

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 a zda je MDS,
- (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. Naopak protože $3 = d(\mathcal{H}) < 7 - 4 + 1 = 4$, vidíme, že nejedná o MDS kód.

13.10.

(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 přímek (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. $\square$

20.10.

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 $2 + 3 < 5 + 1$. $\square$