SAMOOPRAVNÉ KÓDY

Obsah

Motivace a obsah kurzu

Naším úkolem je matematicky modelovat úlohu:

> *Efektivně a bez ztrát přenést informaci prostřednictvím informačního kanálu od zdroje informace k příjemci.*

Jak jednotlivé položky úkolu chápat?
Přednáška je rozdělena podle dvojího přístupu ke konceptu **informace**; zkoumáme

- buď „strukturu", která informaci nese (kódu - textu) bez ohledu na „obsah"
  → teorie (algebraických) kódů,
- nebo „měříme obsah/ztrátu"informace chápané jako náhodná veličina
  → teorie informace (jako součást teorie pravděpodobnosti).

Date: 30. května 2021.

Konkretizace dalších položek úkolu:
informační kanál - fyzikální prostředí, u nějž nás zajímá míra jeho (ne)spolehlivosti
zdroj/příjemce - strany komunikace (2 lidé, 2 stroje, vysílač přijímač apod.)
bezztrátovost - informace zdroje a příjemce by měla být „stejná"
efektivita - snaha o maximalizaci míry informace vzhledem k velikosti struktury, která informaci "nese"

Rozvrh kurzu

(1) základní koncepty teorie kódů (vzdálenost, nosnost, linearita, dualita)
(2) algebraické konstrukce (cyklické kódy, (G)RS, BCH kódy)
(3) teorie informace (kódování zdroje, Shannonova teorie)
(4) kombinatorické a geometrické konstrukce (Golayovy kódy, RM kódy)

1. Vzdálenost a nosnost blokového kódu

Celou přednášku předpokládáme, že $\mathbb{F}_q = \mathbb{F}$ je abeceda znaků zdroje i příjemce pro $\mathbb{F}$ konečné těleso řádu $q = |\mathbb{F}|$.

T&N. Pro $n \in \mathbb{N}$ budeme vektor $\mathbf{v} \in \mathbb{F}^n$ nazývat *slovo* délky n a v souřadnicích ho budeme zapisovat řádkově $\mathbf{v} = v_1 v_2 \dots v_n$.
Množina $\mathcal{C} \subseteq \mathbb{F}^n$ se nazývá *blokový kód délky* n

Definice. Nechť $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$ a $\mathcal{C} \subseteq \mathbb{F}^n$ je neprázdná množina slov. Pak
- $d(\mathbf{u}, \mathbf{v}) = |\{i \mid u_i \neq v_i\}|$ se nazývá *(Hammingova) vzdálenost* slov $\mathbf{u}$ a $\mathbf{v}$,
- položme $d(\mathcal{C}) = \min\{d(\mathbf{u}, \mathbf{v}) \mid \mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\}$ pro $|\mathcal{C}| > 1$ a $d(\mathcal{C}) = n+1$ pro $|\mathcal{C}| = 1$, pak $d(\mathcal{C})$ nazveme *(Hammingova) vzdálenost* kódu $\mathcal{C}$,
- $w(\mathbf{u}) = d(\mathbf{u}, \mathbf{0})$ se nazývá *(Hammingova) váha* slova $\mathbf{u}$.

Poznámka 1.1. Jestliže $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$ pak
(1) $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ pro každé $\mathbf{w} \in \mathbb{F}^n$
(2) $d(\mathbf{u}, \mathbf{v}) = w(\mathbf{u} - \mathbf{v})$

Důkaz. (1) Označme $D(\mathbf{u}, \mathbf{v}) = \{i \mid u_i \neq v_i\}$, pak

$$D(\mathbf{u}, \mathbf{v}) \subseteq D(\mathbf{u}, \mathbf{w}) \cup D(\mathbf{w}, \mathbf{v})$$

proto

$$d(\mathbf{u}, \mathbf{v}) = |D(\mathbf{u}, \mathbf{v})| \leq |D(\mathbf{u}, \mathbf{w}) \cup D(\mathbf{w}, \mathbf{v})| \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v}).$$

(2) Stačí uvážit, že $u_i \neq v_i \Leftrightarrow u_i - v_i \neq 0$. □

T&N. Jestliže $\mathbf{u} \in \mathbb{F}_q^n$ a r je nezáporné celé číslo, pak

$$S(\mathbf{u}, r) := \{\mathbf{v} \in \mathbb{F}_q^n \mid d(\mathbf{u}, \mathbf{v}) \leq r\}$$

je q-ární koule o poloměru r se středem $\mathbf{u}$.
Velikost koule v prostoru $\mathbb{F}_q^n$ se značí $V_q(n, r) = |S(\mathbf{0}, r)|$.

Pozorování. Jestliže $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$ a $r \in \mathbb{N}$ pak
(1) $S(\mathbf{u}, r) = \mathbf{u} + S(\mathbf{0}, r) = \mathbf{u} - \mathbf{v} + S(\mathbf{v}, r)$,

(2) $|S(\mathbf{u},r)| = |S(\mathbf{0},r)| = |S(\mathbf{v},r)|$.

T&N. Je-li r je nezáporné celé číslo, pak o kódu $\mathcal{C} \subseteq \mathbb{F}_q^n$ řekneme, že
- *rozpozná* r chyb, pokud $S(\mathbf{u},r) \cap \mathcal{C} = \{\mathbf{u}\}$ pro každé $\mathbf{u} \in \mathcal{C}$,
- *opraví* r chyb, pokud $S(\mathbf{u},r) \cap S(\mathbf{v},r) = \emptyset$ pro každé $\mathbf{u},\mathbf{v} \in \mathcal{C}$, $\mathbf{u} \neq \mathbf{v}$.

Poznámka 1.2. Je-li $\mathcal{C} \subseteq \mathbb{F}^n$ je aspoň dvouprvkový kód a $r \in \mathbb{N}$ pak

(1) $\mathcal{C}$ rozpozná r chyb $\Leftrightarrow d(\mathcal{C}) > r$,
(2) $\mathcal{C}$ opraví r chyb $\Leftrightarrow d(\mathcal{C}) > 2r$,

Důkaz. (1) $d(\mathcal{C}) > r \Leftrightarrow \forall \mathbf{u} \neq \mathbf{v} \in \mathcal{C}$ platí, že $d(\mathbf{u},\mathbf{v}) > r \Leftrightarrow \forall \mathbf{u} \in \mathcal{C} : S(\mathbf{u},r) \cap \mathcal{C} = \{\mathbf{u}\}$.
(2) Dokážeme nepřímo.
($\Rightarrow$) Nechť $d \leq 2r$. Pak $\exists \mathbf{u} \neq \mathbf{v} \in \mathcal{C}$ splňující $d(\mathbf{u},\mathbf{v}) \leq 2r \Rightarrow$ pro $D := \{i \mid u_i \neq v_i\}$ dostáváme $|D| \leq 2r \Rightarrow \exists B \subset D$, pro něž $|B| \leq r$ a $|D \setminus B| \leq r$. Definujme slovo $\mathbf{w}$:

$$w_i = \begin{cases} u_i & \text{pro } i \in B \\ v_i & \text{pro } i \in D \setminus B \\ u_i = v_i & \text{jinde} \end{cases}$$

Pak $d(\mathbf{u},\mathbf{w}) \leq r$ a $d(\mathbf{v},\mathbf{w}) \leq r$, proto $\mathbf{w} \in S(\mathbf{u},r) \cap S(\mathbf{v},r)$.
($\Leftarrow$) Nechť $\exists \mathbf{u} \neq \mathbf{v} \in \mathcal{C}$ a $\exists \mathbf{w} \in \mathbb{F}^n$ splňující $\mathbf{w} \in S(\mathbf{u},r) \cap S(\mathbf{v},r)$. Pak

$$d(\mathbf{u},\mathbf{v}) \leq d(\mathbf{u},\mathbf{w}) + d(\mathbf{w},\mathbf{v}) \leq 2r$$

díky 1.1(1). □

Pozorování. Pokud kód $\mathcal{C}$ opraví r chyb, $\mathbf{u} \in \mathcal{C}$, $\mathbf{v} \in S(\mathbf{u},r)$, pak $S(\mathbf{v},r) \cap \mathcal{C} = \{\mathbf{u}\}$

Předchozí úvaha vede k opravovacímu algoritmu: je-li $\mathbf{v}$ přijaté slovo, zvol $\mathbf{u} \in \mathcal{C}$, pro něž $S(\mathbf{v},r) \cap \mathcal{C} = \{\mathbf{u}\}$ (oprávněnost algoritmu nám ukáže teorie informace).

Věta 1.3 (Hammingova nerovnost)**.** Nechť $\mathcal{C} \subseteq \mathbb{F}^n$ je aspoň dvouprvkový kód, který opraví r chyb. Pak $2r < d(\mathcal{C})$ a pro $k = \log_q |\mathcal{C}|$ platí, že $V_q(n,r) \leq q^{n-k}$.

Důkaz. $1.2 \Rightarrow 2r < d(\mathcal{C}) \Rightarrow \{S(\mathbf{u},r) \mid \mathbf{u} \in \mathcal{C}\}$ je disjunktní systém podmnožin $\mathbb{F}^n$

$$\Rightarrow \quad V_q(n,r)|\mathcal{C}| = \sum_{\mathbf{u}\in\mathcal{C}} |S(\mathbf{u},r)| = |\dot{\bigcup}_{\mathbf{u}\in\mathcal{C}} S(\mathbf{u},r)| \leq |\mathbb{F}^n| = q^n.$$

Tudíž $V_q(n,r) \leq \frac{q^n}{q^k} = q^{n-k}$. □

Definice. Nechť $\mathcal{C} \subseteq \mathbb{F}^n$, $k = \log_q |\mathcal{C}|$ a r je nezáporné celé číslo. Číslo $\frac{k}{n}$ se nazývá *nosnost* kódu

Kód $\mathcal{C}$ je *r-perfektní*, jestliže opraví r chyb a $V_q(n,r) = q^{n-k}$, $\mathcal{C}$ je *perfektní*, jestliže existuje r, pro něž je r-perfektní.

Pozorování. Nechť $\mathcal{C} \subseteq \mathbb{F}^n$, $k = \log_q |\mathcal{C}| > 0$ a r je kladné celé číslo.

(1) $\frac{k}{n} \in (0,1\rangle$ a $k = n \Leftrightarrow \mathcal{C} = \mathbb{F}_q^n$,
(2) $\mathcal{C}$ je r-perfektní $\Leftrightarrow \mathbb{F}_q^n = \dot{\bigcup}_{\mathbf{u}\in\mathcal{C}} S(\mathbf{u},r)$,
(3) perfektní kód je r-perfektní pro (jediné) $r = \frac{d(\mathcal{C})-1}{2}$.

Příklad 1.4. (1) $\mathbb{F}^n$ je 0-perfektní kód,
(2) $\{\mathbf{0}\} \subseteq \mathbb{F}^n$ je n-perfektní kód.

Věta 1.5 (Singletonův odhad)**.** Jestliže $\mathcal{C} \subseteq \mathbb{F}_q^n, \mathcal{C} \neq \emptyset$ a $k = \log_q |\mathcal{C}|$, pak $d(\mathcal{C}) \leq n-k+1$.

Důkaz. Nechť $A(n,d) := \max\{\log_q |\mathcal{C}| \mid \mathcal{C} \subseteq \mathbb{F}_q^n, d(\mathcal{C}) \geq d\}$. Pak pro každé $\mathcal{C} \subseteq \mathbb{F}_q^n$ splňující $d = d(\mathcal{C})$ platí, že $k \leq A(n,d)$.

Dokazujme indukcí dle $d \geq 1$ tvrzení $\forall n\ A(n,d) \leq n - d + 1$.

Protože $A(n,1) \leq A(n,d) \leq n$, vidíme, že tvrzení pro $d = 1$ platí.

Za platnosti tvrzení pro $d-1$ dokážeme tvrzení pro $d \geq 2$. Pro libovolný kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ splňující $d(\mathcal{C}) \geq d$ definujme kód

$$\overline{\mathcal{C}} := \{v_1 \dots v_{n-1} \in \mathbb{F}_q^{n-1} \mid v_1 \dots v_{n-1} v_n \in \mathcal{C}\}.$$

Pak $|\overline{\mathcal{C}}| = |\mathcal{C}|$ protože $d \geq 2$ a dále $d(\overline{\mathcal{C}}) \geq d - 1$, proto díky indukčnímu předpokladu

$$A(n,d) \leq A(n-1,d-1) \leq (n-1) - (d-1) + 1 = n - d + 1 \Rightarrow$$

$$k \leq A(n, d(\mathcal{C})) \leq n - d(\mathcal{C}) + 1 \quad \Rightarrow \quad d(\mathcal{C}) \leq n - k + 1.$$

□

Definice. Nechť $\mathcal{C} \subseteq \mathbb{F}_q^n$, $k = \log_q |\mathcal{C}|$ a $d = d(\mathcal{C})$. $\mathcal{C}$ se nazývá *MDS* (maximum distance separable), jestliže $d = n - k + 1$.

Příklad 1.6. (1) $\mathbb{F}^n$ i $\{\mathbf{0}\}$ jsou MDS i perfektní kódy.
(2) Pro $n \geq 2$ je tzv. paritní kód $\mathcal{C} = \{\mathbf{v} \in \mathbb{F}_2^n \mid \sum_i v_i = 0\}$ MDS, neboť $d(\mathcal{C}) = 2$ a $k = n - 1$, ovšem nejedná se o perfektní kód.

T&N. Řekneme, že (blokové) kódy $\mathcal{C}, \overline{\mathcal{C}} \subseteq \mathbb{F}^n$ jsou *permutačně ekvivalentní* (prostřednictvím permutace $\sigma \in S_n$), pokud $c_1 \dots c_n \in \mathcal{C} \Leftrightarrow c_{\sigma(1)} \dots c_{\sigma(n)} \in \overline{\mathcal{C}}$.

Pozorování. Nechť $\sigma, \tau \in S_n$, kódy $\mathcal{C}, \overline{\mathcal{C}} \subseteq \mathbb{F}^n$ jsou permutačně ekvivalentní prostřednictvím σ a definujme $\varphi_\sigma : \mathbb{F}^n \to \mathbb{F}^n$ předpisem $\varphi_\sigma(v) = v_{\sigma(1)} \dots v_{\sigma(n)}$. Pak

(1) $\varphi_\sigma : \mathbb{F}^n \to \mathbb{F}^n$ je izomorfismus a $\varphi_\sigma \varphi_\tau = \varphi_{\tau\sigma}$,
(2) $\overline{\mathcal{C}} = \varphi_\sigma(\mathcal{C})$ a $|\mathcal{C}| = |\overline{\mathcal{C}}|$,
(3) pro $\mathbf{u}, \mathbf{v} \in \mathbb{F}^n$ máme $d(\mathbf{u}, \mathbf{v}) = d(\varphi_\sigma(\mathbf{u}), \varphi_\sigma(\mathbf{v}))$ a proto $d(\mathcal{C}) = d(\overline{\mathcal{C}})$,
(4) permutační ekvivalence tvoří ekvivalenci na kódech obsažených v $\mathbb{F}^n$.

Algebraické kódy

2. Lineární kódy

Definice. $\mathcal{C} \subseteq \mathbb{F}^n$ se nazývá *lineární kód*, jde-li o podprostor vektorového prostoru $\mathbb{F}^n$ nad tělesem $\mathbb{F}$.

Pozorování. Pro lineární kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ je $k = \log_q |\mathcal{C}| = \dim_{\mathbb{F}_q}(\mathcal{C})$, tedy nosnost $\mathcal{C}$ je rovna $\frac{\dim(\mathcal{C})}{n}$.

T&N. Je-li $\mathcal{C} \subseteq \mathbb{F}_q^n$ lineární kód délky n nad tělesem $\mathbb{F}_q$, $k = \dim_{\mathbb{F}_q}(\mathcal{C})$ a $d = d(\mathcal{C})$, pak ho označujeme jako kód s parametry

$$[n,k],\ [n,k,d],\ [n,k]_q,\ [n,k,d]_q.$$

Pozorování. Je-li $\mathcal{C}$ lineární kód kladné dimenze, pak

$$d(\mathcal{C}) = \min\{d(\mathbf{u},\mathbf{v}) \mid \mathbf{u},\mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}\} = \min\{w(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C} \setminus \{\mathbf{0}\}\}.$$

T&N. Buď $\mathcal{C}$ $[n,k]$-kód a $\mathbf{C} = \begin{pmatrix} c_1 \\ \cdots \\ \cdots \\ c_k \end{pmatrix} \in \mathbb{F}^{k\times n}$ a $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$, pak $\mathbf{C}$ je *generující* matice kódu $\mathcal{C}$, jestliže $c_1, \ldots, c_k$ je báze $\mathbf{C}$, a a $\mathbf{H}$ *kontrolní* matice kódu $\mathcal{C}$, pokud $\mathcal{C} = \operatorname{Ker} \mathbf{H}$.

Pozorování. Nechť $\mathbf{C} \in \mathbb{F}^{k\times n}$, $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$ a $\mathcal{C}$ je $[n,k]$-kód.

(1) Buď $\mathbf{C}$ generující matice $\mathcal{C}$. Pak $\mathbf{H}$ je kontrolní matice kódu $\mathcal{C}$, právě když řádky $\mathbf{H}$ tvoří bázi řešení soustavy $\mathbf{C}\mathbf{x}^T = \mathbf{0}^T$.
(2) Buď $\mathbf{H}$ kontrolní matice $\mathcal{C}$. Pak $\mathbf{C}$ je generující matice kódu $\mathcal{C}$, právě když řádky $\mathbf{C}$ tvoří bázi řešení soustavy $\mathbf{H}\mathbf{x}^T = \mathbf{0}^T$
(3) $\mathbf{C}$ a $\mathbf{H}$ jsou generující a kontrolní matice kódu $\mathcal{C}$, právě když $\operatorname{rank} \mathbf{C} = k$, $\operatorname{rank} \mathbf{H} = n-k$, $\mathbf{C}\mathbf{H}^T = \mathbf{0}$ a $\mathcal{C} = \operatorname{Im} \mathbf{C}^T = \operatorname{Ker} \mathbf{H}$.

T&N. Generující matice lineárního kódu je ve *standardním tvaru*, má-li formu $(\mathbf{I}_k|\mathbf{A}) \in \mathbb{F}^{k\times n}$.

Poznámka 2.1. Je-li $\mathcal{C}$ lineární kód, pak existuje generující matice ve standardním tvaru nějakého kódu, který je permutačně ekvivalentní k $\mathcal{C}$.

Důkaz. Nechť $\mathbf{C}$ generující matice $[n,k]$-kódu $\mathcal{C}$. Posloupností elementárních úprav (Gaussovou-Jordanovou eliminací) najdeme podobnou, tedy rovněž generující matici $\mathbf{D} = (\mathbf{d}_1^T|\ldots|\mathbf{d}_n^T) \sim \mathbf{C}$ s bázovými sloupci $\mathbf{d}_{i_1}^T = \mathbf{e}_1^T, \ldots, \mathbf{d}_{i_k}^T = \mathbf{e}_k^T T$ tvořící kanonickou bázi prostoru $\mathbb{F}^k$. Vezmeme-li libovolnou permutaci $\sigma \in S_n$ splňující $\sigma(j) = i_j$, pak

$$\tilde{\mathbf{D}} = (\mathbf{d}_{\sigma(1)}^T|\mathbf{d}_{\sigma(2)}^T|\ldots\mathbf{d}_{\sigma(k)}^T\ldots|\mathbf{d}_{\sigma(n)}^T) = (\mathbf{I}_k|\mathbf{d}_{\sigma(k+1)}^T\ldots|\mathbf{d}_{\sigma(n)}^T)$$

$\tilde{\mathbf{D}}$ je generující matice kódu, s nímž je permutačně ekvivalentní prostřednictvím permutace σ kód $\mathcal{C}$. □

Poznámka 2.2. Je-li $(\mathbf{I}_k|\mathbf{A}) \in \mathbb{F}^{k\times n}$ generující matice $[n,k]$-kódu, pak $(-\mathbf{A}^T|\mathbf{I}_{n-k})$ je jeho kontrolní matice.

Důkaz. Zřejmě $\operatorname{rank}((-\mathbf{A}^T|\mathbf{I}_{n-k})) = n-k$ a

$$(-\mathbf{A}^T|\mathbf{I}_{n-k}) \cdot (\mathbf{I}_k|\mathbf{A})^T = \left(-\mathbf{A}^T|\mathbf{I}_{n-k}\right)\begin{pmatrix}\mathbf{I}_k \\ \mathbf{A}^T\end{pmatrix} = -\mathbf{A}^T + \mathbf{A}^T = \mathbf{0}$$

□

Věta 2.3. Je-li $\mathcal{C}$ $[n,k,d]$-kód s kontrolní maticí $\mathbf{H}$ a r je největší hodnota, pro niž je každých r sloupců $\mathbf{H}$ lineárně nezávislých, pak $d = r+1$.

Důkaz. $r = 0 \Leftrightarrow \exists i$, pro něž je i-tý sloupec $\mathbf{H}$ nulový $\Leftrightarrow \exists i$, pro něž $\mathbf{H}\mathbf{e}_i^T = \mathbf{0}^T \Leftrightarrow \exists i : \mathbf{e}_i \in \mathcal{C} \Leftrightarrow d(\mathcal{C}) = 1$.

Jestliže $r = n$, pak $\mathbf{H}$ je regulární čtvercová matice a a $d(\mathcal{C}) = d(\{\mathbf{0}\}) = n + 1$.

Nechť $r < n$ a $d(\mathcal{C}) = d$, $\Rightarrow \exists \mathbf{u} \in \mathcal{C} : w(\mathbf{u}) = d$, tj. $\mathbf{H}\mathbf{u}^T = \mathbf{0}^T \Rightarrow$ d sloupců $\mathbf{H}$ je LZ $\Rightarrow$ $r \leq d - 1$.

Nechť naopak $\exists \mathbf{v}$ $w(\mathbf{v}) = r + 1$ a $\mathbf{H}\mathbf{v}^T = \mathbf{0}^T \Rightarrow \mathbf{v} \in \mathcal{C} \Rightarrow d \leq w(\mathbf{v}) = r + 1$. □

Příklad 2.4 (Hammingův perfektní kód délky 7)**.** Definujme binární kód $\mathcal{H}$ s kontrolní maticí $\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$. Spočítáme $\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ generující matici ve standardním tvaru. Protože jsou každé dva sloupce $\mathbf{H}$ různé, jsou nad $\mathbb{F}_2$ lineárně nezávislé a například první tři sloupce $\mathbf{H}$ už jsou lineárně závislé, proto je podle Věty 2.3 $d(\mathcal{H}) = 3$ a kód podle 1.2 opraví jednu chybu. Snadno spočítáme $V_2(7, 1) = 1 + \binom{7}{1} = 8 = 2^{7-4}$, tedy se jedná o 1-perfektní kód, který zřejmě není MDS.

T&N. Bilineární forma $\cdot : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ daná vztahem $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i$ se nazývá *bodový součin*. Pro $\mathcal{C} \subseteq \mathbb{F}^n$ se $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{F}^n \mid \mathbf{v} \cdot \mathbf{d} = \mathbf{0} \forall \mathbf{d} \in \mathcal{C}\}$ nazývá *duální kód* ke kódu $\mathcal{C}$.

Pozorování. Nechť $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}^n$.

(1) bodový součin $\cdot$ je symetrická, nedegenerovaní (tj. regulární) bilineární forma,
(2) $\mathcal{C}^\perp = (\text{LO } \mathcal{C})^\perp \subseteq \mathbb{F}^n$ je lineární kód,
(3) $\mathcal{C} \subseteq \text{LO } \mathcal{C} = (\mathcal{C}^\perp)^\perp$,
(4) je-li $\mathcal{C}$ lineární, pak $\mathcal{C} = (\mathcal{C}^\perp)^\perp$,
(5) $\mathcal{C} \subseteq \mathcal{D} \Rightarrow \mathcal{D}^\perp \subseteq \mathcal{C}^\perp$.

Poznámka 2.5. Buď $\mathcal{C}$ $[n, k]$-kód, $\mathbf{C} \in \mathbb{F}^{k \times n}$ a $\mathbf{H} \in \mathbb{F}^{n-k \times n}$.

(1) $\mathcal{C}^\perp$ je $[n, n - k]$-kód,
(2) $\mathbf{C}$ je generující matice $\mathcal{C}$, $\Leftrightarrow$ $\mathbf{C}$ je kontrolní matice $\mathcal{C}^\perp$,
(3) $\mathbf{H}$ je kontrolní matice $\mathcal{C}$, $\Leftrightarrow$ $\mathbf{H}$ je generujíc matice $\mathcal{C}^\perp$.

