

1 Lineární kódy

1.1 Hammingovy perfektní kódy

1.1. Necht' $H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ je kontrolní matice binárního lineárního kódu \mathcal{H} .

- (a) Najděte generující matici kódu \mathcal{H} ve standardním tvaru,
- (b) určete vzdálenost kódu \mathcal{H} a rozhodněte, zda je kód perfektní,
- (c) rozhodněte, zda je $v = 1000101$ kódové slovo a případně které je nejbližší kódové slovo ke slovu v .

(a) Najdeme bázi $\text{Ker}H_3 = \mathcal{H}$ a seřadíme ji do nějaké generující matice a tu upravíme pomocí Gaussovy-Jordanovy eliminace na odstupňovanou matici s kanonickými bazickými vektory (v této podobě ji můžeme rovnou hledat bázi):

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

(b) Stačí si všimnout, že žádný sloupec kontrolní matice H_3 není nulový ani není násobkem jiného sloupce, proto má kód vzdálenost aspoň 3. Naopak součet dokonce každých dvou sloupců je opět sloupcem matice, tedy náš kód má vzdálenost právě 3, a proto opraví právě jednu chybu.

Nyní snadno ověříme, že $1 + 7 = 2^{7-4}$, tedy se jedná o 1-perfektní kód.

(c) Stačí spočítat $(Hv^T)^T = 011 \neq 000$, což znamená, že $v = 1000101$ kódové slovo není. Proto 3. sloupec kontrolní matice H obsahuje právě vektor Hv^T stačí změnit 3. souřadnici slova v na slovo $c = 1010101$, aby $(Hc^T)^T = 000$. \square

Pro $l \in \mathbb{N}$ seřadíme všechna nenulová slova množiny \mathbb{F}_2^l do sloupců H_l , položíme $n := 2^l - 1$ a definujeme lineární kód $\mathcal{H}_l := \{c \in \mathbb{F}_2^n \mid Hc^T = 0^T\}$.

1.2. Pro $l \in \mathbb{N}$

- (a) ověřte, že je H_l kontrolní matice kódu \mathcal{H}_l ,

(b) určete vzdálenost a dimenzi \mathcal{H}_l a rozhodněte, zda je kód perfektní,

(c) navrhnete algoritmus, jak opravit jednu chybu přijatého slova.

(a) Stačí si všimnout, že ve sloupcích matice H_l máme kanonickou bázi vektorového prostoru \mathbb{F}_2^l , a tudíž má hodnotu rovnu počtu řádků.

(b) Provedeme-li stejnou úvahu jako v bodu (c) předchozí úlohy, vidíme, že vzdálenost kódu je 3, jedná se tedy o $[2^l-1, 2^l-l-1, 3]_2$ -kód, který opravuje 1 chybu. Snadno tedy zjistíme, že levá strana Hammingovy nerovnosti je rovna $1 + 2^l - 1 = 2^l$ a pravá strana má hodnotu $2^{2^l-1-(2^l-l-1)} = 2^l$. To znamená, že \mathcal{H}_l je o 1-perfektní kód.

(c) Kód je 1-perfektní, tedy pro každé nekódové slovo existuje ve vzdálenosti 1 právě jedno kódové slovo. Nechť v je přijaté slovo. Pokud $H_l v^T = \mathbf{0}^T$, pak $v \in \mathcal{H}_l$. Pokud $H_l v^T \neq \mathbf{0}^T$, pak existuje i , pro něž je $H_l v^T$ právě i -tým sloupcem. Nyní stačí vzít slovo $c = v + e_i$, pro něž platí, že $d(v, c) = 1$ a

$$cH_l^T = (v + e_i)H_l^T = vH_l^T + h_i = h_i + h_i = \mathbf{0}$$

tedy $c \in \mathcal{H}_l$ je opravené slovo.

Označíme-li $\alpha : \mathbb{F}_2^l \setminus \{0\} \rightarrow \{1, \dots, 2^l - 1\}$ zobrazení dané předpisem $\alpha(c_1 \dots c_l) = \sum_{i=1}^l c_i 2^{i-1}$, tj. $\alpha^{-1}(i)$ je právě binární zápis hodnoty $i \in \{1, \dots, 2^l - 1\}$ (doplňný nulami). Předpokládejme, že v i -tém sloupci matice H_l je právě $\alpha^{-1}(i)^T$. Potom každé slovo $c \in \mathbb{F}_2^l \setminus \mathcal{H}_l$ platí, že $c + e_{\alpha(cH^T)} \in \mathcal{H}_l$. \square

1.3. Nad konečným tělesem \mathbb{F}_q spočítejte velikost koule $V_q(n, r)$.

Nejprve spočítáme velikost množiny A_i všech slov váhy i :

$$|A_i| = |\{c \in \mathbb{F}_q^n \mid w(c) = n\}| = |\{I \subseteq \{1, \dots, n\} \mid |I| = i\}| \cdot |(\mathbb{F}_q^*)^i| = \binom{n}{i} (q-1)^i.$$

Potom dostáváme $V_q(n, r) = \sum_{i=0}^r \binom{n}{i} (q-1)^i$ \square

1.4. Nad konečným tělesem \mathbb{F}_q sestrojte obdobným způsobem jako v předchozí úloze kontrolní matici perfektního kódu délky $n := \frac{q^l-1}{q-1} = \sum_{i=0}^{l-1} q^i$ dimenze $n - l$. Jaká je jeho Hammingova vzdálenost?

Vezmeme množinu všech přímk (tj. projektivní prostor) v aritmetickém vektorovém prostoru \mathbb{F}_q^l dimenze l , kterých je právě $n := \frac{q^l-1}{q-1} = \sum_{i=0}^{l-1} q^i$ a z každé přímky vezmeme jeden nenulový vektor h_i . Tyto vektory sestavíme do matice M typu $l \times n$, která je jistě hodnosti l . Každé dva sloupce jsou přitom lineárně nezávislé, neboť neleží na stejné přímce, ale každá dvojice

určuje rovinu, která obsahuje jiný sloupcový vektor, proto je vzdálenost kódu 3. Máme tedy $[n, n-l, 3]_q$ -kód.

Zbývá zjistit, že levá strana Hammingovy nerovnosti je $1 + n(q-1) = 1 + \frac{q^l-1}{q-1}(q-1) = q^l$, zatímco pravá strana je $q^{n-(n-l)} = q^l$, tudíž je kód opět 1-perfektní. \square

16.10.

1.2 Samoduální kódy

1.5. Určete všechny parametry a rozhodněte, zda je samoduální lineární kód nad \mathbb{F}_2 s generující maticí

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

Popište propíchnutý kód $\pi_8(\mathcal{C})$.

Protože je C hodnosti 4, jedná se o kód délky 8 a dimenze 4. Snadno spočítáme, že $CC^T = \mathbf{0}$, proto C generuje samoduální lineární kód. To znamená, že C je kontrolní matice kódu, z níž zjistíme vzdálenost. Protože žádný sloupec matice C není nulový, každé dva jsou různé, součet každých tří má lichou váhu, vidíme $d(\mathcal{C}) \geq 4$. Všechny řádky matice mají váhu 4, je $d(\mathcal{C}) = 4$ a \mathcal{C} je tudíž $[8, 4, 4]_2$ -kód.

Propíchnutí $\pi_8(\mathcal{C})$ je podle pozorování na přednášce $[7, 4, 3]_2$ -kód nebo $[7, 4, 4]_2$ -kód, protože jsme už zjistili, že $[7, 4, 3]_2$ -kód je perfektní, nemůže žádný $[7, 4, 4]_2$ -kód existovat. Můžeme si všimnout, že odstraněním posledního sloupce matice C dostaneme právě generující matici

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Hammingova 1-perfektního $[7, 4, 3]_2$ -kódu z 1.1. \square

1.3 Matice a parametry

1.6. Uvažujme pro $n \geq 2$ paritní kód $\mathcal{C} = \{\mathbf{v} \in \mathbb{F}_2^n \mid \sum_i v_i = 0\}$.

(a) Určete kontrolní matici kódu \mathcal{C} ,

- (b) najděte generující matici \mathcal{C} ve standardním tvaru,
- (c) spočítejte vzdálenost kódu \mathcal{H} a uveďte všechny parametry kódu,
- (d) rozhodněte, zda je kód perfektní či MDS,
- (e) jak vypadá duální kód \mathcal{C}^\perp ?

