SAMOOPRAVNÉ KÓDY

Obsah

Motivace a obsah kurzu

Úkolem teorie kódování je vytvořit matematický model úlohy, kterou můžeme formulovat například následovně:

> *Efektivně a bez ztrát přenést informaci informačním kanálem od zdroje informace k příjemci.*

Zatímco otázkou měření obsahu informace a jeho ztráty se zabývá teorie informace, my se budeme zabývat „strukturu", která informaci nese (kódu - textu, případně jeho kódování) bez ohledu na „obsah".

Ozřejměme si význam jednotlivých složek matematického modelu:

Date: 3. ledna 2023.

Děkuji Dominiku Stejskalovi za upozornění na chyby a Adamu Klepáčovi za šablonu obvodu.

- **informační zdroj/příjemce** - strany komunikace (2 lidé, 2 stroje, vysílač přijímač apod.), model pracuje s odpovídajícími náhodnými veličinami,
- **informační kanál** - fyzikální prostředí, u nějž nás zajímá míra jeho (ne)spolehlivosti, představovaná rovněž náhodnou veličinou chyby kanálu,
- **bezztrátovost** - informace zdroje a příjemce by měla být po odhalení a opravení chyb přenosu stejná,
- **efektivita** - snaha o maximalizaci míry informace vzhledem k velikosti struktury, která informaci nese.

Teorie kódů se zabývá především posledními dvěma složkami modelu, konkrétně otázkou konstrukce efektivních kódů a jejich kódování, které poskytují postupy opravy chyb.

Rozvrh kurzu

(1) základní koncepty teorie kódů (vzdálenost, nosnost, linearita, dualita)
(2) algebraické konstrukce (konečná tělesa a polynomy nad nimi, cyklické kódy, RS, GRS, BCH kódy)
(3) kombinatorické a geometrické konstrukce (Golayovy kódy, RM kódy),
(4) úvod do konvolučních kódů.

Základní koncepty

1. Najít, opravit a neloudat se!

Nejprve zavedeme pojmy délky a vzdálenosti kódu, které nám umožní korektně pracovat s konceptem nalezení a opravení chyby přijatého slova. Hlavním výsledkem sekce budou dva vztahy (Hammingův a Singletonův) ozřejmující pro danou délku kódu protiklad schopnosti opravit chybu a velikosti.

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

T&N. Aritmetický vektor $\mathbf{v} \in \mathbb{F}^n$ budeme 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 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 $d(\mathbf{u},\mathbf{v}) > r$, tudíž $\forall \mathbf{u} \in \mathcal{C} : S(\mathbf{u},r) \cap \mathcal{C} = \{\mathbf{u}\}$.

(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 metodou nejbližšího slova: je-li $\mathbf{v}$ přijaté slovo, zvolíme takové $\mathbf{u} \in \mathcal{C}$, pro něž $S(\mathbf{v},r) \cap \mathcal{C} = \{\mathbf{u}\}$. Je-li pravděpodobnost bezchybného příjetí (q-árního) bitu větší než pravděpodobnost bitové chyby, víme z teorie informace, že se jedná o ML dekódovací schéma.

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. Z 1.2 plyne, že $2r < d(\mathcal{C})$, proto je $\{S(\mathbf{u},r) \mid \mathbf{u} \in \mathcal{C}\}$ disjunktní systém podmnožin $\mathbb{F}^n$. Nyní stačí přepočítat prvky jednotlivých množin:

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

Protože $|\mathcal{C}| = q^k$, dostáváme $V_q(n,r) \leq \frac{q^n}{q^k} = q^{n-k}$. □

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* (nebo také informační poměr) 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 nezáporné 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) pro $r > 0$ je perfektní kód r-perfektní pro (jediné) $r = \frac{d(\mathcal{C})-1}{2}$.

Příklad 1.4. (1) Kód $\mathbb{F}^n$ má vzdálenost 1, neopraví tudíž žádnou chybu a představuje (nezajímavý) 0-perfektní kód,

(2) Triviální jednoprvkový kód $\{\mathbf{0}\} \subseteq \mathbb{F}^n$ dle definice je n-perfektní kód.

(3) Je-li n liché, pak dvouprvkový binární kód $\{\mathbf{0}, 11\ldots1\} \subseteq \mathbb{F}_2^n$ opraví právě $\frac{n-1}{2}$ chyb a protože $\mathbb{F}_2^n = S(\mathbf{0}, \frac{n-1}{2}) \cup S(11\ldots1, \frac{n-1}{2})$ jde o $\frac{n-1}{2}$-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 vzdálenost jedna má totální kód $\mathbb{F}_q^n$, dostáváme $A(n,1) = n = n - 1 + 1$, 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

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

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

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

Protože $k \leq A(n, d(\mathcal{C})) \leq n - d(\mathcal{C}) + 1$, dostáváme, že $d(\mathcal{C}) \leq n - k + 1$. □

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) Všechny kódy z 1.4, tedy $\mathbb{F}^n$, $\{\mathbf{0}\}$ i $\{\mathbf{0}, 11\ldots1\} \subseteq \mathbb{F}_2^n$ pro liché n jsou MDS i perfektní kódy. Binární kód $\{\mathbf{0}, 11\ldots1\}$ je MDS avšak není perfektní pro sudá n.

(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.

2. S linearitou jde všechno lépe

V této kapitole si uvědomíme, že lineární kódy umožňují snadné kódování i testování, zda je přijaté slovo kódové, díky generující a kontrolní matici. Pouhá záměna generující a kontrolní matice ozřejmí velmi užitečný koncept dualizace kódu.

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 lineárního $\mathcal{C}$ je rovna právě $\frac{\dim(\mathcal{C})}{n}$.

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 v závislosti na tom, které z hodnot známe, 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 $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \cdots \\ \cdots \\ \mathbf{c}_k \end{pmatrix} \in \mathbb{F}^{k\times n}$ 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 $\mathcal{C}$, 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 rank $\mathbf{C} = k$, 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. Pro (blokové) kódy $\mathcal{C}, \overline{\mathcal{C}} \subseteq \mathbb{F}^n$ a permutaci $\sigma \in S_n$ označme $\mathcal{C} \sim_\sigma \overline{\mathcal{C}}$, pokud $c_1 \ldots c_n \in \mathcal{C} \Leftrightarrow c_{\sigma(1)} \ldots c_{\sigma(n)} \in \overline{\mathcal{C}}$. Řekneme, že jsou kódy $\mathcal{C}$ a $\overline{\mathcal{C}}$ *permutačně ekvivalentní* (prostřednictvím σ) jestliže existuje $\sigma \in S_n$, pro niž $\mathcal{C} \sim_\sigma \overline{\mathcal{C}}$

Pozorování. Nechť $\sigma \in S_n$, 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 $\varphi_\sigma(v) = v_{\sigma(1)} \ldots v_{\sigma(n)}$. Pak

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

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 $\mathbf{C}$ je generující matice $[n, k]$-kódu $\mathcal{C}$. Posloupností elementárních úprav (Gaussovou-Jordanovou eliminací) najdeme řádkově ekvivalentní, tedy rovněž generující matici $\mathbf{D} = (\mathbf{d}_1^T| \ldots |\mathbf{d}_n^T) \sim \mathbf{C}$ s bázovými sloupci $\mathbf{d}_{i_1}^T = \mathbf{e}_1^T, \ldots, \mathbf{d}_{i_k}^T = \mathbf{e}_k^T$ 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

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

□

Pozorování. Nechť $\mathbf{C}$ je generující a $\mathbf{H}$ kontrolní matice $[n,k]$-kódu $\mathcal{C}$ a definujme zobrazení $c : \mathbb{F}^k \to \mathbb{F}^n$ předpisem $c(\mathbf{v}) = \mathbf{vC}$.

(1) c je prosté lineární zobrazení a $\mathcal{C} = c(\mathbb{F}^k)$.
(2) Opraví-li $\mathcal{C}$ r chyb a $E_r = \{\mathbf{eH}^T \mid \mathbf{e} \in S(\mathbf{0}, r)\}$, pak pro každé $\mathbf{v} \in E_r$ existuje jediné $\mathbf{e} \in S(\mathbf{0}, r)$ pro něž $\mathbf{eH}^T = \mathbf{v}$. Hodnota $\mathbf{u}H^T$ se nazývá *syndrom* slova $\mathbf{u}$, a pokud $\mathbf{u}H^T = \mathbf{eH}^T$, pak $\mathbf{u} - \mathbf{e} \in \mathcal{C}$.
(3) Je-li $\mathbf{C} = (\mathbf{I}_k|\mathbf{A})$ matice ve standardním tvaru, pak $c(\mathbf{v}) = (\mathbf{v}|\mathbf{v}A)$ (mluvíme o *systematickém* kódování zdroje $\mathbb{F}^k$).

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 $\mathbf{He}_i^T = \mathbf{0}^T \Leftrightarrow \exists i : \mathbf{e}_i \in \mathcal{C} \Leftrightarrow d(\mathcal{C}) = 1$.

Všimněme si, že $r = n$, právě když $\mathbf{H}$ je regulární čtvercová matice, právě když $d(\mathcal{C}) = d(\{\mathbf{0}\}) = n+1$.

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

Z maximality r plyne, že $\exists \mathbf{v}$, pro které $w(\mathbf{v}) = r+1$ a $\mathbf{Hv}^T = \mathbf{0}^T$. To znamená, že $\mathbf{v} \in \mathcal{C}$ a $d \le w(\mathbf{v}) = r+1$. Tím jsme ověřili, že $d = r+1$. □

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 (všimněme si, že jsou ve sloupcích v binárním zápisu umístěny hodnoty 1 až 7), jsou nad $\mathbb{F}_2$ lineárně nezávislé. 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) $\mathcal{C}^\perp = (\mathrm{LO}\ \mathcal{C})^\perp \subseteq \mathbb{F}^n$ je lineární kód,
(3) $\mathcal{C} \subseteq \mathrm{LO}\ \mathcal{C} = (\mathcal{C}^\perp)^\perp$,
(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. Označme si řádky matic $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \cdots \\ \cdots \\ \mathbf{c}_k \end{pmatrix}$ 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 $\mathcal{C}^\perp = (\mathbf{c}_1, \ldots, \mathbf{c}_k)^\perp = \mathrm{Ker}\ \mathbf{C}$, potom $\dim \mathcal{C}^\perp = n - \mathrm{rank}\ \mathbf{C} = n - k$, jak víme z lineární algebry.

(2),(3) Je-li $\mathbf{C}$ je generující matice $\mathcal{C}$, pak Ker $\mathbf{C} = \mathcal{C}^\perp$, a proto je $\mathbf{C}$ kontrolní matice $\mathcal{C}^\perp$. Podobně, 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 $\mathcal{C} = \mathrm{Ker}\ \mathbf{H} = (\mathbf{h}_1, \ldots, \mathbf{h}_{n-k})^\perp$, 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 $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. □

Algebraické konstrukce

3. MDS-kódy, jejich duály a propíchnutí

Ukážeme si třídu snadno konstruovatelných lineárních kódů, které jsou nejlepší možné z hlediska Singletonova odhadu, a ověříme, že je uzavřená na propíchnutí i dualitu. Zároveň nahlédneme jejich hlavní nevýhodu, totiž fakt, že vzdálenost použitelných konstrukcí je shora omezena řádem tělesa.

Dříve než vyslovíme užitečnou charakterizaci, 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 $d \geq n - k + 1$, proto je $\mathcal{C}$ MDS.

(2)⇔(3) To, že je čtvercová matice regulární, právě když jsou její sloupce lineárně nezávislé, víme z lineární algebry. □

Spojením tvrzení 3.1 a 2.5 dostáváme jednoduchý důsledek:

Pozorování. Buď $\mathcal{C}$ $[n,k]$-kód s generující maticí $\mathbf{C}$. Pak $\mathcal{C}^\perp$ je MDS $\Leftrightarrow$ 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 (například) jen zpětnou implikaci.

Dokažme ji nepřímo, tedy předpokládejme, že $\mathcal{C}$ je $[n,k,d]$-kód, který není MDS. Pak $d = d(\mathcal{C}) < n-k+1$, tudíž $d \leq n-k$. Protože existuje $\mathbf{v} \in \mathcal{C}$ tak, že $0 < w(\mathbf{v}) \leq n-k$, vidíme, že $|\{i \mid v_i = 0\}| \geq k$. Z lineární algebry 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 (tedy $[n,k,n-k+1]$-kód), právě když je každých k sloupců $\mathbf{C}$ lineárně nezávislých.

Následující tvrzení ozřejmí 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 $\{\mathbf{e}_k \in \mathbb{F}^n \mid k : i \neq k \neq j\} \cup \{\mathbf{a}, \mathbf{b}\}$ 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 posloupnost implikací

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

Ověřili jsme, že pro d i d' platí stejné předpoklady a dokázané tvrzení pro kód $\mathcal{C}$ bude platit i pro duální kód $\mathcal{C}^\perp$, který je podle 3.2 rovněž MDS-kód.

Díky 2.1 můžeme bez újmy na obecnosti 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

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

Odtud okamžitě dostáváme nerovnost $k < q$ a duálně pro MDS kód $\mathcal{C}^\perp$ máme $n-k < q$, a proto $k > n-q$. Z předposlední nerovnosti konečně plyne $d = n+1-k \leq q$. □

Příklad 3.5. Dvouprvkový kód $\{\mathbf{0}, 1\ldots1\}$ je pro $k \geq 1$ 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 by z 3.4 plynulo, že $3 \leq d \leq q = 2$, tedy spor.

Uveďme univerzální konstrukci MDS kódu, jíž se budeme podrobněji zabývat v 6. sekci.

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 sloupců této matice regulární podmatici a proto jsou $\mathcal{C}_{k,\alpha}$ i $\mathcal{C}_{k,\alpha}^{\perp}$ MDS-kódy.

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 3.7. 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 žádný sloupec matice $\mathbf{C}$ není nulový, každé dva jsou různé, součet každých tří má lichou váhu, tedy není nula a součet prvních tří sloupců dá právě pátý sloupec, dává nám 2.3, že $d(\mathcal{C}) = 4$, proto jde 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 $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Kapitolu zakončíme další důležitou uzávěrovou vlastností třídy MDS kódů:

Poznámka 3.8. Buď $\mathcal{C}$ $[n, k, n-k+1]$-kód (tedy se jedná o 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 $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \dots \\ \mathbf{c}_k \end{pmatrix}$ 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 $\begin{pmatrix} \pi_I(\mathbf{c}_1) \\ \dots \\ \pi_I(\mathbf{c}_k) \end{pmatrix}$ je generující matice kódu $\pi_I(\mathcal{C})$, jejíchž každých k sloupců je lineárně nezávislých, proto je díky 3.3 kód $\pi_I(\mathcal{C})$ MDS. Tím jsme ověřili, že $\pi_I(\mathcal{C})$ je $[n-r, k, n-r-k+1]$-kód. □

4. Rozkládáme polynomy nad konečnými tělesy

V této kapitole budeme aplikovat některé výsledky Galoisovy teorie na případ konečných těles. Především nás budou s ohledem na důležitou strukturu cyklických kódů, jíž se budeme zabývat v následující kapitole, zajímat ireducibilní rozklady polynomů $x^n - 1$. Nejdůležitějším nástrojem pro tento úkol budou cyklotomické polynomy, o nichž dokážeme, že na rozdíl od celočíselných cyklotomických polynomů, důležitých v teorii čísel, nemusí být ireducibilní.

$\mathbb{F}$ v celé kapitole značí konečné těleso (prvočíselné) charakteristiky p, čísla n a k jsou přirozená. Nejprve připomeňme popis konečných těles z přednášky Algebra (v loňské verzi skript Davida Stanovského uvedené výsledky najdete ve 24. a 16. kapitole):

Fakt 4.1. Pro konečné těleso $\mathbb{F}$ charakteristiky p a přirozené číslo q platí:

(1) Existuje těleso $\mathbb{F}$ velikosti $q \Leftrightarrow$ existuje n, pro něž $|\mathbb{F}| = p^n$,
(2) jestliže $p^n = |\mathbb{F}|$ pak je $\mathbb{F}$ izomorfní rozkladovému nadtělesu polynomu polynomu $x^{p^n} - x$ nad $\mathbb{F}_p$ a $x^{p^n} - x = \prod_{a \in \mathbb{F}}(x - a)$,
(3) pro každé k existuje ireducibilní polynom m stupně k nad tělesem $\mathbb{F}_p$, pro který $\mathbb{F}_p[x]/(m) \cong \mathbb{F}_{p^k}$,
(4) $\mathbb{F}_q^*$ je cyklická grupa a pro každé $k|(q-1)$ existuje právě jedna podgrupa $\mathbb{F}_q^*$ řádu k.

T&N. Až na izomorfismus jednoznačně určené těleso o p^n prvcích se značí $\mathbb{F}_{p^n}$ (a obvykle se nazývá *Galoisovo* těleso řádu p^n).

Zobrazení $f_{p^k} : \mathbb{F} \to \mathbb{F}$ určené předpisem $f_{p^k}(a) = a^{p^k}$ nazveme *Frobeniův endomorfismus*

Pozorování. Uvažujme $P := \langle 1 \rangle$ a a $U_k := \{t \in \mathbb{F} |\ f_{p^k}(t) = t\}$, pak platí:

(1) f_p je automorfismus a $f_{p^k} = f_{p^{k-1}} \circ f_p$,
(2) $P \subseteq U_k$ jsou podtělesa tělesa $\mathbb{F}$ a $U_1 = P \cong \mathbb{Z}_p$,
(3) f_{p^k} je U_k-automorfismus tělesa $\mathbb{F}$.