Důkaz. Nechť $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \cdots \\ \cdots \\ \mathbf{c}_k \end{pmatrix}$ a $\mathbf{H} = \begin{pmatrix} \mathbf{h}_1 \\ \cdots \\ \cdots \\ \mathbf{h}_{n-k} \end{pmatrix}$.

(1) Nechť $\mathbf{C}$ je generující matice $\mathcal{C}$, tj. rank $\mathbf{C} = k$ a $\mathcal{C}^\perp = (\mathbf{c}_1, \ldots, \mathbf{c}_k)^\perp = \text{Ker } \mathbf{C} \Rightarrow$ $\dim \mathcal{C}^\perp = n - \text{rank } \mathbf{C} = n - k$.

(2),(3) Je-li $\mathbf{C}$ je generující matice $\mathcal{C}$, pak Ker $\mathbf{C} = \mathcal{C}^\perp \Rightarrow$ $\mathbf{C}$ je kontrolní matice $\mathcal{C}^\perp$. Proto, je-li $\mathbf{H}$ je generující matice $\mathcal{C}^\perp$, pak $\mathbf{C}$ je kontrolní matice $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Naopak, je-li $\mathbf{H}$ je kontrolní matice $\mathcal{C}$, potom $\mathcal{C} = \text{Ker } \mathbf{H} = (\mathbf{h}_1, \ldots, \mathbf{h}_{n-k})^\perp$, proto

$$\mathcal{C}^\perp = ((\mathbf{h}_1, \ldots, \mathbf{h}_{n-k})^\perp)^\perp = LO(\mathbf{h}_1, \ldots, \mathbf{h}_{n-k}),$$

tudíž $\mathbf{H}$ je generujíc matice $\mathcal{C}^\perp$. Proto, je-li $\mathbf{C}$ je kontrolní matice $\mathcal{C}^\perp$, pak je $\mathbf{C}$ je generující matice $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. □

Příklad 2.6.] Nechť $\mathbf{C} = \mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ je generující i kontrolní matice kódu $\mathcal{C}$, protože $\mathbf{H}\mathbf{C}^T = \mathbf{0}$, rank $\mathbf{C}$ = rank $\mathbf{H} = 3$. Navíc $\mathcal{C} = \mathcal{C}^\perp$.

3. MDS-kódy

Připomeňme, že $[n, k, d]$-kód je MDS, právě když $d = n - k + 1$.

Poznámka 3.1. Buď $\mathcal{C}$ $[n, k, d]$-kód s kontrolní maticí $\mathbf{H}$. Pak je ekvivalentní:

(1) $\mathcal{C}$ je MDS,
(2) každých $n - k$ sloupců $\mathbf{H}$ je lineárně nezávislých,
(3) každá čtvercová matice, která vznikne z $\mathbf{H}$ vypuštěním k sloupců je regulární.

Důkaz. (1)⇒(2) $\mathcal{C}$ je MDS znamená, že $d - 1 = n - k$, proto (2) plyne z 2.3.
(2)⇒(1) Z 1.5 plyne, že $d \leq n - k + 1$ a z 2.3 plyne, že $d \geq n - k + 1 \Rightarrow \mathcal{C}$ je MDS.
(2)⇔(3) To víme z lineární algebry. □

Pozorování. Buď $\mathcal{C}$ $[n, k]$-kód s generující maticí $\mathbf{C}$. Pak $\mathcal{C}^\perp$ je MDS ⇔ každá čtvercová matice, která vznikne z $\mathbf{C}$ vypuštěním $n - k$ sloupců je regulární.

Věta 3.2. Lineární kód $\mathcal{C}$ je MDS, právě když $\mathcal{C}^\perp$ je MDS.

Důkaz. Protože $\mathcal{C} = (\mathcal{C}^\perp)^\perp$, stačí dokázat jen implikaci (⇐). Dokažme ji nepřímo, tedy předpokládejme, že $\mathcal{C}$ je $[n, k, d]$-kód, který není MDS.

Pak $d = d(\mathcal{C}) < n - k + 1 \Rightarrow d \leq n - k \Rightarrow \exists \mathbf{v} \in \mathcal{C}$ tak, že $0 < w(\mathbf{v}) \leq n - k \Rightarrow |\{i \mid v_i = 0\}| \geq k$. Víme, že existuje báze $\mathcal{C}$ obsahující vektor $\mathbf{v}$, tedy existuje generující matice $\mathbf{C}$, jejíž první řádek tvoří slovo $\mathbf{v}$. Podle 2.5 je $\mathbf{C}$ kontrolní maticí kódu $\mathcal{C}^\perp$, jejíž k sloupců má první souřadnici nulovou. Protože jsou tyto sloupce lineárně závislé, podle 3.1 není $\mathcal{C}^\perp$ MDS. □

Důsledek 3.3. Buď $\mathbf{C}$ generující matice $[n, k]$-kódu $\mathcal{C}$. Pak $\mathcal{C}$ je MDS, právě když je každých k sloupců $\mathbf{C}$ lineárně nezávislých.

Jaký je vztah mezi existencí lineárních MDS-kódů a velikostí tělesa $\mathbb{F}$?

Pozorování. Nechť $i < j \leq n$, $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$, $b_i \neq 0 \neq b_j$, Jestliže $\frac{a_i}{b_i} = \frac{a_j}{b_j}$, pak je množina vektorů $\{\mathbf{e}_k \mid k : i \neq k \neq j\} \cup \{\mathbf{a}, \mathbf{b}\}$ lineárně závislá, neboť se jedná o řádkové vektory matice $\mathbf{I}_{\mathbf{a},\mathbf{b}}$, kterou dostaneme z jednotkové nahrazením i-tého řádku slovem $\mathbf{a}$ a j-tého řádku slovem $\mathbf{b}$ a jejíž determinant je $\det \mathbf{I}_{\mathbf{a},\mathbf{b}} = a_i b_j - a_j b_i = 0$.

Věta 3.4. Jestliže je $[n, k, d]_q$-kód MDS a $3 \leq d \leq n - 1$, pak $n - q < k < q$ a $d \leq q$.

Důkaz. Nechť $\mathcal{C}$ je $[n, k, d]_q$-kód, který je MDS, tedy $d = n - k + 1$. Pak podle 3.2 je $\mathcal{C}^\perp$ MDS $[n, n - k, d']_q$-kód, kde $d' = n - (n + k) + 1 = k + 1 = n - d + 2 \Rightarrow d = n - d' + 2$ a $d' = n - d + 2$. Dosadíme-li vyjádření d do předpokladu $3 \leq d \leq n - 1$ dostáváme

$$3 \leq n - d' + 2 \leq n - 1 \Rightarrow 1 - n \leq -d' \leq -3 \Rightarrow 3 \leq d' \leq n - 1,$$

tj. pro d i d' platí stejný předpoklad.

Díky 2.1 můžeme BÚNO předpokládat, že existuje generující matice kódu $\mathcal{C}$ ve standardním tvaru $(\mathbf{I}_k|\mathbf{A})$, kde $\mathbf{A} \in \mathbb{F}_q^{k\times n-k}$. Protože $d \geq 3$, máme $n-k = d-1 \geq 2$, tedy $\mathbf{A}$ má aspoň dva sloupce.

Uvědomme si, že všechny hodnoty $\mathbf{A}$ jsou nenulové. Kdyby $a_{ij} = 0$, pak by j-tý sloupec matice $\mathbf{A}$ byl lineární kombinací prvních k sloupců matice $(\mathbf{I}_k|\mathbf{A})$ s výjimkou i-tého, což je ve sporu s 3.3. Protože jsou podle 3.3 první dva sloupce matice $\mathbf{A}$ a každých $k-2$ sloupců jednotkové matice lineárně nezávislé, plyne z předchozího pozorování, že $\forall i \neq j$ $\frac{a_{i1}}{a_{i2}} \neq \frac{a_{j1}}{a_{j2}}$, tedy

$$k = |\{\frac{a_{i1}}{a_{i2}} \in \mathbb{F}_q^* \mid i = 1, \ldots, k\}| \leq q-1 \Rightarrow k < q$$

a duálně pro MDS kód $\mathcal{C}^\perp$ je $n-k < q$, a proto $k > n-q$. Odtud konečně plyne $d = n+1-k \leq q$. □

Příklad 3.5. Dvouprvkový kód $\{\mathbf{0}, 1\ldots1\}$ je pro $k > 1$ a $n > 2$ jediný lineární kód s parametry $[n, k, n-k+1]_2$, který opraví aspoň 1 chybu, tedy $d \geq 3$. Kdyby $d < n$, pak bychom z 3.4 plynulo, že $3 \leq d \leq q = 2$, tedy spor.

Příklad 3.6. Nechť $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q^*$ jsou po dvou různé prvky, $k < n$, položme $\alpha = (\alpha_1, \ldots, \alpha_n)$, dále $\mathbf{H}_{k,\alpha} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ . & . & \ldots & . \\ . & . & \ldots & . \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{pmatrix}$ a $\mathcal{C}_{k,\alpha} = \ker \mathbf{H}_{k,\alpha}$. Potom tvoří každých k slouců této matice regulární podmatici a proto jsou $\mathcal{C}_{k,\alpha}$ i $\mathcal{C}_{k,\alpha}^\perp$ MDS-kódy.

T&N. Je-li $(\mathbf{I}_k|\mathbf{A})$ generující (nebo kontrolní) matice MDS kódu, pak se $\mathbf{A}$ nazývá MDS matice.

Obdobným argumentem jako v důkazu 3.4 se dá dokázat, že je matice $\mathbf{A}$ MDS $\Leftrightarrow$ každá čtvercová matice, kterou z $\mathbf{A}$ dostaneme vypuštěním řádků a sloupců je regulární.

Příklad 3.7. Kód s generující maticí $\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{pmatrix}$ je nad tělesem $\mathbb{F}_5$ podle 3.3 MDS kód, tedy $\begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 4 \end{pmatrix}$ je MDS matice.

4. Samoduální a propíchnuté kódy

Nechť $n > 1$ je přirozené.

Definice. Kód $\mathcal{C}$ se nazývá *samoortogonální*, pokud $\mathcal{C} \subseteq \mathcal{C}^\perp$ a $\mathcal{C}$ je *samoduální*, pokud $\mathcal{C} = \mathcal{C}^\perp$.

Pozorování. Samoduální kód je vždy lineární.

Pozorování. Je-li $\mathbf{C}$ generující matice $[n,k]$-kódu $\mathcal{C}$, pak

(1) $\mathcal{C}$ je samoortogonální $\Leftrightarrow \mathbf{C}\mathbf{C}^T = \mathbf{0}$,
(2) $\mathcal{C}$ je samoduální $\Leftrightarrow \mathbf{C}\mathbf{C}^T = \mathbf{0}$ a $n = 2k \Leftrightarrow \mathbf{C}$ je kontrolní matice $\mathcal{C}$.

T&N. Nechť $1 \leq i_1 < \cdots < i_r \leq n$ a $I = \{i_1, \ldots, i_r\}$. Označme $\pi_I : \mathbb{F}^n \to \mathbb{F}^{n-r}$ zobrazení, kde $\pi_I(\mathbf{u})$ vznikne z $\mathbf{u}$ vynecháním všech souřadnic $i_1, \ldots, i_r$ a $\pi_i = \pi_{\{i\}}$. Zobrazení π_I se nazývá *propíchnutí* a $\pi_I(\mathcal{C})$ je pro každé $\mathcal{C} \subseteq \mathbb{F}^n$ *propíchnutý* kód v souřadnicích I.

Pozorování. Nechť $1 \leq i_1 < \cdots < i_r \leq n$ a $I = \{i_1, \ldots, i_r\}$.

(1) $\pi_I = \pi_{i_1} \ldots \pi_{i_r}$ je lineární zobrazení,
(2) propíchnutý kód lineárního kódu je lineární,
(3) je-li $\mathcal{C}$ $[n,k,d]$-kód pro $d > 1$ a $i \in \{1, \ldots, n\}$, pak $\pi_i(\mathcal{C})$ je buď $[n-1,k,d]$-kód nebo $[n-1,k,d-1]$-kód.

Příklad 4.1. Binární lineární kód $\mathcal{C}$ s generující i kontrolní maticí $\mathbf{C} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ z Příkladu 2.6 je samoduální $[6,3,2]$-kód, propíchnutý kód $\pi_i(\mathcal{C})$ má parametry $[5,3,1]$ a není ani samoortogonální (a tedy ani samoduální).

$\pi_{\{5,6\}}(\mathcal{C})$ je opět samoduální $[4,2,2]$-kód s generující maticí $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

Poznámka 4.2. Buď $\mathcal{C}$ $[n,k,n-k+1]$-kód (tedy MDS-kód), $I \subseteq \{1, \ldots, n\}$ a $r := |I| \leq n-k$. Pak $\pi_I(\mathcal{C})$ je MDS $[n-r,k,n-r-k+1]$-kód.

Důkaz. Nechť $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \ldots \\ \mathbf{c}_k \end{pmatrix}$ je generující matice kódu $\mathcal{C}$. Potom z 3.3 plyne, že každých k sloupců je lineárně nezávislých.

Protože $r = |I| \leq n-k$, máme $k \leq n-r$, proto $\begin{pmatrix} \pi_I(\mathbf{c}_1) \\ \ldots \\ \pi_I(\mathbf{c}_k) \end{pmatrix}$ je generující matice kódu $\pi_I(\mathcal{C})$, jejíchž každých k sloupců je lineárně nezávislých $\Rightarrow$ $\pi_I(\mathcal{C})$ je MDS díky 3.3 $\Rightarrow$ $\pi_I(\mathcal{C})$ je $[n-r,k,n-r-k+1]$-kód. □

T&N. Nechť $A, B \subseteq \{1, \ldots, n\}$, $i_A \in \mathbb{F}_2^n$ definujme $i_A = \begin{cases} 1 & \text{jestliže } i \in A \\ 0 & \text{jestliže } i \notin A \end{cases}$ a dále $i_A \cap i_B = i_{A \cap B}$.

Pozorování. Operace $\cap$ je na $\mathbb{F}_2^n$ právě operací násobení po složkách a

(1) $\forall \mathbf{u} \in \mathbb{F}_2^n \; \exists A \subseteq \{1, \ldots, n\}$, pro něž $\mathbf{u} = i_A$, tedy $w(\mathbf{u}) = |A|$,
(2) jestliže $A, B \subseteq \{1, \ldots, n\}$, pak $w(i_A + i_B) = |A \div B| = w(i_A) + w(i_B) - 2w(i_{A \cap B})$.

T&N. Kód $\mathcal{C}$ je *dvojnásobně sudý*, jestliže 4 dělí $w(\mathbf{u})$ $\forall \mathbf{u} \in \mathcal{C}$.

Poznámka 4.3. Nechť $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \ldots \\ \mathbf{c}_k \end{pmatrix}$ je generující matice samoortogonálního $[n,k]_2$-kódu $\mathcal{C}$, pak $\mathcal{C}$ je dvojnásobně sudý $\Leftrightarrow$ 4 dělí $w(\mathbf{c}_i)$ $\forall i \leq k$.

Důkaz. ($\Rightarrow$) Řádky matice $\mathbf{C}$ jsou kódová slova, proto je jejich váha dělitelná 4.

($\Leftarrow$) $\forall \mathbf{u} \in \mathcal{C}\ \exists!\ I \subseteq \{1, \ldots, k\}$, pro kterou $\mathbf{u} = \sum_{i \in I} \mathbf{c}_i$, označme $\delta(\mathbf{u}) = |I|$. Dokážeme tvrzení, že 4 dělí $w(\mathbf{u})$, indukcí podle $\delta = \delta(\mathbf{u})$.

Pro $\mathbf{u} \in \mathcal{C}$ splňující $\delta(\mathbf{u}) = 0$ není co dokazovat, a pokud $\delta(\mathbf{u}) = 1$, pak $\exists i : \mathbf{u} = \mathbf{c}_i$, tedy $4|w(\mathbf{u})$ podle předpokladu.

Nechť tvrzení platí pro $\delta > 0$ a $\delta(\mathbf{u}) = \delta + 1$.

Pak $\exists \mathbf{v}, \mathbf{c} \in \mathcal{C}$, pro něž $\delta(\mathbf{v}) = \delta$, $\delta(\mathbf{c}) = 1$ a $\mathbf{u} = \mathbf{v} + \mathbf{c}$.

Z předpokladu samoortogonality plyne, že $\mathbf{v} \cdot \mathbf{c} = 0$, proto je $w(\mathbf{v} \cap \mathbf{c})$ sudá. Z indukčního předpokladu víme, že $4|w(\mathbf{v})$ i $4|w(\ \mathbf{c})$, proto

$$4 \text{ dělí } w(\mathbf{v}) + w(\mathbf{c}) - 2w(\mathbf{v} \cap \mathbf{c}) = w(\mathbf{v} + \mathbf{c}) = w(\mathbf{u}),$$

kde jsme využili předchozího Pozorování(2). □

Věta 4.4. Nechť $\mathcal{C} \subseteq \mathbb{F}_2^{2k}$, kde $k = \log_2 |\mathcal{C}|$. Jestliže buď

(a) $\mathcal{C}$ je samoortogonální nebo

(b) $\mathbf{0} \in \mathcal{C}$ a $\mathbf{u} + \mathcal{C}$ je pro každé $\mathbf{u} \in \mathcal{C}$ dvojnásobně sudý,

pak je $\mathcal{C}$ samoduální a tedy lineární kód.

Důkaz. Nechť platí (a). Pak $\mathcal{C} \subseteq \mathrm{LO}(\mathcal{C}) \subseteq \mathcal{C}^\perp \subseteq (\mathrm{LO}(\mathcal{C}))^\perp \Rightarrow 2^k = |\mathcal{C}| \leq |\mathrm{LO}(\mathcal{C})| \Rightarrow \dim(\mathrm{LO}(\mathcal{C})) \geq k \Rightarrow \dim((\mathrm{LO}(\mathcal{C}))^\perp) \leq k \Rightarrow 2^k = |\mathcal{C}| \leq |\mathrm{LO}(\mathcal{C})| \leq |(\mathrm{LO}(\mathcal{C}))^\perp)| \leq 2^k$. Proto $\mathcal{C} = \mathrm{LO}(\mathcal{C}) = \mathcal{C}^\perp$.

Předpokládejme, že platí (b). Stačí nám ověřit platnost (a).

Všimněme si, že pro každé $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ máme podle předpokladů, že 4 dělí $w(\mathbf{u}) = w(\mathbf{0}+\mathbf{u})$, $w(\mathbf{v}) = w(\mathbf{0} + \mathbf{v})$ i $w(\mathbf{u} + \mathbf{v})$. Proto

$$2w(\mathbf{u} \cap \mathbf{v}) = w(\mathbf{u} + \mathbf{v}) - w(\mathbf{u}) - w(\mathbf{v}) \ \Rightarrow 2 \text{ dělí } w(\mathbf{u} \cap \mathbf{v}).$$

Odtud vidíme, že $\mathbf{u} \cdot \mathbf{v} = 0$, tedy $\mathcal{C}$ je samoortogonální. □

Příklad 4.5. Je-li $\mathbf{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$ generující matice $[8, 4]_2$-kódu $\mathcal{C}$ ve standardním tvaru, vidíme, že $\mathbf{C}\mathbf{C}^T = \mathbf{0}$, jde o samoduální kód. Protože je kód $\mathcal{C}$ podle 4.3 dvojnásobně sudý a z matice dále vidíme, že $d(\mathcal{C}) \leq 4$, proto jde právě o $[8, 4, 4]_2$-kód.

Všimněme si, že propíchnutí $\pi_8(\mathcal{C})$ je právě Hammingův 1-perfektní $[7, 4, 3]_2$-kód z 2.4 s generující maticí $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

5. Cyklické kódy

Předpokládejme, že $n > 1$ je přirozené.

Souřadnice slov délky n budeme indexovat $\mathbf{c} = c_0 c_1 \ldots c_{n-1}$, tedy čísly $0, \ldots, n-1$.

Definice. Kód $\mathcal{C} \subseteq \mathbb{F}^n$ je *cyklický*, pokud pro každé slovo $c_0c_1 \dots c_{n-2}c_{n-1} \in \mathbb{F}^n$ platí implikace $c_0c_1 \dots c_{n-2}c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1}c_0 \dots c_{n-3}c_{n-2} \in \mathcal{C}$.

Příklad 5.1. Kód $\{0123, 3012, 2301, 1230\} \subset \mathbb{F}_5^4$ je nelineární cyklický a kód LO(1111) $\subset \mathbb{F}_5^4$ je lineární cyklický.

T&N. Uvažujme zobrazení $\nu : \mathbb{F}^n \to \mathbb{F}[x]/(x^n - 1)$ dané vztahem $\nu(c_0c_1 \dots c_{n-1}) = [\sum_{i=0}^{n-1} c_i x^i]$, kde $[p]$ značí rozkladovou třídu modulo hlavní ideál $(x^n - 1)$.

Na množině $\mathbb{F}^n$ uvažujme standardní vektorové operace $+$, $-$ a definujme operaci $\cdot$ pomocí operace násobení na faktorovém okruhu $\mathbb{F}[x]/(x^n - 1)$ tak, aby

$$\nu(\mathbf{u} \cdot \mathbf{v}) = \nu(\mathbf{u}) \cdot \nu(\mathbf{v}) = [\sum_{i=0}^{n-1} u_i x^i \cdot \sum_{i=0}^{n-1} v_i x^i] = [\sum_{i=0}^{2n-2} (\sum_{r=0}^{i} u_r v_{i-r}) x^i].$$

Označme $\mathbf{1} = 10 \dots 00$.

Připomeňme, že $\mathbb{F}[x]$ je Eukleidův obor, kde umíme algoritmicky hledat NSD i nsn, proto jde obor hlavních ideálů.

Pozorování. Uvažujme výše uvedené značení. Potom

(1) $\mathbb{F}[x]_n = (\mathbb{F}^n, +, \cdot, -\mathbf{0}, \mathbf{1})$ tvoří komutativní okruh,
(2) ν je okruhový izomorfismus a zároveň izomorfismus vektorových prostorů,
(3) je-li $\mathbf{e} = \nu^{-1}([1x])$, pak $\mathbf{e} = 010 \dots 00$ a

$$\mathbf{e} \cdot c_0c_1 \dots c_{n-2}c_{n-1} = c_{n-1}c_0 \dots c_{n-3}c_{n-2},$$

(4) $\mathbb{F}[x]/(x^n - 1)$ a $\mathbb{F}[x]_n$ jsou okruhy hlavních ideálů.

T&N. Okruh $(\mathbb{F}^n, +, \cdot, -\mathbf{0}, \mathbf{1})$ z předchozího Pozorování budeme značit $\mathbb{F}[x]_n$.

Poznámka 5.2. Lineární kód $\mathcal{C} \subseteq \mathbb{F}^n$ je cyklický $\Leftrightarrow$ $\mathcal{C}$ je ideál okruhu $\mathbb{F}[x]_n$.

Důkaz. Protože ν je izomorfismus, stačí dokázat, že $\mathcal{C} \subseteq \mathbb{F}^n$ je cyklický lineární kód $\Leftrightarrow$ $\nu(\mathcal{C})$ je ideál okruhu $\mathbb{F}[x]/(x^n - 1)$.

($\Rightarrow$) Nechť $\mathcal{C}$ je cyklický lineární kód $\Rightarrow$ $\nu(\mathcal{C})$ je podprostor vektorového prostoru $\mathbb{F}[x]/(x^n - 1)$ nad tělesem $\mathbb{F}$. Protože je $\mathcal{C}$ uzavřeno na cyklické posunutí, $\nu(\mathcal{C})$ je uzavřeno na násobení třídou $[x]$ monomu x. Indukcí nahlédneme, že $\forall i \geq 1$ a $\forall [p] \in \nu(\mathcal{C})$ $[x^i] \cdot [p] = [x] \cdot [x^{i-1}] \cdot [p] \in \nu(\mathcal{C}) \Rightarrow \forall \sum_i a_i x^i \in \mathbb{F}[x]$ máme

$$[\sum_i a_i x^i] \cdot [p] = \sum_i a_i [x^i \cdot p] \in \nu(\mathcal{C}).$$

($\Leftarrow$) Je-li naopak $\nu(\mathcal{C})$ ideál okruhu $\mathbb{F}[x]/(x^n - 1)$, pak $\mathcal{C}$ je lineární kód, protože ν je izomorfismus vektorových prostorů a $\nu(\mathcal{C})$ podprostor. Podmínka cykličnosti díky Pozorování (3) plyne z uzavřenosti $\nu(\mathcal{C})$ na násobení prvkem $[x]$. □

Pozorování. V okruhu $\mathbb{F}[x]/(x^n - 1)$ platí: .