(a) Protože je paritní kód tvořen právě všemi řešeními jediné lineární rovnice $\sum_{i=1}^n x_i = 0$, je jeho kontrolní matice tvaru $\mathbf{H} = (1, 1, \dots, 1) \in \mathbb{F}_2^n$.

(b) Stačí najít bázi řešení homogenní soustavy rovnic ve tvaru

$$\mathbf{C} = (I_{n-1} | \mathbf{1}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 1 & \dots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{(n-1) \times n}.$$

(c) Například z kontrolní matice, která neobsahuje žádný nulový sloupec, ale každé dva jsou už lineárně závislé vidíme, že $d(\mathcal{C}) = 2$. Jedná se tedy o $[n, n-1, 2]_2$ -kód

(d) Protože je vzdálenost kódu sudá, nemůže jít o perfektní kód. Naopak Singletonův odhad nabývá rovnosti $2 = n - (n-1) + 1$, proto jde o MDS kód.

(e) duální kód má generující matici $\mathbf{H} = (1, 1, \dots, 1) \in \mathbb{F}_2^n$, jedná se tedy $[n, 1, n]_2$ -kód obsahující jen dvě slova $00 \dots 0$ a $11 \dots 1$. \square

1.7. Uvažujme generující matici $\mathbf{C} = \begin{pmatrix} 1 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 3 & 1 \\ 3 & 4 & 3 & 2 & 3 \end{pmatrix}$ nad tělesem \mathbb{F}_5 .

kódu \mathcal{C} .

- (a) Určete kontrolní matici kódu \mathcal{C} ,
- (b) spočítejte všechny parametry kódu \mathcal{C} a kódu \mathcal{C}^\perp ,
- (c) najděte permutaci σ a generující matici ve standardním tvaru permutačně ekvivalentního kódu $\mathcal{C}_\sigma \sim_\sigma \mathcal{C}$
- (d) rozhodněte, zda je kód \mathcal{C} perfektní či MDS.

(a) a (c) Matici upravíme pomocí Gaussovy-Jordanovy eliminace tak, abychom měli v bázických sloupcích kanonickou bázi:

$$\mathbf{C} = \begin{pmatrix} 1 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 3 & 1 \\ 3 & 4 & 3 & 2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

Nyní nejprve snadno najdeme bázi řešení soustavy a dopočítáme tak kontrolní matici $\mathbf{H} = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 4 & 0 & 2 & 2 & 1 \end{pmatrix}$ a přepermutováním sloupců matice \mathbf{C}

permutací $\sigma = (243)$ dostaneme generující matici $\mathbf{C}_\sigma = \begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 3 \end{pmatrix}$

permutačně ekvivalentního kódu $\mathcal{C}_\sigma \sim_\sigma \mathcal{C}$.

(b) Vidíme, že žádný sloupec kontrolní matice \mathbf{H} kódu \mathcal{C} není nulový a například 3. a 4. jsou lineárně závislé, tedy $d(\mathcal{C}) = 2$. Podobně kontrolní matice \mathbf{C} kódu \mathcal{C}^\perp neobsahuje nulový vektor a například 1. a 2. jsou lineárně závislé, proto i $d(\mathcal{C}^\perp) = 2$. Tedy \mathcal{C} je $[5, 3, 2]_5$ -kód a \mathcal{C}^\perp je $[5, 2, 2]_5$ -kód.

(d) Protože je vzdálenost \mathcal{C} sudá nemůže se jednat o perfektní kód a kód není ani MDS, neboť $2 + 3 < 5 + 1$. \square

2 Polynomy nad konečnými tělesy

2.1 Struktura konečných těles

2.1. Buď K konečné těleso charakteristiky p a $P = \langle 1 \rangle$ podgrupa K generovaná prvkem 1. Dokažte, že

- (a) $|P| = p$ je prvočíslo, P je podtěleso K a $P \cong \mathbb{Z}_p$,
- (b) K je vektorový prostor nad tělesem P ,
- (c) existuje přirozené n , pro které $|K| = p^n$,
- (d) K je rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem P .

(a) Z lineární algebry víme, že $|P| = p$ je právě charakteristika tělesa K , která musí být pro konečné těleso prvočíselná. Snadno nahlédneme, že je P uzavřené na násobení, tedy jde o podobor konečného tělesa, což je opět těleso. Zbývá si všimnout, že je zobrazení

$$k \rightarrow \underbrace{1 + 1 + \dots + 1}_{k \times}$$

prostý okruhový homomorfismus $\mathbb{Z}_p \rightarrow P$ stejně velkých konečných okruhů, tedy jde o jejich izomorfismus.

(b) K je rozšíření tělesa P tedy má strukturu vektorového prostoru danou jeho okruhovými operacemi.

(c) Stačí využít (b) a položit

$$n = \dim_P K = [K : P].$$

Potom z lineární algebry víme, že $K \cong \mathbb{F}^n$, a proto $|K| = |P|^n = p^n$. \square

23.10.

(d) K^* je multiplikativní grupa řádu $p^n - 1$, tedy z Lagrangeovy věty plyne, že $a^{p^n-1} = 1$ pro každé $a \in K^*$. Odtud vidíme, že rovnost $a^{p^n} = a$ i $a^{p^n} - a = 0$ platí pro všechny prvky $a \in K^*$ a zřejmě platí i pro nulu. Proto je každý prvek K kořenem polynomu $x^{p^n} - x \in P[x]$, což nutně znamená, že je K rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem P . \square

2.2. Buď K rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem \mathbb{Z}_p a buď zobrazení $f_p : \mathbb{F} \rightarrow \mathbb{F}$ určené předpisem $f_p(a) = a^p$ a dále $f_{p^k} : \mathbb{F} \rightarrow \mathbb{F}$ určená předpisem $f_{p^k}(a) = \underbrace{f_p \circ \dots \circ f_p}_{k \times}$. Ověřte, že platí:

- (a) f_p i $f_{p^k}(a) = a^{p^k}$ jsou izomorfismy $K \rightarrow K$,
- (b) $U = \{a \in K \mid f_{p^n}(a) = a\}$ je podtěleso K ,
- (c) $|U| = p^n$ a $U = K$ je rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem \mathbb{Z}_p ,
- (d) $x^{p^n} - x = \prod_{a \in K} (x - a)$ v oboru $K[x]$,
- (e) existuje ireducibilní polynom m stupně n nad tělesem \mathbb{F}_p , a pro každý takový polynom platí, že $\mathbb{F}_p[x]/(m) \cong K$ a že $m \mid x^{p^n} - x$.

(a) Spočítáme

$$f_p(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = f_p(a) \cdot f_p(b),$$

$$f_p(a + b) = (a + b)^p = a^p + p(\dots) + b^p = f_p(a) + f_p(b),$$

odkud plyne, že je f_p okruhový homomorfismus. Protože je obraz nenulového prvku opět nenulový, jedná se o prostý endomorfismus konečného okruhu do sebe, tedy izomorfismus.

Konečně zřejmě $f_{p^k}(a) = a^{p^k}$ a jedná se izomorfismus, neboť složení izomorfismů je vždy izomorfismus.

(b) Necht' $a, b \in U$. Potom díky (a) dostáváme, že

$$f_{p^k}(a \cdot b) = f_{p^k}(a) \cdot f_{p^k}(b) = a \cdot b,$$

$$f_{p^k}(a + b) = f_{p^k}(a) + f_{p^k}(b) = a + b,$$

tedy $a \cdot b, a + b \in U$. Zřejmě $f_{p^k}(1) = 1$, proto je U podobor konečného tělesa K , tedy jeho podtěleso.