T&N. Podtělesu P tělesa $\mathbb{F}$ z Pozorování budeme říkat *prvotěleso* tělesa $\mathbb{F}$.

Poznámka 4.2. Nechť p je prvočíslo, k, n, r přirozená čísla, $q = p^r$. Pak jsou následující tvrzení ekvivalentní:

(1) $k|n$ v oboru $\mathbb{Z}$,

(2) $(p^k-1)|(p^n-1)$ v oboru $\mathbb{Z}$,
(3) $(q^k-1)|(q^n-1)$ v oboru $\mathbb{Z}$,
(4) $(x^{q^k}-x)|(x^{q^n}-x)$ v oboru $\mathbb{F}[x]$.

Důkaz. (1)⇒(2) Jestliže $n=kd$, snadno spočítáme, že $p^n-1=(p^k-1)\sum_{i=0}^{d-1}p^{ik}$.
(2)⇒(1) Nechť $(p^k-1)|(p^n-1)$ a $n=kd+r$, kde $0\le r<k$. Víme, že

$$p^{kd}-1=(p^k-1)\sum_{i=0}^{d-1}p^{ik},\quad \text{tedy}\quad (p^k-1)|((p^n-1)-p^r(p^{kd}-1)).$$

Protože $(p^n-1)-p^r(p^{kd}-1)=p^r-1$, máme $(p^k-1)|(p^r-1)$. Ovšem $r<k$, proto $r=0$.
(1)⇔(3) Stačí uvážit, že $k|n \Leftrightarrow rk|rn$ a to je dle dokázané ekvivalence ekvivalentní tvrzení $(q^k-1)=(p^{rk}-1)|(p^{rn}-1)=(q^n-1)$.
(3)⇔(4) Použijeme obdobný argument jako v důkazu (1)⇔(2), je-li totiž $(q^n-1)=s(q^k-1)$, pak $(x^{q^n}-x)=x(x^{q^k-1}-1)\sum_{i=0}^{s-1}x^{i(q^k-1)}$, což dokazuje implikaci (3)⇒(4). Obdobně, pokud $(x^{q^k-1}-1)|(x^{q^n-1}-1)$ a vydělíme-li se zbytkem $q^n-1=s(q^k-1)+r$, pak i $(x^{q^k-1}-1)$ dělí $(x^{q^n-1}-1)-x^r(x^{s(q^k-1)}-1)=x^r-1$, odkud opět kvůli argumentu $r<q^k-1$ dostáváme, že $r=0$, a proto $(q^k-1)|(q^n-1)$. □

Poznámka 4.3. Nechť q je přirozené číslo. Pak existuje podtěleso tělesa $\mathbb{F}_{p^n}$ o q prvcích, právě když existuje $k|n$, pro které $q=p^k$. Podtěleso dané velikosti je určeno jednoznačně.

Důkaz. (⇒) Víme, že podtěleso U řádu q má charakteristiku p, proto podle 4.1(2) existuje $k\ge 1$, pro něž $q=p^k$. Z Lagrangeovy věty použité pro $U^*\le\mathbb{F}_{p^n}^*$ plyne, že $(p^k-1)|(p^n-1)$, tudíž $k|n$ díky 4.2.
(⇐) Podle 4.1(2) jsou všechny prvky $\mathbb{F}_{p^n}$ kořeny polynomu $x^{p^n}-x$ a $k|n$, tudíž podle 4.2 $(x^{p^k}-x)|(x^{p^n}-x)$ a $U_k=\{t\in\mathbb{F}_{p^n}|\ f_{p^k}(t)=t\}$ je podtěleso složené právě z p^k kořenů polynomu $x^{p^k}-x$. Tedy U_k je hledané podtěleso řádu p^k. □

Nyní si uvědomíme, že $x^{q^n}-x$ poskytuje všechny ireducibilní polynomy stupně n nad tělesem řádu q.

Věta 4.4. Je-li $m\in\mathbb{F}_q[x]$ ireducibilní polynom stupně k, pak m dělí $x^{q^n}-x \Leftrightarrow k/n$.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že je m monický.
(⇒) Protože m dělí $x^{q^n}-x=\prod_{a\in\mathbb{F}_{q^n}}(x-a)$, existuje podle 4.1(2) $\alpha\in\mathbb{F}_{q^n}$, které je kořenem m, což znamená, že je m minimální polynom prvku α nad $\mathbb{F}_q$. Proto

$$[\mathbb{F}_q(\alpha):\mathbb{F}_q]=\deg(m)=k,$$

tedy $|\mathbb{F}_q(\alpha)|=q^k$, kde $q=p^s$ pro vhodné přirozené s, a podle 4.3 tak dostáváme, že $ks|ns$ a tudíž $k|n$.
(⇐) Známá konstrukce nám říká, že $\mathbb{F}_q[x]/(m)$ kořenové nadtěleso polynomu m nad tělesem $\mathbb{F}_q$ řádu q^k. To je podle 4.1(3) izomorfní tělesu $\mathbb{F}_{q^k}$, které rozkladovým nadtělesem polynomu $x^{q^k}-x$ nad tělesem $\mathbb{F}_p$ a tudíž i nad tělesem $\mathbb{F}_q$, které je podle 4.3 obsaženo v $\mathbb{F}_{q^k}$. Protože existuje společný kořen $\alpha\in\mathbb{F}_{q^k}$ polynomů m a $x^{q^k}-x$, je polynom m opět minimální polynom prvku α nad $\mathbb{F}_q$, a protože díky 4.2 $(x^{q^k}-x)|(x^{q^n}-x)$, dostáváme, že $m|(x^{q^k}-x)|(x^{q^n}-x)$. □

Důsledek 4.5. Polynom $x^{q^n} - x$ je právě součinem všech monických ireducibilních polynomů stupně $k|n$ v $\mathbb{F}_q[x]$.

T&N. Symbolem $\mathbb{F}_{(n)}$ budeme značit rozkladové nadtěleso polynomu $x^n - 1$ nad $\mathbb{F}$ a $\mathbb{E}_{(n)} = \{\alpha \in \mathbb{F}_{(n)} \mid \alpha^n = 1\}$.

Pozorování. Nechť $k > 0$.

(1) $\mathbb{E}_{(n)}$ je podgrupa $\mathbb{F}^*_{(n)}$, tedy cyklická grupa,
(2) pokud p nedělí n, pak $x^n - 1$ má v $\mathbb{F}_{(n)}$ právě n jednoduchých kořenů, $|\mathbb{E}_{(n)}| = n$ a $x^n - 1 = \prod_{\alpha \in \mathbb{E}_{(n)}} (x - \alpha)$,
(3) pokud $n = p^k \cdot m$ a p nedělí m, pak $x^n - 1 = (x^m - 1)^{p^k}$ má v $\mathbb{F}_{(n)}$ právě m kořenů násobnosti p^k, $|\mathbb{E}_{(n)}| = m$ a $x^n - 1 = \prod_{\alpha \in \mathbb{E}_{(n)}} (x - \alpha)^{p^k}$.

Příklad 4.6. (1) Pro $q = |\mathbb{F}|$, $n = q^r - 1$ máme $x^n - 1 = \frac{x^{q^r} - x}{x}$, proto $\mathbb{F}_{(n)} = \mathbb{F}_{q^r}$ a $\mathbb{E}_{(n)} = \mathbb{F}^*_{q^r}$.
(2) Tedy pro $\mathbb{F}_3$ dostáváme
(a) $x^2 - 1 = (x - 1)(x + 1)$, $\mathbb{F}_{(2)} = \mathbb{F}_3$ a $\mathbb{E}_{(2)} = \mathbb{F}^*_3 = \{1, 2\}$.
(b) $x^8 - 1 = \prod_{a \in \mathbb{F}^*_9} (x - a)$ $\mathbb{F}_{(8)} = \mathbb{F}_9$ a $\mathbb{E}_{(8)} = \mathbb{F}^*_9$.

Definice. Označme $\mathbb{P}_{(n)}$ množinu všech generátorů grupy $\mathbb{E}_{(n)}$. Pokud charakteristika tělesa nedělí n, budeme prvkům $\mathbb{P}_{(n)}$ říkat *primitivní n-té odmocniny z jedné* a polynomu $Q_n = \prod_{\alpha \in \mathbb{P}_{(n)}} (x - \alpha) \in \mathbb{F}_{(n)}[x]$ n-tý *cyklotomický polynom.*

Připomeňme, že symbol φ značí Eulerovu funkci.

Pozorování. Nechť $\mathbb{F}$ je těleso charakteristiky p a nechť p nedělí n.

(1) $\mathbb{E}_{(n)} = \bigcup_{k|n} \mathbb{P}_{(k)}$ a sjednocení je disjunktní,
(2) $\deg(Q_n) = |\mathbb{P}_{(n)}| = \varphi(n)$,
(3) pokud $\alpha \in \mathbb{P}_{(n)}$, pak $\mathbb{F}_{(n)} = \mathbb{F}(\alpha)$.

Věta 4.7. Nechť $q = p^r$, p nedělí n, P je prvotěleso tělesa $\mathbb{F}_q$, tj. $P = \mathbb{F}_p$ a d značí řád prvku $(q) \bmod n$ v $\mathbb{Z}^*_n$ (tj. nejmenší kladné d, pro něž $q^d \equiv 1 \pmod{n}$). Potom

(1) $x^n - 1 = \prod_{k|n} Q_k$,
(2) $Q_n \in P[x]$,
(3) Q_n se rozkládá na právě $\frac{\varphi(n)}{d}$ ireducibilních polynomů stupně $d = [\mathbb{F}_{(n)} : \mathbb{F}]$.

Důkaz. (1) Rovnost $x^n - 1 = \prod_{\alpha \in \mathbb{E}_n} (x - \alpha) = \prod_{k|n} Q_k$ plyne z 4.1(2), definice a Pozorování (1).

(2) Indukcí podle n nesoudělného s p nahlédneme, že $Q_n \in P[x]$. Pro $n = 1$ tvrzení platí a nyní předpokládejme, že pro všechna $k < n$, pro která $k|n$, platí $Q_k \in P[x]$. Potom podle (1)

$$Q_n = \frac{x^n - 1}{\prod_{k|n, k<n} Q_k} \in P[x].$$

(3) Uvažme prvek $\alpha \in \mathbb{P}_{(n)}$. Potom díky Lagrangeově větě máme

$$\alpha \in \mathbb{F}^*_{q^k} \Leftrightarrow \alpha^{q^k - 1} = 1 \Leftrightarrow n | q^k - 1 \Leftrightarrow q^k \equiv 1 (\bmod\ n).$$

Proto je-li d řád prvku $(q)\mathrm{mod}\ n$ v $\mathbb{Z}_n^*$, pak podle předchozího pozorování $\alpha \in \mathbb{F}_{q^d}$ a $\alpha \notin \mathbb{F}_{q^i}$ pro všechna $i < d$, tudíž podle 4.3 dostáváme $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$. Je-li nyní m monický ireducibilní faktor Q_n nad $\mathbb{F}_q$, existuje $\alpha \in \mathbb{P}_{(n)}$, pro které $m(\alpha) = 0$, tedy jde o minimální polynom α nad $\mathbb{F}_q$ a podle známého tvrzení z algebry

$$\deg(m) = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^d} : \mathbb{F}_q] = d.$$

Konečně počet polynomů plyne z Pozorování (2). □

Příklad 4.8. (1) Nad $\mathbb{F}_2$ máme

$$Q_1 = x - 1,\ Q_3 = \frac{x^3 - 1}{x - 1} = x^2 + x + 1,\ Q_5 = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1.$$

Potom $Q_{15} = \frac{x^{15}-1}{Q_1 Q_3 Q_5}$.

Zřejmě jsou Q_1 a Q_3 ireducibilní a protože 2 má v $\mathbb{Z}_5^*$ řád 4, je ireducibilní podle 4.7(2) Q_5. 2 má i v $\mathbb{Z}_{15}^*$ řád 4 a Q_{15} je stupně 8, tudíž je součinem dvou ireducibilních polynomů stupně 4.

Dále $x^{30}-1 = (x^{15}-1)^2 = Q_1^2 Q_3^2 Q_5^2 Q_{15}^2$, tedy $x^{30}-1$ má právě 10 ireducibilních faktorů.

(2) Protože 4 má i v $\mathbb{Z}_{15}^*$ řád 2, 8 má i v $\mathbb{Z}_{15}^*$ řád 4 a 16 má i v $\mathbb{Z}_{15}^*$ řád 1, rozkládá se Q_{15} na 4 ireducibilní faktory nad $\mathbb{F}_4$, na 2 ireducibilní faktory nad $\mathbb{F}_8$ a na kořenové činitele nad $\mathbb{F}_{16}$.

5. Cyklické kódy

Cílem kapitoly je kompletní popis třídy lineárních kódů uzavřených na cyklické posunutí souřadnic, kterým se říká cyklické kódy. Ukážeme, že všechny lze nahlížet jako hlavní ideály faktorových okruhů $\mathbb{F}[x]/(x^n - 1)$ určené právě děliteli polynomu $x^n - 1$.

Předpokládáme, že $n > 1$ je přirozené a souřadnice slov délky n budeme indexovat $\mathbf{c} = c_0 c_1 \dots c_{n-1}$, tedy čísly $0, \dots, n-1$.

Definice. Kód $\mathcal{C} \subseteq \mathbb{F}^n$ je *cyklický*, pokud pro každé slovo $c_0 c_1 \dots c_{n-2} c_{n-1} \in \mathbb{F}^n$ platí implikace $c_0 c_1 \dots c_{n-2} c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1} c_0 \dots c_{n-3} c_{n-2} \in \mathcal{C}$.

Příklad 5.1. (1) Kód $\mathcal{C}_1 = \{0123, 3012, 2301, 1230\} \subset \mathbb{F}_5^4$ je nelineární cyklický.

(2) Kód $\mathcal{C}_2 = \mathrm{LO}(1111) \subset \mathbb{F}_5^4$ je lineární cyklický.

(3) Všimněme si, že sjednocení cyklických kódů stejné délky nad stejným tělesem, tedy například $\mathcal{C}_1 \cup \mathcal{C}_2$, tvoří opět cyklický kód.

T&N. Uvažujme zobrazení $\nu : \mathbb{F}^n \to \mathbb{F}[x]/(x^n - 1)$ dané vztahem $\nu(c_0 c_1 \dots c_{n-1}) = [\sum_{i=0}^{n-1} c_i x^i]$, 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 izomorfismus okruhů a zároveň vektorových prostorů,
(3) je-li $\mathbf{e} = \nu^{-1}([1x])$, pak $\mathbf{e} = 010\ldots00$ a

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

(4) $\mathbb{F}[x]/(x^n-1)$ a $\mathbb{F}[x]_n$ jsou izomorfní 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 , právě když je $\nu(\mathcal{C})$ ideál okruhu $\mathbb{F}[x]/(x^n-1)$.

($\Rightarrow$) Nechť $\mathcal{C}$ je cyklický lineární kód. Potom je $\nu(\mathcal{C})$ 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 $\forall [p] \in \nu(\mathcal{C})$ $[x^i] \cdot [p] = [x] \cdot [x^{i-1}] \cdot [p] \in \nu(\mathcal{C})$, z čehož plyne, že pro každý polynom $\sum_i a_i x^i \in \mathbb{F}[x]$ dostáváme

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

($\Leftarrow$) 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 $\mathcal{C}(f)$ 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 $a = \sum_{i=0}^{k-1} a_i x^i$, pak

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

tudíž je $\mathbf{C}$ 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

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

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 $0 \le j \le n-k-1$, a proto $1 \le s \le n-1$.

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

Jakmile 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 délky 3. 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

V této kapitole kapitole se vrátíme ke konstrukcím MDS kódů a ukážeme, že klasická Reedova-Solomonova konstrukce představuje cyklický MDS kód. Zavedeme rovněž obecný pojem reziduálního kódu, který nám umožní některé vlastnosti kódů vybudovaných nad velkým tělesem převést do kódů nad jejich podtělesy.

Uvažujme, že charakteristika p nedělí n a připomeňme, že $\mathbb{F}_{(n)}$ značí rozkladové nadtěleso polynomu $x^n - 1$ nad $\mathbb{F}$.

Zobecněme konstrukci MDS kódu z Příkladu 3.6:

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

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

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

$\mathcal{C}$ se nazývá

- *normovaný* GRS kód, pokud $v_i = 1\ \forall i$,
- *Reedův-Solomonův* (RS), pokud $\exists \alpha \in \mathbb{F}^*$ řádu n a $0 \le b < n$ tak, že $\alpha_i = \alpha^{i-1}$ a $v_i = \alpha^{b(i-1)}$.

Pozorování. Uvažujme předpoklady předchozí terminologické poznámky a $0 < k < n$.