(1) $([f]) = ([\mathrm{NSD}(f, x^n - 1)])$ $\forall$ $f \in \mathbb{F}[x]$,
(2) každý ideál ideál je tvaru $([f])$ pro nějaké $f \in \mathbb{F}[x]$, které dělí $x^n - 1$.

T&N. Pro každý polynom $f \in \mathbb{F}[x]$ stupně menšího než n definujme množinu

$$\mathcal{C}(f) = \{\mathbf{u} \in \mathbb{F}^n \mid \exists g \in \mathbb{F}[x] : \deg g < n - \deg f, \nu(\mathbf{u}) = [f \cdot g]\}$$

Věta 5.3. Lineární kód $\mathcal{C} \subseteq \mathbb{F}^n$ je cyklický $\Leftrightarrow \mathcal{C} = \mathcal{C}(f)$ pro nějaké $f \in \mathbb{F}[x]$, které dělí $x^n - 1$.

Důkaz. Díky 5.2 víme, že $\mathcal{C}$ je cyklický, právě když je to ideál okruhu $\mathbb{F}[x]_n$. Protože $\nu : \mathbb{F}[x]_n \to \mathbb{F}[x]/(x^n-1)$ je izomorfismus okruhů i vektorových prostorů, a ideály druhého (které tvoří podprostor) jsou právě tvaru $([f])$ pro nějaký $f \mid x^n-1$, stačí pro každý takový polynom f ověřit, že $\nu(\mathcal{C}(f)) = ([f])$. Nechť tedy f dělí $x^n - 1$.

($\subseteq$) Z definice $\mathcal{C}(f)$ přitom platí, že $\nu(\mathcal{C}(f)) \subseteq ([f])$.

($\supseteq$) Nechť $[h] \in ([f])$ a označme $g := \frac{x^n-1}{f}$. Potom existuje $a \in \mathbb{F}[x]$, pro které

$$[h] = [a] \cdot [f] = [(af) \bmod x^n - 1] = [(a) \bmod g \cdot f] \in \nu(\mathcal{C}(f)),$$

$\Rightarrow ([f]) \subseteq \nu(\mathcal{C}(f))$. □

Poznámka 5.4. Nechť pro $g = \sum_i g_i x^i, h = \sum_i h_i x^i \in \mathbb{F}[x]$ platí, že $x^n - 1 = g \cdot h$ a označme $k = \deg h$. Pak $\deg g = n - k$, $\mathcal{C}(g)$ je $[n, k]$-kód a

(1) $\mathbf{C} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 & 0 \\ 0 & g_0 & \dots & g_{n-k-1} & g_{n-k} & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & g_{n-k} & 0 \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & g_{n-k-1} & g_{n-k} \end{pmatrix}$ je generující matice $\mathcal{C}(g)$,

(2) $\mathbf{H} = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot & \dots & \dots & \cdot & \cdot \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & h_0 & 0 \\ 0 & 0 & \dots & \cdot & \cdot & \dots & \dots & h_1 & h_0 \end{pmatrix}$ je kontrolní matice $\mathcal{C}(g)$,

kde $\mathbf{C} \in \mathbb{F}^{k \times n}$ $\mathbf{H} \in \mathbb{F}^{n-k \times n}$.

Důkaz. matice $\mathbf{C} \in \mathbb{F}^{k \times n}$ je odstupňovaná s nenulovými řádky, proto je hodnosti k. Podobně $\mathbf{H}$ je hodnosti $n - k$. Pokud $a = \sum_{i=0}^{n-k-1} a_i x^i$, pak

$$\nu^{-1}([ag]) = \nu^{-1}([a])\mathbf{C} = a_0 \dots a_{n-k-1}\mathbf{C} \Rightarrow$$

$\mathbf{C}$ je generující matice $\mathcal{C}(g)$. Zbývá nahlédnout, že $\mathbf{C}\mathbf{H}^T = \mathbf{0}$.

Nejprve spočítáme koeficienty součinu $x^n - 1 = gh = \sum_{s=0}^{n}(\sum_{r=0}^{s} g_r h_{s-r})x^s$. Odtud vidíme, že $\sum_{r=0}^{s} g_r h_{s-r} = 0 \ \forall s \in \{1, \dots, n-1\}$.

Označme $\mathbf{C}_i$ i-tý řádek matice $\mathbf{C}_i$ a $\mathbf{H}_j$ j-tý řádek matice $\mathbf{H}_j$ pro $i = 0, \dots k-1$ a $j = 0, \dots n-k-1$, pak

$$\mathbf{C}_i\mathbf{H}_j^T = \begin{pmatrix} 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 0 \\ . \\ 0 \\ h_k \\ . \\ h_0 \\ 0 \\ . \\ 0 \end{pmatrix} = \sum_{r=i}^{k+j} g_{r-i}h_{k+j-r} = 0,$$

protože $\sum_{r=i}^{k+j} g_{r-i}h_{k+j-r} = \sum_{r=0}^{s} g_r h_{s-r} = 0$ pro $s = k+j-i$, kde $0 \le i \le k-1$ a $0 \le j \le n-k-1 \Rightarrow 1 \le s \le n-1$.

Proto $\mathbf{C}\mathbf{H}^T = \mathbf{0}$, tudíž $\mathbf{C}$ je generující a $\mathbf{H}$ je kontrolní matice kódu $\mathcal{C}(g)$. □

Protože efektivně umíme najít ireducibilní rozklad polynomu $x^n - 1$ a tedy i všechny dělitele tohoto polynomu, umíme najít všechny cyklické kódy délky n nad tělesem $\mathbb{F}$.

Příklad 5.5. Ireducibilní rozklad polynomu $x^3 - 1$ v oboru $\mathbb{F}_2[x]$ je

$$x^3 - 1 = x^3 + 1 = (x+1)(x^2 + x + 1),$$

proto máme právě 4 dělitele $x^3 - 1$ a tedy existují právě 4 cyklické binární lineární kódy. Dva triviální odpovídají triviálním dělitelům $\mathcal{C}(1) = \mathbb{F}_2^3$, $\mathcal{C}(x^3+1) = \{\mathbf{0}\}$.

Potom má kód $\mathcal{C}(x+1)$ generující matici $\mathbf{C} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ a kontrolní matici $\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$, zatímco kód $\mathcal{C}(x^2+x+1)$ má generující matici $\mathbf{H}$ a kontrolní matici $\mathbf{C}$.

6. GRS kódy a jejich reziduální kódy

$\overline{\mathbb{F}}$ značí algebraický uzávěr tělesa $\mathbb{F}$.

Zobecněme konstrukci MDS kódu z Příkladu 3.6:

T&N. Nechť $\alpha_1, \dots, \alpha_n \in \mathbb{F}^*$ jsou po dvou různé prvky, položme $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{F}_q^*)^n$ a nechť $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{F}^*)^n$. Potom pro $r < n$ definujme matice

$$\mathbf{H}_\alpha^r = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ . & . & \dots & . \\ . & . & \dots & . \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \in \mathbb{F}^{r\times n}, \quad \Delta(\mathbf{v}) = \begin{pmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & 0 \\ . & . & \dots & . \\ . & . & \dots & . \\ 0 & 0 & \dots & v_n \end{pmatrix} \in \mathbb{F}^{n\times n}$$

Lineární kód $\mathcal{C} = \ker(\mathbf{H}_\alpha^r \Delta(\mathbf{v}))$ s kontrolní maticí $\mathbf{H}_\alpha^r \Delta(\mathbf{v})$ se nazývá *zobecněný Reedův-Solomonův* (GRS) kód s *lokátory* α a *multiplikátory* $\mathbf{v}$.

$\mathcal{C}$ se nazývá

- normovaný GRS kód, pokud $v_i = 1$ $\forall i$,

- GRS v užším smyslu, pokdu $\mathbf{v} = \alpha$,
- Reedův-Solomonův (RS), pokud $\exists \alpha \in \mathbb{F}^*$ řádu n a $b \in \mathbb{N}$ tak, že $\alpha_i = \alpha^{i-1}$ a $v_i = \alpha^{b(i-1)}$.

Pozorování. Uvažujme předpoklady předchozí terminologické poznámky a $k < n$.

(1) GRS kódy jsou MDS díky 3.1 a 3.6,

(2) RS kód má generující i kontrolní matice tvaru $\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ . & . & \dots & . & \\ . & . & \dots & . & \\ 1 & \alpha^{b+r} & \alpha^{2(b+r)} & \dots & \alpha^{(n-1)(b+r)} \end{pmatrix}$.

(3) Pro kód $\mathcal{C}$ s generující maticí $\mathbf{C} = \mathbf{H}_\alpha^k$ existuje kontrolní matice tvaru $\mathbf{H} = \mathbf{H}_\alpha^{n-k}\Delta(\mathbf{v})$ pro vhodné $\mathbf{v} = (v_1, \dots, v_n) \in (\mathbb{F}^*)^n$. Pro jeho nalezení stačí uvážit podmínku $\mathbf{C}\mathbf{H}^T = \mathbf{0}$, která je ekvivalentní podmínce

$$\sum_{s=1}^{n} \alpha_s^{i+j} v_s = (\alpha_1^i, \alpha_2^i, \dots, \alpha_n^i)\Delta(\mathbf{v})(\alpha_1^j, \alpha_2^j, \dots, \alpha_n^j)^T = 0$$

$\forall i = 0, \dots, k-1, j = 0, \dots, n-k-1 \Leftrightarrow \mathbf{H}_\alpha^{n-1}\mathbf{v} = \mathbf{0}$, tedy $\mathbf{v}$ řeší homogenní soustavu s maticí

$$\mathbf{H}_\alpha^{n-1} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ . & . & \dots & . \\ . & . & \dots & . \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix}.$$

Protože je každých $n-1$ sloupců této matice lineárně nezávislých, jsou všechny souřadnice nenulového řešení nenulové.

Poznámka 6.1. Nechť p je charakteristika tělesa $\mathbb{F}$ a p nedělí n. Označme $\mu(\mathbf{u}) = \sum_{i=0}^{n-1} u_i x^i \ \forall \ \mathbf{u} = u_0 \dots u_{n-1} \in \mathbb{F}^n$ (tedy $\nu(\mathbf{u}) = [\mu(\mathbf{u})]$).

(1) Je-li $\mathcal{C} \subseteq \mathbb{F}^n$ lineární cyklický kód, $M = \{\alpha \in \overline{\mathbb{F}} \mid \mu(\mathbf{u})(\alpha) = 0 \ \forall \mathbf{u} \in \mathcal{C}\}$ a $f = \prod_{\alpha \in M} x - \alpha$, pak pak $f \in \mathbb{F}[x]$, f dělí $x^n - 1$ a $\mathcal{C} = \mathcal{C}(f)$.

(2) Jestliže $\alpha_i \in \overline{\mathbb{F}}$ je kořen $x^n - 1$, m_i je minimální polynom $\alpha_i \ \forall i = 1, \dots, r$ a $\mathcal{C} = \{\mathbf{u} \in \mathbb{F}^n \mid \mu(\mathbf{u})(\alpha_i) = 0 \ \forall i \leq r\}$, pak $\mathcal{C} = \bigcap_{i=1}^r \mathcal{C}(m_i) = \mathcal{C}(\mathrm{nsn}_{i \leq r}(m_i))$ je cyklický kód.

Důkaz. (1) Podle 5.3 existuje $g | x^n - 1$, pro nějž $\mathcal{C} = \mathcal{C}(f)$. Označme $K = \{\alpha \in \overline{\mathbb{F}} \mid \alpha^n = 1\}$. Protože $\mathrm{NSD}(x^n - 1, nx^{n-1}) = 1$, jsou všechny kořeny $x^n - 1$ i g jednoduché $\Rightarrow \exists L \subseteq K$ splňující $g = lc(g) \prod_{\alpha \in L} x - \alpha$.

Nyní $\alpha \in L \Leftrightarrow g(\alpha) = 0 \Leftrightarrow \mu(\mathbf{u})(\alpha) = 0 \ \forall \mathbf{u} \in \mathcal{C}(g) \Leftrightarrow \alpha \in M$.

Proto $g = lc(g)f$ a $\mathcal{C} = \mathcal{C}(g) = \mathcal{C}(f)$.

(2) Položme $f = \mathrm{nsn}_{i \leq r}(m_i)$. Pak $\mathbf{u} \in \mathcal{C} \Rightarrow m_i | \mu(\mathbf{u}) \ \forall i \Rightarrow f | \mu(\mathbf{u}) \Rightarrow \mathbf{u} \in \mathcal{C}(f)$.

Naopak, $\mathbf{u} \in \mathcal{C}(f) \Rightarrow f | \mu(\mathbf{u}) \Rightarrow \mu(\mathbf{u})(\alpha_i) = 0 \ \forall i \Rightarrow \mathbf{u} \in \mathcal{C}$.

To znamená, že $\mathcal{C} = \bigcap_{i=1}^r \mathcal{C}(m_i) = \mathcal{C}(\mathrm{nsn}_{i \leq r}(m_i))$ je cyklický kód. □

Důsledek 6.2. RS kódy jsou cyklické

Důkaz. Buď $\mathcal{C}$ RS kód s lokátory $\alpha_i = \alpha^{i-1}$ pro prvek grupy $\alpha \in F^*$ řádu n a multiplikátory $\alpha_i = \alpha^{b(i-1)}$). Pak $\mathbf{u} \in \mathcal{C} \Leftrightarrow$

$$\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ . & . & \dots & . & \\ . & . & \dots & . & \\ 1 & \alpha^{b+n-k-1} & \alpha^{2(b+n-k-1)} & \dots & \alpha^{(n-1)(b+n-k-1)} \end{pmatrix} \cdot \begin{pmatrix} u_0 \\ u_1 \\ . \\ . \\ u_{n-1} \end{pmatrix} = \mathbf{0}$$

$\Leftrightarrow \mu(\mathbf{u})(\alpha^{b+i}) = 0 \ \forall i < n-k$. Tedy $\mathcal{C}$ je cyklický podle 6.1(2). □

Definice. Nechť $r \in \mathbb{N}$, $\mathbb{F}_q$ je podtěleso $\mathbb{F}_{q^r}$ a $\mathcal{C} \subseteq \mathbb{F}_{q^r}^n$. Pak $\mathcal{C} \cap \mathbb{F}_q^n$ se nazývá *q-ární reziduální kód* kódu $\mathcal{C}$.

Pozorování. Nechť $r \in \mathbb{N}$, $\mathbb{F}_q$ je podtěleso $\mathbb{F}_{q^r}$ a $\mathcal{C} \subseteq \mathbb{F}_{q^r}^n$ je lineární kód.

(1) $\mathbb{F}_{q^r}$ je vektorový prostor dimenze r nad tělesem $\mathbb{F}_q$.
(2) Nechť $B \subset \mathbb{F}_q^n$. Pak B je lineárně nezávislá nad $\mathbb{F}_q \Leftrightarrow B$ je lineárně nezávislá nad $\mathbb{F}_{q^r}$ (zpětná implikace je triviální a pro přímou je třeba zvolit $(\beta_i)_{i \le r}$ bázi $\mathbb{F}_{q^r}$ nad $\mathbb{F}_q$ a lineární kombinaci napsat vzhledem k $(\beta_i)_{i \le r}$).
(3) $\tilde{\mathcal{C}} = \mathcal{C} \cap \mathbb{F}_q^n$ je q-ární lineární kód a $\dim_{\mathbb{F}_q} \tilde{\mathcal{C}} \le \dim_{\mathbb{F}_{q^r}} \mathcal{C}$.
(4) Je-li $\mathcal{C}$ cyklický, pak $\mathcal{C} \cap \mathbb{F}_q^n$ je rovněž cyklický.

Příklad 6.3. Nechť $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$, kde $\alpha\beta = 1 = \alpha + \beta$. Uvažujme reziduální binární kódy kvaternárních kódů.

(1) $\mathrm{LO}(10\alpha 0, 010\beta) \cap \mathbb{F}_2^4 = \{0000\}$,
(2) $\mathrm{LO}(10\alpha 0, 01\beta 0) \cap \mathbb{F}_2^4 = \mathrm{LO}(1110)$,
(3) $\mathrm{LO}(\beta\alpha 1\beta, \alpha\beta 1\alpha) \cap \mathbb{F}_2^4 = \mathrm{LO}(1101, 1011)$.

T&N. *Alternantní* kódy jsou reziduální kódy GRS kódů a reziduální kódy RS kódů se nazývají *BCH* kódy (Bose–Chaudhuri–Hocquenghem).

Pozorování. Nechť $\alpha_i \in \overline{\mathbb{F}_{q^r}} = \overline{\mathbb{F}_q}$, $\alpha_i^n = 1$ a označme m_i minimální polynom prvku α_i nad tělesem $\mathbb{F}_q$ a $m_{i,r}$ minimální polynom prvku α_i nad tělesem $\mathbb{F}_{q^r}$. Pokud $f = \mathrm{nsn}_i(m_{i,r}) \in \mathbb{F}_{q^r}[x]$ a $g = \mathrm{nsn}_i(m_i) \in \mathbb{F}_q[x]$, pak

$$\mathcal{C}(f) = \{\mathbf{u} \in \mathbb{F}_{q^r}^n \mid \mu(\mathbf{u})(\alpha_i) = 0 \forall i\}, \ \mathcal{C}(g) = \{\mathbf{u} \in \mathbb{F}_q^n \mid \mu(\mathbf{u})(\alpha_i) = 0 \forall i\}$$

a $\mathcal{C}(g) = \mathbb{F}_q^n \cap \mathcal{C}(f)$, kde uvažujeme μ z 6.1.

Pozorování. BCH kódy jsou cyklické, neboť RS kódy jsou cyklické

Věta 6.4 (o kódech se zaručenou vzdáleností)**.** Je-li $\mathcal{C}$ $[n, l, D]_{q^r}$ kód, který je MDS, a $\tilde{\mathcal{C}} = \mathcal{C} \cap \mathbb{F}_q^n$ je $[n, k, d]_q$ kód, pak $k \ge n - r(D-1)$ a $d \ge D \ge \frac{n-k}{r} + 1$.

Důkaz. $\mathcal{C}$ je MDS $\Rightarrow D = n - l + 1 \Rightarrow n - l = D + 1$. Dokážeme-li, že $n - k \le r(n - l)$, pak odtud dostaneme obě nerovnosti $k \ge n - r(D-1)$ i $d \ge D \ge \frac{n-k}{r} + 1$. Všimněme si, že $n - k$ je právě počet řádků (libovolné) kontrolní matice kódu $\tilde{\mathcal{C}}$. Zvolme nějakou kontrolní matici $\mathbf{H} = \begin{pmatrix} \mathbf{h}_1 \\ \dots \\ \mathbf{h}_{n-k} \end{pmatrix} \in \mathbb{F}_{q^r}^{(n-l) \times n}$ kódu $\mathcal{C}$ s řádky $\mathbf{h}_i$ a označme $\beta_1, \dots, \beta_r$ nějakou bázi

$\mathbb{F}_{q^r}$ nad $\mathbb{F}_q \Leftarrow \exists \mathbf{a}_{ji} \in \mathbb{F}_q^n$ pro $i = 1, \ldots, n-l$ a $j = 1, \ldots, r$ splňující $\mathbf{h}_i = \sum_{j=1}^{r} \beta_j \mathbf{a}_{ij}$. Definujme matice

$$\mathbf{A}_i = \begin{pmatrix} \mathbf{a}_{1i} \\ \cdots \\ \cdots \\ \mathbf{a}_{ri} \end{pmatrix} \in \mathbb{F}_q^{r \times n} \quad \text{a} \quad \tilde{\mathbf{H}} = \begin{pmatrix} \mathbf{A}_1 \\ \cdots \\ \cdots \\ \mathbf{A}_{n-k} \end{pmatrix} \in \mathbb{F}_q^{(n-l)r \times n}.$$

Potom $\mathbf{u} \in \tilde{\mathcal{C}} \Leftrightarrow \mathbf{u} \in \mathcal{C}$ a $\mathbf{u} \in \mathbb{F}_q^n \Leftrightarrow \mathbf{u}\mathbf{H}^T = \mathbf{0}$ a $\mathbf{u} \in \mathbb{F}_q^n \Leftrightarrow \mathbf{u}\tilde{\mathbf{H}}^T = \mathbf{0}$ a $\mathbf{u} \in \mathbb{F}_q^n$. Proto $\tilde{\mathcal{C}} = \mathrm{Ker}\tilde{\mathbf{H}}$ a počet řádků kontrolní matice kódu $\tilde{\mathcal{C}}$ je roven $\mathrm{rank}\tilde{\mathbf{H}} \leq (n-l)r$ (což je počet řádků $\tilde{\mathbf{H}}$). Dokázali jsme, že $n - k \leq (n-l)r$. □

Důsledek 6.5. Pro BCH (alternantní) $[n, k, d]_q$ kód RS (GRS) $[n, l, D]_{q^r}$ kódu platí odhady $k \geq n - r(D-1)$ a $d \geq \frac{n-k}{r} + 1$.

Příklad 6.6. Uvažujme těleso $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ pro α splňující $\alpha^2 + 1 = 0$ a nad ním GRS $[6, 3, 4]_9$ kód s kontrolní maticí $\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & \alpha & 2\alpha & \alpha+1 & 2\alpha+2 \end{pmatrix}$. Pro reziduální kód $\tilde{\mathcal{C}} = \mathcal{C} \cap \mathbb{F}_3^6$ určíme stejně jako v důkazu 6.4 matic $\tilde{\mathbf{H}}$, pro níž platí, že $\tilde{\mathcal{C}} = \mathrm{Ker}\tilde{\mathbf{H}}$. K tomu zvolíme bázi $1, \alpha$ prostoru $\mathbb{F}_9$ nad $\mathbb{F}_3$.

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

Odtud vidíme, že alternantní kód $\tilde{\mathcal{C}}$ je $[6, 3]_3$ kód a z 6.4 dostáváme odhad jeho vzdálenosti $d \geq \frac{3}{2} + 1$, tedy $d \geq 3$. Naopak více to podle 2.3 být nemůže (součet 1., 3. a 6. sloupce kontrolní matice je nulový), tedy $\tilde{\mathcal{C}}$ je $[6, 3, 3]_3$ kód.

Shannonova teorie informace

7. Úvod do teorie informace

T&N. (Ω, P) je *diskrétní pravděpodobnostní prostor* (DPP), jestliže

(1) Ω je spočetná množina,
(2) funkce $P : \Omega \to \langle 0, 1 \rangle$ splňuje $\sum_{\omega \in \Omega} P(\omega) = 1$.

Prvky $\omega \in \Omega$ se nazývají *elementární jevy* a množiny $E \subset \Omega$ jsou *náhodné jevy*. $P[E] = \sum_{\omega \in E} P(\omega)$ je *pravděpodobnost* náhodného jevu. Pro $E_1, \ldots, E_k \subset \Omega$ značme $P[E_1, \ldots, E_k] = P[\bigcap_{i \leq k} E_i]$.

Jestliže $P[E_2] \neq 0$, pak $P[E_1|E_2] = \frac{P[E_1, E_2]}{P[E_2]}$ se nazývá *podmíněná pravděpodobnost* jevu E_1 jevem E_2.

Pozorování. Je-li (Ω, P) DPP, $E, E_1, \ldots, E_k \subset \Omega$ a $P[E_i] \neq 0 \ \forall i$, pak

(1) pokud $\Omega = \dot{\bigcup}_i E_i$, pak $P[E] = \sum_{i=1}^{k} P[E, E_i] = \sum_{i=1}^{k} P[E|E_i]P[E_i]$,
(2) $P[E_2|E_1]P[E_1] = P[E_1, E_2] = P[E_1|E_2]P[E_2]$.

V následujícím bude (Ω, P) vždy DPP a $r \in \mathbb{N}$, $r > 1$.

T&N. Nechť $A \subseteq R^i$, $i \in \mathbb{N}$, pak se zobrazení $X : \Omega \to A$ se nazývá diskrétní náhodná veličina (DNV) a pro $a \in A$ píšeme:

• $P[X = a] := P[X^{-1}(a)]$, $P[X \leq a] := P[X^{-1}(\{s \mid s \leq a\})]$ a obdodně pro další relace $(<, \geq, >, \neq)$,

• $EX := \sum_{\omega\in\Omega} P(\omega)X(\omega) = \sum_{a\in A} P[X = a]a$ je *střední hodnota* DNV X.

• $H_r(X) := -\sum_{a\in A} P[X = a] \log_r(P[X = a]) = \sum_{a\in A} P[X = a] \log_r \frac{1}{P[X=a]}$ se nazývá *r-ární entropie* veličiny X (kde členy s $P[X = a] = 0$ vynecháváme).