(c) Protože derivace $(x^{p^n} - x)' = -1$, polynom $x^{p^n} - x$ nemá nad tělesem charakteristiky p žádné vícenásobné kořeny. Z definice je patrné, že U obsahuje právě všechny (jednoduché) kořeny polynomu $x^{p^n} - x$ v jeho rozkladovém nadtělese, kterých je právě p^n .

(d) Polynomy vpravo i vlevo mají podle (c) stejný stupeň, oba jsou monické a oba se rozkládají v K na stejné kořenové činitele, tedy se jedná o stejné polynomy.

(e) Připomeňme, že K^* je cyklická grupa. Zvolíme její generátor α a minimální polynomu $m \in \mathbb{Z}_p[x]$ prvku α nad tělesem \mathbb{Z}_p . Potom z kurzu algebry víme, že

$$\deg m = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [K : \mathbb{Z}_p] = n.$$

neboť K obsahuje všechny mocniny prvku α , tedy $K = \mathbb{Z}_p(\alpha)$.

Nechť m je ireducibilní polynom stupně n . Poznamenejme, že bez újmy na obecnosti můžeme předpokládat že je polynom m monický. Protože je těleso $L = \mathbb{Z}_p[x]/(m)$ řádu p^n je podle 2.1(d) izomorfní rozkladovému nadtělesu polynomu $x^{p^n} - x$ nad svým prvotělesem \mathbb{Z}_p . Podle tvrzení z přednášky algebry o jednoznačnosti rozkladových nadtěles je L izomorfní tělesu K . Protože existuje kořen $\alpha \in L$ polynomu m , je m nutně minimálním polynomem prvku α nad tělesem \mathbb{Z}_p . Aplikujeme-li nyní bod (d) na těleso L , plyne z minimality polynomu m , že $m \mid x^{p^n} - x$. \square

30.10.

2.2 Rozklady polynomů

2.3. Určete polynomy Q_1, Q_3, Q_5, Q_{15} nad tělesem \mathbb{F}_2 . Kolik ireducibilních faktorů má nad \mathbb{F}_2 polynom $x^{30} - 1$?

Pro výpočet využijeme vztahu $x^n - 1 = \prod_{k|n} Q_k$. Zřejmě je jediný prvek řádu 1 jednička, proto $Q_1 = x - 1$ a dále

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

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

Zřejmě jsou Q_1 a Q_3 ireducibilní a protože 2 má v \mathbb{Z}_5^* řád 4, je podle věty z přednášky polynom Q_5 ireducibilní. 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. \square

2.4. Určete kolik existuje různých ireducibilních polynomů stupně a) 2, b) 3, c) 4, d) 5, e) 7, f) p pro liché prvočíslo p nad tělesem \mathbb{F}_2 a určete ty z nich, které jsou stupně nejvýše 4.

Stačí uvážit, že

- (a) $x^4 - x$ je součin všech ireducibilních polynomů stupně 1 a 2 nad tělesem \mathbb{F}_2 , přitom $x^2 - x$ je součin všech ireducibilních polynomů stupně 1 nad tělesem \mathbb{F}_2 , tedy existuje jediný polynom stupně 2: $x^2 + x + 1$,
- (b) $x^8 - x$ je součin všech ireducibilních polynomů stupně 1 a 3 nad tělesem \mathbb{F}_2 , součin ireducibilních polynomů stupně 3 je tedy $\frac{x^8 - x}{x^2 - x} = \sum_{i=0}^6 x^i$, proto existují právě dva, snadno zjistíme (neboť stačí ověřit, zda mají v \mathbb{F}_2 kořen), že to jsou polynomy: $x^3 + x + 1$, $x^3 + x^2 + 1$ a

$$\sum_{i=0}^6 x^i = (x^3 + x + 1) \cdot (x^3 + x^2 + 1),$$

- (c) $x^{16} - x$ je součin všech ireducibilních polynomů stupně 1, 2 a 4 nad tělesem \mathbb{F}_2 , součin ireducibilních polynomů stupně 4 je tudíž $\frac{x^{16} - x}{x^4 - x} = \sum_{i=0}^4 x^{3i}$, tento polynom je stupně 12 a proto existují právě 3, víme, že nemají nad \mathbb{F}_2 kořen, tedy mají absolutní člen roven 1 a lichý počet nenulových koeficientů a nepatří mezi ně $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, tedy nutně:

$$\sum_{i=0}^4 x^{3i} = (x^4 + x + 1) \cdot (x^4 + x^3 + 1) \cdot (x^4 + x^3 + x^2 + x + 1)$$

- (d) $x^{32} - x$ je součin všech ireducibilních polynomů stupně 1 a 5 nad tělesem \mathbb{F}_2 , součin ireducibilních polynomů stupně 5 je tudíž $\frac{x^{32} - x}{x^2 - x} = \sum_{i=0}^{30} x^i$, a proto existuje právě $\frac{30}{5} = 6$ různých ireducibilních polynomů stupně 5,
- (e) podobně $x^{128} - x = (x^2 - x) \sum_{i=0}^{126} x^i$ je součin všech ireducibilních polynomů stupně 1 a 7 nad tělesem \mathbb{F}_2 , tedy a proto existuje právě $\frac{126}{7} = 18$ různých ireducibilních polynomů stupně 7.
- (f) Zobecněním předchozích dvou úvah vidíme, že polynom $\sum_{i=0}^{2^p-2} x^i$ je součin všech ireducibilních polynomů stupně p , a proto existuje právě $\frac{2^p-2}{p}$ různých ireducibilních polynomů stupně p .

□

6.11.

3 Konstrukce cyklických kódů

3.1 Obecné cyklické kódy

Připomeňme, že kód $\mathcal{C} \subseteq \mathbb{F}_q^n$ je *cyklický*, jestliže

$$c_0c_1 \dots c_{n-2}c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1}c_0 \dots c_{n-3}c_{n-2} \in \mathcal{C}.$$

Netriviálním kódem míníme vždy nenulový kód, který neobsahuje všechna slova dané délky.

3.1. Najděte všechny binární cyklické kódy délky 3. U netriviálních spočítejte jejich generující a kontrolní matici.

Snadno zjistíme ireducibilní rozklad polynomu $x^3 - 1$ v oboru $\mathbb{F}_2[x]$ je

$$x^3 - 1 = x^3 + 1 = Q_1Q_3 = (x + 1)(x^2 + x + 1),$$

o polynomu Q_3 víme, že je ireducibilní z úlohy 2.4(a). Máme tedy právě 4 dělitele $x^3 - 1$ a existují právě 4 cyklické binární lineární kódy délky 3. Dva jsou triviální odpovídají triviálním dělitelům $\mathcal{C}(1) = \mathbb{F}_2^3$, $\mathcal{C}(x^3 + 1) = \{\mathbf{0}\}$ a dva netriviální $\mathcal{C}(x + 1)$ a $\mathcal{C}(x^2 + x + 1)$.

Generující matici i kontrolní matici kódu $\mathcal{C}(x + 1)$ napíšeme s využitím znalosti rozkladu $x^3 - 1$ a tvrzení z přednášky: $\mathbf{C} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ je jeho generující matice a $\mathbf{H} = (1 \ 1 \ 1)$ kontrolní matici. Kód $\mathcal{C}(x^2 + x + 1)$ má generující matici \mathbf{H} a kontrolní matici \mathbf{C} .

3.2. Uvažujme binární lineární kód \mathcal{C} s generující maticí $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

(a) Ukažte, že \mathcal{C} není cyklický,

(b) najděte cyklický kód permutačně ekvivalentní \mathcal{C} .

□

(a) Stačí si uvědomit, že slovo 0110, které dostaneme z (bázického) slova 1100 cyklickým posunutím neleží v kódu \mathcal{C} .