(1) GRS kódy jsou MDS díky 3.1 a 3.6,

(2) RS kód má pro $r = n-k-1$ a $0 \le b < n$ generující a kontrolní matici tvaru:

$$\begin{pmatrix} 1 & \alpha^{n-b+1} & \alpha^{2(n-b+1)} & \ldots & \alpha^{(n-1)(n-b+1)} \\ 1 & \alpha^{n-b+2} & \alpha^{2(n-b+2)} & \ldots & \alpha^{(n-1)(n-b+2)} \\ . & . & \ldots & . & \\ . & . & \ldots & . & \\ 1 & \alpha^{n-b+k} & \alpha^{2(n-b+k)} & \ldots & \alpha^{(n-1)(n-b+k)} \end{pmatrix}, \quad \begin{pmatrix} 1 & \alpha^{b} & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ . & . & \ldots & . & \\ . & . & \ldots & . & \\ 1 & \alpha^{b+r} & \alpha^{2(b+r)} & \ldots & \alpha^{(n-1)(b+r)} \end{pmatrix},$$

protože hodnost první matice je k, druhé $n-k$ a bodový součin i-tého a j-tého řádku, kde $1 \le i \le k$ a $0 \le j \le n-k-1$, a proto $j \le i+j \le n-1$, je

$$\sum_{s=0}^{n-1} \alpha^{s(n-b+i)}\alpha^{s(b+j)} = \sum_{s=0}^{n-1} \alpha^{s(n-b+i+b+j)} = \sum_{s=0}^{n-1} \alpha^{s(i+j)} = \frac{\alpha^{n(i+j)}-1}{\alpha^{i+j}-1} = 0.$$

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

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

pro všechna $i = 0, \ldots, k-1$ a $j = 0, \ldots, n-k-1$, což je ekvivalentní rovnosti $\mathbf{H}^{n-1}_{\underline{\alpha}}\mathbf{v} = \mathbf{0}$. To znamená, že $\mathbf{v}$ řeší homogenní soustavu s maticí

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

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 $\mu(\mathbf{u}) = \sum_{i=0}^{n-1} u_i x^i \ \forall\ \mathbf{u} = u_0 \ldots u_{n-1} \in \mathbb{F}^n$ (tedy $\nu(\mathbf{u}) = [\mu(\mathbf{u})]$).

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

(2) Jestliže $\alpha_i \in \mathbb{F}_{(n)}$ je kořen $x^n - 1$, m_i je minimální polynom prvku α_i nad tělesem $\mathbb{F}$ pro $i = 1, \ldots, r$ 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 monický polynom g, který dělí $x^n - 1$ a platí, že $\mathcal{C} = \mathcal{C}(g)$. Protože $\mathrm{NSD}(x^n - 1, nx^{n-1}) = 1$, jsou všechny kořeny polynomů $x^n - 1$ i g jednoduché, a proto existuje podmnožina $L \subseteq \mathbb{E}_{(n)} = \{\alpha \in \mathbb{F}_{(n)} \mid \alpha^n = 1\}$ splňující $g = \prod_{\alpha \in L} x - \alpha$. Nyní snadno nahlédneme, že platí řada ekvivalencí

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

Proto $g = f$, $L = M$ a $\mathcal{C} = \mathcal{C}(g) = \mathcal{C}(f)$.

(2) Položme $f = \mathrm{nsn}_{i \leq r}(m_i)$. Protože $\mathbf{u} \in \mathcal{C}$, platí, že $m_i | \mu(\mathbf{u})\ \forall i$, z čehož plyne, že $f | \mu(\mathbf{u})$, a tudíž $\mathbf{u} \in \mathcal{C}(f)$.

Naopak, vezmeme-li $\mathbf{u} \in \mathcal{C}(f)$, pak $f | \mu(\mathbf{u})$, a proto $\mu(\mathbf{u})(\alpha_i) = 0$ pro všechna i, odkud dostáváme, že $\mathbf{u} \in \mathcal{C}$.

Dokázali jsme, 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 $v_i = \alpha^{b(i-1)}$). Pak $\mathbf{u} \in \mathcal{C}$, právě když

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

což nastává, právě když $\mu(\mathbf{u})(\alpha^{b+i}) = 0\ \forall i < n-k$. Tedy $\mathcal{C}$ je cyklický podle 6.1(2). $\square$

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.

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

Protože jsou RS kódy cyklické, dostáváme z posledního pozorování, že

Důsledek 6.3. BCH kódy jsou cyklické.

Příklad 6.4. 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) $\mathrm{LO}(\beta\alpha 1\beta, \alpha\beta 1\alpha) \cap \mathbb{F}_2^4 = \mathrm{LO}(1101, 1011)$.

Pozorování. Nechť $\alpha_i \in (\mathbb{F}_{q^r})_{(n)}$, $\alpha_i^n = 1$ 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.

Věta 6.5 (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. Protože je $\mathcal{C}$ MDS a proto platí, že $D = n - l + 1$, dostáváme rovnost $n - l = D - 1$. Dokážeme-li nerovnost $n - k \le r(n-l)$, snadno z ní odvodíme 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 $\tilde{\mathcal{C}}$ a zvolíme nějakou kontrolní matici $\mathbf{H} = \begin{pmatrix} \mathbf{h}_1 \\ \dots \\ \mathbf{h}_{n-l} \end{pmatrix} \in \mathbb{F}_{q^r}^{(n-l)\times n}$ kódu $\mathcal{C}$ s řádky $\mathbf{h}_i$. Označíme $\beta_1, \dots, \beta_r$ nějakou bázi $\mathbb{F}_{q^r}$ nad $\mathbb{F}_q$ a uvážíme, že existuje posloupnost vektorů $\mathbf{a}_{ji} \in \mathbb{F}_q^n$ pro všechna $i = 1, \dots, n-l$ a $j = 1, \dots, r$ splňující $\mathbf{h}_i = \sum_{j=1}^r \beta_j \mathbf{a}_{ji}$. Nyní definujme matice

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

Všimneme si, že $\mathbf{u} \in \tilde{\mathcal{C}}$, právě když $\mathbf{u} \in \mathcal{C}$ a $\mathbf{u} \in \mathbb{F}_q^n$, což je ekvivalentní tomu, že $\mathbf{u}\mathbf{H}^T = \mathbf{0}$ a $\mathbf{u} \in \mathbb{F}_q^n$ a to nastává, právě když $\mathbf{u}\tilde{\mathbf{H}}^T = \mathbf{0}$ 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 $\operatorname{rank}\tilde{\mathbf{H}} \leq (n-l)r$, což je počet řádků $\tilde{\mathbf{H}}$. Dokázali jsme, že $n - k \leq (n-l)r$. □

Protože BCH i alternantní $[n,k,d]_q$-kódy jsou reziduálními kódy MDS $[n,l,D]_{q^r}$-kódů, odhady $k \geq n - r(D-1)$ a $d \geq \frac{n-k}{r} + 1$ platí.

Příklad 6.6. Uvažujme těleso $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ pro α splňující $\alpha^2 + 1 = 0$ a nad ním GRS $[6,4,3]_9$ 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 6.5 matici $\tilde{\mathbf{H}}$, pro níž platí, že $\tilde{\mathcal{C}} = \mathrm{Ker}\tilde{\mathbf{H}}$. K tomu zvolíme bázi $1, \alpha$ prostoru $\mathbb{F}_9$ nad $\mathbb{F}_3$.

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

Odtud vidíme, že alternantní kód $\tilde{\mathcal{C}}$ je $[6,3]_3$-kód a z 6.5 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.

Kombinatorické konstrukce

7. Reedovy-Mullerovy kódy

Binární Reedovy-Mullerovy kódy představují třídu snadno konstruovatelných lineárních kódů, které disponují efektivním dekódovacím algoritmem. Výhodou konstrukce je předem známá vzdálenost kódu a fakt, který v této kapitole rovněž ověříme, že tentýž postup můžeme použít i pro vytvoření duálního kódu.

V celé kapitole předpokládáme, že $r \leq m \in \mathbb{N}$, $n = 2^m$ a slova $\mathbb{F}_2^m$ si pevně očíslujeme

$$\mathbb{F}_2^m = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}.$$

T&N. Každé množině

$$\mathcal{R}(m,r) = \{f(\beta_0)f(\beta_1)\ldots f(\beta_{n-1}) \in \mathbb{F}_2^n \mid f \in \mathbb{F}_2[x_1,\ldots,x_m], \deg(f) \leq r\}.$$

budeme říkat binární *Reedův-Mullerův* kód (krátce RM-kód).

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

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

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 pomocí přirozených operací:

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

pro libovolné $f, g \in \mathcal{BF}_m$.

Konečně, $i_J = i_1 \ldots, i_n$ je incidenční vektor množiny I, tj. $i_j = 1 \Leftrightarrow j \in J$ a pro $I, J \subseteq \{1, \ldots, m\}$ značme $\chi_I \in \mathcal{BF}_m$ funkci danou podmínkou $\chi_I(i_J) = 1 \Leftrightarrow J = I$.

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

(1) $\mathcal{R}(m, r) = \{p(\beta_0) \ldots p(\beta_{n-1}) \mid p \in \mathcal{BP}_m(r)\}$ je lineární kód délky $n = 2^m$,
(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 okruhů $\mathcal{BP}_m \cong \mathbb{F}_2[x_1, \ldots, x_m]/(x_1^2 + x_1, \ldots, x_m^2 + x_m)$,
(4) zobrazení $f \to (f(\beta_0), \ldots, f(\beta_{n-1}))$ je izomorfismus okruhů $\mathcal{BF}_m \cong \mathbb{F}_2^n$, kde $n = 2^m$,
(5) pro každé $f \in \mathcal{BF}_m$ platí, že $f = \sum_{I:f(i_I)=1} \chi_I$,

Všimněme si, že všechny tři uvažované izomorfní okruhy jsou zároveň vektorové prostory nad tělesem $\mathbb{F}_2$ (tedy $\mathbb{F}_2$-algebry), proto jsou všechny jejich okruhové izomorfismus zároveň izomorfismy vektorových prostorů nad $\mathbb{F}_2$.

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 7.1. 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 $a_1 = 0$, proto $p = 1$ a $|N(p)| = 2 = 2^{1-0}$.

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 $g, h \in \mathbb{F}_2[x_1, \ldots, x_{m-1}]$.

Pokud $g = 0$, pak $\deg h = \deg p$ a platí ekvivalence

$$h(i_1, \ldots, i_{m-1}) = 1 \;\Leftrightarrow\; p(i_1, \ldots, i_{m-1}, 0) = p(i_1, \ldots, i_{m-1}, 1) = 1,$$

proto s využitím indukčního předpokladu pro h dostáváme, že

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

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) Položíme-li $p_J = (\prod_{i \in J} x_i) \cdot (\prod_{i \notin J} x_i + 1)$, pak $\Phi(p_J) = \chi_J$, proto pokud $p = \sum_{I:f(i_I)=1} p_I$ pro $f \in \mathcal{BF}_m$, pak $\Phi(p) = \sum_{I:f(i_I)=1} \Phi(p_I) = \sum_{I:f(i_I)=1} \chi_I = f$,
(2) Φ je izomorfismus okruhů (i vektorových prostorů),
(3) $\{x_I \mid I \subseteq \{1, \ldots, m\}, |I| \leq r\}$ je báze prostoru $\mathcal{BP}_m(r)$, proto je její izomorfní obraz $B_r = \{\Phi(x_I) \mid I \subseteq \{1, \ldots, m\}, |I| \leq r\}$ báze prostoru $\mathcal{R}(m, r)$,
(4) $w(\Phi(p)) = |N(p)|$ $\forall p \in \mathcal{BP}_m$,
(5) $x_J(i_Y) = \prod_{j \in J}(i_Y)_j = 1 \Leftrightarrow J \subseteq Y$.

Věta 7.2. $\mathcal{R}(m, r)$ je $[n, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]_2$ kód.

Důkaz. Díky Pozorování (2) a (3) vidíme, že $\dim(\mathcal{R}(m, r)) = \sum_{i=0}^{r} \binom{m}{i}$.

Jestliže $|I| = r$, potom $\Phi(x_I) \in \mathcal{R}(m, r)$, a proto $w(\Phi(x_I)) = |N(x_I)| = 2^{m-r}$ podle Pozorování (4) a (5). Tím jsme dokázali nerovnost $d(\mathcal{R}(m, r)) \leq 2^{m-r}$.

Naopak z Poznámky 7.1 a Pozorování (4) plyne opačná nerovnost $d(\mathcal{R}(m, r)) \geq 2^{m-r}$. □

Věta 7.3. 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} z Pozorování (3), že pro každou dvojici $\Phi(x_I) \in B_r$, $\Phi(x_J) \in B_{m-r-1}$ je 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 (5) $x_{I \cup J}(i_B) = 1$, právě když $I \cup J \subseteq B$ 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 7.2 $\dim \mathcal{R}(m, r) + \dim \mathcal{R}(m, m - r - 1) =$

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

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

Příklad 7.4. (1) $\mathcal{R}(3, 1)$ je podle 7.2 a 7.3 samoduální $[8, 4, 4]_2$-kód. Všimněme si podobně jako v Příkladu 3.8, že propíchnutí $\mathcal{R}(3, 1)$ v kterékoli souřadnici je permutačně ekvivalentní 1-perfektnímu Hammingovu $[7, 4, 3]_2$-kódu z 2.4.

(2) Obdobně uvážíme, že $\mathcal{R}(m, m - 2) = \mathcal{R}(m, 1)^\perp$ je $[2^m, 2^m - m - 1, 4]_2$-kód a jeho propíchnutí v kterékoli souřadnici je díky 1.3 1-perfektní $[2^m - 1, 2^m - m - 1, 3]_2$-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

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

Poznámka 7.5. 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 předchozího Pozorování, že $f^I(i_Y) = \sum_J a_J x_J^I(i_Y) = a_I$. □

Kódování. Označíme $\mathcal{P}_r^m = \{I \subset \{1, \ldots, m\} \mid |I| \leq r\}$ a $k = \sum_{i=0}^r \binom{m}{i}$. Slovo z $\mathbb{F}_2^k$ reprezentované polynomem $f_{\mathbf{v}} = \sum_{I \in \mathcal{P}_r^m}$ zakódujeme vztahem $\mathbf{v} \to \Phi(f_{\mathbf{v}})$. Dostáváme lineární kódování $\mathbb{F}_2^k \cong \mathbb{F}_2^{\mathcal{P}_r^m} \to \mathcal{BF}(m) \cong \mathbb{F}_2^n$, jehož obrazem je RM-kód $\mathcal{R}(m, r)$.

Dekódování. Zformulujeme algoritmus, který přijaté chybové slovo s váhou chyby menší než 2^{m-r-1} reprezentovaného booleovskou funkcí opraví na původní polynom:

```
Vstup: g ∈ BF_m splňující g = f + e pro f ∈ R(m,r) a e ∈ F_2^n, w(e) < 2^{m-r-1}
Výstup: f̃ ∈ BP_m(r), pro který d(Φ(f̃), g) < 2^{m-r-1}, proto f = Φ(f̃).
for d=r downto 0 do
   for all I ⊆ {1,...,m} splňující |I| = d do
       {α_0 := |{Y ⊆ {1,...,m} : Y ∩ I = ∅, g^I(i_Y) = 0}|;
       α_1 := 2^{m-d} − α_0  (= |{Y ⊆ {1,...,m} : Y ∩ I = ∅, g^I(i_Y) = 1}|);
       if α_0 > α_1 then a_I := 0 else a_I := 1, g := g + Φ(x_I);
       }
return Σ_{I∈P_r^m} a_I x_I .
```

Poznámka 7.6. 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.

Důkaz. Technický důkaz opírající se o myšlenku Poznámky 7.5 vynecháme, zájemci jej naleznou například ve skriptech Aleše Drápala. □

8. Golayovy perfektní kódy

Tentokrát se vrátíme k pojmu perfektního kódu. Zkonstruujeme binární 3-perfektní kód délky 23 a dokážeme o něm, že je určen jednoznačně až na posunutí a permutační ekvivalenci.

V celé kapitole předpokládáme, že $b, v \in \mathbb{N}$ a uvažujeme uspořádané množiny $X = \{x_1, \ldots, x_v\}$ a $\mathcal{B} = \{B_1, \ldots, B_b\} \subseteq \mathcal{P}(X)$.

T&N. Pro $B, C \in \mathcal{B}$ definujme $i_B = i_1 \ldots i_v \in \mathbb{F}_2^v$ podmínkou $i_j = \begin{cases} 1 & \text{pokud } x_j \in B \\ 0 & \text{pokud } x_j \notin B \end{cases}$. Dále označme $i_B \cap i_C = i_{B \cap C}$, tedy $\cap$ představuje na $\mathbb{F}_2^v$ operací násobení po složkách. Řekneme, že matice $M = \begin{pmatrix} i_{B_1} \\ \ldots \\ i_{B_b} \end{pmatrix} \in \mathbb{Z}^{b \times v}$ je *incidenční matice* systému $\mathcal{B}$.

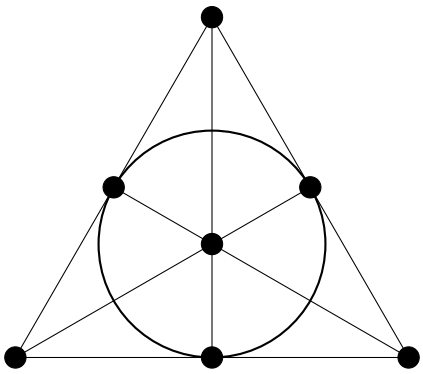
Pozorování. Nechť M je incidenční matice systému $\mathcal{B}$ a položme $U = (u_{ij}) = MM^T$ a $V = (v_{ij}) = M^T M$. Potom platí:

(1) Jestliže $B, C \subseteq X$, pak $w(i_B + i_C) = |B \div C| = w(i_B) + w(i_C) - 2w(i_{B \cap C})$,
(2) U je symetrická čtvercová, $u_{ij} = |B_i \cap B_j| \ \forall i, j$ a $u_{ii} = |B_i|$,
(3) V je symetrická čtvercová, $v_{ij} = |\{s \mid \{x_i, x_j\} \subseteq B_s\}| \ \forall i, j$ a $v_{ii} = |\{s \mid x_i \in B_s\}|$.