Je-li $|A| < \infty$, pak řeknme, že X má *rovnoměrné rozdělení*, jestliže $P[X = a] = \frac{1}{|A|}$ $\forall a \in A$.

Pozorování. Nechť $X : \Omega \to A$ je DNV.

(1) Jestliže $f : A \to B \subseteq \mathbb{R}^j$, pak

$$E(fX) = \sum_{\omega\in\Omega} P(\omega) fX(\omega) = \sum_{a\in A} \Big(\sum_{\omega\in X^{-1}(a))} P(\omega) \Big) f(a) = \sum_{a\in A} P[X = a] f(a).$$

(2) Je-li $S_r(\omega) := \log_r(P[X^{-1}(X(\omega))])$ $\forall \omega \in \Omega$, kde BÚNO předpokládáme, že všechny argumenty funkce $\log_r$ jsou nenulové, pak S_r je DNV a

$$ES_r = -\sum_{a\in A} P[X = a] \log_r(P[X = a]) = H_r(X).$$

(3) $H_r(X) \geq 0$ a $H_r(X) = 0 \Leftrightarrow \exists\, a \in A$, pro něž $P[X = a] = 1$.

Poznámka 7.1. Nechť $a_1, \ldots, a_n \in (0, 1)$, $\sum_{i=1}^n a_i = 1$.

(1) (Jensenova nerovnost) Nechť $f : I \to \mathbb{R}$ je ryze konkávní funkce na intervalu $I \subseteq \mathbb{R}$ a $x_1, \ldots, x_n \in I$. Pak $\sum_{i=1}^n a_i x_i \in I$, $\sum_{i=1}^n a_i f(x_i) \leq f(\sum_{i=1}^n a_i x_i)$ a rovnost nastává $\Leftrightarrow x_i = x_j$ $\forall i, j$.

(2) Jestliže $x_1, \ldots, x_n \in (0, 1)$ a $\sum_{i=1}^n x_i \leq 1$, pak $\sum_{i=1}^n a_i \log_r \frac{1}{a_i} \leq \sum_{i=1}^n a_i \log_r \frac{1}{x_i}$ a rovnost nastává $\Leftrightarrow x_i = a_i$ $\forall i$.

Důkaz. (1) Viz například `https://cs.wikipedia.org/wiki/Jensenova_nerovnost` .

(2) $\log_r$ je ryze konkávní na intervalu $(0, +\infty)$. Proto díky (1):

$$L = \sum_{i=1}^n a_i \log_r \frac{1}{a_i} - \sum_{i=1}^n a_i \log_r \frac{1}{x_i} = \sum_{i=1}^n a_i \log_r \frac{x_i}{a_i} \leq \log_r(\sum_{i=1}^n x_i) \leq 0,$$

protože $\sum_{i=1}^n x_i \leq 1$ a $L = 0 \Leftrightarrow \sum_{i=1}^n x_i = 1$ a $\frac{x_i}{a_i} = \frac{x_j}{a_j}$ $\forall i, j \Leftrightarrow$

$1 = \sum_{i=1}^n x_i = \sum_{i=1}^n a_i = \sum_{i=1}^n a_i \frac{x_i}{a_i} = \frac{x_j}{a_j} \sum_{i=1}^n a_i = \frac{x_j}{a_j}$ $\forall i, j \Leftrightarrow x_j = a_j$ $\forall j$. □

Poznámka 7.2. Buď $X : \Omega \to A$ DNV pro níž platí $P[X = a] \neq 0$ $\forall a \in A$, pak $H_r(X) \leq \log_r(|A|)$ a a rovnost nastává $\Leftrightarrow$ má X rovnoměrné rozdělení.

Důkaz. Máme $H_r(X) = \sum_{a\in A} P[X = a] \log_r \frac{1}{P[X=a]} \leq \log_r(\sum_{a\in A} \frac{P[X=a]}{P[X=a]}) = \log_r(|A|)$ díky 7.1(1) a rovnost nastává $\Leftrightarrow P[X = a] = P[X = b]$ $\forall a, b \in A$. □

T&N. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV, pak definujme

$X \times Y = (X, Y) : \Omega \to A \times B$ je DNV daná vztahem $(X, Y)(\omega) = (X(\omega), Y(\omega))$ a

$P[X = a, Y = b] = P[(X, Y) = (a, b)] = P[X^{-1}(a) \cap Y^{-1}(b)]$ $\forall (a, b) \in A \times B$.

Řekneme, že X a Y jsou *nezávislé* DNV, jestliže $P[X=a, Y=b] = P[X=a]\cdot P[Y=b]$ $\forall (a,b) \in A \times B$.

$H_r(X,Y) := H_r(X \times Y) = \sum_{(a,b)\in A\times B} P[X=a, Y=b] \log_r \frac{1}{P[X=a,Y=b]}$ se nazývá *sdružená entropie.*

Poznámka 7.3 (O sdružené entropii)**.** Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV, pak $H_r(X,Y) \leq H_r(X) + H_r(Y)$. Rovnost nastává $\Leftrightarrow$ X a Y jsou nezávislé.

Důkaz. $P[X=a] = \sum_{b\in B} P[X=a, Y=b] \Rightarrow$

$$H_r(X) + H_r(Y) = \sum_{a\in A}\sum_{b\in B} P[X=a,Y=b](\log_r \frac{1}{P[X=a]} + \log_r \frac{1}{P[Y=b]}) =$$

$$= \sum_{(a,b)\in A\times B} P[X=a,Y=b] \log_r \frac{1}{P[X=a]P[Y=b]}$$

$$\geq \sum_{(a,b)\in A\times B} P[X=a,Y=b] \log_r \frac{1}{P[X=a,Y=b]} = H_r(X,Y)$$

díky 7.1(2), kde $x_{a,b} = P[X=a]P[Y=b]$ a $a_{a,b} = P[X=a,Y=b]$. Navíc rovnost platí $\Leftrightarrow P[X=a]P[Y=b] = P[X=a,Y=b]$ $\forall a,b \Leftrightarrow$ X a Y jsou nezávislé. □

8. Diskrétní informační kanál

Nadále předpokládejme, že (Ω, P) je DPP a $r \in \mathbb{N}$, $r > 1$.

T&N. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV, pak definujme

- $H_r(X|Y=b) := -\sum_{a\in A} P[X=a|Y=b] \log_r(P[X=a|Y=b])$ $\forall b \in B$ a
- $H_r(X|Y) := \sum_{b\in B} P[Y=b] H_r(X|Y=b)$ se nazývá *podmíněná entropie* veličiny X veličinou Y.

Pozorování. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV. Potom $H_r(X|Y) =$
$= -\sum_{b\in B} P[Y=b] \sum_{a\in A} P[X=a|Y=b] \log_r(P[X=a|Y=b]) =$
$= -\sum_{(a,b)\in A\times B} P[X=a,Y=b] \log_r(P[X=a|Y=b])$.

Poznámka 8.1. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV, pak

(1) $H_r(X|Y) = H_r(X,Y) - H_r(Y)$,
(2) $H_r(X|Y) \leq H_r(X)$ a rovnost nastává $\Leftrightarrow$ X a Y jsou nezávislé.

Důkaz. (1) $H_r(X|Y) + H_r(Y) =$
$= -\sum_{(a,b)\in A\times B} P[X=a,Y=b](\log_r(P[X=a|Y=b]) + \log_r(P[Y=b])) =$
$= -\sum_{(a,b)\in A\times B} P[X=a,Y=b] \log_r(P[X=a|Y=b]\cdot P[Y=b]) =$
$= -\sum_{(a,b)\in A\times B} P[X=a,Y=b] \log_r(P[X=a,Y=b]) = H_r(X,Y)$.
(2) $H_r(X|Y) \leq H_r(X) \Leftrightarrow H_r(X|Y) + H_r(Y) \leq H_r(X) + H_r(Y)$.
Podle 7.3 a (1) víme, že $H_r(X|Y) + H_r(Y) = H_r(X,Y) \leq H_r(X) + H_r(Y)$, kde rovnost platí $\Leftrightarrow$ X a Y jsou nezávislé, což je ekvivalentní dokazovanému tvrzení. □

Definice. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV. Pak
- $I_r(X,Y) = H_r(X) + H_r(Y) - H_r(X,Y)$ je *r-ární vzájemná informace* X a Y.

Pozorování. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ jsou DNV, potom

(1) $I_r(X,Y) \geq 0$ a rovnost nastává $\Leftrightarrow$ X a Y jsou nezávislé,
(2) $I_r(X,Y) = I_r(Y,X)$ a $I_r(X,X) = H_r(X)$,
(3) $I_r(X,Y) = H_r(X) - H_r(X|Y) = H_r(Y) - H_r(Y|X) \leq H_r(X), H_r(Y)$.

Definice. Mějme $A = \{a_1, \ldots, a_t\}$ a $B = \{b_1, \ldots, b_s\}$ dvě konečné abecedy, $\mathbf{P} = (P_{ij}) \in \langle 0,1\rangle^{t\times s}$ stochastická matice, tj. $\sum_{j=1}^{s} P_{i,j} = 1 \ \forall i = 1, \ldots, t$. Pak trojici $\Gamma = (A, B, \mathbf{P})$ nazveme *diskrétní informační kanál* (dále jen *kanál*). Náhodné veličiny $X : \Omega \to A$ a $Y : \Omega \to B$ nazveme po řadě *vstup* a *výstup* kanálu Γ splňují-li $\forall i = 1, \ldots, t$, $j = 1, \ldots, s$ podmínku $P[Y = b_j | X = a_i] = P_{ij}$.

Náhodným veličinám, jejímiž hodnotami budou znaky nějaké abecedy kanálu, tedy speciálně jeho vstupu a výstupu, budeme nadále obvykle říkat *informační zdroje*.

Pozorování. Nechť $X : \Omega \to A$ a $Y : \Omega \to B$ představují vstup a výstup kanálu $\Gamma = (A, B, (P_{ij}))$. Označme $p_i = P[X = a_i]$, $q_j = P[Y = b_j]$, $\mathbf{p} = (p_1, \ldots, p_t)$, $\mathbf{q} = (q_1, \ldots, q_s)$ a $Q_{ij} = P[X = a_i | Y = b_j]$. Potom

(1) $\sum_{i=1}^{t} p_i = \sum_{i=1}^{s} q_i = \sum_{i=1}^{t} Q_{ik} = 1 \ \forall k = 1, \ldots s$,
(2) $\sum_{i=1}^{t} p_i P_{ij} = \sum_{i=1}^{t} P[X = a_i] P[Y = b_j | X = a_i] = P[Y = b_j] = q_j \ \forall j$, proto $\mathbf{pP} = \mathbf{q}$ (tedy Γ a X určuje Y),
(3) $P[X = a_i, Y = b_j] = P_{ij} p_i = Q_{ij} q_j$,
(4) $I_r(X,Y) = H_r(Y) - H_r(Y|X) =$

$$= \sum_{i,j} P[X = a_i, Y = b_j] \log_r \frac{P[Y = b_j | X = a_i]}{P[Y = b_j]} = \sum_{i,j} P_{ij} p_i \log_r \frac{P_{ij}}{\sum_k p_k P_{kj}},$$

(5) definujme na $K = \{\mathbf{p} \in \langle 0,1\rangle^t \mid \sum_i p_i = 1\}$ funkci $\mathcal{I}_r(\mathbf{p}) = \sum_{i,j} P_{ij} p_i \log_r \frac{P_{ij}}{\sum_k p_k P_{kj}}$, pak $\mathcal{I}_r(\mathbf{p}) = I_r(X,Y)$ a $\mathcal{I}_r$ je spojitá funkce na kompaktní množině K, a proto na ní nabývá maxima.

Definice. Je-li $K = \{\mathbf{p} \in \langle 0,1\rangle^t \mid \sum_i p_i = 1\}$ a $\mathcal{I}_r$ funkce z Pozorování (5), pak r-ární *kapacita* kanálu $\Gamma = (A, B, (P_{ij}))$ je $C_\Gamma = \max_{\mathbf{p}\in K} \mathcal{I}_r(\mathbf{p})$.

Pozorování. Je-li $\Gamma = (A, B, (P_{ij}))$ kanál, pak

(1) C_Γ je dobře definovaná a $C_\Gamma \leq \min(\log_r |A|, \log_r |B|)$,
(2) pokud $r = |A| = |B|$, pak $C_\Gamma \leq 1$,
(3) pro každý vstup a výstup X, Y kanálu Γ platí, že $I_r(X,Y) \leq C_\Gamma$,
(4) $\exists$ vstup a výstup $X_{\max}, Y_{\max}$ kanálu Γ, pro něž $I_r(X_{\max}, Y_{\max}) = C_\Gamma$.

T&N. Pokud $A = B = \mathbb{F}_2$ a $\mathbf{P} = \begin{pmatrix} P & 1-P \\ 1-P & P \end{pmatrix}$ pro $P \in (0,1)$, pak $\Gamma = (A, B, \mathbf{P}) = (\mathbb{F}_2, \mathbb{F}_2, \mathbf{P})$ říkáme *binární symetrický kanál* (BSC) se spolehlivostí P.

Poznámka 8.2. Nechť Γ je BSC se spolehlivostí P a X a Y představují jeho vstup a výstup.

(1) Pokud $P \neq \frac{1}{2}$, pak X má rovnoměrné rozdělení $\Leftrightarrow$ Y má rovnoměrné rozdělení.
(2) Pokud $P = \frac{1}{2}$, pak má Y vždy rovnoměrné rozdělení.

Důkaz. Všimněme si, že $\mathbf{P} = \begin{pmatrix} P & 1-P \\ 1-P & P \end{pmatrix}$ je regulární $\Leftrightarrow \det \mathbf{P} = 2P - 1 \neq 0 \Leftrightarrow P \neq \frac{1}{2}$.

(1) Jestliže $P \neq \frac{1}{2}$ snadno spočítáme, že $(\frac{1}{2}, \frac{1}{2})\mathbf{P} = (\frac{1}{2}, \frac{1}{2}) = (\frac{1}{2}, \frac{1}{2})\mathbf{P}^{-1}$, což znamená, že $P[X=0] = P[X=1] = \frac{1}{2} \Leftrightarrow P[Y=0] = P[Y=1] = \frac{1}{2}$.

(2) Pro $P = \frac{1}{2}$ dostáváme $(p, 1-p)\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = (\frac{1}{2}, \frac{1}{2})$ pro libovolné p. □

Příklad 8.3. Uvažujme vstup X s rozdělením $(p_0, p_1) = (P[X=0], P[X=1]) = (\frac{9}{10}, \frac{1}{10})$ BSC se spolehlivostí $\frac{4}{5}$. Určíme rozdělení odpovídajícího výstupu Y:

$$(q_0, q_1) = (P[Y=0], P[Y=1]) = (p_0, p_1)\mathbf{P} = \begin{pmatrix} \frac{9}{10}, & \frac{1}{10} \end{pmatrix} \begin{pmatrix} \frac{4}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{4}{5} \end{pmatrix} = \begin{pmatrix} \frac{37}{50}, & \frac{13}{50} \end{pmatrix}.$$

Spočítáme ještě podmíněné pravděpodobnosti $P[X=i|Y=j]$:

$$\begin{pmatrix} P[X=0|Y=0] & P[X=0|Y=1] \\ P[X=1|Y=0] & P[X=1|Y=1] \end{pmatrix} = \begin{pmatrix} \frac{p_0 P}{q_0} & \frac{p_0(1-P)}{q_1} \\ \frac{p_1(1-P)}{q_0} & \frac{p_1 P}{q_1} \end{pmatrix} = \begin{pmatrix} \frac{36}{37} & \frac{9}{13} \\ \frac{1}{37} & \frac{4}{13} \end{pmatrix},$$

Všimněme si, že ať zde předpokládáme hodnotu výstupu Y jakoukoli, je vždy větší hodnota podmíněné pravděpodobnosti pro vstup $X = 0$.

Definice. Zobrazení $H : \langle 0,1\rangle \to \langle 0,1\rangle$ dané podmínkami $H(0) = H(1) = 0$ a

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p) = p\log_2 \frac{1}{p} + (1-p)\log_2 \frac{1}{1-p}$$

pro $p \in (0,1)$ se nazývá *entropická funkce*.

Poznámka 8.4. Pro entropickou funkci H platí
(1) $H(p) = H(1-p)\ \forall p \in \langle 0,1\rangle$,
(2) $H \in C^1(\langle 0,1\rangle)$, $H(\frac{1}{2}) = 1$ a $H'(\frac{1}{2}) = 0$,
(3) H roste na $\langle 0, \frac{1}{2}\rangle$ a klesá na $\langle \frac{1}{2}, 1\rangle$.

Důkaz. Elementární matematická analýza. □

Poznámka 8.5. Nechť Γ je BSC se spolehlivostí P, se vstupem X a výstupem Y. Jestliže $q = P[Y=0]$ a C_Γ je binární kapacita, potom
(1) $H_2(Y|X) = H(P)$ a $H_2(Y) = H(q)$,
(2) $I_2(X,Y) = H(q) - H(P)$ a $C_\Gamma = 1 - H(P)$,
(3) $I_2(X,Y) = C_\Gamma \Leftrightarrow q = \frac{1}{2}$.

Důkaz. (1) Označíme-li $p_i = P[X=i]$, $q_i = P[Y=1]$ a $P_{ij} = P[Y=j|X=i]$. Pak $p_0 + p_1 = 1$ a platí

$$H_2(Y|X) = -\sum_{ij} p_i P_{ij} \log_2 P_{ij} = -(p_1+p_2)(P\log_2 P + (1-P)\log_2(1-P)) = H(P)$$

Rovnost $H_2(Y) = H(q)$ dostáváme přímo z definic entropie a entropické funkce.

(2) a (3) $I_2(X,Y) = H_2(Y) - H_2(Y|X) = H(q) - H(P)$ z (1) a popisu $I_2(X,Y)$.

Maxima hodnota $H(q) - H(P)$ nabývá podle 8.4 právě pro $q = \frac{1}{2}$, proto dostáváme $C_\Gamma = H(\frac{1}{2}) - H(P) = 1 - H(P)$. □

Příklad 8.6. Pro hodnoty Příkladu 8.3 a spočítejme binární kapacitu kanálu Γ:

$$C_\Gamma = 1 - H(\frac{4}{5}) = 1 - (\frac{4}{5}\log_2\frac{5}{4} + \frac{1}{5}\log_2 5) = \frac{13}{5} - \log_2 5 \doteq 0,278.$$

Potom $I_2(X,Y) = H(\frac{37}{50}) - H(\frac{4}{5}) \doteq 0,827 - 0,722 = 0,105$.

9. Kódování zdroje

V celé kapitole je (Ω, P) DPP a S je abeceda pro informační zdroj $X : \Omega \to S$.

T&N. Nechť je T konečná abeceda, pak značme $T^n = \{t_1 \dots t_n \mid t_i \in T\}$, $T^0 = \{\epsilon\}$ (prázdné slovo), $T^+ = \bigcup_{n>0} T^n$ a $T^* = T^+ \cup T^0$.

Každé zobrazení $C : S \to T^+$ se nazývá *kódování*.

Pozorování. Buď $C : S \to T^+$ kódování.

(1) $CX : \Omega \to C(S) \subseteq T^+$ je informační zdroj,

(2) zobrazení $C^* : S^* \to T^*$ dané podmínkou $C^*(s_1, \dots s_k) = C(s_1) \dots C(s_k)$ a $C(\epsilon) = \epsilon$ rozšiřuje zobrazení C.

Příklad 9.1. (1) Je-li $S = \mathbb{F}_q^k$ a $\mathbf{C} \in \mathbb{F}_q^{k\times n}$ generující matice $[n,k]_q$ kódu $\mathcal{C}$, pak lineární zobrazení $C : S \to \mathbb{F}_q^n$ dané vztahem $c(s) = s\mathbf{C}$ je kódování a $C(S) = \mathcal{C}$.

(2) Je-li $S = \{a,b,c\}$ a $C(a) = 1$, $C(b) = 01$, $C(c) = 00$, pak $C : S \to \mathbb{F}_2^+$ je kódování a $C(S)$ není blokový kód.

T&N. Nechť $C : S \to T^+$ je kódování, pak nadále značme C^* zobrazení z Pozorování (2). Pro slovo $s = s_1 \dots s_n \in S^*$ a $s_i \in S$ se hodnota $l(s) = n$ nazve *délka slova* s.

Pro $u, v \in S^*$ řekneme, že u je prefix v, pokud $\exists\, t \in S^*$ splňující $v = ut$.

Definice. Kódování $C : S \to T^+$ se nazve

- *prosté*, pokud C^* je prosté zobrazení,

- *prefixové*, pokud $\forall s \in S$ a $\forall w \in T^*$ $C(s)w \notin C(S \setminus \{s\})$ (tj. $\forall s \neq t \in S$ není $C(s)$ prefixem $C(t)$).

Poznámka 9.2. Prefixové kódování je prosté.

Důkaz. Předpokládejme ke sporu, že $C : S \to T^+$ je prefixové kódování, které není prosté, tedy $\exists s = s_1 \dots s_a, \tilde{s} = \tilde{s}_1 \dots \tilde{s}_b \in S^*$, pro které $s \neq \tilde{s}$ a $C^*(s) = C^*(\tilde{s})$. BÚNO $a \geq b$.

(a) Kdyby $s_i = \tilde{s}_i$ $\forall i \leq \min(a,b)$, pak $a > b$

$$C^*(s) = C(s_1) \dots C(s_b)C(s_{b+1}) \dots C(s_a) =$$

$$= C(\tilde{s}_1) \dots C(\tilde{s}_b)C(s_{b+1}) \dots C(s_a) = C(\tilde{s})C(s_{b+1}) \dots C(s_a),$$

proto $C(s_{b+1}) \dots C(s_a) = \epsilon$, což je spor s podmínkou $C(s_{b+1}) \in T^+$.

(b) Nechť existuje i, pro něž $s_i \neq \tilde{s}_i$, vezměme minimální takové. Potom

$$C(s_i) \dots C(s_a) = C(\tilde{s}_i) \dots C(\tilde{s}_b),$$

proto buď $C(s_i)$ je prefix $C(\tilde{s}_i)$ nebo $C(\tilde{s}_i)$ je prefix $C(s_i)$, což je spor. □

Příklad 9.3. (1) Je-li $C : S \to T^n$ prosté zobrazení, jedná se o prefixové blokové kódování. Každé lineární kódování pomocí generující matice (viz 9.1(1)) je prefixové.

(2) Kódování $C : \{a, b, c\} \to \{0, 1\}^+$: $C(a) = 1$, $C(b) = 01$, $C(c) = 00$ je prefixové.

(3) Kódování $C : \{a, b, c\} \to \{0, 1\}^+$: $C(a) = 1$, $C(b) = 10$, $C(c) = 00$ není prefixové, ale je prosté.

(4) Kódování $C : \{a, b, c\} \to \{0, 1\}^+$: $C(a) = 0$, $C(b) = 1$, $C(c) = u$ není pro žádné $u \in \{0, 1\}^+$ prosté.

T&N. Pro informační zdroj $X : \Omega \to S$ a kódování $C : S \to T^+$ definujme $L_X(S) = E(l(CX)) = \sum_{s \in S} P[X = s] l(C(s))$ *průměrnou délku kódování* zdroje X.

Příklad 9.4. (1) $L_X(C_n) = n$ pro každé blokové kódování $S \to T^n$ a každý informační zdroj $X : \Omega \to S$.

(2) Nechť $S = \{a, b, c\}$ a $X : \Omega \to S$ má rozdělení
$P[X = a] = \frac{1}{2}$, $P[X = b] = P[X = c] = \frac{1}{4}$ a uvažme kódování $C_i : \{a, b, c\} \to \{0, 1\}^+$:
(a) $C_1(a) = 1$, $C_1(b) = 00$, $C_1(c) = 01$, pak $L_X(C_1) = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot (2 + 2) = \frac{3}{2}$,
(b) $C_2(a) = 00$, $C_2(b) = 1$, $C_2(c) = 01$, pak $L_X(C_2) = \frac{1}{2} \cdot 2 + \frac{1}{4} \cdot (1 + 2) = \frac{7}{4}$.

Nadále budeme předpokládat, že S je konečná q-prvková abeceda.

Věta 9.5 (Kraftova věta)**.** Buď $q, r \geq 2$ přirozená čísla a $S = \{s_1, \ldots, s_q\}$, T abecedy splňující $|S| = q$, $|T| = r$ a $l_1, \ldots, l_q \in \mathbb{N}$. Potom $\exists$ prefixové kódování $C : S \to T^+$ splňující $l(C(s_i)) = l_i \ \forall\, i \Leftrightarrow \sum_{j=1}^{q} r^{-l_j} \leq 1$.

