižších bitů nosiče a stegoobjektu.
- Zpráva má dvě části $\mathbf{z}' \in \mathbb{F}_2^{m_1}$ a $\mathbf{z}'' \in \mathbb{F}_2^{m_2}$.

Extrakce:

$$\mathbf{z}' = \mathrm{Ext}_{\mathbf{H}}(\mathbf{y}') \quad \text{a} \quad \mathbf{z}'' = \mathrm{Ext}_{\mathcal{B}}(\mathbf{y}'').$$

Dvouúrovňové ± 1 vkládání

Vkládání:

- První zpráva bude vložena maticovým vkládáním

$$\mathbf{y}' = \mathrm{Emb}_{\mathbf{H}}(\mathbf{x}', \mathbf{z}').$$

- Na pozicích, kde dochází ke změnám, jsme schopni ovlivnit druhý nejnižší bit. Tyto označíme jako suché

$$\mathcal{S} = \{\, i \mid x'_i \neq y'_i \,\}; \quad \mathrm{E}[|\mathcal{S}|] = r_{\mathrm{a}}.$$

- Druhá zpráva bude vložena metodou psaní na mokrý papír

$$\mathbf{y}'' = \mathrm{Emb}_{\mathcal{B}}(\mathbf{x}'', \mathcal{S}, \mathbf{z}'').$$

- Stegoobjekt $\mathbf{y}$ se vytvoří z nosiče $\mathbf{x}$ změnami $+1$ nebo -1 tak, aby $\mathbf{y}'$ byly nejnižší bity a $\mathbf{y}''$ druhé nejnižší bity stegoobjektu.

Dvouúrovňové ± 1 vkládání

Relativní kapacita a efektivita:

- Efektivita kódu $\mathcal{C}$ je $e = m_1/r_\mathrm{a}$, čili $r_\mathrm{a} = m_1/e$.
- Podle věty o mokrém nosiči je $m_2 \approx |\mathcal{S}|$ a víme, že $|\mathcal{S}| \approx r_\mathrm{a}$.
- Relativní kapacita a efektivita dvouúrovňového ± 1 vkládání je tedy

$$\alpha_{\pm 1} = \frac{m_1 + m_2}{n} \approx \frac{m_1 + m_1/e}{n} = \alpha + \frac{\alpha}{e},$$
$$e_{\pm 1} = \frac{m_1 + m_2}{r_\mathrm{a}} \approx \frac{m_1 + m_1/e}{m_1/e} = e + 1.$$

- Zároveň si můžeme všimnout, že

$$\frac{\alpha}{e} = \frac{\frac{m_1}{n}}{\frac{m_1}{r_\mathrm{a}}} = \frac{r_\mathrm{a}}{n} = \frac{\frac{m_1+m_2}{n}}{\frac{m_1+m_2}{r_\mathrm{a}}} = \frac{\alpha_{\pm 1}}{e_{\pm 1}}.$$

Dvouúrovňové ± 1 vkládání

Tvrzení

Nechť $\mathcal{C}$ je binární kód, jehož efektivita dosahuje horní meze na spodní efektivitu binárních kódů. Potom dvouúrovňovým ± 1 vkládání s kódem $\mathcal{C}$ lze dosáhnout efektivity libovolně blízké horní mezi na spodní efektivitu ternárních kódů, za předpokladu, že kód $\mathcal{C}$ je dostatečně dlouhý.

Dvouúrovňové ± 1 vkládání

Důkaz.

- Připomeňme, že

$$H_q(x) := -x \log_q x - (1-x) \log_q (1-x) + x \log_q (q-1).$$

- Dle předpokladu je $e = \alpha / H_2^{-1}(\alpha)$, čili $\alpha = H_2(\alpha/e)$.
- Dosadíme a upravíme

$$\begin{aligned} \alpha_{\pm 1} \approx \alpha + \frac{\alpha}{e} &= H_2\left(\frac{\alpha}{e}\right) + \frac{\alpha}{e} \\ &= (\log_2 3) H_3\left(\frac{\alpha}{e}\right) = (\log_2 3) H_3\left(\frac{\alpha_{\pm 1}}{e_{\pm 1}}\right). \end{aligned}$$