(b) Snadno nahlédneme, že kód s generující maticí $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ je cyklický kód tvaru $\mathcal{C}(x^2 + 1)$ a z kódu \mathcal{C} ho obdržíme přehozením druhého a třetího sloupce, tedy $\mathcal{C}(x^2 + 1) \sim_{(12)} \mathcal{C}$. □

3.3. Najděte všechny binární lineární cyklické kódy délky 5. Pro netriviální z nich určete jejich generující a kontrolní matici a jejich parametry.

Protože víme, že

$$x^5 - 1 = Q_1 \cdot Q_5 = (x + 1)(1 + x + x^2 + x^3 + x^4),$$

kde Q_5 je ireducibilní neboť 2 má v \mathbb{Z}_5^* řád 4 (což víme už z 2.3), jedná se ireducibilní rozklad v $\mathbb{F}_2[x]$, a proto snadno určíme všechny dělitele $x^5 - 1$. Najdeme tedy právě čtyři kódy:

$$\mathcal{C}(1) = \mathbb{F}_2^5, \quad \mathcal{C}(x^5 - 1) = \mathbf{0}, \quad \mathcal{C}(x + 1), \quad \mathcal{C}\left(\sum_{i=0}^4 x^i\right).$$

Označíme-li

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad B = (1 \ 1 \ 1 \ 1 \ 1),$$

pak A tvoří generující matici kódu $\mathcal{C}(x+1)$ a kontrolní matici kódu $\mathcal{C}(\sum_{i=0}^4 x^i)$ a B tvoří kontrolní matici kódu $\mathcal{C}(x+1)$ a generující matici kódu $\mathcal{C}(\sum_{i=0}^4 x^i)$. Z kontrolních matice snadno určíme vzdálenost kódů, proto je $\mathcal{C}(x+1)$ $[5, 4, 2]_2$ -kód a $\mathcal{C}(\sum_{i=0}^4 x^i)$ je $[5, 1, 5]_2$ -kód \square

3.4. Uvažujme binární kódy délky 7.

- ověřte, že $\mathcal{C}(x^3 + x + 1)$ je cyklický kód a jeho najděte generující a kontrolní matici,
- určete, kolik různých binárních cyklických kódů délky 7 existuje,
- ověřte, že je kód \mathcal{H} z úlohy 1.1 permutačně ekvivalentní s kódy $\mathcal{C}(x^3 + x + 1)$ a $\mathcal{C}(x^3 + x^2 + 1)$.
- najděte permutaci zprostředkující permutační ekvivalenci mezi kódy $\mathcal{C}(x^3 + x + 1)$ a $\mathcal{C}(x^3 + x^2 + 1)$.

Využijeme ireducibilní rozklad $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ v oboru $\mathbb{Z}_2[x]$, který známe z úlohy 2.4(b).

(a) Okamžitě ze znalosti koeficientů polynomu $x^3 + x + 1$ dostáváme generující matici

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

Pro kontrolní matici nám stačí spočítat $(x+1)(x^3+x^2+1) = x^4+x^2+x+1$ a kontrolní matici tedy dostaneme obdobnou konstrukcí

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

(b) Různých binárních cyklických kódů délky 7 máme právě tolik kolik je (neasociovaných) dělitelů polynomu f , tedy

$$|\{(x+1)^{i_1}(x^3+x+1)^{i_2}(x^3+x^2+1)^{i_3} \mid i_1, i_2, i_3 \in \mathbb{Z}_2\}| = 8.$$

(c) Nejprve stejně jako v úloze (a) spočítáme kontrolní matici cyklického kódu $\mathcal{C}(x^3+x^2+1)$. Protože $\frac{x^7-1}{x^3+x^2+1} = (x+1)(x^3+x+1) = x^4+x^3+x^2+1$, dostáváme

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

kontrolní matici kódu $\mathcal{C}(x^3+x^2+1)$. Vidíme, že obě kontrolní matice stejně jako kontrolní matice Hammingova kódu z 1.1 obsahují jen v různém pořadí právě všechny nenulové sloupcové vektory z \mathbb{F}_2^3 , proto se jedná o permutačně ekvivalentní kódy.

(d) Snadno určíme, že permutace (246)(35) aplikovaná na sloupce matice K ji změní na matici H , jedná se o permutaci zprostředkující permutační ekvivalenci kódů $\mathcal{C}(x^3+x^2+1)$ a $\mathcal{C}(x^3+x+1)$. \square

3.5. Rozhodněte, kolik a pro která i existuje cyklických $[10, i]$ kód nad tělesem (a) \mathbb{F}_2 , (b) \mathbb{F}_3 .

Obdobně jako v úlohách 3.3 a 3.4 máme spočítat počet všech dělitelů polynomu $x^{10}-1$ a rozhodnout, které stupně pro takové dělitele připadají v úvahu.

(a) V oboru $\mathbb{F}_2[x]$ charakteristika tělesa dělí délku kódu, proto upravíme výraz $x^{10}-1 = (x^5-1)^2$ a poté rozložíme polynom x^5-1 :

$$x^{10}-1 = (x^5-1)^2 = Q_1^2 \cdot Q_5^2 = (x+1)^2(1+x+x^2+x^3+x^4)^2 \in \mathbb{F}_2[x].$$

Z úlohy 3.3 víme, že je Q_5 je ireducibilní, proto jsou dělitele polynomu $x^{10}-1$ právě tvaru $(x+1)^i(1+x+x^2+x^3+x^4)^j$ pro $(i, j) \in \mathbb{Z}_3^2$. Dělitelů i lineárních cyklických kódů je právě $3^2 = 9$.

Z ireducibilního rozkladu rovněž vidíme, že stupně dělitelů polynomu $x^{10}-1$ leží v množině

$$\{i \cdot 1 + j \cdot 4 \mid (i, j) \in \mathbb{Z}_3^2\} = \{0, 1, 2, 4, 5, 6, 8, 9, 10\},$$

odkud vidíme, že neexistují žádné cyklické kódy s parametry $[10, 3]_2$ a $[10, 7]_2$.

(b) Opět určíme ireducibilní rozklad polynomu $x^{10} - 1 \in \mathbb{F}_3[x]$ je tvaru $(x - 1)(x + 1)Q_5Q_{10}$

$$x^{10} - 1 = Q_1Q_2Q_5Q_{10} = (x - 1)(x + 1)Q_5Q_{10} \in \mathbb{F}_3[x],$$

kde Q_5 a Q_{10} jsou ireducibilní (cyklotomické) polynomy stupně 4, neboť prvek 3 je řádu 4 v grupách \mathbb{Z}_5^* i \mathbb{Z}_{10}^* . Dělitele polynomu $x^{10} - 1$ jsou tedy

$$\{Q_1^{i_1}Q_2^{i_2}Q_5^{i_5}Q_{10}^{i_{10}} \mid (i_1, i_2, i_5, i_{10}) \in \mathbb{Z}_2^4\},$$

proto existuje $2^4 = 16$ dělitelů a cyklických $[10, i]_3$ kódů a možné dimenze těchto kódů jsou opět $\{1i + 4j \mid (i, j) \in \mathbb{Z}_3^2\} = \{0, 1, 2, 4, 5, 6, 8, 9, 10\}$. \square

7.11.

3.2 Konstrukce GRS a RS kódů

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

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

Lineární kód $\mathcal{C} = \ker(\mathbf{H}_\alpha^r \Delta(\mathbf{v}))$ s kontrolní maticí $\mathbf{H}_\alpha^r \Delta(\mathbf{v})$ se nazývá *zobecněný Reedův-Solomonův* (GRS) kód s *lokátory* α a *multiplikátory* \mathbf{v} . \mathcal{C} se nazývá Reedův-Solomonův (RS), pokud $\exists \alpha \in \mathbb{F}^*$ řádu n a $b \in \mathbb{N}$ tak, že $\alpha_i = \alpha^{i-1}$ a $v_i = \alpha^{b(i-1)}$.

3.6. Najděte MDS kód s parametry $[n, k, d]$

- (a) pro daná $0 < k < n$,
- (b) pro daná $0 < d < n$,
- (c) pro daná $0 < d, k$.

Ve všech případech využijeme vztahu $d = n - k + 1$ a konstrukce GRS-kódu.