T&N. Pro $v, k, \lambda \in \mathbb{N}$ řekneme, že $\mathcal{B}$ je *symetrický* $2 - (v, k, \lambda)$ *design*, pokud

- $v = |X| = |\mathcal{B}|$,
- $k = |B| = |\{C \in \mathcal{B} \mid x \in C\}|$ pro $\forall B \in \mathcal{B}$ a $\forall x \in X$,
- $\lambda = |B_i \cap B_j| = |\{C \in \mathcal{B} \mid \{x, y\} \subseteq C\}| \ \forall i \neq j$ a $\forall x \neq y \in X$.

Příklad 8.1. (1) Přímky Fanovy roviny, tj. projektivního prostoru $P_2(\mathbb{F}_2)$ všech jednodimenzionálních podprostorů vektorového prostoru $\mathbb{F}_2^3$ tvoří symetrický $2 - (7, 3, 1)$ design.



(2) Obecněji, 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 $2 - (q^2 + q + 1, q + 1, 1)$ design.

Pozorování. Systém $\mathcal{B}$ s incidenční maticí M je symetrický $2 - (v, k, \lambda)$ design, právě když $MM^T = M^T M = \begin{pmatrix} k & \lambda & \ldots & \lambda \\ \lambda & k & \ldots & \lambda \\ . & . & \ldots & . \\ \lambda & \lambda & \ldots & k \end{pmatrix}$.

Konstrukce

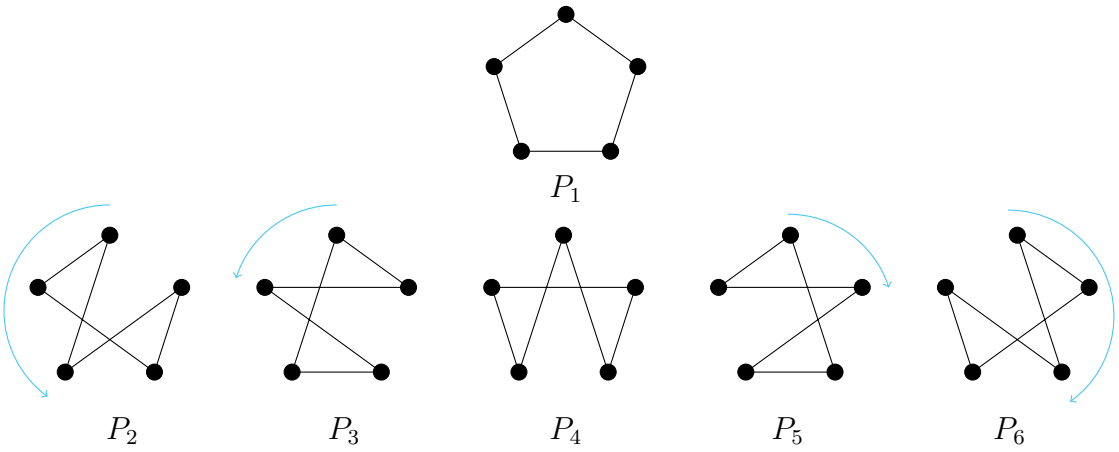
Nechť $Y = \{1, \ldots, 5\}$, $Z = \{A \subset \mathcal{P}(Y) \mid |A| = 2\}$, $\Phi = \{\sigma \in S_5 \mid \sigma^5 = 1, \sigma \neq \mathrm{id}\}$, $P_\varphi = \{\{i, \varphi(i)\} \mid i \in Y\} \ \forall \varphi \in \Phi$.

Pozorování. Pro množiny Y, Z, Φ a P_φ a $\forall \varphi, \psi \in \Phi$ 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) $|P_\varphi \cap P_\psi| \leq 1 \Rightarrow |P_{\varphi^2} \cap P_\psi| \geq 4 \Rightarrow P_\varphi \cap P_\psi = \emptyset$,

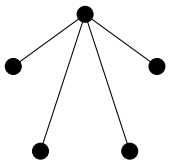
Definujme množiny

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



P_1 P_2 P_3 P_4 P_5 P_6

Položme $X = Z \cup \{0\}$ a $\forall i \in Y$:

$$F_i = \{\{i, a\} \mid a \in Y, a \neq i\} \cup \{0\} =$$  $$\cup \{0\},$$

nyní zkonstruujme symetrický $2-(11,5,2)$ design: $\mathcal{B} = \{P_i \mid i \leq 6\} \cup \{F_j \mid j \leq 5\}$

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

Fakt 8.2. Systém $\mathcal{B}$ z předchozí konstrukce je až na izomorfismus jediný symetrický $2-(11,5,2)$ design.

Důsledek 8.3. $\mathcal{C} = \{X \setminus B \mid B \in \mathcal{B}\}$ pro $\mathcal{B}$ z předchozí konstrukce tvoří až na izomorfismus jediný symetrický $2-(11,6,3)$ design.

Důkaz. Definujme zobrazení $c : \mathcal{P}(X) \to \mathcal{P}(X)$ vztahem $c(A) = X \setminus A$ a označme M incidenční matici $\mathcal{B}$, N incidenční matici $\mathcal{C}$ a $J = (1) \in \mathbb{Z}^{11\times 11}$ matici sestávající ze samých hodnot 1. Potom vidíme, že $N = J - M$ a snadno spočítáme

$$N \cdot N^T = J^2 - JM - MJ + MM^T = 11J - 5J - 5J + MM^T = J + MM^T.$$

Podobně $N^T \cdot N = J + M^T M = J + MM^T$, proto

$$N \cdot N^T = N^T \cdot N = J + \begin{pmatrix} 5 & 2 & \dots & 2 \\ 2 & 5 & \dots & 2 \\ . & . & \dots & . \\ 2 & 2 & \dots & 5 \end{pmatrix} = \begin{pmatrix} 6 & 3 & \dots & 3 \\ 3 & 6 & \dots & 3 \\ . & . & \dots & . \\ 3 & 3 & \dots & 6 \end{pmatrix}$$

a $\mathcal{C}$ je tudíž symetrický $2-(11,6,3)$ design.

Obdobně nahlédneme, že pro symetrický $2-(11,6,3)$ design $\mathcal{C}$ s incidenční maticí N platí pro incidenční maticí $M = J - N$ systému $c(\mathcal{C})$, že je $M^TM = MM^T = N^TN - J$, proto je $c(\mathcal{C})$ symetrický $2-(11,5,2)$ design. Kdybychom nyní měli dva neizomorfní symetrické $2-(11,6,3)$ 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 $E \in \mathbb{F}_2^{12\times 24}$ sestává z bloku s jednotkovou maticí I_{12} a dále z bloku tvořeným maticí N s řádkem nad a sloupcem vlevo obsahujícím na první souřadnici 0 a jinde 1 a $G \in \mathbb{F}_2^{12\times 24}$ 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.

Je-li $\mathcal{C}$ blokový kód délky n a $f_i = |\{\mathbf{v} \in \mathcal{C} \mid w(w) = i\}|$, pak se polynom $f_{\mathcal{C}} = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$ nazývá *váhový polynom* kódu $\mathcal{C}$.

1 bude značit slovo sestávající ze samých souřadnic 1.

Pozorování. Protože $V_2(23,3) = \sum_{i=0}^{3}\binom{23}{i} = 1 + 23 + 23\cdot 11 + 23\cdot 77 = 2048 = 2^{23-12}$, je binární kód délky 23, velikosti 2^{12} a vzdálenosti 7 3-perfektní. Pokud takový kód $\mathcal{C}$ obsahuje slovo **0** spočítáme jeho váhový polynom $f_{\mathcal{C}} = 1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$ ze vztahu $\binom{23}{i} = \sum_{s=-3}^{3} c_{i,s} f_{i+s}$ pro $i \geq 3$ a počáteční podmínky $f_0 = 1$, $f_i = 0$ pro $i = 1,\dots,6$, kde

$c_{i,-3} = \binom{23-i+3}{3}$, $c_{i,-2} = \binom{23-i+2}{2}$, $c_{i,-1} = \binom{i-1}{1}\binom{23-i+1}{2} + \binom{23-i+1}{1}$,

$c_{i,0} = \binom{i}{1}\binom{23-i}{1} + 1$, $c_{i,1} = \binom{i+1}{2}\binom{23-i-1}{1} + \binom{i+1}{1}$, $c_{i,2} = \binom{i+2}{2}$, $c_{i,3} = \binom{i+3}{3}$. Vztah plyne z vlastnosti 3-perfektního kódu, že každé slovo váhy i leží právě v jedné kouli o poloměru 3 a středu v kódovém slově. Hodnoty $c_{i,j}$ reprezentují počty slov které daným způsobem změníme na slovo váhy i:

$c_{i,-3}$ - počet 3 bitových změn $0 \to 1$ kódového slova váhy $i-3$,
$c_{i,-2}$ - počet 2 bitových změn $0 \to 1$ kódového slova váhy $i-2$,
$c_{i,-1}$ - 1 změna $0 \to 1$ plus 2 změny $0 \to 1$ a jedna $1 \to 0$ kódového slova váhy $i-1$,
$c_{i,0}$ - kódová slova plus 1 změna $0 \to 1$ a jedna $1 \to 0$ kódového slova váhy i,
$c_{i,1}$ - 1 změna $1 \to 0$ plus 2 změny $1 \to 0$ a jedna $0 \to 1$ kódového slova váhy $i+1$,
$c_{i,2}$ - 2 změny $1 \to 0$ kódového slova váhy $i+2$,
$c_{i,3}$ - 3 změny $1 \to 0$ kódového slova váhy $i+3$.

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

Poznámka 8.4. Nechť $\mathbf{C} = \begin{pmatrix} \mathbf{c}_1 \\ \dots \\ \mathbf{c}_k \end{pmatrix}$ 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.

($\Leftarrow$) Pro všechna $\mathbf{u} \in \mathcal{C}$ existuje jediná množina $I \subseteq \{1, \ldots, k\}$, pro niž $\mathbf{u} = \sum_{i \in I} \mathbf{c}_i$. Označíme $\delta(\mathbf{u}) = |I|$ a 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 existuje i splňující $\mathbf{u} = \mathbf{c}_i$, tedy $4|w(\mathbf{u})$ podle předpokladu.

Nechť tvrzení platí pro $\delta > 0$ a $\delta(\mathbf{u}) = \delta + 1$. Pak existuje $\mathbf{v}, \mathbf{c} \in \mathcal{C}$, 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 dělí váhy $w(\mathbf{v})$ i $w(\mathbf{c})$, a proto 4 dělí i váhu $w(\mathbf{u}) = w(\mathbf{v} + \mathbf{c}) = w(\mathbf{v}) + w(\mathbf{c}) - 2w(\mathbf{v} \cap \mathbf{c})$. □

Poznámka 8.5. $\mathcal{E}$ 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 plyne, že $w(\mathbf{u}_1) = 12$, $w(\mathbf{u}_i) = 8$, $w(\mathbf{u}_1 \cap \mathbf{u}_i) = 6$ pro všechna $i > 1$ a $w(\mathbf{u}_i \cap \mathbf{u}_j) = 4$ pro všechna $i > j > 1$.

Ze sudosti hodnot $w(\mathbf{u}_i \cap \mathbf{u}_j)$ plyne, že $\mathbf{u}_i \cdot \mathbf{u}_j = 0$ pro všechna i, j, proto je $\mathcal{E}$, který obsahuje právě 2^{12} slov samoduální a díky 8.4 i dvojnásobně sudý. Z matice E vidíme, že $d(\mathcal{E}) \leq 8$, předpokládejme ke sporu, že $d(\mathcal{E}) < 8$ a tedy $d(\mathcal{E}) = 4$. To znamená, že existuje $I \subset \{1, \ldots, 12\}$, 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 $a = |A|$. Potom $\mathbf{v} = i_A \cdot E$, $1 < a \leq w(\mathbf{v}) = 4$, a $a = |I|$. Uvážíme-li kontrolní matici $\mathcal{E}$ podle 2.2:

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

pak jde zároveň o generující matici samoduálního kódu $\mathcal{E}$ a slova $\tilde{\mathbf{u}}_i$ mají stejné vlastnosti jako slova $\mathbf{u}_i$, protože rovněž N^T je incidenční matice symetrického $2-(11, 6, 3)$ designu. Tudíž existuje $\tilde{I} \subset \{1, \ldots, 12\}$, pro něž $\mathbf{v} = \sum_{i \in \tilde{I}} \tilde{\mathbf{u}}_i$ a platí $a = 4 - |\tilde{I}| > 1$. Vidíme, že $a = 2$, proto existují $i \neq j$, pro která

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

což je spor. Dokázali jsme, že je $\mathcal{E}$ 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 8.6. 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 8.5.

Nechť $\mathcal{C}$ splňuje předpoklady tvrzení. Pak existuje $\mathbf{u} \in \mathcal{C}$ váhy 12, proto $\mathbf{1}, \tilde{\mathbf{u}} = \mathbf{1} + \mathbf{u} \in \mathcal{C}$ a $w(\mathbf{u}) = w(\tilde{\mathbf{u}}) = 12$. Bez újmy na obecnosti můžeme předpokládat (tj. permutujeme souřadnice), že $\mathbf{u} = 0 \ldots 01 \ldots 1$ a $\tilde{\mathbf{u}} = 1 \ldots 10 \ldots 0$ a propichovanou souřadnici nastavíme jako první.

Nechť $I = \{13, \ldots, 24\}$ a $\pi_I : \mathbb{F}_2^{24} \to \mathbb{F}_2^{12}$ je propíchnutí v souřadnicích I. Dále předpokládejme, že $\mathbf{v} \in \mathcal{C} \setminus \{\mathbf{0}\}$ a $\pi_I(\mathbf{v}) = \mathbf{0}$, z čehož plyne, že $w(\mathbf{u} + \mathbf{v}) + w(\mathbf{v}) = 12, w(\mathbf{v}) \geq 8$,

tudíž $w(\mathbf{u}+\mathbf{v}) \leq 4$. Proto $\mathbf{u} = \mathbf{v}$ a $\mathrm{Ker}\pi_I = \{\mathbf{0}, \mathbf{u}\}$. Protože $\tilde{\mathbf{u}}\mathbf{c} = 0$ pro všechna slova $\mathbf{c} \in \mathcal{C}$ je $\pi_I(\mathcal{C})$ $[12, 11]_2$-kód s kontrolní maticí $\mathbf{1} \in \mathbb{F}_2^{1\times 12}$. To znamená, že umíme zkonstruovat generujíc matici kódu $\mathcal{C}$ tvaru

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

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 8.3 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 $\mathbf{v}_1, \dots, \mathbf{v}_{11}$. Protože je $\mathcal{C}$ dvojnásobně sudý kód, 4 dělí $w(\mathbf{c}_i)$ i $w(\mathbf{c}_i+\mathbf{c}_j)$ a $d(\mathcal{C}) = 8$ vidíme, že $w(\mathbf{v}_i), w(\mathbf{v}_i+\mathbf{v}_j) \in \{6, 10\}$. Ukážeme, že připadá v úvahu pouze hodnota 6.

Kdyby $w(\mathbf{v}_i) = 10$, pak by $w(\mathbf{c}_i + \mathbf{c}_0) = 2 + 2 = 4$, z čehož plyne spor.

Kdyby $w(\mathbf{v}_i + \mathbf{v}_j) = 10$, pak by $w(\mathbf{c}_i + \mathbf{c}_j + \mathbf{c}_0) = 2 + 2 = 4$, opět tedy dostáváme spor.

Proto pro $i \neq j$

$$6 = w(\mathbf{v}_i) = w(\mathbf{v}_i + \mathbf{v}_j) = w(\mathbf{v}_i) + w(\mathbf{v}_j) - 2w(\mathbf{v}_i \cap \mathbf{v}_j),$$

z čehož plyne, že $w(\mathbf{v}_i \cap \mathbf{v}_j) = 3$. 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 generující matice samoduálního kódu $\tilde{\mathcal{C}}$.

Tedy M je incidenční matice symetrického $2-(11, 6, 3)$ designu, která je podle 8.3 určena až na permutaci řádků a sloupců jednoznačně. Nyní je už snadné nahlédnout že je původní kód permutačně ekvivalentní kódu $\mathcal{E}$ a jeho propíchnutí v libovolné předem zvolené souřadnici je permutačně ekvivalentní kódu $\mathcal{G}$. □

Poznámka 8.7. 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 $\mathcal{C} \subseteq \mathrm{LO}(\mathcal{C}) \subseteq \mathcal{C}^\perp \subseteq (\mathrm{LO}(\mathcal{C}))^\perp$, proto $2^k = |\mathcal{C}| \leq |\mathrm{LO}(\mathcal{C})|$ a $\dim(\mathrm{LO}(\mathcal{C})) \geq k$. Uvážíme-li, že $\dim((\mathrm{LO}(\mathcal{C}))^\perp) \leq k$, vidíme, že $2^k = |\mathcal{C}| \leq |\mathrm{LO}(\mathcal{C})| \leq |(\mathrm{LO}(\mathcal{C}))^\perp)| \leq 2^k$, čímž jsme ověřili, že $\mathcal{C} = \mathrm{LO}(\mathcal{C}) = \mathcal{C}^\perp$.

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

Všimněme si, že pro každé $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ plyne z 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 $2w(\mathbf{u}\cap\mathbf{v}) = w(\mathbf{u}+\mathbf{v}) - w(\mathbf{u}) - w(\mathbf{v})$, tedy váha $w(\mathbf{u}\cap\mathbf{v})$ je sudá a $\mathbf{u}\cdot\mathbf{v} = 0$. Ověřili jsme, že je $\mathcal{C}$ samoortogonální. □

Věta 8.8. 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 8.5.