- Vyjádříme

$$e_{\pm 1} \approx \frac{\alpha_{\pm 1}}{H_3^{-1}(\alpha_{\pm 1} / \log_2 3)}.$$

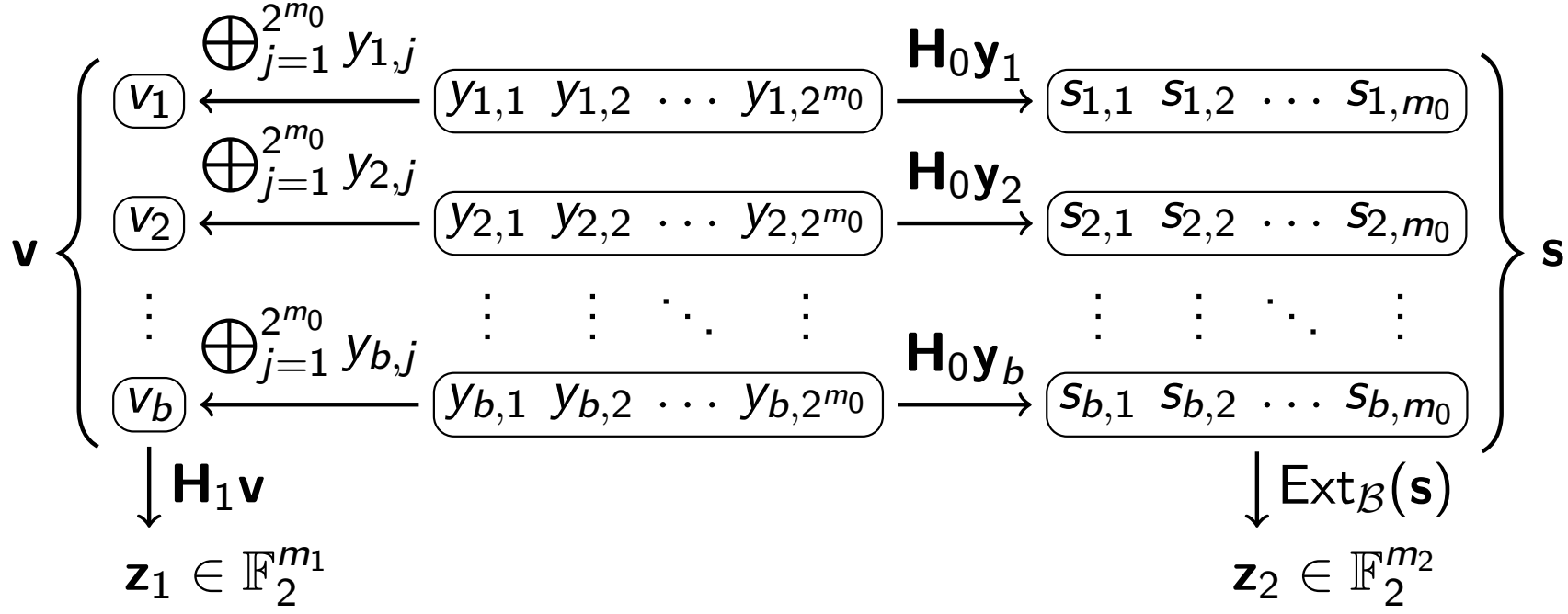
□

Stegosystém ZZW

Značení:

- $\mathbf{H}_0$ vzniká přidáním nulového sloupce k paritní matici Hammingova kódu délky $2^{m_0} - 1$.
- $\mathbf{H}_1$ je paritní matice nějakého $[b, b - m_1]_2$ kódu $\mathcal{C}$ s průměrnou vzdáleností od kódu r_{a}.
- $\mathcal{B}$ je kódová kniha, která umožňuje vkládat m_2 bitů do nosiče délky bm_0 bitů, z nichž $r_{\mathrm{a}} m_0$ je suchých.