(a), (b) zvolíme těleso \mathbb{F}_q pro $q > n$ a jeho po dvou různé prvky $\alpha_1, \dots, \alpha_n$.

(c) Položíme $n = k + d - 1$ a pokračujeme jako v (a)

Nyní je $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \cdot & \cdot & \dots & \cdot \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \dots & \alpha_n^{n-k-1} \end{pmatrix}$ kontrolní matice hleda-

ného kódu. \square

3.7. Najděte generující a kontrolní matici nějakého MDS kódu s parametry $[5, 3, 3]$ a $[5, 2, 4]$

Zvolíme například těleso \mathbb{F}_7 .

Pak je matice $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ kontrolní maticí GRS kódu s parametry $[5, 3, 3]_7$ a generující maticí GRS kódu s parametry $[5, 2, 4]_7$.

Snadno dopočítáme, že například matice $G = \begin{pmatrix} 1 & 5 & 1 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 1 \end{pmatrix}$ je odpovídající generující matice GRS kódu s parametry $[5, 2, 4]_7$ a kontrolní matice GRS kódu s parametry $[5, 3, 3]_7$. \square

3.8. Najděte normovaný RS-kód s parametry (a) $[5, 3, 3]_q$, (b) $[7, 5, 3]_q$.

(a) Hledáme q , pro které 5 dělí $q - 1$. Víme, že q musí být mocninou prvočísla a snadno tedy nahlédneme, že nejmenší přípustné $q = 11$. Nyní musíme zvolit prvek řádu 5 v \mathbb{F}_{11} . Protože $2^5 = -1$ v \mathbb{F}_{11} , vidíme, že vyhovuje například prvek 4, tedy kontrolní matice RS $[5, 3, 3]_{11}$ je tvaru $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \end{pmatrix}$.

(b) Tentokrát hledáme q , pro které 7 dělí $q - 1$, zřejmě je to právě $q = 2^3$. Reprezentujme si prvky tělesa \mathbb{F}_8 pomocí kořenu α polynomu $x^3 + x + 1$ ireducibilního nad \mathbb{F}_2 , tedy $\mathbb{F}_8 = \mathbb{F}_2[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2\}$. Protože je grupa \mathbb{F}_8^* cyklická, je každý nejednotkový prvek řádu 7. Nyní dopočítáme, že například matice

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha + 1 & \alpha^2 + \alpha & \alpha^2 + \alpha + 1 & \alpha^2 + 1 \end{pmatrix}.$$

je kontrolní maticí RS $[7, 5, 3]_8$ -kódu \square

13.11.

3.3 Konstrukce reziduálních kódů

3.9. Najděte všechny ireducibilní polynomy stupně 2 nad tělesem \mathbb{F}_3 , zkonstruujte těleso \mathbb{F}_9 a popište řády všech jeho prvků.

Víme, že ireducibilní rozklad $x^9 - x = x^{3^2} - x$ obsahuje všechny monické ireducibilní polynomy stupně 1 a 2, protože takové polynomy jsou ireducibilní, právě když nemají v \mathbb{F}_3 nemají kořen snadno určíme, že

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1),$$

tedy uvážíme-li všechny násobky prvky z \mathbb{F}_3^* představují všechny ireducibilní polynomy stupně 2:

$$x^2 + 1, x^2 + x - 1, x^2 - x - 1, -x^2 - 1, -x^2 - x + 1, -x^2 + x + 1.$$

Nyní stačí vzít například ireducibilní polynom $x^2 + 1 \in \mathbb{F}_3[x]$ a pak dostaneme

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1) = \mathbb{F}_3[\alpha] = \{a_0 + a_1\alpha \mid a_i \in \mathbb{F}_3\},$$

kde $\alpha = x + ((x^2 + 1))$, a proto $\alpha^2 = -1 = 2$. Zřejmě 1 je jediný prvek řádu 1 a 2 jediný prvek řádu 2. Protože $\alpha^2 = -1$ jsou α a 2α prvky řádu 4 a zbylé prvky, tj. $\alpha + 1, \alpha + 2, 2\alpha + 1$ a $2\alpha + 2$ jsou nutně prvky řádu 8. \square

3.10. Určete řády všech prvků z \mathbb{F}_8^* .

Protože je \mathbb{F}_8^* grupa prvočíselného řádu, obsahuje jediný prvek 1 řádu 1 a všechny zbylé prvky jsou řádu 7. \square

3.11. Najděte kontrolní matici a určete parametry binárního reziduálního kódu určeného normovaným RS kódem nad tělesem $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ s parametry $[7, 5, 3]_8$, prezentací danou $\alpha^3 + \alpha + 1 = 0$, a lokátory $\alpha^0, \alpha^1, \dots, \alpha^6$.

V úloze 3.8(2) jsme spočítali kontrolní matici RS kódu, jehož reziduální kód hledáme:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha + 1 & \alpha^2 + \alpha & \alpha^2 + \alpha + 1 & \alpha^2 + 1 \end{pmatrix}.$$

Pro popis reziduálního kódu využijme konstrukci důkazu Věty 6.4 z přednášky. Hledáme binární slova délky 7, která jsou řešením homogenní soustavy rovnic s maticí H , tedy řešíme pro $\mathbf{u} \in \mathbb{F}_2^7$ vektorovou rovnici $H\mathbf{u}^T = 0^T$.

Když si soustavu rozepíšeme pro bázi α^0, α^1 a α^2 prostoru \mathbb{F}_8 nad tělesem \mathbb{F}_2 , dostáváme matici:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Našli jsme kontrolní matici $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$ hledaného reziduálního kódu, z níž obvyklým způsobem určíme parametry $[7, 3, 4]_2$. \square

3.12. Najděte kontrolní matici a určete parametry binárního reziduálního kódu určeného normovaným RS kódem s parametry $[7, 4, 4]_8$ nad týmž tělesem a se stejnými lokátory jako v úloze 3.11.

Využijeme popis reziduálního kódu cyklického kódu, který je opět cyklický a generující polynom je právě $\text{nsn}\{m_1, m_\alpha, m_{\alpha^2}\}$. Nyní si stačí všimnout, že je α^2 kořenem polynomu $x^3 + x + 1$, tedy $m_{\alpha^2} = x^3 + x + 1 = m_\alpha$, což znamená, že náš reziduální kód je též jako kód určený RS kódem s parametry $[7, 5, 3]_8$ z předchozí úlohy, a tudíž má stejnou kontrolní matici a stejné parametry $[7, 3, 4]_2$. \square

20.11.

4 Reedovy-Mullerovy kódy

4.1. Určete parametry a generující matici binárního RM kódu $\mathcal{R}(3, 1)$. Jaký kód dostaneme propíchnutím $\mathcal{R}(3, 1)$ v jedné souřadnici?

Protože jsou parametry obecného binárního RM kódu $\mathcal{R}(m, r)$ právě $[2^m, \sum_{i=0}^r \binom{m}{i}, 2^{m-r}]_2$, vidíme, že $\mathcal{R}(3, 1)$ je $[8, 4, 4]_2$ -kód. To nutně znamená, že propíchnutí má dimenzi 4 a vzdálenost 3 (jinak bychom došli ke sporu s Hammingovým odhadem), snadno nahlédneme, že se jedná právě o kód permutačně ekvivalentní Hammingovu perfektnímu $[7, 4, 3]_2$ -kódu.