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 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 pro každé $\mathbf{u} \in \tilde{\mathcal{E}} \setminus \{\mathbf{0}, \mathbf{1}\}$ existují $j, k \leq 24$ 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 váhy 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 neplatí. Podobně $\tilde{\mathcal{E}}$ nemůže obsahovat slova váhy 9, 13, ani 17. Proto $f_{\tilde{\mathcal{E}}} = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$, tedy $\tilde{\mathcal{E}}$ je dvojnásobně sudý. Protože $\mathbf{v} + \tilde{\mathcal{E}}$ má stejné parametry jako $\tilde{\mathcal{E}}$, je to dvojnásobně sudý kód pro všechna $\mathbf{v} \in \tilde{\mathcal{E}}$ a tedy je $\tilde{\mathcal{E}}$ lineární samoduální kód podle 8.7 a $\tilde{\mathcal{E}}$ je permutačně ekvivalentní $\mathcal{E}$ podle 8.6.

Splňuje-li $\tilde{\mathcal{G}}$ předpoklady tvrzení, pak kód $\hat{\mathcal{E}} = \{c_1 \dots c_{23} \sum_i c_i \mid c_1 \dots c_{23} \in \tilde{\mathcal{G}}\}$ má délku 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 díky 8.6 permutačně ekvivalentní $\mathcal{G}$.

Zbytek plyne z 8.5. □

Důsledek 8.9. Je-li $\mathcal{C}$ binární kód velikosti 2^{12} délky 23 a vzdálenosti 7, pak $\forall \mathbf{u} \in \mathcal{C}$ je kód $\mathbf{u} + \mathcal{C}$ permutačně ekvivalentní $\mathcal{G}$.

Konvoluční kódy

9. Kódujme konvolučním kódem!

Následující kapitoly budou věnovány odlišnému konceptu kódování, kdy budeme pracovat nikoli s množinou přípustných kódových slov, nýbrž s množinou přípustných posloupností kódových slov, které budou ovšem opět kódovat všechny posloupnosti slov totálního kódu. V úvodní části nastíníme formalizaci problematiky a kromě základních pojmů konvolučního kódu a konvolučního kódovače, zavedeme klíčové nástroje jejich popisu. Na závěr kapitoly si uvědomíme, že naše definice fyzického konvolučního kódovače detailně popisuje jeho technickou realizaci jako elektrického obvodu.

V celé kapitole předpokládáme, že $\mathbb{F}$ je konečné těleso a D neznámá.

T&N. Na množině formálních *Laurentových řad* $\mathbb{F}((D)) = \{\sum_{i\geq r} u_i D^i \mid r \in \mathbb{Z}, u_i \in \mathbb{F}\}$ uvažujme obvyklé operace

$$\sum_{i\geq r} u_i D^i \pm \sum_{i\geq s} v_i D^i = \sum_{i\geq \min(r,s)} (u_i \pm v_i) D^i, \quad \sum_{i\geq r} u_i D^i \cdot \sum_{i\geq s} v_i D^i = \sum_{i\geq r+s} \sum_{k=r}^{i-s} u_k v_{i-k} D^i,$$

kde položíme $u_i = v_j = 0\ \forall i < r, j < s$. Dále značme:
$\mathbb{F}[[D]] = \{\sum_{i\geq 0} u_i D^i \mid u_i \in \mathbb{F}\}$ - formální *mocninné řady*,
$\mathbb{F}[D] = \{\sum_{i=0}^{n} u_i D^i \mid n \in \mathbb{N}, u_i \in \mathbb{F}\}$ - *polynomy*,
$\mathbb{F}[D^{-1}] = \{\sum_{i=0}^{n} u_i D^{-i} \mid n \in \mathbb{N}, u_i \in \mathbb{F}\}$ - *inverzní polynomy*,
$\mathbb{F}[D, D^{-1}] = \{\sum_{i=k}^{n} u_i D^i \mid k \in \mathbb{Z}, n \in \mathbb{N}, u_i \in \mathbb{F}\}$ - *Laurentovy polynomy*.

Poznámka 9.1. $\mathbb{F}((D))$ tvoří s výše zavedenými operacemi a konstantami 0 a 1 komutativní těleso a $\mathbb{F}[D]$, $\mathbb{F}[D^{-1}]$, $\mathbb{F}[D, D^{-1}]$, $\mathbb{F}[[D]]$ jsou jeho podokruhy.

Důkaz. Obdobnými argumenty jako v případě oboru polynomů je snadné nahlédnout, že $\mathbb{F}((D))$ představuje komutativní okruh. Abychom ověřili, že jde o těleso, vezeme nenulový prvek $f \in \mathbb{F}((D))$. Potom existuje celé číslo d a mocninná řada $g \in \mathbb{F}[[D]]$ s nenulovým absolutním členem, pro který $f = D^d g$. Potom je mocninná řada $h = \sum h_0 D^i$ s koeficienty danými rekurentním vztahem $h_0 = g_0^{-1}$ a $h_n = g_0^{-1} \sum_{i=0}^{n-1} h_i g_{n-i}$ inverzní k řadě g, a proto $f^{*-1} = D^{-d} h$.

Důkaz uzavřenost množin $\mathbb{F}[D]$, $\mathbb{F}[D^{-1}]$, $\mathbb{F}[D, D^{-1}]$, $\mathbb{F}[[D]]$ na operace je zcela přímočarý. □

Definice. Podílovému tělesu $\mathbb{F}(D) = \{\frac{p}{q} \mid p, q \in \mathbb{F}[D], q \neq 0\}$ oboru $\mathbb{F}[D]$ říkáme *racionální funkce*, racionální funkce $f \in \mathbb{F}(D)$ je *realizovatelná*, pokud $f = \frac{p}{q}$ pro vhodný polynom p a polynom s nenulovým absolutním členem q.

Pozorování. Uvažujme zobrazení $\nu : \mathbb{F}(D) \to \mathbb{F}((D))$ dané vztahem $\nu(\frac{p}{q}) = p \cdot q^{-1}$.

(1) ν je prostý okruhový homomorfismus,
(2) $f \in F(D)$ je realizovatelná $\Leftrightarrow \nu(f) \in \mathbb{F}[[D]]$

Nadále budeme ztotožňovat prvky $\mathbb{F}(D)$ a $\nu(\mathbb{F}(D))$ a prvkům $\nu(\mathbb{F}(D)) \cap \mathbb{F}[[D]]$ budeme říkat *realizovatelné řady*.

T&N. Pro $c \in \mathbb{N}$ označme $\mathbb{F}^c((D)) = \{\sum_{i\geq r} \mathbf{u}_i D^i \mid r \in \mathbb{Z}, \mathbf{u}_i \in \mathbb{F}^c\}$, kde souřadnice značíme horními indexy $\mathbf{u}_i = u_i^{(1)} \dots u_i^{(c)}$.

Pozorování. Pro $c \in \mathbb{N}$ platí, že

(1) zobrazení $\mu(\sum_{i\geq r} \mathbf{u}_i D^i) = (\sum_{i\geq r} u_i^{(1)} D^i, \dots, \sum_{i\geq r} u_i^{(c)} D^i)$ je bijekce $\mu : \mathbb{F}^c((D)) \to \mathbb{F}((D))^c$,
(2) $\mathbb{F}((D))^c$ představuje aritmetický vektorový prostor nad tělesem $\mathbb{F}((D))$ a jeho strukturu můžeme pomocí bijekce μ přenést na množinu $\mu : \mathbb{F}^c((D))$ (tedy μ je izomorfismus).

Na základě předchozího pozorování budeme nadále ztotožňovat prvky prostorů $\mathbb{F}^c((D))$ a $\mathbb{F}((D))^c$ prostřednictvím izomorfismu μ.

Definice. Je-li $B \subset \mathbb{F}(D)^c$, nazveme $\mathcal{C} = LO(B) \subseteq \mathbb{F}((D))^c$ *konvoluční kód* s parametry (c, k), pokud $\dim_{\mathbb{F}((D))} \mathcal{C} = k$. Každou matici $G \in (\mathbb{F}(D) \cap \mathbb{F}[[D]])^{k\times c}$, jejíž řádky tvoří bázi $\mathcal{C}$, nazveme *generující maticí* konvolučního kódu $\mathcal{C}$. Pokud $G \in \mathbb{F}[D]^{k\times c}$ mluvíme o *polynomiální* generující matici.

Poznámka 9.2. Je-li $\mathcal{C} \subseteq \mathbb{F}((D))^c$ konvoluční kód, pak

(1) existuje nějaká polynomiální generující matice $\mathcal{C}$,
(2) je-li $G = (g_{ij})$ generující matice $\mathcal{C}$, pak existují polynomy $p_{ij}, q_i \in \mathbb{F}[D]$: $q_i(0) = 1$, $\mathrm{NSD}(p_{i1}, \ldots, p_{ic}, q_i) = 1$ a $g_{ij} = \frac{p_{ij}}{q_i}$ $\forall i, j$,
(3) všechny polynomy z bodu (2) (a tedy i jejich stupně) jsou maticí G určeny jednoznačně.

Důkaz. (1) Nejprve zvolíme libovolnou bázi $(\mathbf{b}_1, \ldots, \mathbf{b}_k) \subset \mathbb{F}(D)$. Pro ni existují polynomy $f_{ij}, q_{ij} \in \mathbb{F}[D]$, $i \leq k$, $j \leq c$ splňující $\mathbf{b}_i = (\frac{f_{i1}}{q_{i1}}, \ldots, \frac{f_{ic}}{q_{ic}})$ pro všechna i a položme $q = \mathrm{nsn}(q_{ij} \mid i \leq k,\ j \leq c)$ a $\mathbf{g}_i = q \cdot \mathbf{b}_i$. Z toho plyne, že $G = \begin{pmatrix} \mathbf{g}_1 \\ \ldots \\ \mathbf{g}_k \end{pmatrix}$ je generující matice konvolučního kódu $\mathcal{C}$.

(2) Nechť $g_{ij} = \frac{f_{ij}}{q_{ij}}$ pro nesoudělné f_{ij} a q_{ij} a $q_{ij}(0) \neq 0$, což můžeme předpokládat, pro všechna i, j.

Pro každé i položme $\tilde{q}_i = \mathrm{nsn}(q_{ij} \mid j \leq c)$, dále $q_i = \frac{\tilde{q}_i}{\tilde{q}_i(0)}$, což znamená, že $q_i(0) = 1$, a $p_{ij} = f_{ij}\frac{q_i}{q_{ij}}$ pro všechna $j = 1, \ldots, c$. Ukážeme, že $\mathrm{NSD}(p_{i,1}, \ldots, p_{i,c}, q_i) = 1$.

Předpokládejme, že existuje ireducibilní polynom r, který dělí všechny $p_{i,1}, \ldots, p_{i,c}$ i q_i. Kdyby $r|f_{ij}$ pro všechna j, pak by r nedělilo q_{ij} pro žádné j, a tudíž by r nedělilo q_i, což je ve sporu s předpokladem. Nechť nyní $\emptyset \neq J = \{j \mid r \text{ nedělí} f_{ij}\}$. Potom $r \mid \frac{q_i}{q_{ij}}$, a proto $q_{ij}r \mid q_i$ pro všechna $j \in J$, tudíž r dělí $\frac{q_i}{\mathrm{nsn}(q_{i,j}|j\in J)}$. Odtud plyne, že existuje $j \notin J$, pro něž r dělí q_{ij}, tudíž r nedělí f_{ij}, což je spor s volbou J.

(3) Zvolme i, j libovolně. Protože $\frac{f_{ij}}{q_{ij}} = \frac{p_{ij}}{q_i}$, dostáváme, že $q_i = q_{ij}\frac{p_{ij}}{f_{ij}}$, což je polynom, kde f_{ij} a q_{ij} jsou nesoudělné a $\frac{p_{ij}}{f_{ij}}$ je polynom. Tudíž q_i je společný násobek polynomů $q_{i1}, \ldots, q_{ic}$. Budeme-li předpokládat, že existuje polynom r, který dělí $\frac{q_i}{\mathrm{nsn}(q_{i1},\ldots,q_{ic})}$, pak obdobně jako v důkazu (2a) nahlédneme, že r dělí p_{ij}, což je spor. Tím jsme dokázali, že q_i je až na skalární násobek určen jednoznačně. Uvážíme-li, že se absolutní člen polynomů q_i rovná 1, jsou všechny polynomy určeny jednoznačně. □

T&N. Uvážíme-li vyjádření generující matice $G = (\frac{p_{ij}}{q_j})$ konvolučního kódu z 9.2(2a), pak definujme $\nu_i = \max(\deg(p_{i1}), \ldots, \deg(p_{ic}), \deg(q_i))$ a $\mathrm{extdeg}(G) = \sum_{i=1}^k \nu_i$ je *vnější stupeň* matice G.

Věta 9.3. Jsou-li G a $\tilde{G}$ dvě generující matice konvolučního kódu $\mathcal{C}$ s minimálním vnějším stupněm $\nu = \sum_{i=1}^k \nu_i = \sum_{i=1}^k \tilde{\nu}_i$, kde ν_i a $\tilde{\nu}_i$ jsou zavedeny stejně jako výše a $\nu_1 \leq \cdots \leq \nu_k$ a $\tilde{\nu}_1 \leq \cdots \leq \tilde{\nu}_k$, pak $\nu_i = \tilde{\nu}_i$ pro všechna $i = 1, \ldots, k$.

Důkaz. Označme si řádky generujících matic $G = \begin{pmatrix} \mathbf{g}_1 \\ \ldots \\ \mathbf{g}_i \end{pmatrix}$ a $\tilde{G} = \begin{pmatrix} \tilde{\mathbf{g}}_1 \\ \ldots \\ \tilde{\mathbf{g}}_k \end{pmatrix}$ a ke sporu předpokládejme, že existuje i, pro něž $\nu_i \neq \tilde{\nu}_i$. Vezměme nejmenší takové i bez újmy

na obecnosti předpokládejme, že $\nu_i < \tilde{\nu}_i$. Doplníme-li nyní bázi $\mathbf{g}_1, \ldots, \mathbf{g}_i$ na bázi $\mathbf{g}_1, \ldots, \mathbf{g}_i, \tilde{\mathbf{g}}_{j_1}, \ldots, \tilde{\mathbf{g}}_{j_{k-i}}$ konvolučního kódu $\mathcal{C}$ pomocí řádků generující matice $\tilde{G}$, potom je matice $\hat{G} = \begin{pmatrix} \mathbf{g}_1 \\ \ldots \\ \mathbf{g}_i \\ \tilde{\mathbf{g}}_{j_1} \\ \ldots \\ \tilde{\mathbf{g}}_{j_{k-i}} \end{pmatrix}$ rovněž generující maticí konvolučního kódu $\mathcal{C}$ a dostáváme

$$\operatorname{extdeg}(\hat{G}) = \sum_{s=1}^{i} \nu_s + \sum_{s=1}^{n-k} \tilde{\nu}_{j_s} \leq \sum_{s=1}^{i} \nu_s + \sum_{s=i+1}^{k} \tilde{\nu}_s = \nu_i + \sum_{s \neq i} \tilde{\nu}_s < \sum_{s=1}^{k} \tilde{\nu}_s = \nu,$$

což je spor s minimalitou volby ν. □

Definice. Hodnoty ν_i z předchozí věty se nazývají *Forneyho indexy* a $\deg \mathcal{C} = \sum_{i=1}^{k} \nu_i$ je stupeň konvolučního kódu $\mathcal{C}$.

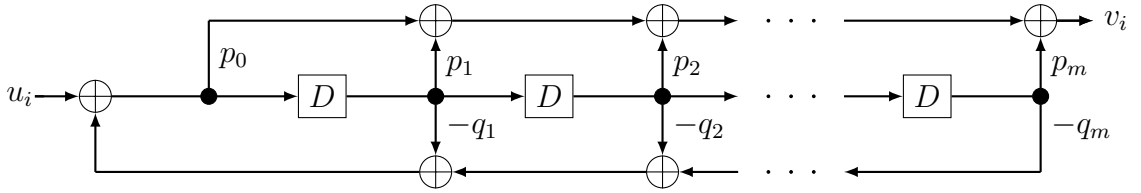
Je-li G generující matice konvolučního kódu $\mathcal{C}$ s parametry (c, k), pak zobrazení $K : \mathbb{F}((D))^k \to \mathbb{F}((D))^c$ dané podmínkou$K(\mathbf{u}) = \mathbf{u}G$ nazveme *konvoluční kódovač* a dvojici (K, G) *fyzický konvoluční kódovač.*

Pozorování. Je-li (K, G) fyzický konvoluční kódovač pro $G = (\frac{p_{ij}}{q_i})$ generující matici konvolučního kódu $\mathcal{C}$ s parametry (c, k) a $\mathbf{u} = \sum_i \mathbf{u}_i D^i \in \mathbb{F}((D))^k$, pak

(1) $K(\mathbb{F}((D))^k) = \mathcal{C}$ a K je prosté lineární zobrazení,
(2) $\mathbf{v}^{(j)} = \sum_i \mathbf{v}_i^{(j)} D^i = \sum_{s=1}^{k} \mathbf{u}^{(s)} \frac{p_{sj}}{q_s}$ pro $\mathbf{v} = \sum_i \mathbf{v}_i D^i = K(\mathbf{u})$.

V předchozím pozorování jsme si uvědomili, že fyzický konvoluční kódovač umíme vždy vyjádřit jako jistou konečnou posloupnost součtů konvolucí s realizovatelnou racionální funkcí. Následující znázornění konvoluce obvodem nepředstavuje jen formální zápis realizovatelné racionální funkcí pomocí schématu, nýbrž ukazuje, jak konvoluční kódovač „fyzicky"realizovat pomocí elektrotechnického obvodu, do nějž vstupuje jistou frekvencí posloupnost signálů hodnoty u_i, symbol $\boxed{D}$ představuje součástku zpožďující výstup proti vstupu o jednu časovou jednotku a $\oplus$ spolu ohodnocením hrany znamená přičtení násobku hodnoty na vstupu.