Extrakce:



Stegosystém ZZW

Zakódování první části zprávy:

- Nosič je rozdělen na b bloků velikosti 2^{m_0}.
- Pro každý blok spočteme $u_i = \bigoplus_{j=1}^{2^{m_0}} x_{i,j}$.
- Zakódujeme první část zprávy $\mathbf{v} = \mathrm{Emb}_{\mathbf{H}_1}(\mathbf{u}, \mathbf{z}_1)$.
- Jestliže $u_i = v_i$, pak $\mathbf{y}_i = \mathbf{x}_i$.
- Jestliže $u_i \neq v_i$, pak $\mathbf{y}_i$ získáme tak, že v $\mathbf{x}_i$ provedeme právě jednu změnu. (Volba její pozice v bloku dává prostor k zakódování další zprávy.)
- Očekávaný počet změn je tedy r_{a}.

Stegosystém ZZW

Zakódování druhé části zprávy:

- Syndrom $\mathbf{H}_0\mathbf{x}_i$ lze upravit na libovolnou hodnotu provedením *právě jedné* změny v $\mathbf{x}_i$.
- Pro každý blok spočteme $\mathbf{r}_i = \mathbf{H}_0\mathbf{x}_i$.
- Když $u_i = v_i$, označíme složky vektoru $\mathbf{r}_i$ jako mokré, v opačném případě jako suché.
- Všechna $\mathbf{r}_1, \ldots, \mathbf{r}_b$ sřetězíme do jediného vektoru $\mathbf{r}$.
- Vektor $\mathbf{r}$ je mokrý nosič s očekávaným počtem suchých prvků $r_{\mathrm{a}} m_0$.
- Podle věty o mokrém nosiči lze do $\mathbf{r}$ vložit $m_2 \approx r_{\mathrm{a}} m_0$ bitů informace.

Stegosystém ZZW

Parametry stegosystému:

- Délka nosiče $= b2^{m_0}$.
- Celkový počet bitů zprávy $= m_1 + m_2 \approx m_1 + r_{\mathrm{a}} m_0$.
- Očekávaný počet změn $= r_{\mathrm{a}}$.
- Relativní kapacita a efektivita:

$$\alpha \approx \frac{m_1 + r_{\mathrm{a}} m_0}{b2^{m_0}} \quad \text{a} \quad e \approx \frac{m_1 + r_{\mathrm{a}} m_0}{r_{\mathrm{a}}}.$$