Připomeňme, že $\Phi : \mathcal{BP}_3 \rightarrow \mathcal{BF}_3$ je zobrazení, které Booleovskému polynomu p přiřadí právě Booleovskou funkci $\mathbf{c} \rightarrow p(\mathbf{c})$, kterou reprezentujeme

slovem $p(\mathbf{c}_0) \dots p(\mathbf{c}_7)$, kde \mathbf{c}_i je právě trojice cifer z \mathbb{F}_2 představující binární zápis čísla i . K nalezení matice stačí spočítat

$$\Phi(1) = 11111111, \Phi(x_1) = 00001111, \Phi(x_2) = 00110011, \Phi(x_3) = 01010101.$$

To znamená, že $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ generující matice kódu

$\mathcal{R}(3, 1)$. □

4.2. Určete parametry a generující matici binárních RM kódů $\mathcal{R}(3, 0)$ a $\mathcal{R}(3, 2)$.

Protože $\Phi(x_\emptyset) = \Phi(1) = 1$, je generující matice $[8, 1, 8]_2$ -kód kódu $\mathcal{R}(3, 0)$ tvaru $(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)$. Tato matice je zároveň kontrolní maticí $[8, 7, 2]_2$ -kód $\mathcal{R}(3, 2) = \mathcal{R}(3, 0)^\perp$. To znamená, že je $\mathcal{R}(3, 2)$ paritní kód jehož generující

maticí je například $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$. □

5.12.

5 Konvoluční kódy

5.1 Abstraktní a fyzický konvoluční kódovač

5.1. Pro generující polynomiální matici

$$G = (1 + D^2 \quad 1 + D + D^2) \in \mathbb{F}_2[D]^{1 \times 2}$$

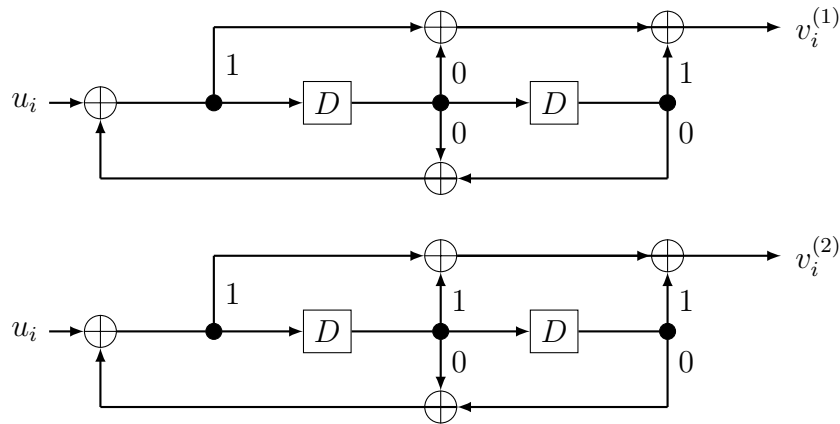
určete vnější stupeň a odpovídající fyzický konvoluční kódovač (K, G) realizujte obvodem.

Snadno určíme $\text{extdeg}(G) = \max(\deg 1 + D^2, \deg 1 + D + D^2) = 2$.

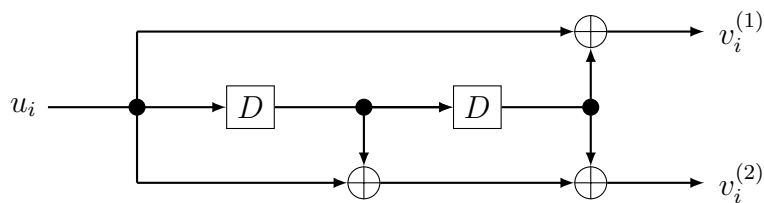
Pro každou souřadnici $v = \sum_i \mathbf{v}_i D^i = K(u) =$

$$= \sum_i u_i D^i (1 + D^2 \quad 1 + D + D^2) = \left(\sum_i (u_i + u_{i-2}) D^i, \sum_i (u_i + u_{i-1} + u_{i-2}) D^i \right)$$

můžeme namalovat obvod podle definice:



Nebo lépe zjednodušenou realizaci vypouštějící všechny nulové hrany a zahrnující oba obvody:



□

5.2. Rozhodněte, které z matic tvoří generující matice konvolučního kódu nad tělesem \mathbb{F}_3 :

$$G_1 = \begin{pmatrix} D \\ D^2 - D \end{pmatrix}, G_2 = \begin{pmatrix} D^2 - 1 \\ D^2 + D \end{pmatrix}, G_3 = \begin{pmatrix} \frac{D+1}{D} & \frac{1}{D+1} \\ \frac{D^2+D}{D} & \frac{1}{D^2+1} \end{pmatrix}, G_4 = \begin{pmatrix} \frac{D+1}{D-1} & \frac{1}{D+1} \\ \frac{D-1}{D^2+D} & \frac{1}{D^2+1} \end{pmatrix}.$$

Pro generující matice konvolučního kódu spočítejte vnější stupeň a najděte nějakou polynomiální generující matici téhož konvolučního kódu

$G_1 = \begin{pmatrix} D \\ D^2 - D \end{pmatrix} = \begin{pmatrix} 1 \\ D-1 \end{pmatrix}$ je generující matice konvolučního kódu $\mathbb{F}((D))$, protože její jediná racionální funkce je realizovatelná, tedy ji lze napsat jako podíl polynomů s nenulovým absolutním členem ve jmenovateli. Matice G_1 má vnější stupeň (tj. maximální stupeň polynomu v redukovaném vyjádření) právě 1 a polynomiální generující matici konvolučního kódu $\mathbb{F}((D))$ představuje například matice (1).

Matice $G_2 = \begin{pmatrix} D^2 - 1 \\ D^2 + D \end{pmatrix}$ ani G_3 nejsou generující matice, neboť obsahují nerealizovatelnou racionální funkci. Matice

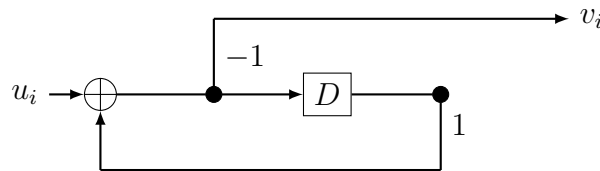
$$G_4 = \begin{pmatrix} \frac{D+1}{D-1} & \frac{1}{D+1} \\ \frac{D^2+D}{D} & \frac{1}{D^2+1} \end{pmatrix} = \begin{pmatrix} \frac{D^2 - D + 1}{D^2 - 1} & \frac{D-1}{D^2 - 1} \\ \frac{D^3 + D^2 + D + 1}{D^2 + 1} & \frac{1}{D^2 + 1} \end{pmatrix}$$

je generující maticí konvolučního kódu a z vyjádření se společným jmenovatelem na řádcích snadno určíme vnější stupeň $\text{extdeg}(G_4) = 2 + 3 = 5$. Vynásobením řádků matice společnými jmenovateli dostaneme polynomiální generující matici $\begin{pmatrix} D^2 - D + 1 & D^2 - 1 \\ D^3 + D^2 + D + 1 & 1 \end{pmatrix}$ daného konvolučního kódu. \square

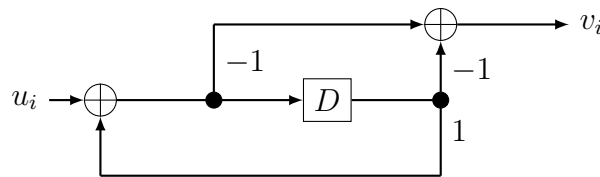
11.12.

5.3. Fyzické konvoluční kódovače určené generujícími maticemi (a) $G_1 = \begin{pmatrix} -1 \\ 1-D \end{pmatrix}$, (b) $G_1 = \begin{pmatrix} -1-D \\ 1-D \end{pmatrix} \in \mathbb{F}_3^{1 \times 1}$ realizujte obvody.

(a) Přímou nakreslíme zjednodušenou variantu obvodu podle údajů matice:



(b) Tentokrát přidáme jednu hranu a součet:



\square

5.4. Jestliže $f = \sum_{i \geq 0} f_i D^i \in \mathbb{F}[[D]]$ a $g \in \mathbb{F}((D)) \setminus \{0\}$, ověřte, že

(a) f je invertibilní v $\mathbb{F}[[D]]$, právě když $f(0) \neq 0$,

(b) existuje inverz $g^{-1} \in \mathbb{F}((D))$.