T&N. Je-li p, q jako v 10.2, $u = \sum_{i \geq z} u_i D^i \in \mathbb{F}((D))$ a $v = \sum_{i \geq z} v_i D^i = u \cdot \frac{p}{q}$, pak je konvoluce $u \cdot \frac{p}{q}$ *realizována obvodem*:



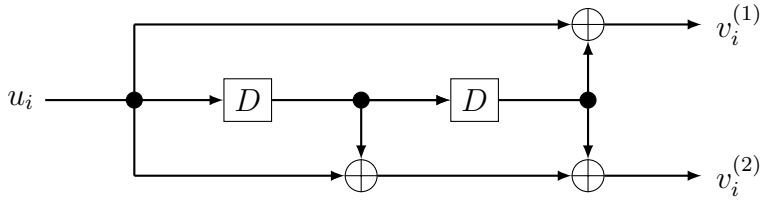
Za šablonu obvodu děkuji Adamu Klepáčovi.

Poznamenejme, že ohodnocení hrany nulou se obvykle znázorňuje vypuštěním hrany/vodiče (a příslušný čítač tak můžeme rovněž vypustit) a ohodnocení hodnotou 1 se vynechává.

Příklad 9.4. Uvážíme fyzický konvoluční kódovač (K, G) pro generující matici $G = \begin{pmatrix} 1+D^2 & 1+D+D^2 \end{pmatrix} \in \mathbb{F}_2[D]^{1\times 2}$. Nechť $u = \sum_i u_i D^i \in \mathbb{F}_2((D))$, potom

$$K(u) = \sum_i u_i D^i \begin{pmatrix} 1+D^2 & 1+D+D^2 \end{pmatrix} = (\sum_i (u_i + u_{i-2})D^i, \sum_i (u_i + u_{i-1} + u_{i-2})D^i).$$

Fyzický konvoluční kódovač ještě realizujme obvodem:

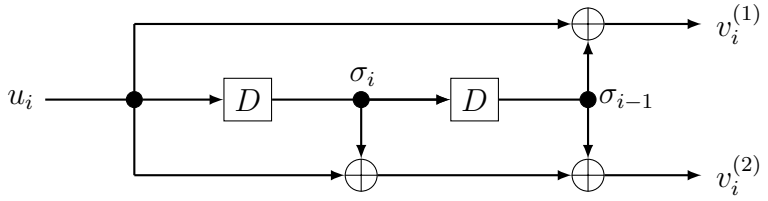


10. Konvoluční kódovač: obvod nebo překladač?

Rozmyslíme si, že konvoluční kódovač můžeme pojmout jako jistý typ překladače, který nám díky znalosti hodnoty a stavu systému v daném čase umožní algoritmicky určit následující hodnoty a stavy. Vedle toho nahlédneme, jak naše původní definice konvolučního kódovače detailně souvisí s definicí algoritmickou.

Definice. Nechť $n, k, m \in \mathbb{N}$, $k \leq n$, $z \in \mathbb{Z}$ a uvažme matice $P \in \mathbb{F}^{m\times m}$, $Q \in \mathbb{F}^{k\times m}$, $R \in \mathbb{F}^{m\times n}$, $S \in \mathbb{F}^{k\times n}$ a zobrazení $\delta : \mathbb{F}^m \times \mathbb{F}^k \to \mathbb{F}^m$ a $\lambda : \mathbb{F}^m \times \mathbb{F}^k \to \mathbb{F}^n$ daná předpisem $\delta(\mathbf{s}, \mathbf{u}) = \mathbf{s}P + \mathbf{u}Q$ a $\lambda(\mathbf{s}, \mathbf{u}) = \mathbf{s}R + \mathbf{u}S$. Buď $u = \sum_{i\geq z} \mathbf{u}_i D^i \in \mathbb{F}((D))^k$ a $\mathbf{s}_z = \mathbf{0} \in \mathbb{F}^m$ a definujme $\mathbf{s}_{i+1} = \delta(\mathbf{s}_i, \mathbf{u}_i)$, $\mathbf{v}_{i+1} = \lambda(\mathbf{s}_i, \mathbf{u}_i)$ $\forall i \geq z$ a $K(u) = \sum_i \mathbf{v}_i D^i$. Je-li zobrazení K prosté, potom trojici (K, δ, λ) nazveme *abstraktní konvoluční kódovač* s přechodovou funkcí δ a výstupní funkcí λ s parametry (n, k, m). $\mathbb{F}^m$ se nazývá stavový prostor.

Příklad 10.1. Označíme v obvodu z Příkladu 9.4 σ_i a σ_{i-1} hodnoty po prvním a druhém použití zpožďovače $\boxed{D}$ v čase i (tedy v okamžiku, kdy máme na vstupu hodnotu u_i) a dvojici těchto hodnot označíme jako stav $\mathbf{s}_i = (\sigma_i, \sigma_{i-1})$:



Potom $\mathbf{s}_{i+1} = (\sigma_{i+1}, \sigma_i) = (u_i, u_{i-1}) = \mathbf{s}_i P + \mathbf{u}_i Q$ a

$$\mathbf{v}_i = (u_i + u_{i-2}, u_i + u_{i-1} + u_{i-2}) = (\sigma_{i-1}, \sigma_i + \sigma_{i-1}) + (u_i, u_i) = \mathbf{s}_i R + \mathbf{u}_i S$$

pro matice $P = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, Q = \begin{pmatrix} 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \end{pmatrix}$, proto lze konvoluční kódovač K z 9.4 popsat jako abstraktní konvoluční kódovač (K, δ, λ) s parametry $(2, 1, 2)$, kde $\delta(\mathbf{s}, \mathbf{u}) = \mathbf{s}P + \mathbf{u}Q$ a $\lambda(\mathbf{s}, \mathbf{u}) = \mathbf{s}R + \mathbf{u}S$.

Pozorování. Nechť (K, δ, λ) je abstraktní konvoluční kódovač s parametry (n, k, m), pak $\forall u \in \mathbb{F}((D))^k$

(1) K je $\mathbb{F}$-lineární a $K(uD) = K(u)D$,
(2) pro všechna $p, q \in \mathbb{F}[D] \setminus \{0\}$ máme $K(u \cdot p) = K(u)p$ a $Ku \cdot \frac{p}{q})q = K(u \cdot p)$, proto $K(u \cdot \frac{p}{q}) = K(u)\frac{p}{q}$,
(3) pokud $k = 1$ a $u \in \mathbb{F}(D)$, pak $K(u) = K(1)u$.

Poznamenejme, že vlastnost $K(uD) = K(u)D$ z bodu (1) se obvykle nazývá *časová invariance* a hodnota $K(1)$ *odezva* kódovače K.

Poznámka 10.2. Nechť $m \in \mathbb{N}$, $p = \sum_{i=0}^{m} p_i D^i \neq 0$, $q = 1 + \sum_{i=1}^{m} q_i D^i$ a $K : \mathbb{F}((D)) \to \mathbb{F}((D))$ je konvoluce daná předpisem $K(u) = u\frac{p}{q}$, tedy $(K, (\frac{p}{q}))$ je fyzický konvoluční kódovač. Definujme $\delta : \mathbb{F}^m \times \mathbb{F}^1 \to \mathbb{F}^m$ a $\lambda : \mathbb{F}^m \times \mathbb{F}^1 \to \mathbb{F}^1$ předpisem

$$\delta(\mathbf{s}, t) = (t - \sum_{j=1}^{m} q_j \mathbf{s}^{(j)}, \mathbf{s}^{(1)}, \ldots, \mathbf{s}^{(m-1)}) \quad \text{a} \quad \lambda(\mathbf{s}, t) = p_0 t + \sum_{j=1}^{m} (p_j - p_0 q_j)\mathbf{s}^{(j)}.$$

Potom

(1) $\delta(\mathbf{s}, u) = \mathbf{s} \cdot \begin{pmatrix} -q_1 & & \\ \cdot & & I_{m-1} \\ -q_{m-1} & & \\ -q_m & 0 \quad \ldots \quad 0 & \end{pmatrix} + u \cdot (1, 0, \ldots, 0),$

$\lambda(\mathbf{s}, u) = \mathbf{s} \cdot \begin{pmatrix} p_1 - p_0 q_1 \\ \ldots \\ p_m - p_0 q_m \end{pmatrix} + u \cdot p_0,$

(3) (K, δ, λ) je abstraktní konvoluční kódovač.

Důkaz. (1) Jedná se jen o maticový zápis definice δ a λ.

(2) Pro $u = \sum_{i \geq z} u_i D^i$ položme $\mathbf{s}_z = \mathbf{0}$,$\mathbf{s}_{i+1} = \delta(\mathbf{s}_i, u_i)$ a $\mathbf{v}_i = \lambda(\mathbf{s}_i, u_i)$ pro každé $i \geq z$. Definujeme-li $\sigma_i = \mathbf{s}_{i+1}^{(1)}$ a $\sigma = \sum_{i \geq z} \sigma_i D^i$, pak vidíme, že $\mathbf{s}_{i+1} = (\sigma_i, \sigma_{i-1}, \ldots, \sigma_{i-m+1})$ a dále

$$\sigma \cdot q = \sum_{i \geq z} (\sigma_i + \sum_{j=1}^{m} \sigma_{i-j} q_j) D^i = \sum_{i \geq z} u_i D^i = u,$$

$$\sigma \cdot p = \sum_{i \geq z} (\sum_{j=0}^{m} \sigma_{i-j} p_j) D^i = \sum_{i \geq z} (p_0 (u_i - \sum_{j=1}^{m} \sigma_{i-j} q_j) + \sum_{j=1}^{m} p_j \mathbf{s}_i^{(j)}) D^i =$$

$$= \sum_{i \geq z} (p_0 u_i + \sum_{j=1}^{m} (p_j - p_0 q_j)\mathbf{s}_i^{(j)}) D^i = v.$$

Odtud dostáváme, že $\frac{v}{p} = \sigma = \frac{u}{q}$, a proto $v = u\frac{p}{q}$ a $K(u) = v$. □

Věta 10.3. Abstraktní konvoluční kódovač lze realizovat jako fyzický konvoluční kódovač a naopak.

Důkaz. Předpokládejme, že (K, δ, λ) je abstraktní konvoluční kódovač daný maticemi P, Q, R, S, tedy $\mathbf{s}_{i+1} = \mathbf{s}_i P + \mathbf{u}_i Q$ $\mathbf{v}_{i+1} = \mathbf{s}_i R + \mathbf{u} - iS$ pro všechna $i \geq z$ a pro $\mathbf{s}_z = \mathbf{0}$. Položíme-i $u = \sum_{i\geq z} \mathbf{u}_i D^i$, $s = \sum_{i\geq z} \mathbf{s}_i D^i$ a $v = \sum_{i\geq z} \mathbf{v}_i D^i$, pak

$$D^{-1}s = \sum_{i\geq z} \mathbf{s}_{i+1} D^i = \sum_{i\geq z} \mathbf{s}_i D^i P + \sum_{i\geq z} \mathbf{u}_i D^i Q = sP + uQ.$$

To snadno upravíme na $uQ = sD^{-1}(I_m - DP)$, proto $s = uQ(I_m - DP)^{-1}D$, kde po dosazení 0 za D dostaneme $\det(I_m - DP)(0) = \det I_m = 1$, tedy matice $(I_m - DP)$ je nad tělesem $\mathbb{F}((D))$ opravdu invertibilní. Podobně

$$v = \sum_{i\geq z} \mathbf{v}_i D^i = \sum_{i\geq z} \mathbf{s}_i D^i R + \sum_{i\geq z} \mathbf{u}_i D^i S = sR + uS = u(S + Q(I_m - DP)^{-1}DR).$$

Tedy $G = DQ(I_m - DP)^{-1}R + S \in \mathbb{F}(D) \cap \mathbb{F}[[D]]$, protože $(I_m - DP)^{-1} = \sum_{i\geq 0} P^i D^i$. To znamená, že $K(u) = uG$, a protože je K podle definice prosté, je G generující matice konvolučního kódu a (K, G) je tudíž fyzický konvoluční kódovač.

Nyní předpokládejme, že $G = (\frac{p_{ij}}{q_i})_{ij} \in (\mathbb{F}(D) \cap \mathbb{F}[[D]])^{k\times n}$ je generující matice ve značení 9.2, pro niž $K(u) = uG$. Označme $\nu_i = \max(\deg(p_{i1}), \ldots, \deg(p_{ic}), \deg(q_i))$, $\nu = \sum_{i=1}^{k} \nu_i = \operatorname{extdeg}(G)$ a koeficienty polynomů $p_{ij} = \sum_{s=0}^{\nu_i} (p_{ij})_s D^s$. Definujme matice

$$P_i = \begin{pmatrix} -(q_i)_1 & & & \\ \cdot & & I_{\nu_i - 1} & \\ -(q_i)_{\nu_i - 1} & & & \\ -(q_i)_{\nu_i} & 0 & \ldots & 0 \end{pmatrix} \in \mathbb{F}^{\nu_i \times \nu_i}, \quad P = \begin{pmatrix} P_1 & 0_{\nu_1\times\nu_2} & \ldots & 0_{\nu_1\times\nu_k} \\ 0_{\nu_2\times\nu_1} & P_2 & \ldots & 0_{\nu_2\times\nu_k} \\ \cdot & \cdot & \ldots & \cdot \\ 0_{\nu_k\times\nu_1} & 0_{\nu_k\times\nu_2} & \ldots & P_k \end{pmatrix} \in \mathbb{F}^{\nu\times\nu},$$

$$\mathbf{e}_{\nu_i} = (1, 0, \ldots, 0) \in \mathbb{F}^{\nu_i}, \qquad Q = \begin{pmatrix} \mathbf{e}_{\nu_1} & 0_{1\times\nu_2} & \ldots & 0_{1\times\nu_k} \\ 0_{1\times\nu_1} & \mathbf{e}_{\nu_1} & \ldots & 0_{1\times\nu_k} \\ \cdot & \cdot & \ldots & \cdot \\ 0_{1\times\nu_1} & 0_{1\times\nu_2} & \ldots & \mathbf{e}_{\nu_k} \end{pmatrix} \in \mathbb{F}^{k\times\nu},$$

$$R_i = \begin{pmatrix} (p_{i1})_1 - (p_{i1})_0(q_i)_1 & \ldots & (p_{in})_1 - (p_{in})_0(q_i)_1 \\ (p_{i1})_2 - (p_{i1})_0(q_i)_2 & \ldots & (p_{in})_2 - (p_{in})_0(q_i)_2 \\ \cdot & \ldots & \cdot \\ (p_{i1})_{\nu_i} - (p_{i1})_0(q_i)_{\nu_i} & \ldots & (p_{in})_{\nu_i} - (p_{in})_0(q_i)_{\nu_i} \end{pmatrix} \in \mathbb{F}^{\nu_i\times n}, \quad R = \begin{pmatrix} R_1 \\ R_2 \\ \cdot \\ \cdot \\ R_k \end{pmatrix} \in \mathbb{F}^{\nu\times n}$$

a $S = \begin{pmatrix} (p_{11})_0 & \ldots & (p_{1n})_0 \\ (p_{21})_0 & \ldots & (p_{2n})_0 \\ \cdot & \ldots & \cdot \\ (p_{k1})_0 & \ldots & (p_{kn})_0 \end{pmatrix} \in \mathbb{F}^{k\times n}$. Nyní díky 10.2 dostáváme, že $\mathbf{s}_{i+1} = \mathbf{s}_i P + \mathbf{u}_i Q$ $\mathbf{v}_{i+1} = \mathbf{s}_i R + \mathbf{u}_i S$. □

Příklad 10.4. (1) Aplikujme důkaz 10.3 na abstraktní konvoluční kódovač K z 10.1 s maticemi

$$P = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, Q = \begin{pmatrix} 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

Potom $\tilde{G} = D \cdot Q \cdot (I_2 - DP)^{-1} \cdot R + S =$

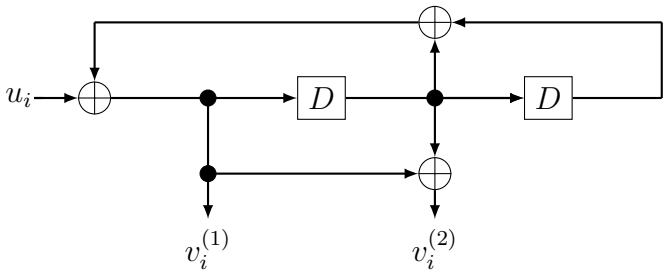
$$= D \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -D \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \end{pmatrix} = \begin{pmatrix} 1+D^2 & 1+D+D^2 \end{pmatrix}.$$

Tedy $\tilde{G} = G$ z 9.4.