Důkaz. BÚNO $l_1 \leq \cdots \leq l_q$. Položme $l = l_q$ a označme $T^{\leq l} = \bigcup_{i=0}^{l} T^i$. Nechť $\mathcal{T}$ je r-ární strom s vrcholy $T^{\leq l}$ a kořenem $\epsilon \in T^0$. Z vrcholu $c \in T^i$ vedou hrany právě do všech vrcholů $ct \in T^{i+1}\ \forall t \in T \Rightarrow c$ je prefixem právě všech listů z T^l, které leží ve stromě pod ním a těch je právě $|T|^{l-l_i} = r^{l-l_i}$.

($\Rightarrow$) Je-li C prefixové, pak každý list T^l leží nejvýše pod jedním slovem $C(s_i)$ a pod $C(s_i)$ je právě r^{l-l_i} listů, proto $\sum_{j=1}^{q} r^{l-l_j} \leq r^l \Rightarrow \sum_{j=1}^{q} r^{-l_j} \leq 1$.

($\Leftarrow$) Indukcí zkonstruujme $c_1, \ldots, c_q$ splňující $C(s_i) = c_i \in T^{l_i}$ a c_j není prefixem $c_i\ \forall\, j < i$.

• $C(s_1) \in T^{l_1}$ zvolme libovolně.

• Máme-li $c_1, \ldots, c_k$ pro $k < q$, které $\forall\, i \leq k$ splňují, že $\exists\, r^{l-l_i}$ listů s prefixem $c_i \Rightarrow \sum_{j=1}^{k} r^{l-l_j} < \sum_{j=1}^{q} r^{l-l_j} = r^l \sum_{j=1}^{q} r^{-l_j} \leq r^l \Rightarrow \exists\, u \in T^l$, jehož prefixem není žádné ze slov $c_1, \ldots, c_k$. Nyní stačí zvolit $c_{k+1} \in T^{l_{k+1}}$, které je prefixem slova u délky l_{k+1}. □

Konstrukce Shannonova-Fanova kódování informačního zdroje:

Buď informační zdroj $X : \Omega \to S = \{s_1, \ldots, s_q\}$ a nechť $p_i = P[X = s_i] \neq 0$. Definujeme-li $l_i := \lceil \log_r \frac{1}{p_i} \rceil$, pak $\log_r \frac{1}{p_i} \leq l_i < 1 + \log_r \frac{1}{p_i} \Rightarrow r^{-l_i} \leq p_i \Rightarrow \sum_{i=1}^{q} r^{-l_i} \leq \sum_{i=1}^{q} p_i = 1$. Proto podle 9.5 existuje prefixové kódování $C : S \to T^+$ splňující $l(C(s_i)) = l_i\ \forall\, i$ (samotná konstrukce viz důkaz), kterému budeme říkat *Shannonovo-Fanovo* kódování zdroje X.

Pozorování. Je-li C Shannonovo-Fanovo kódování zdroje X ve značení předchozí konstrukce, pak

$$H_r(X) = \sum_{i=1}^{q} p_i \log_r \frac{1}{p_i} \leq \sum_{i=1}^{q} p_i l_i = L_X(C) < \sum_{i=1}^{q} p_i (1 + \log_r \frac{1}{p_i}) = H_r(X) + 1.$$

Poznámka 9.6. Je-li C prefixové r-ární kódování zdroje $X : \Omega \to S$, pak $H_r(X) \leq L_X(C)$ a rovnost nastává $\Leftrightarrow l(C(s)) = -log_r P[X = s]\ \forall s \in S$.

Důkaz. Nechť $S = \{s_1, \ldots, s_q\}$, $l_i = l(C(s_i))$ a BÚNO $p_i = P[X = s_i] \neq 0\ \forall i = 1, \ldots, q$. Položíme-li v 7.1(2) $a_i = p_i$ a $x_i = r^{-l_i}$, kde víme, že $\sum_i x_i = \sum_i r^{-l_i} \leq 1$, z 9.5, potom z 7.1(2) plyne, že

$$H_r(X) = \sum_i p_i \log_r \frac{1}{p_i} \leq \sum_i p_i \log_r r^{l_i} = \sum_i p_i l_i = L_X(C)$$

a rovnost platí $\Leftrightarrow p_i = r^{-l_i}\ \forall i = 1, \ldots, q$. □

T&N. Pro informační zdroj $X : \Omega \to S$ položme $X = X_i\ \forall i = 1, \ldots, n$ a předpokládejme $X_1, \ldots, X_n$ jsou $\forall n$ nezávislé.

Kódování $C_n : S^n \to T^+$ nazveme r-ární *kódování zdroje X bloky* délky n a $\frac{L_{X^n}(C_n)}{n}$ je relativní průměrná délka kódování C zdroje $X^n = \prod_{i=1}^n X_i$.

Pozorování. Za předpokladů předchozí terminologické poznámky platí, že $H_r(X^n) =$
$= -\sum_{\mathbf{s} \in S^n} P[X^n = \mathbf{s}] \log_r P[X^n = \mathbf{s}] =$
$= -\sum_{\mathbf{s} \in S^n} P[X_1 = s_1, \ldots, X_n = s_n] \sum_{i=1}^n \log_r P[X_i = s_i] =$
$= -\sum_{i=1}^n \sum_{s_i \in S} P[X_i = s_i] \log_r P[X_i = s_i] \sum_{\tilde{\mathbf{s}} \in S^{n-1}} P[X^{n-1} = \tilde{\mathbf{s}}] = nH_r(X)$

Věta 9.7 (První Shannonova - Noisless Coding Theorem)**.** Je-li $r \geq 2$ a $X : \Omega \to S$ informační zdroj, potom $\exists$ posloupnost prefixových kódování $C_n : S^n \to T^+$ bloky délky n splňující $\frac{L_{X^n}(C_n)}{n} \to H_r(X)$.

Důkaz. Vezmeme-li C_n Shannonovo-Fanovo kódování zdroje X^n

$$\Rightarrow nH_r(X) = H_r(X^n) \leq L_{X^n}(C_n) \leq H_r(X^n) + 1 = nH_r(X) + 1 \Rightarrow$$

$H_r(X) \leq \frac{L_{X^n}(C_n)}{n} \leq H_r(X) + \frac{1}{n}$. □

Příklad 9.8. Uvažujme zdroj $X : \Omega \to \mathbb{Z}_2$ s rozdělením $P[X = 0] = \frac{2}{3}$ a $P[X = 1] = \frac{1}{3}$ a nechť C_n je Shannonovo-Fanovo kódování zdroje $X^n = \prod_{i=1}^n X_i$ pro $X = X_i\ \forall i = 1, \ldots, n$ po dvou nezávislé.

Pro $s \in \mathbb{Z}_2^n$ položme $k = n - w(s) \Rightarrow P[X = s] = \frac{2^k}{3^n}$. Označme $l_k = l(C(s))$ a $d_n = \lceil n \log_2 3 \rceil$. Potom

$$l_k = \lceil \log_2 \frac{3^n}{2^k} \rceil = \lceil n \log_2 3 - k \rceil = d_n - k \Rightarrow$$

$$L_{X^n}(C_n) = \sum_{k=0}^n \binom{n}{k} \frac{2^k}{3^n} l_k = \sum_{k=0}^n \binom{n}{k} (\frac{2^k}{3^n} d_n - \frac{2^k}{3^n} k) =$$

$$= \frac{d_n}{3^n} \sum_{k=0}^n \binom{n}{k} 2^k - \frac{1}{3^n} \sum_{k=0}^n \binom{n}{k} k 2^k = d_n - \frac{2}{3} n,$$

kde jsme využili rovnost $nx(1+x)^{n-1} = \sum_{k=0}^n \binom{n}{k} k x^k$.

Označíme $L_n = \frac{L_{X^n}(C_n)}{n}$, pak spočítáme

n	1	2	3	4	5	6
d_n	2	4	5	7	8	10
L_n	$\frac{4}{3}$	$\frac{4}{3}$	1	$\frac{13}{12}$	$\frac{14}{15}$	1

pro $H_2(X) \doteq 0,918$.

Definice. Prefixové r-ární kódování zdroje X se nazývá *optimální*, je-li $L_X(C)$ minimální mezi všemi prefixovými r-árními kódováními.

Příklad 9.9. Pro kódování zdroje $X : \Omega \to S$ s rozdělením $P[X = a] = \frac{1}{2}$, $P[X = b] = P[X = c] = \frac{1}{4}$ z úlohy 9.4 máme:

(a) C_1, kde $C_1(a) = 1$, $C_1(b) = 00$, $C_1(c) = 01$, je optimální binární kódování, neboť $L_X(C_1) = \frac{3}{2} = H_2(X)$, zatímco

(b) kódování $C_2(a) = 00$, $C_2(b) = 1$, $C_2(c) = 01$ optimální není, protože $L_X(C_2) = \frac{7}{4} > L_X(C_1)$.

Poznámka 9.10. Pro každé $r \geq 2$ a informační zdroj $X : \Omega \to S$, existuje jeho r-ární optimální kódování.

Důkaz. BÚNO $P[X = s] \neq 0 \ \forall s \in S$ a položme $p = \min_{s \in S} P[X = s]$, $l := \lceil \log_r \frac{1}{p} \rceil$. Označme $S = \{s_1, \ldots, s_q\}$. Potom $r^{-l} \leq p \Rightarrow qr^{-l} \leq qp \leq 1$. Potom 9.5 $\Rightarrow \exists C : S \to T^+$ prefixové kódování splňující $l(C(s_i)) = l \ \forall i = 1, \ldots, q \Rightarrow L_X(C) = l$.

Nechť $D : S \to T^+$ je prefixové kódování s délkami $l_i = l(D(s_i)) \ \forall i = 1, \ldots, q$.

Jestliže $\exists k$, pro něž $l_k > \frac{l}{p} \Rightarrow L_X(D) = \sum_{i=1}^{q} p_i l_i \geq p_k l_k \geq p_k l_k > l$. To znamená, že $L_X(D) \leq l \Rightarrow l_i \leq \frac{l}{p} \ \forall i = 1, \ldots, q$, tedy existuje jen konečně mnoho prefixových kódování splňujících $L_X(D) \leq l$ a mezi nimi lze najít to s minimální průměrnou délkou, tedy optimální kódování. □

Konstrukce Huffmanova kódování informačního zdroje:

Uvažujme informační zdroj $X : \Omega \to S = \{s_1, \ldots, s_q\}$ a r-ární abecedu T, BÚNO $T = \mathbb{Z}_r$. Nejprve indukcí zkonstruujme posloupnost zdrojů $X^{(i)} : \Omega \to S^{(i)}$, kde $|S^{(i)}| = q - i(r-1)$:

- $S^{(0)} = S$ a $X^{(0)} = X$.
- Mějme $X^{(i)}$.
  - Pokud $q - i(r-1) > r$, pak si označíme prvky $S^{(i)} = \{s_1^{(i)}, \ldots, s_{q-i(r-1)}^{(i)}\}$ tak, aby platilo, že $\sum_{j=1}^{r} P[X^{(i)} = s_j^{(i)}] \leq \sum_{j=1}^{r} P[X^{(i)} = s_{a_j}^{(i)}] \ \forall a_1 < \cdots < a_r$ a položíme $S^{(i+1)} = \{\tilde{s}, s_{r+1}^{(i)}, \ldots, s_{q-i(r-1)}^{(i)}\}$, kde $\tilde{s} = \bigvee_{j=1}^{r} s_j^{(i)}$ (stačí vzít „nejméně pravděpodobnou" r-tici $s_1, \ldots, s_r$). $X^{(i+1)}$ má rozdělení pravděpodobností:
    $P[X^{(i+1)} = \tilde{s}] = \sum_{j=1}^{r} P[X^{(i)} = s_j^{(i)}]$ a
    $P[X^{(i+1)} = s_j^{(i)}] = P[X^{(i)} = s_j^{(i)}] \ \forall j = r+1, \ldots, q - i(r-1)$.
  - Pokud $t := q - i(r-1) \leq r$ pak položíme $S^{(i+1)} = \{\tilde{s}\}$, kde $\tilde{s} = \bigvee_{j=1}^{t}$. Rozdělení pravděpodobností $X^{(i+1)}$ bude triviální $P[X^{(i+1)} = \tilde{s}] = 1$. Dále položíme $n := i+1$ a proces skončí.

Nyní opačným postupem indukčně vytvoříme posloupnost zobrazení $C^{(i)} : S^{(i)} \to T^*$ pro $i = n, \ldots, 0$, tak, že C^i je pro $i > 0$ prefixové kódování.

- $C^n = S^{(n)} \to T^0$ je dáno $C(s) = \epsilon$ (což není kódování).
- Máme-li definováno $C^{(i+1)} : S^{(i+1)} \to T^+$, kde $S^{(i+1)} = \{\tilde{s}, s_{r+1}^{(i)}, \ldots, s_{q-i(r-1)}^{(i)}\}$, pak položíme

$C^{(i)}(s_{j+1}^{(i)} = C^{(i+1)}(\tilde{s})j \ \forall j = 0, \ldots, r-1$ a

$C^{(i)}(s_j^{(i)} = C^{(i+1)}(s_j^{(i)}\ \forall j = r, \ldots, q - i(r-1)$.
Získané kódování $C = C^{(0)}$ je tzv. r-ární *Huffmanovo* kódování zdroje X.

Pozorování. Huffmanovo kódování je prefixové.

Příklad 9.11. Pro zdroj $X : \Omega \to S = \{a, b, c, d, e\}$ s distribucí pravděpodobností $P[X = a] = 0,1, \quad P[X = b] = P[X = c] = P[X = d] = 0,2, \quad P[X = e] = 0,3$, najdeme binární Huffmanovo kódování zdroje X.

	$\forall$	$a \vee b \vee e$	$c \vee d$	$a \vee b$	a	b	c	d	e
$X^{(0)}$					$0,1$	$0,2$	$0,2$	$0,2$	$0,3$
$X^{(1)}$				$0,3$			$0,2$	$0,2$	$0,3$
$X^{(2)}$			$0,4$	$0,3$					$0,3$
$X^{(3)}$		$0,6$	$0,4$						
$X^{(4)}$	1								

	$\forall$	$a \vee b \vee e$	$c \vee d$	$a \vee b$	a	b	c	d	e
$C^{(4)}$	ϵ								
$C^{(3)}$		0	1						
$C^{(2)}$			1	00					01
$C^{(1)}$				00			10	11	01
$C^{(0)}$					000	001	10	11	01

Zkonstruovali jsme Huffmanovo kódování

$$C(a) = 000, \quad C(b) = 001, \quad C(c) = 10, \quad C(d) = 11, \quad C(0) = 01.$$

Vidíme, že $L_X(C) = \frac{3}{10} + \frac{3}{5} + 2 \cdot \frac{2}{5} + \frac{6}{10} = \frac{11}{5} = 2,3$ a snadno spočítáme, že $H_2(X) \doteq 2,246$.

Věta 9.12. Huffmanovo kódování je optimální.

Optimalitu Huffmanova kódování nebudeme využívat, proto (poněkud zdlouhavý) důkaz vynecháme

10. Dekódovací schéma

V celé kapitole budeme předpokládat, že (Ω, P) je DPP, náhodné veličiny $X : \Omega \to A$ a $Y : \Omega \to B$ jsou vstup a výstup diskrétní informační kanálu $\Gamma = (A, B, \mathbf{P})$.

T&N. Řekneme, že $C : S \to A^+$ je *blokové kódování* (délky n), existuje-li $n \in \mathbb{N}$, pro něž $C(S) \subseteq A^n$ (tj.$C(S)$ je blokový kód délky n). Je-li $C : S \to C(S) \subseteq A^+$ kódování zdroje X a $r = |A|$, pak $\frac{H_r(CX)}{L_X(S)}$ se nazývá *nosnost kódování.*

Poznámka 10.1. Nechť $C : S \to C(S) \subseteq A^n$ blokové kódování zdroje $Z : \Omega \to S$ a projekce $\pi_i : A^n \to A$ je daná podmínkou $\pi_i(a_1, \ldots, a_n) = a_i$, pak

(1) nosnost kódování $C \leq$ nosnost kódu $C(S)$ a rovnost nastává $\Leftrightarrow$ má CZ rovnoměrné rozdělení,
(2) $Z_i^C = \pi_i CZ : \Omega \to A$ je zdroj a $\forall\ \mathbf{v} \in C(S)$ platí, že $P[CZ = \mathbf{v}] = P[\prod_i Z_i^C = \mathbf{v}]$.

Důkaz. (1) Z 7.2 plyne, že $H_r(CZ) \leq \log_r(C(S))$ a rovnost nastává $\Leftrightarrow$ má CZ rovnoměrné rozdělení. Protože $n = L_Z(C)$ díky 9.4(1), zbývá obě strany nerovnosti vydělit hodnotou n.

(2) Stačí uvážit, že pro každé $\omega \in \Omega$
$CZ(\omega) = (v_1, \ldots, v_n) \Leftrightarrow Z_i^C(\omega) = v_i \ \forall i.$ □

T&N. Posloupnost DNV $\{X_i\}_{i\geq 1}$ je *stacionární diskrétní náhodný proces*, jsou-li $X_i : \Omega \to A$ DNV se stejným rozdělením, tj. $P[X_i = a] = P[X_j = a] \ \forall i, j$ a $\forall a \in A$. Budeme značit $X^n = \prod_{i=1}^n X_i$.

Budeme předpokládat $\{X_i\}_{i\geq 1}$, resp. $\{Y_i\}_{i\geq 1}$ jsou stacionární diskrétní náhodné procesy se stejným rozdělením jako má vstup X, resp. výstup Y kanálu Γ.

T&N. O kanálu $\Gamma = (A, B, \mathbf{P})$ řekneme, že je *bez paměti*, splňuje-li $\forall n \geq 1$ a $\forall \mathbf{a} = (a_1, \ldots, a_n) \in A^n$ a $\mathbf{b}(b_1, \ldots, b_n) \in B^n$, že $P[Y^n = \mathbf{b}|X^n = \mathbf{a}] = \prod_{i=1}^n P[Y_i = b_i|X_i = a_i]$.

O kanálu Γ budeme nadále vždy předpokládat, že je bez paměti.

T&N. Nechť $n \in \mathbb{N}$ a $\mathcal{C} = X^n(\Omega)$, pak každému (parciálnímu) zobrazení $\delta : B^n \to \mathcal{C}$ budeme říkat *dekódovací schéma*. Jestliže dekódovací schéma δ splňuje $\forall \mathbf{u} \in B^n$ rovnost

$$P[Y^n = \mathbf{u}|X^n = \delta(\mathbf{u})] = \max_{\mathbf{v}\in\mathcal{C}} P[Y^n = \mathbf{u}|X^n = \mathbf{v}],$$

pak mluvíme *ML schématu* (maximum likelihood).

Příklad 10.2. Buď $\Gamma = (\mathbb{F}_2, \mathbb{F}_2, \mathbf{P})$ BSC bez paměti se spolehlivostí $P > \frac{1}{2}$. Víme, že $\mathbf{P} = \begin{pmatrix} P & 1-P \\ 1-P & P \end{pmatrix}$ a $P[Y^n = \mathbf{u}|X^n = \mathbf{v}] = P^{n-d(\mathbf{u},\mathbf{v})}(1-P)^{d(\mathbf{u},\mathbf{v})} = P^n \left(\frac{1-P}{P}\right)^{d(\mathbf{u},\mathbf{v})}$, proto zvolíme-li za $\delta(\mathbf{v}) = \mathbf{u}$ pro slovo $\mathbf{u} \in \mathcal{C}$ s minimální vzdáleností od $\mathbf{v}$, pak je δ ML dekódovací schéma.

T&N. ML dekódovací schéma z předchozího příkladu nazveme *metodou nejbližšího slova*.

T&N. Nechť $C : S \to A^n$ je kódování zdroje $Z : \Omega \to S$ splňující $X^n = \prod_i \pi_i CZ$ pro projekci π_i z 10.1 a $\delta : B^n \to \mathcal{C} = C(S)$ je dekódovací schéma kanálu Γ. Pak značme $\forall s \in S$ a $\forall \mathbf{u} \in \mathcal{C}$:

(1) $P_E(s) = P[\delta Y^n \neq C(s)|Z = s] = \sum_{\mathbf{v}\in\mathcal{C}\setminus\{C(s)\}} P[\delta Y^n = \mathbf{v}|Z = s]$,
$P_E(\mathbf{u}) = P[\delta Y^n \neq \mathbf{u}|X^n = \mathbf{u}] = \sum_{\mathbf{v}\in\mathcal{C}\setminus\{\mathbf{u}\}} P[\delta Y^n = \mathbf{v}|X^n = \mathbf{u}]$,

(2) ${}_C P_E = \sum_{s\in S} P_E(s)P[Z = s]$ a ${}_{\mathcal{C}}P_E = \sum_{\mathbf{u}\in\mathcal{C}} P_E(\mathbf{u})P[X^n = \mathbf{u}]$
(střední pravděpodobnost chyby dekódování),

(3) ${}_C P_E^{av} = \frac{1}{|S|}\sum_{s\in S} P_E(s)$ a ${}_{\mathcal{C}}P_E^{av} = \frac{1}{|\mathcal{C}|}\sum_{\mathbf{u}\in\mathcal{C}} P_E(\mathbf{u})$
(uniformě průměrná pravděpodobnost chyby dekódování),

(4) ${}_C P_E^{max} = \max_{s\in S} P_E(s)$ a ${}_{\mathcal{C}}P_E^{max} = \max_{\mathbf{u}\in\mathcal{C}} P_E(\mathbf{u})$
(maximální pravděpodobnost chyby dekódování).

Pozorování. Pro pravděpodobnosti chyby dekódování platí:

(1) ${}_C P_E,\ {}_{\mathcal{C}}P_E,\ {}_C P_E^{av},\ {}_{\mathcal{C}}P_E^{av} \leq {}_C P_E^{max} = {}_{\mathcal{C}}P_E^{max}$,
(2) je-li C prosté, pak ${}_C P_E =_{\mathcal{C}} P_E$ a ${}_C P_E^{av} =_{\mathcal{C}} P_E^{av}$.

T&N. Je-li $A = B$ a $(A, +, -, 0)$ je abelovská grupa, označme $E_i(\omega) := Y_i(\omega) - X_i(\omega)$ (mluvíme o *chybě* kanálu).

Poznámka 10.3. Jestliže $\Gamma = (A, A, \mathbf{P})$ pro abelovskou grupu $(A, +, -, 0)$, potom $\{E_i\}_{i\geq 1}$ tvoří stacionární diskrétní náhodný proces a platí-li $\forall\ a, b, e \in A$, že

$$c_e = P[Y = a + e | X = a] = P[Y = b + e | X = b],$$

pak

$$P[E^n = \mathbf{e}] = \prod_{i=1}^{n} P[E_i = e_i] = \prod_{i=1}^{n} c_{e_i}\ \forall \mathbf{e} = (e_1, \ldots, e_n) \in A^n.$$

Důkaz. $P[E^n = \mathbf{e}] = \sum_{\mathbf{u}\in A^n} P[Y^n = \mathbf{u} + \mathbf{e}, X^n = \mathbf{u}] =$

$$= \sum_{\mathbf{u}\in A^n} P[Y^n = \mathbf{u} + \mathbf{e} | X^n = \mathbf{u}] P[X^n = \mathbf{u}] = \sum_{\mathbf{u}\in A^n} \prod_{i=1}^{n} \underbrace{P[Y = a_i + e_i | X_i = a_i]}_{=c_{e_i}} P[X^n = \mathbf{u}] =$$

$$= \prod_{i=1}^{n} c_{e_i} \sum_{\mathbf{u}\in A^n} P[X^n = \mathbf{u}] = \prod_{i=1}^{n} c_{e_i} = \prod_{i=1}^{n} c_{e_i} \sum_{a\in A} P[X_i = a] =$$

$$= \prod_{i=1}^{n} \sum_{a\in A} P[Y_i = a + e_i | X_i = a] P[X_i = a] = \prod_{i=1}^{n} \sum_{a\in A} P[Y_i = a + e_i, X_i = a] = \prod_{i=1}^{n} P[E_i = e_i]$$

□

Důsledek 10.4. Je-li $\Gamma = (\mathbb{F}_2, \mathbb{F}_2, \mathbf{P})$ BSC se spolehlivostí $P > \frac{1}{2}$, potom $P[E^n = \mathbf{e}] = P^{n-w(\mathbf{e})}(1-P)^{w(\mathbf{e})} = P^n \left(\frac{1-P}{P}\right)^{w(\mathbf{e})}$.