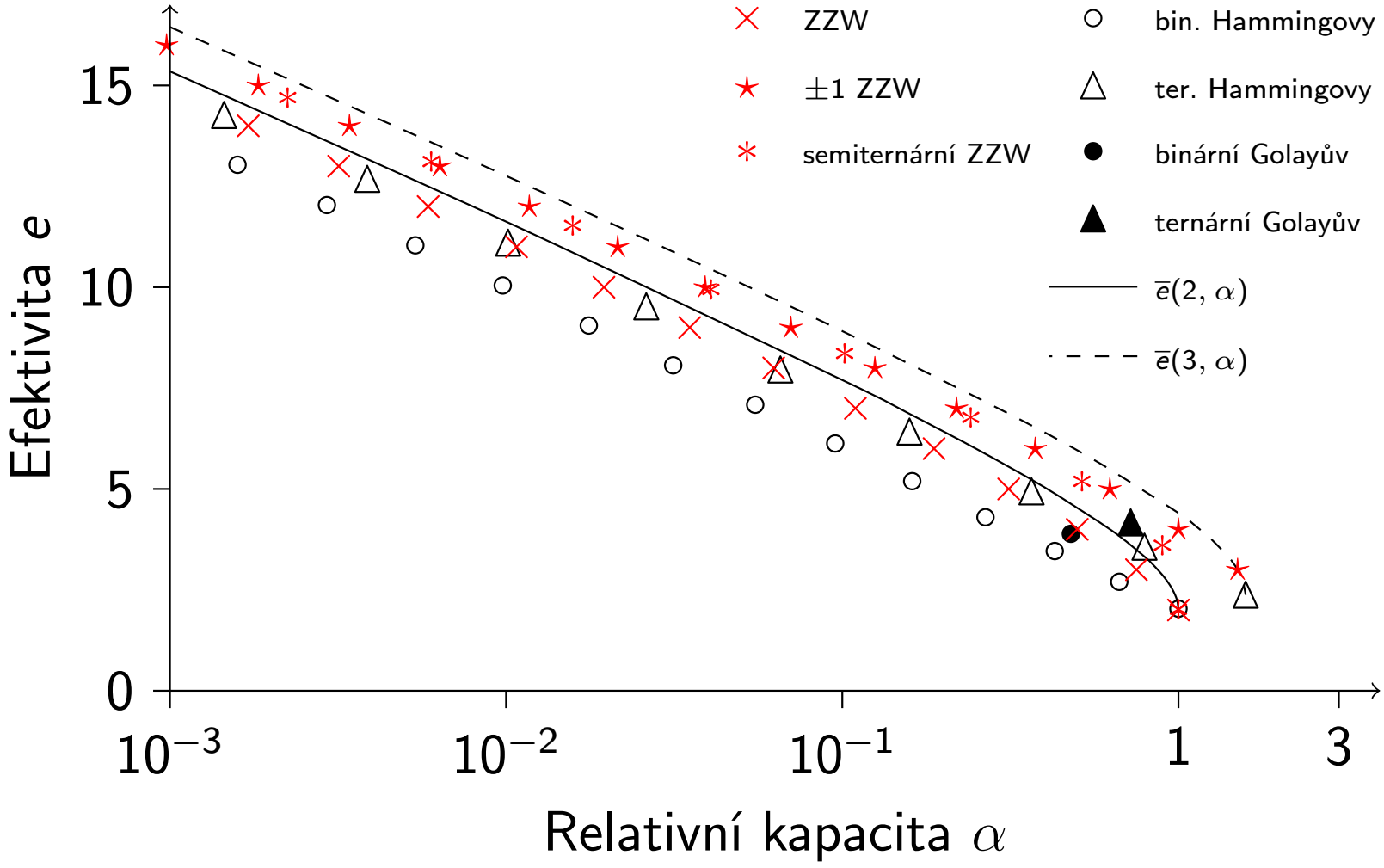
Stegosystém ZZW

Zobecnění a vylepšení:

- Bloky nemusejí mít všechny stejnou délku 2^{m_0}.
- Zpráva $\mathbf{z}_1$ se nemusí kódovat do $\mathbf{u}$ najednou. Lze postupovat po blocích.
- Můžeme použít dvouúrovňové ± 1 vkládání.
- Místo binárních Hammingových kódů lze použít ternární. (Kód $\mathcal{C}$ však zůstává binární.)

Dokonce i pro triviální kód $\mathcal{C}$ (tj. $\mathbf{z}_1 = \mathbf{v}$) dosahuje stegosystém ZZW výborných výsledků.

Triviální ZZW vs. perfektní kódy



Odstup od obou mezí je $< 0{,}6$.

Psaní na mokrý papír pomocí matic

Značení:

- $\mathbf{x}$, $\mathbf{y} \in \mathbb{F}_q^n$ posloupnost hodnot spjatých s blokem nosiče a s blokem stegoobjektu.
- $\mathbf{z} \in \mathbb{F}_q^m$ zpráva vkládaná do daného bloku.
- $\mathbf{H}$ paritní matice typu $m \times n$ nad $\mathbb{F}_q$.
- $\mathcal{S}$ množina indexů suchých složek a jejich počet $s := |\mathcal{S}|$.
- $\mathcal{M} = \{1, \ldots, n\} \setminus \mathcal{S}$ množina indexů mokrých složek.
- $\mathbf{u}_\mathcal{S} \in \mathbb{F}_q^s$ vektor, který vznikne zúžením vektoru $\mathbf{u}$ na složky indexované množinou $\mathcal{S}$.
- $\mathbf{H}_\mathcal{S}$ matice, která vznikne zúžením matice $\mathbf{H}$ na sloupce indexované množinou $\mathcal{S}$.