(a) Úloha je rovněž řešena na přednášce Počítačová algebra. Označíme-li $h = \sum_{i \geq 0} h_i D^i$, pak platí, že $hf = 1$, právě když

$$f_0 h_0 = 1 \quad \text{a} \quad \sum_{i=0}^n f_i h_{n-i} = 0 \quad \forall n > 0.$$

Pokud je f je invertibilní, vidíme, že f_0 je nutně invertibilní. Naopak existuje-li inverz f_0^{-1} , stačí položit $h_0 = f_0^{-1}$ a ostatní koeficienty h vyjádříme rekurentním vztahem

$$h_n = -f_0^{-1} \sum_{i=1}^n f_i h_{n-i} = 0 \quad \forall n > 0.$$

□

5.6. Pro dvě polynomiální matice $G = \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D+D^2 & D^2 & 1 \end{pmatrix}$ a $\tilde{G} = \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 1 & 0 & 1 & D \end{pmatrix}$ téhož konvolučního kódu nad \mathbb{F}_2 najděte matice určující abstraktní konvoluční kódovače a $(\tilde{K}, \tilde{\delta}, \tilde{\lambda})$ pro $K(u) = uG$ a $\tilde{K}(u) = u\tilde{G}$.

Postupujeme stejně jako v předchozí úloze, všimněme si přitom, že i matice R a \tilde{R} je pro polynomiální matice velmi snadné určit, neboť obsahují po řádcích jen koeficienty jmenovatelů u jednotlivých kladných mocnin D .

Nejprve určíme $\text{extdeg } G = 2 + 2 = 4$ a z důkazu Věty 10.3 dostaneme matice

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

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

Podobně pro generující matici \tilde{G} spočítáme $\text{extdeg } \tilde{G} = 2+1 = 3$ a matice určující abstraktní konvoluční kódovač

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

□

5.7. Fyzický konvoluční kódovač (K, G) nad \mathbb{F}_3 popište jako abstraktní konvoluční kódovač, pokud (a) $G = \begin{pmatrix} D \\ 1+D^2 \end{pmatrix}$ (b) $G = \begin{pmatrix} D & 1+D^3 \\ 1+D^2 & 1-D \end{pmatrix}$.

(a) Všimněme si, že $\text{extdeg}(G) = 2$ a využijeme Poznámku 10.2 z přednášky pro výpočet matic $P \in \mathbb{F}_3^{2 \times 2}$, $Q \in \mathbb{F}_3^{1 \times 2}$, $\tilde{Q} \in \mathbb{F}_3^{2 \times 1}$, $R \in \mathbb{F}_3^{1 \times 1}$ z koeficientů polynomů p, q ve vyjádření $\frac{p}{q} = \frac{D}{1+D^2}$:

$$P = \begin{pmatrix} -q_1 & 1 \\ -q_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Q = (1 \ 0), \quad R = \begin{pmatrix} p_1 - p_0q_1 \\ p_2 - p_0q_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad S = (0)$$

Hledaná přechodová funkce je $\delta((s_1, s_2), u) = (s_1, s_2)P + uQ = (u - s_2, s_1)$, výstupní funkce $\lambda((s_1, s_2), u) = (s_1, s_2)R + uS = s_1$ a abstraktní konvoluční kódovač (K, δ, λ) .

(b) Spočítáme, že $G = \begin{pmatrix} \frac{D-D^2}{1-D+D^2-D^3} & \frac{1+D^2+D^3+D^5}{1-D+D^2-D^3} \end{pmatrix}$, proto je

$$\text{extdeg}(G) = \max(3, 2, 5) = 5$$

a využijeme opět Poznámku 10.2 a důkaz Věty 10.3 z přednášky pro výpočet matic $P \in \mathbb{F}_3^{5 \times 5}$, $Q \in \mathbb{F}_3^{1 \times 5}$, $Q \in \mathbb{F}_3^{5 \times 2}$, $R \in \mathbb{F}_3^{1 \times 2}$ z koeficientů polynomů $G = \begin{pmatrix} p & \tilde{p} \\ q & q \end{pmatrix}$:

$$P = \begin{pmatrix} -q_1 & 1 & 0 & 0 & 0 \\ -q_2 & 0 & 1 & 0 & 0 \\ -q_3 & 0 & 0 & 1 & 0 \\ -q_4 & 0 & 0 & 0 & 1 \\ -q_5 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, Q = (1 \ 0 \ 0 \ 0 \ 0),$$

$$R = \begin{pmatrix} p_1 - p_0q_1 & \tilde{p}_1 - \tilde{p}_0q_1 \\ p_2 - p_0q_2 & \tilde{p}_2 - \tilde{p}_0q_2 \\ p_3 - p_0q_3 & \tilde{p}_3 - \tilde{p}_0q_3 \\ p_4 - p_0q_4 & \tilde{p}_4 - \tilde{p}_0q_4 \\ p_5 - p_0q_5 & \tilde{p}_5 - \tilde{p}_0q_5 \end{pmatrix} = \begin{pmatrix} 1 - 0 \cdot (-1) & 0 - 1 \cdot (-1) \\ -1 - 0 \cdot 1 & 1 - 1 \cdot 1 \\ 0 - 0 \cdot (-1) & 1 - 1 \cdot (-1) \\ 0 - 0 \cdot 0 & 0 - 1 \cdot 0 \\ 0 - 0 \cdot 0 & 1 - 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & -1 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

a $S = (0 \ 1)$. Přechodová funkce je

$$\delta(\mathbf{s}, u) = \mathbf{s}P + uQ = (u + s_1 - s_2 + s_3, s_1, s_2, s_3, s_4)$$

a výstupní funkce

$$\lambda(\mathbf{s}, u) = \mathbf{s}R + uS = (s_1 - s_2, u + s_1 - s_3 + s_5)$$

Abstraktní konvoluční kódovač je tedy (K, δ, λ) . □

5.8. Necht' matice nad tělesem \mathbb{F}_2

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

určují abstraktní konvoluční kódovač (K, δ, λ) , tj. $\delta(\mathbf{s}, \mathbf{u}) = \mathbf{s}P + \mathbf{u}Q$ a $\lambda(\mathbf{s}, \mathbf{u}) = \mathbf{s}R + \mathbf{u}S$. Najděte jeho fyzickou realizaci (K, G) a určete $\text{extdeg}(G)$.

Stačí nám přímočaře využít důkazu Věty 10.3, který nám dává vyjádření $G = Q(I_2 - DP)^{-1}RD + S \in \mathbb{F}(D)^{2 \times 3}$ generující matice hledaného fyzického

konvolučního kódovače (K, G) . Spočítáme-li pomocí faktu z lineární algebry $A^{-1} = \det(A)^{-1} \text{adj}(A)$ pro každou regulární matici A matici

$$(I_2 - DP)^{-1} = \begin{pmatrix} 1+D & 0 \\ D & 1+D \end{pmatrix}^{-1} = \frac{1}{1+D^2} \begin{pmatrix} 1+D & 0 \\ D & 1+D \end{pmatrix}.$$

Proto dostáváme, že $Q(I_2 - DP)^{-1}RD + S =$

$$\begin{aligned} &= \frac{D}{1+D^2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1+D & 0 \\ D & 1+D \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \\ &= \frac{1}{1+D^2} \left(\begin{pmatrix} D+D^2 & D^2 & D \\ 0 & D+D^2 & D+D^2 \end{pmatrix} + \begin{pmatrix} 1+D^2 & 0 & 1+D^2 \\ 1+D^2 & 1+D^2 & 0 \end{pmatrix} \right) = \\ &= \frac{1}{1+D^2} \begin{pmatrix} 1+D & D^2 & 1+D+D^2 \\ 1+D^2 & 1+D & D+D^2 \end{pmatrix} = \begin{pmatrix} \frac{1+D}{1+D^2} & \frac{D^2}{1+D} & \frac{1+D+D^2}{1+D^2} \\ \frac{1+D}{1+D^2} & \frac{1}{1+D} & \frac{D}{1+D} \end{pmatrix}. \end{aligned}$$

Našli jsme vyjádření fyzického konvolučního kódovače (K, G) s maticí $G = \begin{pmatrix} \frac{1+D}{1+D^2} & \frac{D^2}{1+D^2} & \frac{1+D+D^2}{1+D^2} \\ \frac{1+D}{1+D^2} & \frac{1}{1+D} & \frac{D}{1+D} \end{pmatrix}$, odkud snadno zjistíme $\text{extdeg}(G) = 2 + 1 = 3$. \square

19.12.