11. Shannonovy věty o kapacitě kanálu

Budeme předpokládat, že $\Gamma = (\mathbb{F}_2, \mathbb{F}_2, \mathbf{P})$ je BSC bez paměti se spolehlivostí $P > \frac{1}{2}$ a $\{X_i\}_{i\geq 1}$, $\{Y_i\}_{i\geq 1}$ a $\{E_i\}_{i\geq 1}$ jsou po řadě stacionární diskrétní náhodné procesy jeho vstupu, výstupu a chyby. Položme $\overline{P} = 1 - P$.

Věta 11.1 (Slabý zákon velkých čísel)**.** Pokud je $\{Z_i\}_{i\geq 1}$ diskrétní náhodný proces, $\mu = EZ_i\ \forall i$ a $\eta > 0$, potom $P[|\frac{1}{n}\sum_{i=1}^{n} Z_i - \mu| \geq \eta] = P[\frac{1}{n}|\sum_{i=1}^{n} Z_i - n\mu| \geq \eta] \to 0$ pro $n \to \infty$.

Důsledek 11.2. Nechť $\eta > 0$ a položme $\overline{E}_i = 1 - E_i$ a $\overline{E}^n = \prod_{i=1}^{n} \overline{E}_i$. Potom pro $n \to \infty$

(1) $P[|w(E^n) - n\overline{P}| \geq n\eta] \to 0$,
(2) $P[w(E^n) > n(\overline{P} + \eta)] \to 0$,
(3) $P[w(\overline{E}^n) > n(P + \eta)] \to 0$,
(4) $P[w(E^n) < n(\overline{P} - \eta)] \to 0$.

Důkaz. (1) Protože $E_i = Y_i - X_i$ a střední hodnota $EE_i = 0 \cdot P + 1 \cdot \overline{P} = \overline{P}$, dostáváme z 11.1, že

$$P[|w(E^n) - n\overline{P}| \geq n\eta] = P[\frac{1}{n}|\sum_{i=1}^{n} E_i - n\overline{P}| \geq \eta] \to 0 \text{ pro } n \to \infty.$$

(2) Díky (1):

$$P[w(E^n) > n(\overline{P}+\eta)] = P[w(E^n) - n\overline{P} > n\eta)] \leq P[|w(E^n) - n\overline{P}| \geq n\eta] \to 0$$

pro $n \to \infty$

(3) Protože střední hodnota $E\overline{E}_i = 0 \cdot \overline{P} + 1 \cdot P = P$, dostáváme závěr použitím (1) a (2) na $\overline{E}^n$.

(4) Protože $w(E^n) < n(\overline{P}-\eta) \Leftrightarrow w(\overline{E}^n) = n - w(E^n) > n - n(\overline{P}-\eta) = n(P+\eta)$, využijeme (3) $P[w(E^n) < n(\overline{P}-\eta)] = P[w(\overline{E}^n) > n(P+\eta)] \to 0$. □

Připomeňme, že $V_2(n,r) = \sum_{i=0}^{r} \binom{n}{i}$ je velikost binární koule o poloměru r v $\mathbb{F}_2^n$.

Poznámka 11.3. Pro $r, n \in \mathbb{N}$ splňující $2r \leq n$ platí, že $V_2(n,r) \leq \frac{n^n}{r^r(n-r)^{n-r}} = 2^{nH(\frac{r}{n})}$.

Důkaz. $nH(\frac{r}{n}) = r\log_2 \frac{n}{r} + (n-r)\log_2 \frac{n}{n-r} \Rightarrow 2^{nH(\frac{r}{n})} = (\frac{n}{r})^r \cdot (\frac{n}{n-r})^{n-r} = \frac{n^n}{r^r(n-r)^{n-r}}$.

Dále $2r \leq n \Rightarrow r \leq n-r \Rightarrow \frac{r}{n-r} \leq 1$, proto

$$\begin{aligned} n^n &= (r + (n-r))^n \\ &\geq \sum_{i=0}^{r} \binom{n}{i} r^i (n-r)^{n-i} = \sum_{i=0}^{r} \binom{n}{i} \left(\frac{r}{n-r}\right)^i (n-r)^n \\ &\geq \left(\frac{r}{n-r}\right)^r (n-r)^n \sum_{i=0}^{r} \binom{n}{i} = r^r \cdot (n-r)^{n-r} \cdot V_2(n,r). \end{aligned}$$

□

Připomeňme, že $C_\Gamma = 1 - H(P) = 1 - H(\overline{P})$ podle 8.4(2).

Vyslovíme tvrzení, které říká, že blokovým kódováním vhodného zdroje nosnosti r libovolně blízké (ale menší), než je kapacita C_Γ (tj. přeneseme r bitů informace na bit zprávy) umíme kanálem Γ přenést informaci s maximální pravděpodobností chyby libovolně blízkou nule:

Věta 11.4 (Shannonova, Hlavní věta teorie informace)**.** Pro BSC se spolehlivostí $P > \frac{1}{2}$ existuje posloupnost blokových kódování C_k vhodných zdrojů s nosností $r_k < C_\Gamma = 1 - H(P)$ splňující ${}_{C_k}P_E^{max} \to 0$ a $r_k \to C_\Gamma$ pro $k \to \infty$.

Důkaz. Uvažujme informační zdroj $Z : \Omega \to S$ a jeho kódování $C : Z \to \mathbb{F}_2^n$. Označme $m := |S|$, $r = \frac{\log_2 m}{n}$ a $X^n = \prod_{i=1}^n \pi_i CZ$ a pro projekce π_i z 10.1. Posloupnost vstupů BSC a Y^n odpovídající posloupnost výstupů a $E^n = Y^n - X^n$ posloupnost chyb kanálu.

Zdroj Z budeme vždy volit tak, aby měl rovnoměrné rozdělení pravděpodobností, tedy $P[Z = s] = \frac{1}{m}\ \forall s \in S$. Nejprve ukážeme, že pro dostatečně velké m a n existuje kódování C zdroje Z, jehož nosnost je libovolně blízká kapacitě kanálu a jehož střední chyba dekódování ${}_C P_E^{av}$ je libovolně blízká 0.

Zvolme libovolně $\varepsilon \in (0, 1 - H(P))$ a připomeňme, že $\overline{P} < \frac{1}{2}$. Pak podle 8.4 $H(P) = H(\overline{P})$ a $\exists n_0 \in \mathbb{N}\ \forall n \geq n_0\ \exists m \in \mathbb{N}$ splňující

$$2^{n(1-H(\overline{P})-\varepsilon)} \leq m \leq 2^{n(1-H(\overline{P})-\frac{\varepsilon}{2})},$$

a proto $1 - H(\overline{P}) - \varepsilon \leq r \leq 1 - H(\overline{P}) - \frac{\varepsilon}{2}$.

Zvolme m a n splňující uvedené nerovnosti, označme $V = \{C : S \to \mathbb{F}_2^n\}$ a uvažujme rovnoměrně rozdělenou DNV volby kódování, kterou označíme $\mathfrak{C} : \Omega \to U$. Protože $|V| = 2^{nm}$ máme $P[\mathfrak{C} = C] = 2^{-nm}\ \forall C \in V$.

Označme $\delta : \mathbb{F}_2^n \to C(S)$ dekódovací metodu nejbližšího slova a odhadněme P_E střední hodnotu DNV vzniklou složením $C \to {}_CP_E^{av}$ a $\mathfrak{C}$, tedy

$$\begin{aligned}
P_E &= \sum_{C\in V} {}_CP_E^{av} P[\mathfrak{C} = C] = 2^{-nm} \sum_{C\in V} \frac{1}{m} \sum_{s\in S} P[\delta Y^n \neq C(s)|Z = s] \\
&= 2^{-nm} \sum_{C\in V} \sum_{s\in S} P[Z = s]P[\delta Y^n \neq C(s)|Z = s] = \\
&= 2^{-nm} \sum_{C\in V} \sum_{s\in S} P[\delta Y^n \neq C(s), Z = s] \\
&= 2^{-nm} \sum_{C\in V} P[\delta Y^n \neq X^n]
\end{aligned}$$

Nyní zvolíme $\eta > 0$ splňující (a) $\overline{P} + \eta < \frac{1}{2}$ a (b) $H(\overline{P} + \eta) - H(\overline{P}) < \frac{\varepsilon}{2}$, což podle 8.4 lze, a položme $\rho := n(\overline{P} + \eta)$. Nechť

$$P_1 = 2^{-nm} \sum_{C\in V} P[w(E^n) > \rho], \quad P_2 = 2^{-nm} \sum_{C\in V} P[w(E^n) \leq \rho, \delta Y^n \neq X^n],$$

pak $P_E \leq P_1 + P_2$, proto stačí odhadnout P_1 a P_2.

$$P_1 = \frac{|V|}{2^{nm}} P[w(E^n) > \rho] = P[w(E^n) > \rho] \to 0 \text{ pro } n \to \infty$$

11.2(2), neboť o $\{E_i\}_{i\geq 1}$ předpokládáme, že je stacionární diskrétní náhodný proces, tedy pro dostatečně velké n je P_1 libovolně malé, kde $P[w(E^n) > \rho]$ podle 10.4 nezávisí na volbě kódování. Dále

$$\begin{aligned}
P_2 &\leq 2^{-nm} \sum_{C\in V} \sum_{z\in S} P[w(E^n) \leq \rho, \delta Y^n = C(z), Z \neq z] \\
&\leq 2^{-nm} \sum_{C\in V} \sum_{z\in S} P[d(Y^n, C(z)) \leq w(E^n) \leq \rho, Z \neq z] \\
&\leq 2^{-nm} \sum_{C\in V} \sum_{z\in S} P[d(Y^n, C(z)) \leq \rho] \\
&\leq 2^{-nm} \sum_{z\in S} \sum_{\mathbf{v}\in\mathbb{F}_2^n} P[Y^n = \mathbf{v}] \sum_{C\in V} P[d(Y^n, C(z)) \leq \rho|Y^n = \mathbf{v}] \\
&= 2^{-nm} \sum_{z\in S} \sum_{\mathbf{v}\in\mathbb{F}_2^n} P[Y^n = \mathbf{v}] \underbrace{|\{C \in V \mid d(C(z), \mathbf{v}) \leq \rho\}|}_{2^{nm-n}V_2(v,\lfloor\rho\rfloor)} \\
&= 2^{-n}V_2(v, \lfloor\rho\rfloor) \sum_{z\in S} \sum_{\mathbf{v}\in\mathbb{F}_2^n} P[Y^n = \mathbf{v}] = m \cdot 2^{-n}V_2(v, \lfloor\rho\rfloor).
\end{aligned}$$

Nyní využijeme 11.3 a předpokladu (b), že $H(\overline{P}+\eta) - H(\overline{P}) - \frac{\varepsilon}{2} < 0$:

$$\begin{aligned} P_2 &\leq m2^{-n}V_2(v, \lfloor\rho\rfloor) \leq 2^{n(1-H(\overline{P})-\frac{\varepsilon}{2})}2^{-n}2^{nH(\overline{P}+\eta))} \\ &\leq 2^{n(H(\overline{P}+\eta)-H(\overline{P})-\frac{\varepsilon}{2})} \to 0 \text{ pro } n \to \infty, \end{aligned}$$

tedy opět pro dostatečně velké n je P_2 libovolně malé.

Pro každou posloupnost $\varepsilon_k \to 0$ jsme dokázali, že pro dostatečně velké n_k platí, že $2^{-n_k m_k} \sum_{C \in V} {}_C P_E^{av} \leq \varepsilon_k$, proto $\exists C_n : S_k \to \mathbb{F}_2^{n_k}$ kódování vhodného uniformního zdroje $Z_k : \Omega \to S_k$ splňující ${}_{C_k}P_E^{av} \leq \varepsilon_k$. BÚNO C_k můžeme vzít bez zvýšení ${}_{C_k}P_E^{av}$ prosté („slepené" prvky totiž v odhadu počítáme za chybně dekódované), proto je $C_k Z_k$ rovnoměrně rozdělený zdroj s nosností $r_k = \frac{\log_2 |S_k|}{n_k}$ podle 10.1(1) $\Rightarrow r_k \in (1-H(P)-\varepsilon_k, 1-H(P)-\frac{\varepsilon_k}{2})$. Dokázali jsme, že ${}_{C_k}P_E^{av} \to 0$ a $r_k \to C_\Gamma$ pro $k \to \infty$.

Zbývá dokázat stejné tvrzení pro ${}_{C_k}P_E^{max}$. Vezmeme-li posloupnost $\varepsilon_k \to 0$ a prosté kódování $C_k : S_k \to \mathbb{F}_2^{n_k}$ tak, že $n_k \geq k$, $|S_k| = 2m$, $r, r - \frac{1}{k} \in (C_\Gamma - \varepsilon_k, C_\Gamma)$ a ${}_{C_k}P_E^{av} < \frac{\varepsilon_k}{2}$. Jestliže $N = \{s \in S_k \mid P_E(s) \geq \varepsilon_k\} \Rightarrow |N| \leq m \Rightarrow \exists \tilde{S}_k \subseteq S_k \setminus N$ o m prvcích.

Nyní stačí zakódovat rovnoměrně rozdělený zdroj $Z_k : \Omega \to \tilde{S}_k$ prostým kódováním $\tilde{C}_k := C_k|_{\tilde{S}_k}$. Potom ${}_{\tilde{C}_k}P_E^{max} < \varepsilon_k$, protože $P_E(\tilde{s}) < \varepsilon_k \ \forall \tilde{s} \in \tilde{S}$, a nosnost $\tilde{C}_k$ je

$$\frac{\log_2 \frac{2m}{2}}{n_k} = \frac{(\log_2 2m) - 1}{n_k} = r - \frac{1}{n_k} \geq r - \frac{1}{k} > C_\Gamma - \varepsilon_k$$

a $r - \frac{1}{n_k} < r < C_\Gamma$ □

Nyní ukážeme, že kódem nosnosti překračující kapacitu kanálu pro žádné dekódování nelze spolehlivě přenášet informaci.

Věta 11.5 (Inverzní Shannonova)**.** Je-li Γ BSC se spolehlivostí $P > \frac{1}{2}$ a $\varepsilon > 0$, pak pro každou posloupnost blokových kódování $C_k : S_k \to \mathbb{F}_2^{n_k}$ délky $n_k \to \infty$ libovolných zdrojů s nosností $r_k \geq C_\Gamma + \varepsilon$ a libovolné dekódování δ platí, že ${}_{C_k(S_k)}P_E^{av} \to 1$ pro $k \to \infty$.

Důkaz. $\overline{P} < \frac{1}{2} < P \Rightarrow \frac{\overline{P}}{P} < 1 \Rightarrow \exists \eta > 0$ splňující $\left(\frac{\overline{P}}{P}\right)^{-\eta} < 2^{\frac{\varepsilon}{2}}$. Zvolíme takové η.

Uvažujme blokové kódování $C : S \to \mathbb{F}_2^n$ zdroje Z nosnosti $r = \frac{H_2(CZ)}{n}$ a označme tentokrát $m = |C(S)|$ (je-li C prosté, pak $m = |S|$). Potom $\frac{\log_2 m}{n} \geq r \geq 1 - H(P) + \varepsilon$ díky 10.1 $\Rightarrow \frac{1}{m} \leq 2^{-n(1-H(P)+\varepsilon)}$. Stejně jako v důkazu Věty 11.4 budeme značit po řadě $X^n = \prod_{i=1}^n \pi_i CZ$, Y^n a E^n posloupnosti vstupů, výstupů a chyb BSC Γ.

Položíme $\mathcal{C} = C(S)$ a místo uniformě průměrné chybovosti ${}_{\mathcal{C}}P_E^{av}$ spočítáme hodnotu $1 - {}_{\mathcal{C}}P_E^{av}$ a ukážeme, že je pro dostatečně velké n libovolně blízká nule.

$$\begin{aligned}
1 - {}_{\mathcal{C}}P_E^{av} &= 1 - \frac{1}{m}\sum_{c\in\mathcal{C}} P[\delta Y^n \neq c | X^n = c] \\
&= \frac{1}{m}\sum_{c\in\mathcal{C}} 1 - P[\delta Y^n \neq c | X^n = c] = \frac{1}{m}\sum_{c\in\mathcal{C}} P[\delta Y^n = c | X^n = c] \\
&= \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in\mathbb{F}_2^n} \frac{P[\delta Y^n = c, Y^n = c+e, X^n = c]}{P[X^n = c]} \\
&= \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in\mathbb{F}_2^n} \frac{P[\delta Y^n = c, Y^n = c+e, X^n = c]}{P[X^n = c]} \cdot \frac{P[Y^n = c+e, X^n = c]}{P[Y^n = c+e, X^n = c]} \\
&= \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in\mathbb{F}_2^n} P[Y^n = c+e | X^n = c] \cdot P[\delta Y^n = c | Y^n = c+e, X^n = c]
\end{aligned}$$

Označme $P_{c,e} = P[\delta Y^n = c | Y^n = c+e, X^n = c] = P[\delta Y^n = c | E^n = e, X^n = c]$ a všimněme si, že 10.3 a 10.4 $\Rightarrow P[Y^n = c+e | X^n = c] = P[E^n = e] \Rightarrow$

$$1 - {}_{\mathcal{C}}P_E^{av} \leq \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in\mathbb{F}_2^n} P[E^n = e] \cdot P_{c,e}.$$

Rozdělme si množinu $\mathbb{F}_2^n = E_1 \cup E_2$, kde

$$E_1 = \{e \in \mathbb{F}_2^n \mid w(e) < n(\overline{P} - \eta)\}, \quad E_2 = \{e \in \mathbb{F}_2^n \mid w(e) \geq n(\overline{P} - \eta)\},$$

a definujme

$$P_i = \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in E_i} P[E^n = e] \cdot P_{c,e}.$$

Potom $1 - {}_{\mathcal{C}}P_E^{av} \leq P_1 + P_2$. Protože $P_{c,e} \leq 1$ snadno odhadneme

$$P_1 \leq \frac{1}{m}\sum_{c\in\mathcal{C}}\sum_{e\in E_1} P[E^n = e] = P[w(E) < n(\overline{P} - \eta)] \to 0$$

pro $n \to \infty$ díky 11.2(4), tedy P_1 je libovolně malé pro dostatečně velké n.

Než určíme P_2, odhadneme s využitím 10.4 a předpokladu o η pro každé $e \in E_2$ hodnotu

$$P[E^n = e] = P^n \left(\frac{\overline{P}}{P}\right)^{w(\mathbf{e})} \leq P^n \left(\frac{\overline{P}}{P}\right)^{n(\overline{P}-\eta)} =$$

$$= \underbrace{\left(\frac{\overline{P}}{P}\right)^{n\eta}}_{\leq 2^{n\varepsilon/2}} \cdot \underbrace{\overline{P}^{n\overline{P}} \cdot P^{nP}}_{\leq 2^{-nH(P)}} \leq 2^{n(\frac{\varepsilon}{2} - H(P))}.$$

Nyní odhadněme P_2. Nejprve využijeme toho, že $\frac{1}{m} \leq 2^{-n(1-H(P)+\varepsilon)}$:

$$\begin{aligned} P_2 &= \frac{1}{m} \sum_{c\in\mathcal{C}} \sum_{e\in E_2} \underbrace{P[E^n = e]}_{\leq 2^{n(\frac{\varepsilon}{2}-H(P))}} P_{c,e} \\ &\leq 2^{-n(1-H(P)+\varepsilon)} \sum_{c\in\mathcal{C}} \sum_{e\in E_2} 2^{n(\frac{\varepsilon}{2}-H(P))} P_{c,e} \\ &= 2^{-n(1+\frac{\varepsilon}{2})} \sum_{c\in\mathcal{C}} \sum_{e\in E_2} P_{c,e}. \end{aligned}$$

Spočítáme

$$\begin{aligned} \sum_{c\in\mathcal{C}} \sum_{e\in E_2} P_{c,e} &\leq \sum_{c\in\mathcal{C}} \sum_{e\in\mathbb{F}_2^n} P[\delta Y^n = c | Y^n = c+e, X^n = c] \\ &\leq \sum_{c\in\mathcal{C}} \sum_{y\in\mathbb{F}_2^n} P[\delta Y^n = c | Y^n = y, X^n = c] \\ &\leq \sum_{y\in\mathbb{F}_2^n} \sum_{c\in\mathcal{C}} P[\delta Y^n = c | Y^n = y, X^n = c] = \sum_{y\in\mathbb{F}_2^n} 1 = 2^n, \end{aligned}$$

neboť za předpokladu, že $Y^n = y$ platí, že $\delta Y^n = c \Leftrightarrow c = \delta y$. Zbývá spojit dvě poslední nerovnosti

$$P_2 \leq 2^{-n(1+\frac{\varepsilon}{2})} \sum_{c\in\mathcal{C}} \sum_{e\in E_2} P_{c,e} \leq 2^{-n(1+\frac{\varepsilon}{2})} \cdot 2^n = 2^{-n\frac{\varepsilon}{2}} \to 0$$

pro $n \to \infty$. Dokázali jsme, že pro dostatečně velké n je $1 - {}_{\mathcal{C}}P_E^{av}$ libovolně blízké 0. Tedy pro každou posloupnost blokových kódování $C_k : S_k \to \mathbb{F}_2^{n_k}$ rostoucí délky zdrojů s nosností $\geq C_\Gamma + \varepsilon$ chyba jakéhokoli dekódování ${}_{C_k(S_k)}P_E^{av}$ roste k jedné. □

Zformulujme ještě obě Shannonovy věty v jazyce blokových kódů:

Důsledek 11.6. Prostřednictvím BSC Γ s kapacitou C_Γ lze pomocí blokového kódu dostatečné délky s nosnosti libovolně blízkou C_Γ přenést informaci s průměrnou pravděpodobností chyby dekódování metodou nejbližšího slova libovolně blízkou 0.

Naopak uniformní průměrná pravděpodobnost chyby jakéhokoli dekódování při přenosu pomocí kódu nosnosti $\geq C_\Gamma + \varepsilon$ roste $\forall \varepsilon > 0$ s délkou kódu k 1.

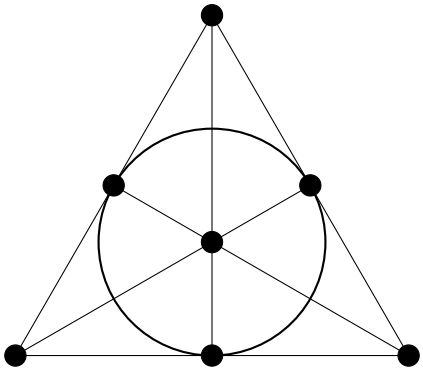
Kombinatorické konstrukce

12. Symetrické designy

T&N. Buď $X \neq \emptyset$, $\mathcal{B} \subseteq \mathcal{P}(X)$, $t, v, k, \lambda \in \mathbb{N}$. Řekneme, že $\mathcal{B}$ je $t-(v,k,\lambda)$ *design*, pokud

- $|X| = v$,
- $|B| = k \ \forall B \in \mathcal{B}$,
- $|\{B \in \mathcal{B} \mid T \subseteq B\}| = \lambda \ \forall T \subseteq X$ splňující $|T| = t$.

Příklad 12.1. Přímky Fanovy roviny, tj. projektivního prostoru $P_2(\mathbb{F}_2)$ všech jednodimenzionálních podprostorů vektorového prostoru $\mathbb{F}_3^3$ tvoří $2-(7,3,1)$ design a zároveň $1-(7,3,3)$ design



Poznámka 12.2. Nechť $\mathcal{B} \subseteq \mathcal{P}(X)$ je $2-(v,k,\lambda)$ design a $b = |\mathcal{B}|$. Potom

(1) $\lambda(v-1)v = b(k-1)k$,
(2) pokud $k > 1$, pak $\exists r$ splňující $r = |\{B \in \mathcal{B} \mid x \in B\}|\ \forall x \in X$,
(3) pro r z (2) platí, že $\lambda(v-1) = r(k-1)$ a $rv = bk$.

Důkaz. (1) Označme $W = \{(A,B) \in \mathcal{P}(X)^2 \mid B \in \mathcal{B}, A \subseteq B, |A| = 2\}$. Spočítáme počet prvků W dvěma způsoby:

Vybíráme-li nejprve B a k němu volím všechna možná A dostáváme $|W| = b \cdot \binom{k}{2}$. Vybíráme-li nejprve A a k němu volím všechna možná B podle definice dostáváme $|W| = \binom{v}{2} \cdot \lambda \Rightarrow b(k-1)k = 2|W| = \lambda(v-1)v$.