(2) Pro generujíc matici $G = \begin{pmatrix} \frac{1}{1+D+D^2} & \frac{1+D}{1+D+D^2} \end{pmatrix}$ nad $\mathbb{F}_2$ vidíme, že $\operatorname{extdeg} G = 2$ a pomocí důkazu předchozí věty spočítáme matice určující abstraktní konvoluční kódovač pro fyzický kódovač $K(u) = uG$:

$$P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, Q = \begin{pmatrix} 1 & 0 \end{pmatrix}, R = \begin{pmatrix} 0-1\cdot 1 & 1-1\cdot 1 \\ 0-1\cdot 1 & 0-1\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

a snadno znázorníme obvod popisující daný fyzický konvoluční kódovač:



(3) Pro polynomiální matici $G = \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D+D^2 & D^2 & 1 \end{pmatrix}$ nad $\mathbb{F}_2$ určíme $\operatorname{extdeg} G = 2+2 = 4$ a opět z důkazu předchozí věty spočítáme matice určující abstraktní konvoluční kódovač pro fyzický kódovač $K(u) = uG$:

$$P_i = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{proto} \quad P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$Q = \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} R = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

(4) Pro generující matici $\tilde{G} = \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D+D^2 & D^2 & 1 \end{pmatrix}$ nad $\mathbb{F}_2$ téhož konvolučního kódu jako v (2) opět spočítáme $\operatorname{extdeg} \tilde{G} = 2+1 = 3$ a matice určující abstraktní konvoluční kódovač pro $\tilde{K}(u) = u\tilde{G}$:

$$\tilde{P} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tilde{Q} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tilde{R} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \tilde{S} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

11. Polynomiální generující matice

V této sekci se budeme věnovat hledání popisu minimálních kódování konvolučního kódu pomocí jistých algebraických vlastností generující matice. Polynomiální generující matici daného kódu, která bude disponovat těmito vlastnostmi a které budeme říkat kanonická matice, a díky tomu i odpovídající fyzický i abstraktní konvoluční kódovač, budeme navíc s to efektivně zkonstruovat.

V následujícím bude $\mathbb{F}$ značit konečné těleso a k a n přirozená čísla.

T&N. Nechť $A \in \mathbb{F}[D]^{n\times n}$ $C, M \in \mathbb{F}[D]^{k\times n}$. Řeknem, že je matice A *unimodulární*, pokud $\exists A^{-1} \in \mathbb{F}[D]^{n\times n}$. Jsou-li L a P unimodulární a $M = \begin{pmatrix} \delta_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \delta_2 & \dots & 0 & 0 & \dots & 0 \\ . & . & \dots & . & 0 & \dots & 0 \\ 0 & 0 & \dots & \delta_k & 0 & \dots & 0 \end{pmatrix}$ pro monické nebo nulové polynomy $\delta_i \in \mathbb{F}[D]$ splňující podmínku $\delta_i | \delta_{i+1}$ pro všechna $i = 1, \dots, k-1$, pak $C = LMP$ nazveme *Smithův rozklad* matice C, kde M je *Smithova normální forma* (SNF) matice C.

Pozorování. Je-li $A \in \mathbb{F}[D]^{n\times n}$ a $p \in \mathbb{F}[D]$, pak

(1) A je unimodulární $\Leftrightarrow \det A \in \mathbb{F}^*$,
(2) elementární matice přičtení p násobku řádku k jinému je unimodulární,
(3) jsou-li $a, b \in \mathbb{F}[D]$ nesoudělné, a proto existuje $u, v \in \mathbb{F}[D]$, pro něž $ua + bv = 1$, je matice $\begin{pmatrix} a & -v \\ b & u \end{pmatrix}$ unimodulární.

Důkaz následujícího tvrzení, který je založen na myšlence Gaussovy eliminace nad okruhem polynomů s využitím Eukleidova algoritmu a Bezoutových koeficientů, vynecháme.

Fakt 11.1. Polynomiální matice má nějaký Smithův rozklad a její SNF je určen jednoznačně.

Třebaže nebudeme formálně popisovat algoritmus hledání SNF, zkusíme ho v jednoduchých příkladech pomocí Pozorování najít:

Příklad 11.2. (1) Pro $A = \begin{pmatrix} 1+D & -D \\ D & 1-D \end{pmatrix} \in \mathbb{F}[D]^{2\times 2}$ je $A^{-1} = \begin{pmatrix} 1-D & D \\ -D & 1+D \end{pmatrix}$, tedy se jedná o unimodulární matici s determinantem $\det A = 1$. Potom SNF matice C je I_2 a její Smithův rozklad je například tvaru $A = A \cdot I_2 \cdot I_2 = I_2 \cdot I_2 \cdot A$.

(2) Hledáme Smithův rozklad matice $G = \begin{pmatrix} 1+D^2 & 1+D^3 & D+D^2 \\ 1+D & 1+D^2 & 1+D \end{pmatrix}$ nad $\mathbb{F}_2$. Nejprve přehodíme dva řádky a $(1+D)$ násobek nového prvního řádku přičteme k druhému a poté upravujeme pomocí sloupcových úprav:

$$G \sim \begin{pmatrix} 1+D & 1+D^2 & 1+D \\ 0 & D+D^2 & 1+D \end{pmatrix} \sim \begin{pmatrix} 1+D & 0 & 0 \\ 0 & 1+D & D+D^2 \end{pmatrix} \sim \begin{pmatrix} 1+D & 0 & 0 \\ 0 & 1+D & 0 \end{pmatrix}$$

Snadno zaznamenáme řádkové a sloupcové úpravy do matic

$$L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1+D & 1 \end{pmatrix} = \begin{pmatrix} 1+D & 1 \\ 1 & 0 \end{pmatrix},$$

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1+D \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & D \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & D \end{pmatrix},$$

pro něž dostáváme Smithův rozklad

$$G = \begin{pmatrix} 1+D & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1+D & 0 & 0 \\ 0 & 1+D & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & D \end{pmatrix}.$$

V následujícím uvažujme $G = \begin{pmatrix} \mathbf{g}_1 \\ \dots \\ \mathbf{g}_k \end{pmatrix} \in \mathbb{F}[D]^{k\times n}$ pro $\mathbf{g}_i = (g_{i1}, \dots, g_{in}) \in \mathbb{F}[D]^n$ generující matici konvolučního kódu $\mathcal{C}$, kde $\nu_i = \deg \mathbf{g}_i := \max(\deg g_{i1}, \dots, \deg g_{in})$.

T&N. *Vnitřní stupeň* matice G je hodnota

$$\operatorname{intdeg} G = \max\{\deg\det(H) \mid H \in \mathbb{F}[D]^{k\times k} \text{ vznikne vypuštěním } n-k \text{ sloupců z } G\}.$$

Pro $\tilde{G} \in \mathbb{F}[D]^{k\times n}$ platí, že $\tilde{G} \sim G$, pokud existuje $T \in \mathbb{F}(D)^{k\times k}$ invertibilní, pro kterou $TG = \tilde{G}$. Řekneme, že generující matice G je *základní*, pokud

$$\operatorname{intdeg} G = \min\{\operatorname{intdeg}\tilde{G} \mid \tilde{G} \in \mathbb{F}[D]^{k\times n}, \tilde{G} \sim G\}.$$

Pozorování. Je-li $T \in \mathbb{F}[D]^{k\times k}$ a $\det(T) \neq 0$, pak

(1) $\operatorname{intdeg} TG = \deg\det(T) + \operatorname{intdeg} G$, proto $\operatorname{intdeg} G \leq \operatorname{intdeg} TG$,
(2) $\operatorname{intdeg} G = \operatorname{intdeg} TG \Leftrightarrow \deg\det(T) = 0 \Leftrightarrow T$ je unimodulární,
(3) $\exists M = \begin{pmatrix} \mathbf{m}_1 \\ \dots \\ \mathbf{m}_k \end{pmatrix} \in \mathbb{F}[D]^{k\times k}$ složená ze sloupců matice G, pro niž $\operatorname{intdeg} G =$

$$= \deg\det(M) = \deg \sum_{\sigma\in S_k} \operatorname{sgn}\sigma \prod_i \mathbf{m}_i^{(\sigma(i))} \leq \max_{\sigma\in S_k}(\sum_i \deg \mathbf{m}_i^{(\sigma(i))}) \leq \sum_i \nu_i = \operatorname{extdeg} G.$$

Následující charakterizace je užitečná pro konstrukce základních matici.

Poznámka 11.3. Následující je pro matici G ekvivalentní:

(1) G je základní,
(2) SNF matice G je tvaru $(I_k|\mathbf{0})$,
(3) G lze doplnit $n-k$ polynomiálními řádky na unimodulární matici,
(4) $\exists R \in \mathbb{F}[D]^{n\times k}$, pro niž $GR = I_k$.

Důkaz. (1) $\Rightarrow$ (2) Nechť $G = L(S|\mathbf{0})R$ je Smithův rozklad, kde $S = \operatorname{Diag}(\delta_1, \dots, \delta_k) \in \mathbb{F}[D]^{k\times k}$ je diagonální čtvercová matice. Potom $G = LSR_1$ pro matici R_1, která vznikne z R vypuštěním posledních $n-k$ sloupců, a proto podle Pozorování (1) platí, že

$$\operatorname{intdeg} G = \deg(\det(LS)) + \operatorname{intdeg} R_1 = \deg\det L + \deg\det S + \operatorname{intdeg} R_1.$$

Protože je G základní a $G \sim R_1$, dostáváme, že $\deg\det L = \deg\det s = 0$, což znamená, že $\delta_i = 1$ pro všechna $i = 1, \dots, k$, neboť je matice S hodnosti k.

(2) ⇒ (3) Podle předpokladu existují matice $L \in \mathbb{F}[D]^{k\times k}$, $R_1 \in \mathbb{F}[D]^{k\times n}$ a $R_2 \in \mathbb{F}[D]^{(n-k)\times n}$, pro něž $G = L\begin{pmatrix} I_k & \mathbf{0}\end{pmatrix}\begin{pmatrix} R_1 \\ R_2\end{pmatrix}$. Nyní vidíme, že $\begin{pmatrix} G \\ R_2\end{pmatrix} = \begin{pmatrix} L & \mathbf{0} \\ \mathbf{0} & I_{n-k}\end{pmatrix}\begin{pmatrix} R_1 \\ R_2\end{pmatrix}$ je unimodulární matice.

(3) ⇒ (4) Je-li $C \in \mathbb{F}[D]^{(n-k)\times n}$ matice, pro niž je $\begin{pmatrix} G \\ C\end{pmatrix}$ unimodulární, pak existují matice $H_1 \in \mathbb{F}[D]^{n\times k}$ a $H_2 \in \mathbb{F}[D]^{n\times(n-k)}$, pro které platí, že $\begin{pmatrix} G \\ C\end{pmatrix}\begin{pmatrix} H_1 & H_2\end{pmatrix} = I_n$. Potom $GH_1 = I_k$.

(4) ⇒ (1) Nechť $GR = I_k$ pro nějakou matici $R \in \mathbb{F}[D]^{n\times k}$. Zvolme $T \in \mathbb{F}(D)^{k\times k}$, pro kterou $TG \in \mathbb{F}[D]^{k\times n}$. Potom i $T = TGR \in \mathbb{F}[D]^{k\times n}$ a proto podle Pozorování (1) platí, že $\operatorname{intdeg} G \le \operatorname{intdeg} TG$, proto je G základní. □

T&N. Řekneme, že G je *redukovaná*, pokud

$$\operatorname{extdeg} G = \min\{\operatorname{extdeg} TG \mid T \in \mathbb{F}[D]^{k\times k} \text{ je unimodulární}\}.$$

Označíme-li $\overline{g}_{ij}$ koeficient termu D^{ν_i} polynomu $\mathbf{g}_i^{(j)}$ v G, pak $\overline{G} = (\overline{g}_{ij})_{ij} \in \mathbb{F}^{k\times n}$ se nazývá *matice nejvyšších koeficientů*.

Poznámka 11.4. Následující je pro matici G ekvivalentní:

(1) G je redukovaná,
(2) $\operatorname{rank}\overline{G} = k$,
(3) $\operatorname{intdeg} G = \operatorname{extdeg} G$.

Důkaz. (1) ⇒ (2) Tvrzení dokážeme nepřímo a budeme předpokládat, že $\operatorname{rank}\overline{G} < k$, což znamená, že existuje vektor nenulový $\mathbf{y} \in \mathbb{F}^k$, pro který $\mathbf{y}\overline{G} = \mathbf{0}$. Bez újmy na obecnosti můžeme předpokládat, že $\nu_1 \le \nu_2 \le \cdots \le \nu_k$, zvolíme $s \ge k$ největší takové, že $\mathbf{y}^{(s)} \neq 0$ a definujeme polynom $\tilde{\mathbf{g}}_s = \sum_{j=1}^{s} \mathbf{y}^{(j)} D^{\nu_s-\nu_j}\mathbf{g}_j$. Protože mají všechny sčítance stupeň právě ν_s a koeficienty termu D^{ν_s} polynomiálního vektoru $\tilde{\mathbf{g}}_s$ se vynulují, dostáváme, že $\deg\tilde{\mathbf{g}}_s < \nu_s$. Vytvoříme-li nyní matici T z jednotkové matice stupně k tak, že nahradíme její s-tý řádek řádkem $(\mathbf{y}^{(1)}D^{\nu_s-\nu_1}, \mathbf{y}^{(2)}D^{\nu_s-\nu_2}, \ldots, \mathbf{y}^{(s)}D^{\nu_s-\nu_s}, 0\ldots, 0)$, platí, že $\det T = \mathbf{y}^{(s)} \in \mathbb{F}^*$, a tudíž jde o unimodulární matici. Protože matice TG vznikne z G právě nahrazením s-tého řádku vektorem $\tilde{\mathbf{g}}_s$, vidíme, že

$$\operatorname{extdeg} TG = \deg\tilde{\mathbf{g}}_s + \sum_{j\neq s}\nu_j < \sum_{j=1}^{k}\nu_j = \operatorname{extdeg} G,$$

proto matice G není redukovaná.

(2) ⇒ (3) Protože $\operatorname{rank}\overline{G} = k$, existuje čtvercová matice $M \in \mathbb{F}^{k\times k}$ vzniklá vypuštěním vhodných $n-k$ sloupců G tak, aby platilo, že $\det\overline{M} \neq 0$. Protože jsme si všimli, že $\operatorname{intdeg} M \le \operatorname{extdeg} M \le \operatorname{extdeg} G$ a $\det\overline{M}$ je nenulový koeficient u $D^{\operatorname{extdeg} G}$, vidíme, že $\operatorname{extdeg} G \le \operatorname{intdeg} M \le \operatorname{intdeg} G$, tudíž $\operatorname{extdeg} G = \operatorname{intdeg} G$.

(3) ⇒ (1) Pro každou unimodulární matici T platí, že $\operatorname{intdeg} G = \operatorname{intdeg} TG$ díky Pozorování(2), proto

$$\operatorname{extdeg} G = \operatorname{intdeg} G = \operatorname{intdeg} TG \le \operatorname{extdeg} TG,$$

odkud už podle definice plyne, že je G je redukovaná. □

Definice. Řekneme, že G je *kanonická*, je-li základní a redukovaná.

Věta 11.5. Generující matice G konvolučního kódu $\mathcal{C}$ je kanonická právě tehdy, když $\operatorname{extdeg} G = \deg \mathcal{C}$.

Důkaz. Označme $\hat{G}$ polynomiální matici nejmenšího možného vnitřního stupně splňující $G \sim \hat{G}$. Podle definice existuje generující matice $G' \sim G$, pro níž $\operatorname{extdeg} G' = \deg \mathcal{C}$, kterou díky 9.2 můžeme vzít polynomiální, neboť stačí každý její řádek přenásobit společným jmenovatelem. Protože $\operatorname{intdeg} G' \leq \operatorname{extdeg} G' = \deg \mathcal{C}$ podle Pozorování (3), plyne z minimality volby $\operatorname{intdeg} \hat{G}$, že rovněž $\operatorname{intdeg} \hat{G} \leq \deg \mathcal{C}$. Protože existuje unimodulární matice $T \in \mathbb{F}[D]^{k\times k}$, pro niž $\tilde{G} = T\hat{G}$ má nejmenší možný vnější stupeň, platí díky Pozorování (2), že

$$\operatorname{intdeg} \tilde{G} = \operatorname{intdeg} \hat{G} \leq \deg \mathcal{C} \leq \operatorname{extdeg} \tilde{G}.$$

Podle definice je tedy $\tilde{G}$ redukovaná, tudíž díky 11.4 platí, že $\operatorname{intdeg} \tilde{G} = \operatorname{extdeg} \tilde{G} = \deg \mathcal{C}$. Z předchozího plyne, že

$$\deg \mathcal{C} = \operatorname{intdeg} \tilde{G} \leq \operatorname{intdeg} G \leq \operatorname{extdeg} G.$$

Odtud vidíme, že $\deg \mathcal{C} = \operatorname{extdeg} G$, právě když jsou všude v předchozí nerovnosti rovnosti, což nastává, právě když je G kanonická matice. □

Příklad 11.6. (1) Matice $G = \begin{pmatrix} D & 1+D^2 \end{pmatrix}$ má SNF tvaru $\begin{pmatrix} 1 & 0 \end{pmatrix}$, neboť D a $1+D^2$ jsou nesoudělné, proto je G podle 11.3 základní. Dále $\overline{G} = \begin{pmatrix} 0 & 1 \end{pmatrix}$, proto je G podle 11.4 redukovaná, tudíž je kanonická.

(2) Čtvercová matice je redukovaná, právě když je unimodulární.

Čtvercová matice G je kanonická $\Leftrightarrow$ G je unimodulární a $\operatorname{extdeg} G = \operatorname{intdeg} G \Leftrightarrow$ $G \in \mathbb{F}^{k\times k}$ je regulární.

O stupni konvolučního kódu (a tedy vnějším i vnitřním stupni každé jeho kanonické generující matice) se dá dále dokázat, že se rovná dimenzi takzvaného prostoru abstraktních stavů, která je nejmenší možnou dimenzí stavového prostoru pro jakoukoli jeho realizaci abstraktním konvolučním kódovačem.

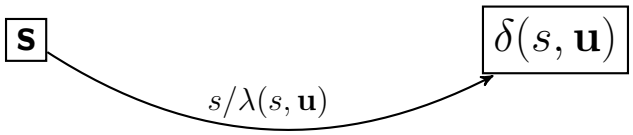
To znamená, že stavový prostor abstraktního konvolučního kódovače, který sestrojíme pomocí kanonické matice a Věty 10.3 nabývá minimální možné dimenze.