Psaní na mokrý papír pomocí matic

Maticová extrakce:

$$\mathbf{z} = \mathbf{H}\mathbf{y}.$$

Maticové vkládání do mokrého nosiče:

vstup: nosič $\mathbf{x} \in \mathbb{F}_q^n$, zpráva $\mathbf{z} \in \mathbb{F}_q^m$, matice $\mathbf{H}$, množina $\mathcal{M}$
výstup: stegoobjekt $\mathbf{y} \in \mathbb{F}_q^n$ takový, že $\mathbf{H}\mathbf{y} = \mathbf{z}$ a $\mathbf{y}_\mathcal{M} = \mathbf{x}_\mathcal{M}$

1 $\mathbf{y}_\mathcal{M} := \mathbf{x}_\mathcal{M}$
2 $\mathbf{b} := \mathbf{z} - \mathbf{H}_\mathcal{M}\,\mathbf{x}_\mathcal{M}$
3 **if** $(\,\mathbf{H}_\mathcal{S} \mid \mathbf{b}\,)$ má řešení **then**
4 za $\mathbf{y}_\mathcal{S}$ zvol libovolné řešení soustavy $(\,\mathbf{H}_\mathcal{S} \mid \mathbf{b}\,)$
5 **return** $\mathbf{y}$
6 **else**
7 **return** fail

Důkaz.

$\mathbf{H}\mathbf{y} = \mathbf{H}_\mathcal{S}\,\mathbf{y}_\mathcal{S} + \mathbf{H}_\mathcal{M}\,\mathbf{y}_\mathcal{M} = \mathbf{b} + \mathbf{H}_\mathcal{M}\,\mathbf{x}_\mathcal{M} = \mathbf{z}.$ □

Jak vybrat matici $\mathbf{H}$?

Chceme,

1. aby soustava $(\,\mathbf{H}_{\mathcal{S}} \mid \mathbf{b}\,)$ měla řešení,
2. aby řešení bylo možné efektivně spočítat.

Ad 1:

- $(\,\mathbf{H}_{\mathcal{S}} \mid \mathbf{b}\,)$ má řešení pro každou pravou stranu, právě když $\operatorname{rank}(\mathbf{H}_{\mathcal{S}}) = m$.
- Nutnou podmínkou je tedy $|\mathcal{S}| \geq m$.
- Ideálně chceme, aby $\operatorname{rank}(\mathbf{H}_{\mathcal{S}}) = m$ kdykoliv $|\mathcal{S}| \geq m$.
- Jinými slovy, aby každých m sloupců matice $\mathbf{H}$ tvořilo lineárně nezávislou množinu.
- To jsou právě MDS kódy!

Problém s MDS maticemi

Vlastnosti MDS kódů:

- Pro $q = 2$ existují jen triviální MDS kódy s parametry $[n, 1]_2$, $[n, n]_2$ nebo $[n, n-1]_2$.
- Z netriviálních známe např. zobecněné RS kódy, ale pro ně $n \leq q - 1$.
- Obecně se domníváme, že každý netriviální MDS kód má $n \leq q + 2$.

Naše požadavky:

- Velikost tělesa chceme malou.
- Délku bloku chceme velkou.

Generovat **H** náhodně?

Matici **H** typu $\mu n \times n$ sestrojíme náhodně.

- Pak pravděpodobnost, že libovolná podmatice $\mathbf{H}_S$ typu $\mu n \times \sigma n$ má lineárně nezávislé řádky, se s rostoucím n blíží jedné, za předpokladu, že $\mu < \sigma$.

Půjde $(\, \mathbf{H}_S \mid \mathbf{b} \,)$ efektivně řešit?

- Obecně Gaussovou eliminací v čase $O(n^3)$.
- Když bude $\mathbf{H}_S$ řídká, tak možná permutacemi v čase $O(n)$.

Příklad (řešení soustavy permutacemi)

Mějme matici

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

zprávu $\mathbf{z} = (1, 0, 1)^{\mathrm{T}}$, $\mathcal{S} = \{3, 4, 5, 7\}$, $\mathcal{M} = \{1, 2, 6\}$ a

blok nosiče: $\begin{matrix} 13 & 12 & 16 & 17 & 16 & 15 & 14 \end{matrix}$

$$\mathbf{x} = (\ 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0\ )^{\mathrm{T}} \in \mathbb{F}_2^7.$$

Tedy

$$\mathbf{H}_{\mathcal{S}} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad \mathbf{H}_{\mathcal{M}} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Příklad (řešení soustavy permutacemi)