(2), (3) Položme $W_x = \{(A,B) \in W \mid x \in A\}$ a $r_x = |\{B \in \mathcal{B} \mid x \in B\}|$ pro $x \in X$. Opět spočítáme počet prvků W_x dvěma způsoby $|W_x| = r_x(k-1) = (v-1)\lambda$, kde první rovnost dostaneme při prvním výběru B a druhou při prvním výběru A. Vidíme, že $r_x = \lambda\frac{v-1}{k-1}$ nezávisí na volbě x, tedy $r = r_x$ a platí

$$r(k-1) = (v-1)\lambda \quad \Rightarrow \quad r(k-1)v = \lambda(v-1)v = b(k-1)k \quad \Rightarrow \quad rv = bk.$$

□

Pro $2-(v,k,\lambda)$ design $\mathcal{B}$ budeme značit parametry $b = |\mathcal{B}|$ a $r = |\{B \in \mathcal{B} \mid x \in B\}|$ pro $x \in X$.

T&N. Jestliže $b = v$ řekneme, že je $2-(v,k,\lambda)$ design *symetrický*.

Pozorování. Je-li $k > 1$, pak pro parametry $2-(v,k,\lambda)$ designu platí:

(1) $b = \lambda\frac{\binom{v}{2}}{\binom{k}{2}}$, $r = \lambda\frac{v-1}{k-1}$,
(2) každý $2-(v,k,\lambda)$ design je zároveň $1-(v,k,r)$ design,
(3) $k < v \Rightarrow r < b$ a $\lambda < r$.

T&N. Označme $X = \{x_1, \ldots, x_v\}$ a $\mathcal{B} = \{B_1, \ldots, B_b\} \subseteq \mathcal{P}(X)$. Pak řekneme, že je matice $M = \begin{pmatrix} i_{B_1} \\ \ldots \\ i_{B_b} \end{pmatrix} \in \mathbb{Z}^{b \times v}$ *incidenční matici* systému $\mathcal{B}$. Dále značme I_v jednotkovou matici a $J_v = (1)_{v \times v} \in \mathbb{Z}^{v \times v}$ matici, obsahující na všech pozicích 1.

Pozorování. Pro incidenční matici M systému $\mathcal{B} = \{B_1, \ldots, B_b\} \subseteq \mathcal{P}(\{x_1, \ldots, x_v\})$ položme $U = (u_{ij}) = MM^T$ a $V = (v_{ij}) = M^TM$. Potom platí:

(1) U je symetrická čtvercová, $u_{ii} = |B_i|$ a $u_{ij} = |B_i \cap B_j|$ $\forall i \neq j$,
(2) V je symetrická čtvercová, $v_{ii} = |\{s \mid x \in B_s\}|$ a $v_{ij} = |\{s \mid \{x_i, x_j\} \subseteq B_s\}|$ $\forall i \neq j$,
(3) Jeli $\mathcal{B}$ $2-(v,k,\lambda)$ design, pak $u_{ii} = k$, $v_{ii} = r$ a $v_{ij} = \lambda$ $\forall i \neq j$.

Poznámka 12.3. Nechť $\mathcal{B} \subseteq \mathcal{P}(X)$ a $k, v \in \mathbb{N}$ splňuje, že $k > 1$, $v = |X|$, $k = |B|$ $\forall B \in \mathcal{B}$ a $r = \lambda\frac{v-1}{k-1}$. Mějme dále M incidenční matici systému $\mathcal{B}$ a $U = (u_{ij}) = MM^T$ a $V = (v_{ij}) = M^TM$.

(1) Je-li M regulární čtvercová, pak $V = U \Leftrightarrow MU = UM \Leftrightarrow MV = VM$,
(2) $\mathcal{B}$ je $2-(v,k,\lambda)$ design $\Leftrightarrow v_{ii} = r$ a $v_{ij} = \lambda$ $\forall i \neq j$.

Důkaz. (1) Stačí dokázat první ekvivalenci, druhá plyne z první použité na rovněž regulární matici M^T.

($\Rightarrow$) $MM^T = U = V = M^TM \Rightarrow MU = MMM^T = MM^TM = UM$.

($\Leftarrow$) $MU = UM \Rightarrow U = M^{-1}MU = M^{-1}UM = M^{-1}MM^TM = M^TM = V$.

(2) ($\Rightarrow$) Je-li $\mathcal{B}$ $2-(v,k,\lambda)$ design, pak podle 12.2 a předchozího Pozorování (3) je $v_{ii} = r$ a $v_{ij} = \lambda$ $\forall i \neq j$.

($\Leftarrow$) Z předpokladu tvrzení víme, že podmínky $v = |X|$, $k = |B|$ $\forall B \in \mathcal{B}$ jsou splněny. Z Pozorování (2) potom plyne, že $\forall i \neq j$ $|\{B \in \mathcal{B} \mid \{x_i, x_j\} \subseteq B\}| = \lambda$ $\forall T \subseteq X$ $\forall i \neq j$, tedy se jedná o $2-(v,k,\lambda)$ design. □

Věta 12.4. Nechť $k, v \in \mathbb{N}$, $k > 1$, $\mathcal{B} \subseteq \mathcal{P}(X)$, $v = |X| = |\mathcal{B}|$, $k = |B|$ $\forall B \in \mathcal{B}$ a $r = |\{B \in \mathcal{B} \mid x \in B\}|$ $\forall x \in X$. Potom $k = r$ a platí, že

$\mathcal{B}$ je (symetrický) $2-(v,k,\lambda)$ design $\Leftrightarrow |B \cap C| = \lambda$ $\forall B \neq C \in \mathcal{B}$.

Důkaz. Všimněme si, že $\forall x \in X$

$$|\{(x,B) \mid B \in \mathcal{B}, x \in B\}| = \left\{ \begin{array}{l} |\mathcal{B}| \cdot k = v \cdot k \\ |X| \cdot r = v \cdot r \end{array} \right\} \Rightarrow k = r.$$

Podle Pozorování (1),(2) a 12.3(2) stačí dokázat

$$U = \begin{pmatrix} k & \lambda & \dots & \lambda \\ \lambda & k & \dots & \lambda \\ . & . & \dots & . \\ \lambda & \lambda & \dots & k \end{pmatrix} \Leftrightarrow V = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ . & . & \dots & . \\ \lambda & \lambda & \dots & r \end{pmatrix},$$

a protože $k = r$ budeme dokazovat jako přímou implikaci, že pokud je U uvedeného tvaru, potom $U = V$, a jako zpětnou implikaci, že pokud je V uvedeného tvaru, potom $U = V$.

($\Rightarrow$) Jestliže $k = \lambda \Rightarrow |\mathcal{B}| = |X| = 1 \Rightarrow U = V = (k)$.

Jestliže $k \neq \lambda$, pak snadno zjistíme, že $U \in \mathbb{Z}^{v \times v}$ má vlastní číslo $k - \lambda \neq 0$ geometrické násobnosti $v - 1$ a jedno vlastní číslo $k + (v-1)\lambda > 0 \Rightarrow U$ je regulární M je regulární. Podle 12.3(1) stačí ověřit $MU = UM$:

$$MU = M((k-\lambda)I_v + \lambda J_v) = (k-\lambda)MI_v + \lambda MJ_v =$$
$$= (k-\lambda)I_vM + \lambda kJ_v = ((k-\lambda)I_v + \lambda J_v)M = UM$$

$\Rightarrow U = V$

($\Leftarrow$) Důkaz je stejný jako u přímé implikace, jen pomocí 12.3(1) ověřujeme $MV = VM$. □

Příklad 12.5. Nechť $\mathcal{P} = \{\mathrm{LO}(\mathbf{v}) \mid \mathbf{v} \in \mathbb{F}_q^3 \setminus \{\mathbf{0}\}\}$, $B_V = \{p \in \mathcal{P} \mid p \subseteq V\}$, pak $\mathcal{B} = \{B_v \mid V \leq \mathbb{F}_q^3, \dim V = 2\}$ je symetrický design.

Konstrukce

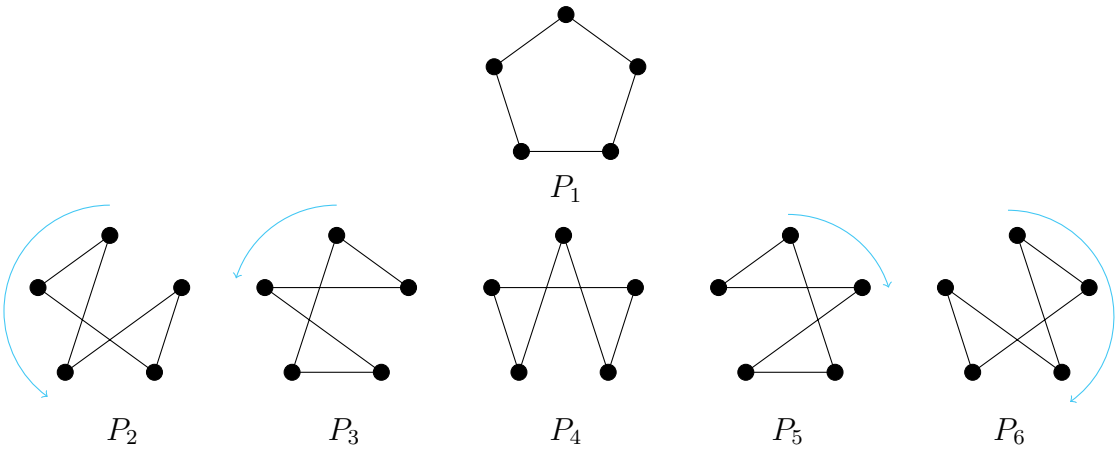
Nechť $Y = \{1, \ldots, 5\}$, $Z = \{A \subset \mathcal{P}(Y) \mid |A| = 2\}$, $\Phi = \{\sigma \in S_5 \mid \sigma^5 = 1, \sigma \neq \mathrm{id}\}$, $P_\varphi = \{\{i, \varphi(i)\} \mid i \in Y\}$ $\forall \varphi \in \Phi$.

Pozorování. Pro množiny Y, Z, Φ a P_φ a $\forall \varphi \in \Phi$ platí:

(1) $|Z| = 10$, $|\Phi| = 24$, $|\{P_\varphi \mid \varphi \in \Phi\}| = 12$,
(2) φ nemá pevný bod $\Rightarrow P_\varphi \cap P_{\varphi^2} = \emptyset$ $\forall \varphi \in \Phi$,
(3) $|P_\varphi \cap P_\psi| \geq 4 \Rightarrow P_\varphi = P_\psi$,
(4) $|P_\varphi \cap P_\psi| \leq 1 \Rightarrow |P_{\varphi^2} \cap P_\psi| \geq 4 \Rightarrow P_\varphi \cap P_\psi = \emptyset$,

Definujme množiny

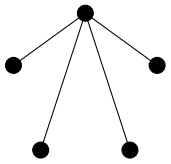
$$P_1 = P_{(12345)},\ P_2 = P_{(14235)},\ P_3 = P_{(14352)},\ P_4 = P_{(13254)},\ P_5 = P_{(13425)},\ P_6 = P_{(13542)},$$



P_1 P_2 P_3 P_4 P_5 P_6

Pozorování. Pro $\{P_1, \ldots, P_6\} \subset \{P_\varphi \mid \varphi \in \Phi\}$ je největší (vzhledem k inkluzi) takový systém, že obsahuje P_1 a $|P_i \cap P_j| = 2$ $\forall i \neq j$.

Zkonstruujme $2 - (11, 5, 2)$ design:

$X = Z \cup \{0\}$, $\forall i \in Y$: $F_i = \{\{i, a\} \mid a \in Y, a \neq i\} \cup \{0\} =$  $\cup\{0\}$.
$\mathcal{B} = \{P_i \mid i \leq 6\} \cup \{F_j \mid j \leq 5\}$

Poznámka 12.6. $\mathcal{B}$, je symetrický $2 - (11, 5, 2)$ design.

Důkaz. Důsledek Pozorování a Věty 12.4. □

13. Golayovy perfektní kódy

T&N. Nechť $\mathcal{B}_i \subseteq \mathcal{P}(X_i)$, $i = 1, 2$. Pak $\mathcal{B}_1 \cong \mathcal{B}_2$ (tj. jsou izoromfní), pokud $\exists$ bijekce $b : X_1 \to X_2$, pro níž $\mathcal{B}_2 = \{b(B) \mid B \in \mathcal{B}_1\}$.

Poznámka 13.1. Existuje až na izomorfismus právě jeden $2 - (11, 5, 2)$ design a právě jeden $2 - (11, 6, 3)$ design.

Důkaz. Existence.

Existence $2-(11,5,2)$ designu plyne z 12.6. Nechť je $\mathcal{B}$ $2-(11,5,2)$ design a definujme zobrazení $c:\mathcal{P}(X)\to\mathcal{P}(X)$ zobrazení $c(A)=X\setminus A$. Potom vidíme, že pro $\mathcal{C}=\{c(B)\mid B\in\mathcal{B}\}$ platí pro $B_1\neq B_2\in\mathcal{B}$, že $|\mathcal{C}|=11$, $|c(B)|=6$ platí, že

$|B_1\cap B_2|=2\Rightarrow|c(B_1)\cap c(B_2)|=|X\setminus(B_1\cup B_2)|=11-(|B_1|+|B_2|-|B_1\cap B_2|)=3$

a podobně pro $C_1\neq C_2\in\mathcal{C}$

$|C_1\cap C_2|=3\Rightarrow|c(C_1)\cap c(C_2)|=11-(6+6-3)=2$

Z 12.4 plyne, že $\mathcal{B}$ je $2-(11,5,2)$ design $\Leftrightarrow$ $\mathcal{C}$ je $2-(11,6,3)$ design, tedy $2-(11,6,3)$ design existuje.

Jednoznačnost.

Uvažujme $\mathcal{B}$ a $\tilde{\mathcal{B}}\subseteq\mathcal{P}(\tilde{X})$ dva $2-(11,5,2)$ designy, z nichž první je výše zkonstruovaný design $\mathcal{B}$. Najdeme mezi nimi izomorfismus.

$12.2\Rightarrow b=2\cdot\frac{(11-1)\cdot11}{(5-1)\cdot5}=11\Rightarrow\tilde{\mathcal{B}}$ je symetrický.

Zvolme $x_0\in\tilde{X}$ a definujme $\tilde{Z}=\tilde{X}\setminus\{x_0\}$. Pak $12.4\Rightarrow\exists$ právě 5 množin $\tilde{\mathcal{B}}$, které obsahují x_0, označme je $\tilde{F}_i$, $i=1,\dots5$.

Z definice designu plyne, že $\forall i<j$ $\exists$ právě jedno $x_{ij}\in\tilde{Z}$ splňující $\tilde{F}_i\cap\tilde{F}_j=\{x_0,x_{ij}\}$.

Označme $\tilde{\mathcal{P}}=\tilde{\mathcal{B}}\setminus\{\tilde{F}_i\mid i\leq5\}$. To, že $\lambda=2$ znamená, že $\{i<j\}\to x_{ij}$ je bijekce zobrazení 10-ti prvkové množiny dvojic $\{i<j\}$ na $\tilde{Z}$, proto $\tilde{Z}=\{x_{ij}\mid i<j\leq5\}$.

Definujme bijekci $b:\tilde{X}\to X$: $b(x_0)=0$ a $b(x_{ij})=\{i,j\}$. Potom $\{b(\tilde{F}_i)\}=F_i$. Pokud $P_1\notin\mathcal{P}=\{b(\tilde{B})\mid\tilde{B}\in\tilde{\mathcal{P}}\}$, změníme pořadí $\tilde{F}_i$ tak, aby $P_1\in\mathcal{P}$.

Množina $\mathcal{P}=\{b(\tilde{P})\mid\tilde{P}\in\tilde{\mathcal{P}}\}$ obsahuje P_1 a $|b(\tilde{P}_1)\cap b(\tilde{P}_2)|=2$ $\forall\tilde{P}_1\neq\tilde{P}_2\in\mathcal{P}$. Protože $|\mathcal{P}|=6$, a $P_1\in\mathcal{P}$ plyne z maximality systému $\{P_i\mid i\leq6\}$, že $\mathcal{P}=\{P_i\mid i\leq6\}$ a proto $\tilde{\mathcal{B}}=\{b(B)\mid B\in\mathcal{B}\}$.

Kdybychom měli dva neizomorfní $2-(11,6,3)$ designy, pak by je bijekce c převedla na neizomorfní $2-(11,5,2)$ designy. Proto jsou i $2-(11,6,3)$ designy určeny až na izomorfismus jednoznačně. □

T&N. Nechť N je incidenční matice $2-(11,6,3)$ designu a uvažujme blokové matice

$$E=\begin{pmatrix}1&0&\dots&0&0&1&\dots&1\\0&1&\dots&0&1&&&\\.&.&\dots&.&.&&N&\\0&0&\dots&1&1&&&\end{pmatrix},\quad G=\begin{pmatrix}1&0&\dots&0&1&\dots&1\\0&1&\dots&0&&&\\.&.&\dots&.&&N&\\0&0&\dots&1&&&\end{pmatrix},$$

kde $E\in\mathbb{F}^{12\times24}$ sestává s bloku s jednotkovou maticí I_{12} a dále s bloku tvořeným maticí N s řádkem nad a sloupcem vlevo obsahujícím na první souřadnici 0 a jinde 1 a $G\in\mathbb{F}^{12\times24}$ vznikne z E vypuštěním 13. sloupce.

Dále $\mathcal{E}$ buď $[24,12]_2$-kód s generující maticí E a $\mathcal{G}$ $[23,12]_2$-kód s generující maticí G.

1 bude značit slovo sestávající ze samých souřadnic 1.

Pozorování. Binární koule v $\mathbb{F}_2^{23}$ má

$$V_2(23,3)=\sum_{i=0}^{3}\binom{23}{i}=1+23+23\cdot11+23\cdot77=2048=2^{23-12}$$

prvků, tedy binární kód délky 23 a velikosti 2^{12} má vzdálenosti nejvýše 7 a v případě, že je vzdálenosti 7 je 3-perfektní.

Poznámka 13.2. $\mathcal{E}$ je samoduální dvojnásobně sudý $[24, 12, 8]_2$-kód a $\mathcal{G}$ je 3-perfektní $[23, 12, 7]_2$-kód.

Důkaz. Označme si řádky matice E po řadě $\mathbf{u}_1, \ldots, \mathbf{u}_{12}$ a všimněme si s využitím vlastností matice N z 12.4, že $w(\mathbf{u}_1) = 12$, $w(\mathbf{u}_i) = 8$, $w(\mathbf{u}_1 \cap \mathbf{u}_i) = 6$ $\forall i > 1$ a $w(\mathbf{u}_i \cap \mathbf{u}_j) = 4$ $\forall i > j > 1$.

Protože $\mathbf{u}_i \cdot \mathbf{u}_j = 0$ $\forall i, j$ a $|\mathcal{E}| = 2^{12}$, je $\mathcal{E}$ samoduální a podle 4.3 dvojnásobně sudý. Předpokládejme ke sporu, že $d(\mathcal{E}) = 4$, tj. $\exists I \subset \{1, \ldots, 12\}$, pro něž $\mathbf{v} = v_1 \ldots v_{24} = \sum_{i \in I} \mathbf{u}_i$ a $w(\mathbf{v}) = 4$. Označme $A = \{i \leq 12 \mid v_i = 1\}$ a $a = |A| \Rightarrow a \leq w(\mathbf{v}) = 4$, $a > 1$ a $a = |I|$.

Uvážíme-li kontrolní matici $\mathcal{E}$ podle 2.2:

$$\tilde{E} = \begin{pmatrix} 0 & 1 & \ldots & 1 & 1 & 0 & \ldots & 0 \\ 1 & & & & 0 & 1 & \ldots & 0 \\ . & & N^T & & . & . & \ldots & . \\ 1 & & & & 0 & 0 & \ldots & 1 \end{pmatrix} = \begin{pmatrix} \tilde{\mathbf{u}}_1 \\ \tilde{\mathbf{u}}_2 \\ \ldots \\ \tilde{\mathbf{u}}_{12} \end{pmatrix}.$$

mají slova $\tilde{\mathbf{u}}_i$ stejné vlastnosti jako slova $\mathbf{u}_i$, protože je N^T podle 12.4 rovněž incidenční matice $2 - (11, 6, 3)$ designu.

$\mathcal{E}$ je samoduální $\Rightarrow \tilde{E}$ je generujíc matice $\mathcal{E} \Rightarrow \exists \tilde{I} \subset \{1, \ldots, 12\}$, pro něž $\mathbf{v} = \sum_{i \in \tilde{I}} \tilde{\mathbf{u}}_i$. Pak platí $a = 4 - |\tilde{I}| > 1 \Rightarrow a = 2 \Rightarrow \exists i \neq j$, pro něž

$$4 = w(\mathbf{u}_i + \mathbf{u}_j) = w(\mathbf{u}_i) + w(\mathbf{u}_j) - 2w(\mathbf{u}_i \cap \mathbf{u}_j)) = 8,$$

což je spor.

Protože $w(\mathbf{u}_2) = 8$ a $\mathcal{E}$ je dvojnásobně sudý, dostáváme, že $\mathcal{E}$ je vzdálenosti 8.

Protože $\mathcal{G}$ vznikne z $\mathcal{E}$ propíchnutím v 13. souřadnici, jedná se podle Pozorování o 3-perfektní $[23, 12, 7]_2$-kód. □

Věta 13.3. Až na permutační ekvivalenci existuje právě jeden $[24, 12, 8]_2$-kód, který je samoduální, dvojnásobně sudý a obsahuje slova váhy 12 a 24. Kód je permutačně ekvivalentní $\mathcal{E}$ a jeho propíchnutí v kterékoli souřadnici je permutačně ekvivalentní $\mathcal{G}$.

Důkaz. Existence plyne z 13.2.

Nechť $\mathcal{C}$ splňuje předpoklady tvrzení. Pak $\exists \mathbf{u} \in \mathcal{C}$ váhy $12 \Rightarrow \mathbf{1}, \tilde{\mathbf{u}} = \mathbf{1} + \mathbf{u} \in \mathcal{C} \Rightarrow w(\mathbf{u}) = w(\tilde{\mathbf{u}}) = 12$. BÚNO (tj. permutujeme souřadnice)

$\mathbf{u} = 0 \ldots 01 \ldots 1$ a $\tilde{\mathbf{u}} = 1 \ldots 10 \ldots 0$ a propichovanou souřadnici nastavíme jako první. Nechť $I = \{13, \ldots, 24\}$ a $\pi_I : \mathbb{F}^{24} \to \mathbb{F}^{12}$ je propíchnutí v souřadnicích I.

Nechť $\mathbf{v} \in \mathcal{C} \setminus \{\mathbf{0}\}$ a $\pi_I(\mathbf{v}) = \mathbf{0} \Rightarrow$

$$w(\mathbf{u} + \mathbf{v}) + w(\mathbf{v}) = 12, w(\mathbf{v}) \geq 8 \Rightarrow w(\mathbf{u} + \mathbf{v}) \leq 4 \Rightarrow \mathbf{u} = \mathbf{v} \Rightarrow$$

$\mathrm{Ker}\pi_I = \{\mathbf{0}, \mathbf{u}\}$. Protože $\tilde{\mathbf{u}}\mathbf{c} = 0$ $\forall \mathbf{c} \in \mathcal{C}$ je $\pi_I(\mathcal{C})$ $[12, 11]_2$-kód s kontrolní maticí $\not\vdash \in \mathbb{F}_2^{1 \times 12}$ $\Rightarrow \mathcal{C}$ má generujíc matic tvaru

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 \\ 1 & & & & 0 & & & \\ . & & I_{11} & & . & & M & \\ 1 & & & & 0 & & & \end{pmatrix}.$$

Vyměníme-li její 1. a 13. sloupec dostaneme generující matici

$$\tilde{C} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 1 & \dots & 1 \\ 0 & 1 & \dots & 0 & 1 & & & \\ . & . & \dots & . & . & & M & \\ 0 & 0 & \dots & 1 & 1 & & & \end{pmatrix},$$

permutačně ekvivalentního kódu $\tilde{\mathcal{C}}$. Nyní díky 13.1 stačí ukázat, že je M incidenční matice $2-(11,6,3)$ designu.

Označme řádky matice $\tilde{C}$ po řadě $\mathbf{c}_0, \dots, \mathbf{c}_{11}$ a řádky matice M $\mathbf{v}_1, \dots, v_{11}$.

$\mathcal{C}$ dvojnásobně sudý $\Rightarrow$ 4 dělí $w(\mathbf{c}_i)$ i $w(\mathbf{c}_i + \mathbf{c}_j)$ a $d(\mathcal{C}) = 8 \Rightarrow w(\mathbf{u}_i), w(\mathbf{u}_i + uu_j) \in \{6, 10\}$.