12. Viterbiho dekódování

Na závěr nabídneme dvě těsně související prezentace abstraktního konvolučního kódovače pomocí multigrafů. Postupné procházení jejich cest po vrstvách odpovídajícím jednotlivým časovým okamžikům kódování nám poskytne velmi přirozený a efektivní dekódovací algoritmus, který najde vstupní posloupnost s nějvyšší pravděpodobností podmíněnou předpokladem přijetí konkrétní chybové posloupnosti, tedy tu, jejíž zakódování je v Hammingově metrice nejblíže přijaté posloupnosti.

V celé kapitole uvažujeme abstraktní konvoluční kódovač (K, δ, λ) se stavovým prostorem $S = \mathbb{F}^m$ a konvolučním kódovačem $K : \mathbb{F}((D))^k \to \mathbb{F}((D))^n$. Dále označme $q = |\mathbb{F}|$, tedy $\mathbb{F} = \mathbb{F}_q$.

T&N. *Multigrafem konvolučního kódovače* (K, δ, λ) budeme rozumět orientovaný ohodnocený multigraf (což je přímočaré zobecnění pojmu graf připouštějící více hran mezi stejnými vrcholy) s vrcholy danými množinou S, jehož ohodnocené hrany jsou právě tvaru

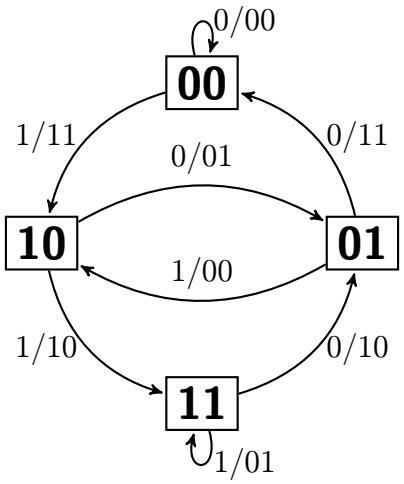


pro všechna $s \in S$ a $\mathbf{u} \in \mathbb{F}^k$.

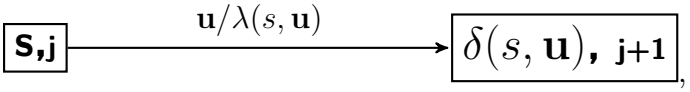
Příklad 12.1. Konvoluční kódovač z Příkladů 9.4, 10.1 a 10.4(1), kde pro $S = \mathbb{F}^2$ máme

$$\delta(\mathbf{s}, \mathbf{u}) = \mathbf{s}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \mathbf{u}\begin{pmatrix} 1 & 0 \end{pmatrix} \quad \text{a} \quad \lambda(\mathbf{s}, \mathbf{u}) = \mathbf{s}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \mathbf{u}\begin{pmatrix} 1 & 1 \end{pmatrix},$$

popíšeme následujícím multigrafem



T&N. *Mřížoví* (*trellis diagram*) konvolučního kódovače (K, δ, λ) je nekonečný ohodnocený orientovaný multigraf s vrcholy $\{(\mathbf{0}, 0)\} \cup S \times \mathbb{N}$, jehož ohodnocené hrany jsou právě tvaru



pokud do vrcholu (s, j) vede nějaká hrana nebo $(s, j) = (\mathbf{0}, 0)$. Je-li $j \geq 0$, pak se úplný podgraf mřížoví sestávající z hran začínajících ve vrcholech (s, j) pro libovolné $s \in S$ nazývá *j-tou vrstvou mřížoví*.

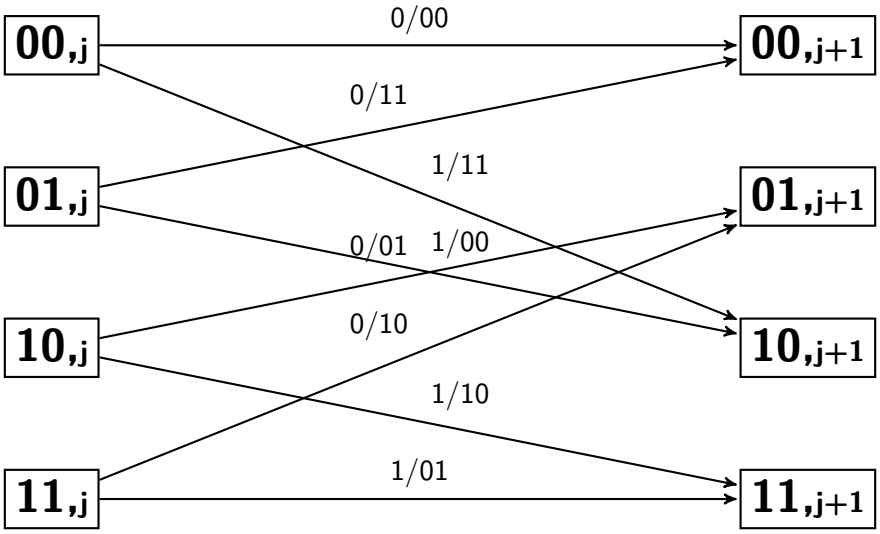
Nadéle bude značit $\mathcal{M} = (\{(\mathbf{0}, 0)\} \cup S \times \mathbb{N}, H)$, kde H představuje množinu hran, mřížoví konvolučního kódovače (K, δ, λ).

Pozorování. Pro $\mathcal{M}$ platí, že

(1) vrstva mřížoví (K, δ, λ) je bipartitní ohodnocený orientovaný multigraf, který obsahuje nejvýše $|S| = |\mathbb{F}_q^m| = q^m$ počátečních i koncových vrcholů a nejvýše $|S| \cdot |\mathbb{F}_q^k| = q^{m+k}$ hran,

(2) orientovaná cesta $h_0h_1h_2\ldots$ s ohodnocením hrany h_i tvaru $\mathbf{u}_i/\mathbf{v}_i$ reprezentuje kódování $\sum_{i\geq 0}\mathbf{v}_iD^i = K(\sum_{i\geq 0}\mathbf{u}_iD^i)$.

Příklad 12.2. Pro konvoluční kódovač z Příkladu 12.1 máme j-tou vrstvu mřížoví pro každé $j > 1$ ve tvaru



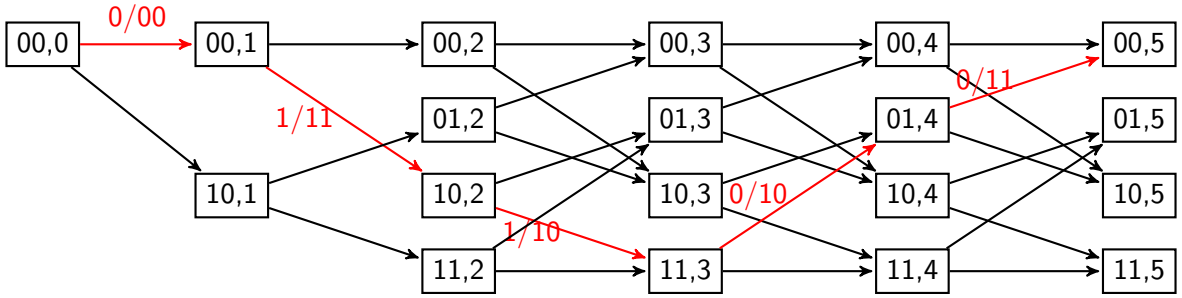
Nyní zakódujme polynom $\mathbf{u} = D+D^2$ a obdržíme $\mathbf{v} = K(\mathbf{u}) = \mathbf{u}(1+D^2, 1+D+D^2) =$

$$= (D + D^2 + D^3 + D^4, D + D^4) \sim 00D^0 + 11D^1 + 10D^2 + 10D^3 + 11D^4,$$

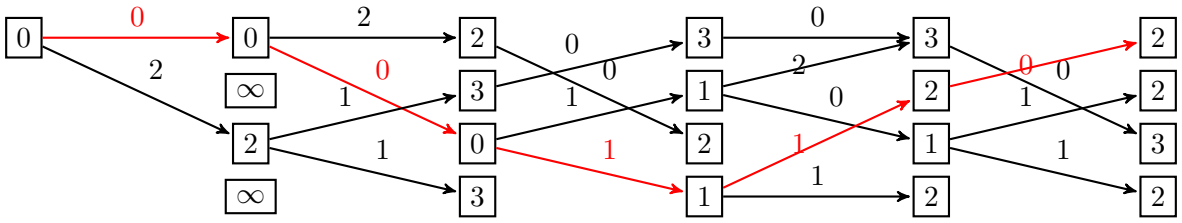
které reprezentuje posloupnost $(00, 11, 10, 10, 11)$. Přijmeme-li posloupnost s dvěma bitovými chybami $\mathbf{y} = (00, 11, 1\mathbf{1}, \mathbf{0}0, 11)$, která odpovídá polynomu

$$y = 00D^0 + 11D^1 + 11D^2 + 00D^3 + 11D^4,$$

snažíme se ji aproximovat „nejbližší" ohodnocenou cestou v mřížoví tj. hledáme takové $\hat{\mathbf{u}}$, aby $P[\mathbf{y} \mid K(\hat{\mathbf{u}})]$ byla minimální, tj. aby byl minimální součet $\sum d(\mathbf{y}_i, K(\mathbf{u})_i)$:

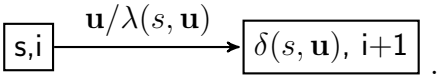


Zapíšeme si do grafu součet vzdáleností přijaté dvojice bitů a dvojici z kódové posloupnosti, což je myšlenka dekódovacího algoritmu, který následně popíšeme. V každém stavu v každé vrstvě vybereme ty hrany, které prodlužují dosavadní minimální cestu, která do tohoto stavu vede, tak, aby byla cesta opět minimální:



Ačkoli do vrcholů v čase 5 vedou tři cesty s váhou 2, vybereme tu, která končí ve stavu 00, neboť ta reprezentuje polynom stupně 4, což je parametr polynomu, o němž víme, že ho máme přijmout, ostatní cesty totiž reprezentují polynom vyššího stupně a vyšší váhy.

T&N. Nechť $s \in S$, $l \in \mathbb{N}$, $P = h_1 \dots h_l \in \mathcal{P}_l(\mathcal{M})$, kde $h_i \in H$ a $\mathcal{P}_l(\mathcal{M})$ značí množinu všech orientovaných cest délky l. Označme $i(P)$ počáteční vrchol, $t(P)$ koncový vrchol a $l(p) = l$ délku cesty P. Nechť $y = \sum \mathbf{y}_i D^i \in \mathbb{F}^n[[D]]$ a definujme $\mu_y : \bigcup_l \mathcal{P}_l(\mathcal{M}) \to \mathbb{N} \cup \{0\}$ předpisem $\mu_y(P) = \sum_{i=1}^{l} \mu_y(h_i)$, kde $\mu_y(P)$ představuje Hammingovu vzdálenost $\mu_y(h_i) = d(\mathbf{y}_i, \lambda(s, \mathbf{u}))$ pro hranu h_i tvaru



Dále řekneme, že je cesta P *minimální pro* y, pokud

$$\mu_y(P) = \min\{\mu_y(Q) \mid Q \in \mathcal{P}_l(\mathcal{M}) : i(Q) = i(P), t(Q) = t(P)\}.$$

Pozorování. Nechť $l, r \in \mathbb{N}$, $y \in \mathbb{F}^n[[D]]$, $P \in \mathcal{P}_l(\mathcal{M})$, $Q \in \mathcal{P}_r(\mathcal{M})$ a $i(Q) = t(P)$.

(1) Pokud $i(P) = (s, j)$, pak existuje $\tilde{s} \in S$, pro které $t(P) = (\tilde{s}, j + l)$,
(2) $\mu_y(PQ) = \mu_y(P) + \mu_y(Q)$,
(3) je-li PQ minimální cesta pro y, pak P i Q jsou minimální cesty pro y.

Poznámka 12.3. Nechť $y \in \mathbb{F}^n[[D]]$, $l \in \mathbb{N}$ a $s \in S$. Označme pro každé $z \in S$ minimální cestu $P_z \in \mathcal{P}_l(\mathcal{M})$ pro y splňující $i(P_z) = (\mathbf{0}, 0)$ a $t(P_z) = (z, l)$, dále seřaďme $h_1, \dots, h_r \in H$ všechny ohodnocené hrany splňující $i(h_j) = (s_j, l)$ pro nějaké $s_j \in S$. Pokud $i = \arg\min_j(\mu_y(P_{s_j}) + \mu_y(h_j))$, pak je $P_{s_i} h_i$ minimální cesta pro y.

Důkaz. Vezměme cestu $P \in \mathcal{P}_{l+1}(\mathcal{M})$, která splňuje $i(P) = (\mathbf{0}, 0)$ a $t(P) = (s, l + 1)$. Potom existuje j a cesta $Q \in \mathcal{P}_l(\mathcal{M})$, pro něž platí $i(Q) = (\mathbf{0}, 0)$, $t(Q) = (s_j, l)$ a $P = Qh_j$. Z Pozorování (2) potom plyne, že

$$\mu_y(P) = \mu_y(Q) + \mu_y(h_j) \geq \mu_y(P_{s_j}) + \mu_y(h_j) \geq \mu_y(P_{s_i}) + \mu_y(h_i) = \mu_y(P_{s_i} h_i),$$

což znamená, že $\mu_y(P_{s_i} h_i)$ je minimální možné a to jsme potřebovali dokázat. □

Nyní už máme zavedeny všechny nástroje, abychom mohli formalizovat postup dekódování z Příkladu 12.2.

VITERBIHO ALGORITMUS
Vstup: $f \in \mathbb{N}$, $z \in S$, $y \in \mathbb{F}^n[[D]]$
Výstup: $P \in \mathcal{P}_l(\mathcal{M})$ minimální cesta pro y, kde $i(P) = (\mathbf{0}, 0)$ a $t(P) = (z, f)$
0. for $j = 0$ to f & for all $s \in S$ polož $\mu(s, j) := \infty$;
1. $\mu(\mathbf{0}, 0) := 0$; $P(\mathbf{0}, 0) :=$ prázdná cesta;

```
2. for j = 1 to f do
       for h ∈ H & s ∈ S splňující μ(s, j−1) < ∞ & i(h) = (s, j−1) do
           if μ_y(h) + μ(s, j−1) < μ(t(h)) then
               {P(t(h)) := P(s, j−1)h; μ(t(h)) := μ_y(h) + μ(s, j−1);
               }
3. return P(z, f)
```

Věta 12.4. Viterbiho algoritmus pracuje správně v čase $O(fq^{m+k})$ operací v $\mathbb{Z}$.

Důkaz. Korektnost plyne z 12.3 a časový odhad dostáváme aplikací pozorování o počtu vrcholů a hran jedné vrstvy. □

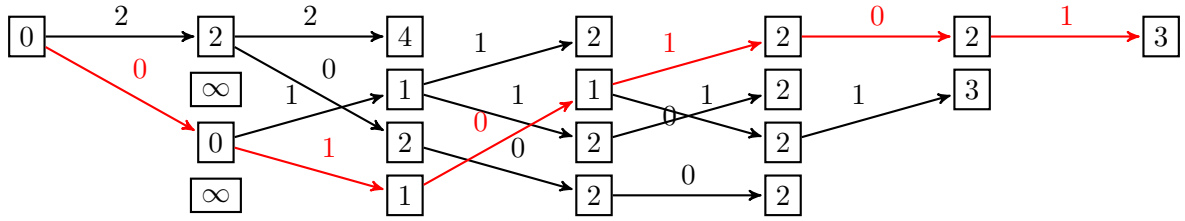
Dekódování

Pro přijatý (poškozený) polynom $y = \sum_{j=0}^{f-1} \mathbf{y}_j$ najdeme Viterbiho algoritmem orientovanou cestu $P = h_1 \dots h_{f-1}$ s hranou h_i ohodnocenou dvojicí $\mathbf{u}_i/\mathbf{v}_i$ pro $i = 1, \dots, f-1$, která splňuje

- buď $t(P) = (\mathbf{0}, f)$ (obvykle pro konvoluční kódovač bez zpětné vazby),
- nebo pro takové $t(P) = (z, f)$, aby $\mu_y(P)$ bylo minimální

Hledaný vzor $u = \sum_{i=0}^{f-1} \mathbf{u}_i$, který přečteme z ohodnocení hran nalezené cesty P, mimimalizuje vzdálenost $\sum_{j=0}^{f-1} d(\mathbf{y}_j, \mathbf{v}_j)$ pro polynom $v = \sum_{i=0}^{f-1} \mathbf{v}_i$, obsahující prvních f členů mocninné řady $K(u)$.

Příklad 12.5. Pro konvoluční kódovač z Příkladů 12.1 a 12.2 uvažujme přijatou posloupnost popsanou polynomem $y = 11D^0 + 11D^1 + 10D^2 + 01D^3 + 00D^4 + 01D^5$, o němž předpokládáme, že vznikl (omezeným) poškozením polynomu v stupně nejvýše 3 a budeme Viterbiho algoritmem hledat polynom $v = K(u)$ i původní zprávu u tak, abychom v čase 5 skončili ve stavu $\mathbf{0}$. Za využití 12.2 budeme průběh Viterbiho algoritmu zapisovat do následujícího multigrafu:



Vyznačená cesta odpovídá kódovému polynomu

$$v = 11D^0 + 10D^1 + 10D^2 + 11D^3 + 00D^4 + 00D^5,$$

který je obrazem zdrojového polynomu $u = 0D^0 + 1D^1 + 1D^2$.