Spočteme $\mathbf{b} = \mathbf{z} - \mathbf{H}_{\mathcal{M}}\,\mathbf{x}_{\mathcal{M}} = (0,1,0)^{\mathrm{T}}$.
Najdeme řešení $\mathbf{y}_{\mathcal{S}}$ soustavy

$$(\,\mathbf{H}_{\mathcal{S}} \mid \mathbf{b}\,) = \begin{array}{c} \begin{matrix} y_3 & y_4 & y_5 & y_7 \end{matrix} \\ \left(\begin{array}{cccc|c} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{array}\right) \end{array} \quad \rightarrow \quad \begin{array}{c} \begin{matrix} y_4 & y_3 & y_5 & y_7 \end{matrix} \\ \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right) \end{array}$$

$$\rightarrow \quad \begin{array}{c} \begin{matrix} y_4 & y_5 & y_3 & y_7 \end{matrix} \\ \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right) \end{array} \quad \rightarrow \quad \begin{array}{c} \begin{matrix} y_4 & y_5 & y_3 & y_7 \end{matrix} \\ \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right) \end{array}$$

$$(1 \quad 1 \quad 1 \quad 0)^{\mathrm{T}}$$

Abychom minimalizovali počet změn, vezmeme $y_7 = x_7 = 0$.
Zbylé proměnné dopočítáme.
Máme tedy $\mathbf{y} = (1,0,1,1,1,1,0)^{\mathrm{T}}$.

Příklad (řešení soustavy permutacemi)

$$
\begin{array}{rccccccc}
\text{Blok nosiče:} & 13 & 12 & 16 & 17 & 16 & 15 & 14 \\
\mathbf{x} = (& 1 & 0 & 0 & 1 & 0 & 1 & 0). \\
\mathbf{y} = (& 1 & 0 & 1 & 1 & 1 & 1 & 0). \\
\text{Blok stegoobjektu:} & 13 & 12 & 17 & 17 & 17 & 15 & 14
\end{array}
$$

Kdyby $\mathcal{M} = \{1, 2, 4\}$, pak by

$$
\mathbf{H}_{\mathcal{S}} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}
$$

a soustava by nebyla řešitelná pomocí permutací, i když $\mathrm{rank}(\mathbf{H}_{\mathcal{S}}) = 3$.

Řešní soustavy permutacemi

Převod matice $\mathbf{H}_S$ do odstupňovaného tvaru:

- V k-tém kroku najdeme sloupec, který ve své spodní části obsahuje pouze jednu jedničku.
- Jedničku přemístíme na diagonálu permutacemi řádků a sloupců.

$$
\begin{array}{c} \\ \\ \\ k \\ i \\ \\ \end{array}
\begin{array}{c}
\begin{array}{ccc|cccc} 1 & \dots & k-1 & k & & j & \end{array} \\
\left(\begin{array}{ccc|cccc}
1 & * & * & * & * & * & * \\
0 & 1 & * & * & * & * & * \\
0 & 0 & 1 & * & * & * & * \\
\hline
0 & 0 & 0 & * & * & 0 & * \\
0 & 0 & 0 & * & * & 1 & * \\
0 & 0 & 0 & * & * & 0 & *
\end{array}\right)
\end{array}
\quad \rightarrow \quad
\begin{array}{c} \\ \\ \\ i \\ k \\ \\ \end{array}
\begin{array}{c}
\begin{array}{ccc|cccc} 1 & \dots & k-1 & j & & k & \end{array} \\
\left(\begin{array}{ccc|cccc}
1 & * & * & * & * & * & * \\
0 & 1 & * & * & * & * & * \\
0 & 0 & 1 & * & * & * & * \\
\hline
0 & 0 & 0 & 1 & * & * & * \\
0 & 0 & 0 & 0 & * & * & * \\
0 & 0 & 0 & 0 & * & * & *
\end{array}\right)
\end{array}
$$

Soustavu dořešíme zpětnou substitucí.