Kdyby $w(\mathbf{u}_i) = 10 \Rightarrow w(\mathbf{c}_i + \mathbf{u}) = 2 + 2 = 4$, což je spor.

Kdyby $w(\mathbf{u}_i + \mathbf{u}_j) = 10 \Rightarrow w(\mathbf{c}_i + \mathbf{c}_j + \mathbf{u}) = 2 + 2 = 4$, což je opět spor.

Proto pro $i \neq j$

$$6 = w(\mathbf{u}_i) = w(\mathbf{u}_i + \mathbf{u}_j) = w(\mathbf{u}_i) + w(\mathbf{u}_j) - 2w(\mathbf{u}_i \cap \mathbf{u}_j) \Rightarrow w(\mathbf{u}_i \cap \mathbf{u}_j) = 3.$$

Totéž lze dokázat i pro matici M^T, neboť

$$\begin{pmatrix} 0 & 1 & \dots & 1 & 1 & 0 & \dots & 0 \\ 1 & & & & 0 & 1 & \dots & 0 \\ . & & M^T & & . & . & \dots & . \\ 1 & & & & 0 & 0 & \dots & 1 \end{pmatrix}$$

je rovněž je generujíc matice kódu $\tilde{\mathcal{C}}$.

Nyní zbývá použit 12.4

□

T&N. Buď $\mathcal{C}$ blokový kód délky n a označme $f_i = |\{\mathbf{v} \in \mathcal{C} \mid w(w) = i\}|$. Pak polynom $f_{\mathcal{C}} = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$ se nazývá váhový polynom kódu $\mathcal{C}$

Poznámka 13.4. Je-li $\mathcal{C} \subseteq \mathbb{F}_2^{23}$ blokový kód délky n vzdálenosti 7 a mohutnosti $|\mathcal{C}| = 2^{12}$, který obsahuje nulové slovo, pak je $\mathcal{C}$ nutně 3-perfektní s váhovým polynomem $f_{\mathcal{C}} = 1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$.

Důkaz. Perfektnost plyne z Pozorování a pro spočítání vah zkuste sami sestavit algoritmus na jejich výpočet (návod viz skripta Aleše Drápala). □

Věta 13.5. Až na permutační ekvivalenci existují jednoznačně určené binární kódy $\tilde{\mathcal{G}}$ a $\tilde{\mathcal{E}}$ velikosti 2^{12} obsahující nulové slovo, první délky 23 a vzdálenosti 7 a druhý délky 24 a vzdálenosti 8. Tyto kódy jsou nutně lineární a platí, že $\tilde{\mathcal{G}}$ je permutačně ekvivalentní $\mathcal{G}$, $\tilde{\mathcal{E}}$ je permutačně ekvivalentní $\mathcal{E}$ a $f_{\mathcal{E}} = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$.

Důkaz. Existence plyne z 13.2.

Nechť $\pi_i : \mathbb{F}_2^{24} \to \mathbb{F}_2^{23}$ označuje propíchnutí v i-té souřadnici. Pak je $\pi_i(\tilde{\mathcal{E}})$ kód velikosti 2^{12} obsahující nulové slovo a podle Pozorování a 13.4 je vzdálenosti 7 a tedy 3-perfektní a $f_{\pi_i(\tilde{\mathcal{E}})} = 1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$.

Protože $\forall \mathbf{u} \in \tilde{\mathcal{E}} \setminus \{\mathbf{0}, \mathbf{1}\}\ \exists j, k \leq 24$ splňující $w(\pi_j(\mathbf{u})) = w(\pi_k(\mathbf{u})) - 1$. Kód $\tilde{\mathcal{E}}$ neobsahuje slovo váhy 7, tedy všechna slova váhy 7 kódu $\pi_i(\tilde{\mathcal{E}})$ vznikla ze slov délky 8. Kdyby $\tilde{\mathcal{E}}$

obsahoval slovo váhy 11, 15 nebo 23, pak by pro vhodném i obsahoval kód $\pi_i(\tilde{\mathcal{E}})$ slovo stejné váhy, což podle 13.4 neplatí. Podobně $\tilde{\mathcal{E}}$ nemůže obsahovat slova váhy 9, 13, ani 17. Proto $f_{\tilde{\mathcal{E}}} = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24} \Rightarrow \tilde{\mathcal{E}}$ je dvojnásobně sudý $\Rightarrow \mathbf{v} + \tilde{\mathcal{E}}$ má stejné parametry, tudíž je dvojnásobně sudý $\forall \mathbf{v} \in \tilde{\mathcal{E}} \Rightarrow \tilde{\mathcal{E}}$ je lineární samoduální kód podle 4.4 $\tilde{\mathcal{E}}$ je permutačně ekvivalentní $\mathcal{E}$ podle 13.3.

Splňuje-li $\tilde{\mathcal{G}}$ předpoklady tvrzení, pak kód $\hat{E} = \{c_1 \dots c_{23} \sum_i c_i \mid c_1 \dots c_{23} \in \tilde{\mathcal{G}}\}$ má délky 24 a vzdálenosti 8 mohutnosti 2^{12} slov a obsahuje $\mathbf{0} \Rightarrow \hat{E}$ je permutačně ekvivalentní $\mathcal{E}$. Protože $\pi_{24}(\hat{E}) = \tilde{\mathcal{G}}$ je podle 13.3 permutačně ekvivalentní $\mathcal{G}$.

Zbytek plyne z 13.2. □

Důsledek 13.6. Je-li $\mathcal{C}$ binární kód velikosti 2^{12} délky 23 a váhy 7, pak $\forall \mathbf{u} \in \mathcal{C}$ je kód $\mathbf{u} + \mathcal{C}$ permutačně ekvivalentní $\mathcal{G}$.

14. Reedovy-Mullerovy kódy

V celé kapitole předpokládáme, že $r \leq m \in \mathbb{N}$, $\mathbb{F}_q$ je těleso a $n = q^m$ a slova $\mathbb{F}_q^m$ si pevně očíslujeme

$$\mathbb{F}_q^m = \{\beta_0, \beta_1, \dots, \beta_{n-1}\}.$$

T&N. Každé množině

$$\mathcal{R}_q(m, r) = \{f(\beta_0)f(\beta_1)\dots f(\beta_{n-1}) \mid f \in \mathbb{F}_q[x_1, \dots, x_m], \deg(f) \leq r\}.$$

budeme říkat q-ární Reedův-Mullerův kód (krátce RM-kód). Binární RM-kód značíme prostě $\mathcal{R}(m, r) = \mathcal{R}_2(m, r)$.

Dále označme $x_I = \prod_{i \in I} x_i$ pro každé $I \subseteq \{1, \dots, m\}$, speciálně $x_\emptyset = 1$ a definujme množiny Boolevých polynomů

$$\mathcal{BP}_m(r) = \{\sum_{I:|I| \leq r} f_I x_I \mid f_I \in \mathbb{F}_2 \forall I \subseteq \{1, \dots, m\}\},$$

speciálně $\mathcal{BP}_m = \mathcal{BP}_m(m)$ a množinu Boolevých funkcí

$$\mathcal{BF}_m = \{\mathbb{F}_2^m \to \mathbb{F}_2\}.$$

Na $\mathcal{BP}_m$ zavedeme strukturu okruhu

$$\sum_I a_I x_I \pm \sum_I b_I x_I = \sum_I (a_I \pm b_I) x_I$$
$$\sum_I a_I x_I \cdot \sum_J b_J x_J = \sum_{I,J} (a_I \cdot b_J) x_{I \cup J} = \sum_K \sum_{I,J:K=I\cup J} (a_I \cdot b_J) x_K.$$

Na $\mathcal{BF}_m$ máme k dispozici přirozeně definovanou strukturu okruhu po složkách, tj. $\forall f, g \in \mathcal{BF}_m$

$$f \pm g(\beta) = f(\beta) \pm g(\beta), \quad f \cdot g(\beta) = f(\beta) \cdot g(\beta).$$

Připomeňme, že i_J značí incidenční vektor množiny I a pro $I, J \subseteq \{1, \dots, m\}$ značme $\chi_I \in \mathcal{BF}_m$ funkci danou podmínkou $\chi_I(i_J) = 1 \Leftrightarrow J \in I$.

Konečně izomorfismus $\mathbb{F}_2$-algeber je bijekce, která tvoří izomorfismus okruhů a zároveň vektorových prostorů.

Pozorování. Pro RM kódy a Booleovy polynomy a funkce platí:

(1) $\mathcal{R}_q(m,r)$ je lineární kód délky $n = q^m$,
(2) $(\mathcal{BP}_m, +, -, \cdot, 0, 1)$ a $(\mathcal{BF}_m, +, -, \cdot, 0, 1)$ jsou komutativní okruhy,
(3) přirozená projekce $p \to [p]$ je izomorfismus $\mathbb{F}_2$-algeber
$\mathcal{BP}_m \cong \mathbb{F}_2[x_1, \ldots, x_m]/(x_1^2 + x_1, \ldots, x_m^2 + x_m)$,
(4) zobrazení $f \to (f(\beta_0), \ldots, f(\beta_{n-1}))$ je izomorfismus $\mathbb{F}_2$-algeber $\mathcal{BF}_m \cong \mathbb{F}_2^n$, kde $n = 2^m$,
(5) dosazovací zobrazení $p \to p(\beta)$ tvoří pro každé $\beta \in \mathbb{F}_2^m$ okruhový homomorfismus $\mathcal{BP}_m \to \mathbb{F}_2$,
(6) $\mathcal{R}(m,r) = \{p(\beta_0) \ldots p(\beta_{n-1}) \mid p \in \mathcal{BP}_m(r)\}$,
(7) pro každé $f \in \mathcal{BF}_m$ platí, že $f = \sum_{I:f(i_I)=1} \chi_I$,
(8) položíme-li $p_I = (\prod_{i \in I} x_i) \cdot (\prod_{i \notin I} x_i + 1)$ pro $I \subseteq \{1, \ldots, m\}$ a $p = \sum_{I:f(i_I)=1} p_I$ pro nějaké $f \in \mathcal{BF}_m$, pak $f(\beta) = p(\beta)\ \forall \beta \in \mathbb{F}_2^m$.

T&N. Pro $p = \sum_i p_I x_I \in \mathcal{BP}_m$ značme $N(p) = \{i_I \in \mathbb{F}_2^m \mid p(i_I) = 1\}$ a $\deg(p) = \max\{|I| \mid p_I \neq 0\} \cup \{-1\}$.

Poznámka 14.1. Jestliže $p \in \mathcal{BP}_m(r) \setminus \{0\}$, pak $|N(p)| \geq 2^{m-r}$.

Důkaz. Dokazujeme indukcí podle $m \geq 1$ a p stupně $\deg(p) \leq r$.

(a) Pro $m = 1$ uvažujeme polynomy tvaru $p = a_0 + a_1 x_1 \in K[x_1]$. Provedeme diskusi pro oba případy $r = 0, 1$.

Pro $r = 0$ máme $a_0 = 1$ a $a_1 = 0 \Rightarrow p = 1 \Rightarrow |N(p)| = 2 = 2^{1-0}$.

Pro $r = 1$ triviálně dostáváme $|N(p)| \geq 1 = 2^{1-1}$.

(b) Předpokládejme, že tvrzení platí pro $m - 1$ a dokážeme ho pro $m > 1$. Nechť $p = x_m g + h$, kde $g, h \in K[x_1, \ldots, x_{m-1}]$.

Pokud $g = 0$, pak $\deg h = \deg p$ a platí $h(i_1, \ldots, i_{m-1}) = 1 \Leftrightarrow p(i_1, \ldots, i_{m-1}, 0) = p(i_1, \ldots, i_{m-1}, 1) = 1$, proto s využitím indukčního předpokladu pro h

$$|N(p)| = 2|N(h)| \geq 2 \cdot 2^{m-1-r} = 2^{m-r}.$$

Pokud $g \neq 0$, pak $\deg g \leq r - 1$ a $\forall (i_1, \ldots, i_{m-1}) \in \mathbb{N}(g)$ existuje $t \in \mathbb{F}_2$ splňující $p(i_1, \ldots, i_{m-1}, t) = g(i_1, \ldots, i_{m-1})t + h(i_1, \ldots, i_{m-1}) = t + h(i_1, \ldots, i_{m-1}) = 1$, proto

$$|N(p)| \geq |N(g)| \geq 2^{m-1-(r-1)} = 2^{m-r}.$$

díky platnosti indukčního předpokladu pro g. □

T&N. Označme zobrazení $\Phi : \mathcal{BP}_m \to \mathcal{BF}_m$ dané podmínkou $\Phi(p)(\beta) = p(\beta)$.

Nadále budeme ztotožňovat $\mathcal{BF}_m \cong \mathbb{F}_2^n$ bijekcí $f \to (f(\beta_0), \ldots, f(\beta_{n-1}))$, proto lze zobrazení Φ popsat vztahem $\Phi(p) = (p(\beta_0), \ldots, p(\beta_{n-1}))$.

Pozorování. Pro zobrazení $\Phi : \mathcal{BP}_m \to \mathcal{BF}_m$ a množiny $J, Y \subseteq \{1, \ldots, m\}$ platí:

(1) Φ je izomorfismus $\mathbb{F}_2$-algeber (tj. okruhů i vektorových prostorů),
(2) $\{x_I \mid I \subseteq \{1, \ldots, m\}, |I| \leq r\}$ je báze $\mathcal{BP}_m(r)$, proto je množina $B_r = \{\Phi(x_I) \mid I \subseteq \{1, \ldots, m\}, |I| \leq r\}$ báze $\mathcal{R}(m,r)$,
(3) $w(\Phi(p)) = |N(p)|\ \forall p \in \mathcal{BP}_m$,
(4) $x_J(i_Y) = \prod_{j \in J} (i_Y)_j = 1 \Leftrightarrow J \subseteq Y$.

Věta 14.2. $\mathcal{R}(m,r)$ je $[n, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]_2$ kód.

Důkaz. Z Pozorování (1) a (2) dostáváme, že $\dim(\mathcal{R}(m,r)) = \sum_{i=0}^{r} \binom{m}{i}$.

Jestliže $|I| = r \Rightarrow x_I \in \mathcal{R}(m,r) \Rightarrow w(x_I) = |N(x_I)| = 2^{m-r}$ podle Pozorování (3) a (4) $\Rightarrow d(\mathcal{R}(m,r)) \leq 2^{m-r}$.

Naopak díky 14.1 a Pozorování (3) dostáváme $d(\mathcal{R}(m,r)) \geq 2^{m-r}$. □

Poznámka 14.3. Kódy $\mathcal{R}(m,r)$ a $\mathcal{R}(m, m-r-1)$ jsou vzájemně duální.

Důkaz. Nejprve dokážeme pro báze B_r a B_{m-r-1}, že $\forall\, \Phi(x_I) \in B_r$, $\Phi(x_J) \in B_{m-r-1}$ platí, že pro bodový součin $\Phi(x_I) \cdot \Phi(x_J) = 0$. Protože $|I| \leq r$ a $|J| \leq m-r-1$, spočítáme

$$\Phi(x_I) \cdot \Phi(x_J) = \sum_B x_I(i_B) \cdot x_J(i_B) = \sum_B x_{I \cup J}(i_B).$$

Uvědomíme-li si, že podle Pozorování (4) $x_{I\cup J}(i_B) = 1 \Leftrightarrow I \cup J \subseteq B$ a že $|I \cup J| \leq r + m - r - 1 = m - 1$ dostáváme

$$\Phi(x_I) \cdot \Phi(x_J) \equiv \sum_{B: I \cup J \subseteq B} 1 \equiv 2^{m-|I\cup J|} \equiv 0 \pmod 2.$$

Dokázali jsme, že $\mathcal{R}(m,r) \subseteq \mathcal{R}(m, m-r-1)^{\perp}$ a $\mathcal{R}(m, m-r-1) \subseteq \mathcal{R}(m,r)^{\perp}$. Protože navíc podle 14.2 $\dim \mathcal{R}(m,r) + \dim \mathcal{R}(m, m-r-1) =$

$$= \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{m-r-1} \binom{m}{i} = \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=r+1}^{m} \binom{m}{i} = 2^m$$

jsou prostory $\mathcal{R}(m,r)$ a $\mathcal{R}(m, m-r-1)$ vzájemně duální. □

Příklad 14.4. $\mathcal{R}(3,1)$ je podle 14.2 $[8,4,4]_2$ kód a má generující matici, která je zároveň podle 14.3 jeho kontrolní maticí, $\begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \end{pmatrix}$, tudíž jde o samoduální kód.

T&N. Je-li $f \in \mathcal{BP}_m$ nebo $f \in \mathcal{BF}_m$, $I, Y \subseteq \{1, \ldots, m\}$, pak definujme $f^I \in \mathcal{BF}_m$ předpisem

$$f^I(i_Y) = \sum_{B: Y \subseteq B \subseteq I \cup Y} f(i_B).$$

Pozorování. Nechť $I, J, Y \subseteq \{1, \ldots, m\}$, pak $x_J^I(i_Y) = 1 \Leftrightarrow$

$$1 = \sum_{B: Y \subseteq B \subseteq I \cup Y} x_J(i_B) = \sum_{B: J \cup Y \subseteq B \subseteq I \cup Y} 1 \Leftrightarrow J \cup Y = I \cup Y.$$

Věta 14.5. Nechť $I, Y \subseteq \{1, \ldots, m\}$, $d \in \mathbb{N}$, $f = \sum_J a_J x_J \in \mathcal{BP}_m(d)$, $I \cap Y = \emptyset$, $|I| = d$. Pak $a_I = f^I(i_Y)$.

Důkaz. Nejprve dosadíme do vyjádření $f^I(i_Y) = \sum_{B: Y \subseteq B \subseteq I \cup Y} f(i_B)$ za f:

$$f^I(i_Y) = \sum_{B: Y \subseteq B \subseteq I \cup Y} \sum_J a_J x_J(i_B) = \sum_J a_J \sum_{B: Y \subseteq B \subseteq I \cup Y} x_J(i_B) = \sum_J a_J x_J^I(i_Y).$$

Protože $I \cup Y = J \cup Y \Leftrightarrow I = J$, neboť $|J| \leq d$, $|I| = d$ a $I \cap Y = \emptyset$, dostáváme z Pozorování:

$$f^I(i_Y) = \sum_J a_J x_J^I(i_Y) = a_I.$$

□

Uvážíme pro $k = \sum_{i=0}^{r} \binom{m}{i}$ (lineární) kódování $\mathbb{F}_2^k = \mathbb{F}_2^{\{I||I|\leq r\}} \to \mathcal{BF}(m) \cong \mathbb{F}_2^n$ dané vztahem $\mathbf{v} \to \Phi(f_\mathbf{v})$, kde $f_\mathbf{v} = \sum_{I:|I|\leq r} v_I x_I$.

Na základě předchozí věty můžeme formulovat dekódovací algoritmus, který přijaté chybové slovo s váhou chyby menší než 2^{m-r-1} reprezentovaného booleovskou funkcí opraví na původní booleovský polynom:

`VSTUP:` $g \in \mathcal{BF}_m$ `splňující` $g = f + e$ `pro` $f \in \mathcal{R}(m,r)$ `a` $e \in \mathbb{F}_2^n$, $w(e) < 2^{m-r-1}$
`VÝSTUP:` $\tilde{f} \in \mathcal{BP}_m(r)$, `pro který` $d(\Phi(\tilde{f}), g) < 2^{m-r-1}$, `proto` $f = \Phi(\tilde{f})$.
`for d=r downto 0 do`
  `for all` $I \subseteq \{1,\ldots,m\} : |I| = d$ `do`
    $\alpha_0 := |\{Y \subseteq \{1,\ldots,m\} : Y \cap I = \emptyset, g^I(i_Y) = 0\}|$;
    $\alpha_1 := 2^{m-d} - \alpha_0$ $(= |\{Y \subseteq \{1,\ldots,m\} : Y \cap I = \emptyset, g^I(i_Y) = 1\}|)$;
    `if` $\alpha_0 > \alpha_1$ `then` $a_I := 0$ `else` $a_I := 1$, $g := g + \Phi(x_I)$;
`return` $\sum_{I \in \mathcal{P}_r^m} a_I x_I$.

Poznámka 14.6. Algoritmus je korektní, tj. má-li na vstupu slovo $g = f + e$ pro $f \in \mathcal{R}(m,r)$ a $e \in \mathbb{F}_2^n$ váhy $w(e) < 2^{m-r-1}$, vrátí f.

Příklad 14.7. Pro RM-kódu $\mathcal{R}(3,1)$ najdeme pomocí uvedeného algoritmu nejbližší kódové slovo a Booleův polynom, který ho kóduje, ke slovu $g = 11000100$ (tj. dekódujeme zakódované slovo k přijatému slovo g v kódování Φ) reprezentující boolovskou funkci stejně jako v Příkladu 14.4.

Budeme používat značení z algoritmu. Booleovskou funkci $\mathbf{c} \to p(\mathbf{c})$ reprezentujme slovem $p(\mathbf{c}_0)\ldots p(\mathbf{c}_7)$, kde $\mathbf{c}_i$ je právě trojice cifer z $\mathbb{F}_2$ představující binární zápis čísla i.

Nechť $d = 1$.

$I = \{1\}$: $g^{\{1\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{1\}} g(i_B) = g_0 + g_4 = 1 + 0 = 1$,
$g^{\{1\}}(i_{\{2\}}) = \sum_{B:\{2\}\subseteq B\subseteq\{1,2\}} g(i_B) = g_2 + g_6 = 0 + 0 = 0$,
$g^{\{1\}}(i_{\{3\}}) = \sum_{B:\{3\}\subseteq B\subseteq\{1,3\}} g(i_B) = g_1 + g_5 = 1 + 1 = 0$,
$g^{\{1\}}(i_{\{2,3\}}) = \sum_{B:\{2,3\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_3 + g_7 = 0 + 0 = 0$.
Tedy $\alpha_0 = 3 > \alpha_1 = 1$ a volíme $a_{\{1\}} := 0$.

$I = \{2\}$: $g^{\{2\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{2\}} g(i_B) = g_0 + g_2 = 1 + 0 = 1$,
$g^{\{2\}}(i_{\{1\}}) = \sum_{B:\{1\}\subseteq B\subseteq\{1,2\}} g(i_B) = g_4 + g_6 = 0 + 0 = 0$,
$g^{\{2\}}(i_{\{3\}}) = \sum_{B:\{3\}\subseteq B\subseteq\{2,3\}} g(i_B) = g_1 + g_3 = 1 + 0 = 1$,
$g^{\{2\}}(i_{\{1,3\}}) = \sum_{B:\{1,3\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_5 + g_7 = 1 + 0 = 1$.
Tedy $\alpha_0 = 1 < \alpha_1 = 3$ a volíme $a_{\{2\}} := 1$ a
$g := g + \Phi(x_{\{2\}}) = 11000100 + 00110011 = 11110111$.

$I = \{3\}$: $g^{\{3\}}(i_\emptyset) = \sum_{B:\emptyset\subseteq B\subseteq\{3\}} g(i_B) = g_0 + g_1 = 1 + 1 = 0$,
$g^{\{3\}}(i_{\{1\}}) = \sum_{B:\{1\}\subseteq B\subseteq\{1,3\}} g(i_B) = g_4 + g_5 = 1 + 0 = 1$,
$g^{\{3\}}(i_{\{2\}}) = \sum_{B:\{2\}\subseteq B\subseteq\{2,3\}} g(i_B) = g_2 + g_3 = 1 + 1 = 0$,

$g^{\{3\}}(i_{\{1,2\}}) = \sum_{B:\{1,2\}\subseteq B\subseteq\{1,2,3\}} g(i_B) = g_6 + g_7 = 1 + 1 = 0.$
Tedy $\alpha_0 = 3 > \alpha_1 = 1$ a volíme $a_{\{3\}} := 0$.

Nechť $d = 0$.

$I = \emptyset$: Všimněme si, že $g^{\emptyset}(i_Y) = g(i_Y)$, proto
$g^{\emptyset}(i_{\{1\}}) = g_4 = 0$ a
$g^{\emptyset}(i_I) = 1$ pro všechny zbylé množiny $I \neq \{1\}$.
Tudíž $\alpha_0 = 1 < \alpha_1 = 7$ a volíme $a_{\emptyset} := 1$.

Našli jsme booleovský polynom $x_{\{2\}} + x_{\emptyset} = x_2 + 1$, pro který snadno ověříme, že $d(g, \Phi(x_2 + 1)) = d(11000100, 11001100) = 1$. □