5.2 Základní, redukované a kanonické matice

5.9. Kdy je čtvercová polynomiální matice (a) základní, (b) kanonická?

(a) Matice je podle Poznámky 11.3 základní, právě když ji lze řádkově doplnit na unimodulární čtvercovou matici. V případě, že uvažujeme čtvercovou základní matici, pak je tedy nutně unimodulární. Naopak unimodulární čtvercová matice je zřejmě základní.

Vidíme, že je čtvercová matice základní, právě když je unimodulární.

(b) Využijeme-li (a) charakterizaci redukované matice jako matice se shodným vnitřním a vnějším stupněm, je čtvercová matice G kanonická $\Leftrightarrow G$ je unimodulární a $\text{extdeg } G = \text{intdeg } G \Leftrightarrow G \in \mathbb{F}^{k \times k}$ je regulární. \square

5.10. Pro konvoluční kód s generující maticí G nad tělesem \mathbb{F}_3 najděte nějakou jeho kanonickou generující matici a určete jeho stupeň, pokud

$$(a) \ G = \begin{pmatrix} \frac{D}{1-D^2} & \frac{D}{1+D} & 1 \end{pmatrix}, \quad (b) \ G = \begin{pmatrix} 1 - D^3 & D - 1 \end{pmatrix}$$

(a) Upravíme matici G pomocí řádkových ekvivalentních úprav nad tělesem $\mathbb{F}_3(D)$ tak, abychom dostali generující matici s nesoudělnými polynomy na řádku, tj. stačí nám přenásobení společným jmenovatelem $1 - D^2$:

$$G = \begin{pmatrix} \frac{D}{1-D^2} & \frac{D}{1+D} & 1 \end{pmatrix} \sim \begin{pmatrix} D & D - D^2 & 1 - D^2 \end{pmatrix}$$

Protože je největší společný dělitel polynomů na řádku invertibilní, má Smithův normální tvar $(1 \ 0 \ 0)$, tedy se jedná o základní matici. Protože z definice $\text{intdeg}(G) = \text{extdeg}(G) = 2$, je matice $(D \ D - D^2 \ 1 - D^2)$ redukovaná, a proto kanonická a $\text{deg } \mathcal{C} = \text{extdeg}(G) = 2$

(b) Kanonickou generující matici $(1 + D + D^2 \ -1)$ dostáváme stejným argumentem jako v (a) po vydělení polynomem $1 - D$. Odtud opět vidíme, že $\text{deg } \mathcal{C} = \text{extdeg}(G) = 2$. \square

5.11. Pro polynomiální matice

$$G = \begin{pmatrix} 1 & 1 + D + D^2 & 1 + D^2 & 1 + D \\ D & 1 + D + D^2 & D^2 & 1 \end{pmatrix},$$

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

konvolučního kódu $\mathcal{C} \subseteq \mathbb{F}_2((D))^4$ určete jejich vnitřní a vnější stupeň.

Vnější stupeň spočítáme z definice

$$\text{extdeg}(G) = 2 + 2 = 4 \quad \text{a} \quad \text{extdeg}(\tilde{G}) = 2 + 1 = 3.$$

Všimněme si, že $\tilde{G} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} G$, proto podle pozorování z přednášky

$$\text{intdeg}(G) = \text{intdeg}(\tilde{G}) \leq \text{extdeg}(\tilde{G}) = 3.$$

Protože podle definice

$$\text{intdeg}(G) = \max\{\text{deg } m \mid m \text{ je subdeterminant } G \text{ stupně } 2\},$$

stačí si všimnout, že $\text{deg} \begin{vmatrix} 1 & 1 + D + D^2 \\ 1 + D & 0 \end{vmatrix} = 3$, tedy $3 \leq \text{intdeg}(\tilde{G}) \leq 3$, proto $\text{intdeg}(G) = \text{intdeg}(\tilde{G}) = 3$. \square

5.12. Pro generující matice G a \tilde{G} z úlohy 5.11 rozhodněte, zda jsou (a) redukované, (b) základní, (c) kanonické. Nakreslete realizaci příslušných fyzických kódovačů obvodem.

(a) Protože jsme ve 5.11 zjistili, že

$$3 = \text{extdeg}(\tilde{G}) = \text{intdeg}(\tilde{G}) = \text{intdeg}(G) < \text{extdeg}(G) = 4,$$

dostáváme jako důsledek charakterizace redukovaných matic pomocí rovnosti vnitřního a vnějšího stupně, že G není redukovaná, zatímco \tilde{G} redukovaná je.

(b) nebo Upravíme posloupností řádkových a sloupcových ekvivalentních polynomiálních (tedy polynomiálně invertovatelných) úprav jednodušší matici \tilde{G} , kde \sim_s značí sloupcovou ekvivalenci:

$$\begin{aligned} \tilde{G} &= \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 1+D & 0 & 1 & D \end{pmatrix} \sim_s \\ &\sim_s \begin{pmatrix} 1 & D & 1+D^2 & D \\ 1+D & 1 & 1 & 1 \end{pmatrix} \sim_s \begin{pmatrix} 1 & D & 1+D^2 & 0 \\ 1+D & 1 & 1 & 0 \end{pmatrix} \sim \\ &\begin{pmatrix} 1 & D & 1+D^2 & 0 \\ 0 & 1+D+D^2 & D+D^2+D^3 & 0 \end{pmatrix} \sim_s \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1+D+D^2 & 0 & 0 \end{pmatrix}, \end{aligned}$$

kde jsem nejprve přičetli 3. sloupec k 2. a 1. sloupec ke 4., poté jsme přičetli 2. sloupec ke 4. Následně jsme přičetli $(1+D)$ násobek 1. řádku k 2. a nakonec nejprve vhodné násobky 1. sloupce ke 2. a 3. a pak D násobek 2. sloupce k třetímu. Zjistili jsme, že Smithův normální tvar matice \tilde{G} je $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1+D+D^2 & 0 & 0 \end{pmatrix}$, proto se podle charakterizační poznámky z přednášky nejedná o základní matici. Protože $\text{intdeg}(\tilde{G}) = \text{intdeg}(G)$, není základní ani matice G .

(c) Matice nejsou základní, proto ani kanonické. \square

5.13. Pro konvoluční kód \mathcal{C} nad tělesem \mathbb{F}_2 z úlohy 5.11 spočítejte jeho stupeň a Forneyho indexy a najděte nějakou jeho kanonickou matici.

Nejprve najdeme pomocí pouze řádkových ekvivalentních úprav \tilde{G} nad tělesem $\mathbb{F}_2(D)$ základní generující matici

$$\begin{aligned} \tilde{G} &\sim \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D^3 & D+D^2+D^3 & 1+D+D^2 \end{pmatrix} \sim \\ &\sim \begin{pmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D & D & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{pmatrix}, \end{aligned}$$

kde jsme nejprve přičetli $(1+D)$ násobek 1. řádku k 2. a poté jsme druhý vydělili polynomem $1+D+D^2$ a nakonec, abychom snížili stupeň (víme, že 3 je moc) přičetli D násobek 2. řádku k 1. Protože snadno sloupcově polynomiálně upravíme

$$\hat{G} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{pmatrix} \sim_s \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

našli jsme základní generující matici \hat{G} . Snadno určíme z definice její vnitřní i vnější stupeň $\text{intdeg}(\hat{G}) = \text{extdeg}(\hat{G}) = 1$, tedy jde i o redukovanou a proto kanonickou matici. Konečně Forneyho indexy kódu jsou 0, 1 a věta z přednášky říká, že $\text{deg } \mathcal{C} = 1$. \square