Řešení soustavy permutacemi

vstup: soustava $(\mathbf{A} \mid \mathbf{b})$, kde $\mathbf{A} \in \mathbb{F}_q^{m \times s}$, vektor $\mathbf{u} \in \mathbb{F}_q^s$
výstup: řešení soustavy, které se na alespoň $s - m$ pozicích shoduje s $\mathbf{u}$

1 $\pi := \mathrm{id} \in S_s$
2 **for** $k = 1, \ldots, m$ **do**
3 v matici $\mathbf{A}$ najdi j-tý sloupec tak, že $w(a_{k,j}, \ldots, a_{m,j}) = 1$
4 **if** j neexistuje **then**
5 **return** fail
6 buď $i \geq k$ takové, že $a_{i,j} \neq 0$
7 swap$(\mathbf{A}_{i*}, \mathbf{A}_{k*})$
8 swap(b_i, b_k)
9 swap$(\mathbf{A}_{*j}, \mathbf{A}_{*k})$
10 $\pi := \pi \circ (j, k)$
11 **for** $k = m, \ldots, 1$ **do**
12 $u_{\pi(k)} := a_{k\,k}^{-1}(b_k - \sum_{i=k+1}^{s} a_{k\,i} u_{\pi(i)})$
13 **return** $\mathbf{u}$

Definice (robustní solitonové rozdělení)

Nechť m je přirozené číslo, $\delta > 0$ a $c > 0$. Označme $R = c \cdot \ln(m/\delta)\sqrt{m}$,

$$\rho(i) = \begin{cases} \frac{1}{m} & \text{pro } i = 1, \\ \frac{1}{i(i-1)} & \text{pro } i = 2, \ldots, m, \\ 0 & \text{pro } i > m, \end{cases} \quad \text{a}$$

$$\tau(i) = \begin{cases} \frac{R}{m}\frac{1}{i} & \text{pro } i = 1, \ldots, m/R - 1, \\ \frac{R}{m}\ln(R/\delta) & \text{pro } i = m/R, \\ 0 & \text{pro } i > m/R. \end{cases}$$

Řekneme, že diskrétní náhodná veličina X má *robustní solitonové rozdělení* s parametry (m, δ, c), jestliže

$$\Pr[X = i] = \frac{\rho(i) + \tau(i)}{\sum_{j=1}^{m} \rho(j) + \tau(j)}.$$

Řešení soustavy permutacemi

Věta

Máme-li soustavu rovnic nad tělesem $\mathbb{F}_q$ s alespoň $s \approx m + c\sqrt{m}(\ln(m/\delta))^2$ sloupci takovými, že jejich Hammingovy váhy mají robustní solitonové rozdělení s parametry (m, δ, c), pak pravděpodobnost selhání algoritmu řešení soustavy permutacemi je nejvýše δ.

Máme návod na sestrojení **H**:

- Zvolíme velikost bloku n, horní mez δ na pravděpodobnost selhání a parametr $c \approx 10^{-1}$.
- Máme dáno buď σ, nebo μ. Určíme druhý z nich tak, aby

$$\sigma > \mu + c\frac{\sqrt{\mu n}}{n}\left(\ln\frac{\mu n}{\delta}\right)^2.$$

- Matici $\mathbf{H} \in \mathbb{F}_q^{\mu n \times n}$ sestroj náhodně, aby Hammingovy váhy sloupců měly robustní solitonové rozdělení $(\mu n, \delta, c)$.

Očekávaná váha sloupce matice **H**

Lemma

Očekávaná hodnota náhodné veličiny s robustním solitonovým rozdělením s parametry m a δ je $O\left(\log \frac{m}{\delta}\right)$.

Důkaz.

Především si všimněme, že

$$\sum_{i=1}^{\infty} \rho(i) = \frac{1}{m} + \sum_{i=2}^{m} \frac{1}{i(i-1)} = \frac{1}{m} + \sum_{i=2}^{m} \frac{1}{i-1} - \frac{1}{i} = 1.$$

Očekávaná váha sloupce matice **H**

Důkaz (pokračování).

Očekávaná hodnota náhodné veličiny s robustním solitonovým rozdělením je

$$\sum_{i=1}^{\infty} i \cdot \frac{\rho(i)+\tau(i)}{\sum_{j=1}^{m}\rho(j)+\tau(j)} \leq \sum_{i=1}^{\infty} i(\rho(i)+\tau(i))$$

$$= \frac{1}{m} + \sum_{i=2}^{m} \frac{1}{i-1} + \sum_{i=1}^{m/R-1} \frac{R}{m} + \ln\frac{R}{\delta}$$

$$\leq \ln(m) + 1 + 1 + \ln\frac{c\cdot\ln(m/\delta)\sqrt{m}}{\delta} = O\left(\log\frac{m}{\delta}\right)$$

V předposledním kroku jsme využili odhadu $\sum_{i=1}^{m} 1/i \leq \log(m)+1$.

□

Složitost vkládání do mokrého nosiče

Tvrzení

Jestliže Hammingovy váhy sloupců matice $\mathbf{H}$ *typu* $m \times n$ *mají robustní solitonové rozdělení s parametry* (m, δ, c)*, pak časová složitost maticového vkládání do mokrého nosiče je* $O(n \log(m/\delta))$.

Důkaz.

Matice $\mathbf{H}$ bude uložena po řádcích v řídké reprezentaci.

Chceme:

(1) spočítat $\mathbf{b} = \mathbf{z} - \mathbf{H}_{\mathcal{M}}\mathbf{x}_{\mathcal{M}}$,

(2) sestavit $\mathbf{H}_{\mathcal{S}}$,

(3) vyřešit $(\,\mathbf{H}_{\mathcal{S}} \mid \mathbf{b}\,)$.

(1) a (2) provedeme současně jedním průchodem všech (nenulových) prvků matice $\mathbf{H}$. Těch je celkem $O\left(n \log \frac{m}{\delta}\right)$.

Složitost řešení soustavy permutacemi

vstup: soustava $(\mathbf{A} \mid \mathbf{b})$, kde $\mathbf{A} \in \mathbb{F}_q^{m \times s}$, vektor $\mathbf{u} \in \mathbb{F}_q^s$

výstup: řešení soustavy, které se na alespoň $s - m$ pozicích shoduje s $\mathbf{u}$

1 $\pi := \mathrm{id} \in S_s$
2 **for** $k = 1, \ldots, m$ **do**
3 v matici $\mathbf{A}$ najdi j-tý sloupec tak, že $w(a_{k,j}, \ldots, a_{m,j}) = 1$
4 **if** j neexistuje **then**
5 **return** fail
6 buď $i \geq k$ takové, že $a_{i,j} \neq 0$
7 swap$(\mathbf{A}_{i*}, \mathbf{A}_{k*})$
8 swap(b_i, b_k)
9 swap$(\mathbf{A}_{*j}, \mathbf{A}_{*k})$
10 $\pi := \pi \circ (j, k)$
11 **for** $k = m, \ldots, 1$ **do**
12 $u_{\pi(k)} := a_{k\,k}^{-1}(b_k - \sum_{i=k+1}^{s} a_{k\,i} u_{\pi(i)})$
13 **return** $\mathbf{u}$

Složitost řešení soustavy permutacemi

Důkaz (pokračování).

- Očekávaná Hammingova váha sloupce matice $\mathbf{H}$ je $O\left(\log \frac{m}{\delta}\right)$.
- Očekávaná váha řádku matice $\mathbf{H}_S$ je $O\left(\frac{s}{m} \log \frac{m}{\delta}\right)$.

Při řešení $(\,\mathbf{H}_S \mid \mathbf{b}\,)$ provádíme m-krát následující:

(3.1) Nalezením sloupce, jehož spodní část má váhu 1, v čase $O(1)$ (povedeme záznam o vahách).

(3.2) Transpozice řádků a sloupců v čase $O(1)$ (na ukazatelích).

(3.3) Aktualizace záznamu o vahách spodních částí, v čase $O\left(\frac{s}{m} \log \frac{m}{\delta}\right)$.

(3.4) $a_{k\,k}^{-1}\left(b_k - \sum_{i=k+1}^{s} a_{k\,i} u_{\pi(i)}\right)$ v čase $O\left(\frac{s}{m} \log \frac{m}{\delta}\right)$.

Celkem v čase $O\left(s \log \frac{m}{\delta}\right) = O\left(\sigma n \log \frac{m}{\delta}\right) = O\left(n \log \frac{m}{\delta}\right)$. □