

# Kombinatorika a grafy I — 13. cvičení\*

2. ledna 2023

## 1 Samoopravné kódy

Abeceda  $\Sigma$  je konečná množina  $q$  symbolů. Slovo délky  $n$  je uspořádání  $n$ -tice symbolů. Jako  $\Sigma^n$  označíme množinu slov délky  $n$ . Hammingova vzdálenost slov  $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \Sigma^n$  je definována jako  $d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$ . (Blokový) kód je množina  $C \subseteq \Sigma^n$  takzvaných *kodových slov*. Řekneme, že s kódem  $C$  je možné *opravit nanejvýš  $t$  chyb*, pokud pro každé  $y \in \Sigma^n$  existuje nanejvýš jedno  $x \in C$  takové že  $d(x, y) \leq t$ . Parametry kódu  $C$  jsou  $(n, k, d)_q$ , kde  $k = \log_q |C|$  a  $d = \min_{x \neq y \in C} \{d(x, y)\}$ .

Lineární kód  $C$  je podprostorem vektorového prostoru  $\mathbb{F}_q^n$ , kde  $\Sigma = \mathbb{F}_q$  je konečné těleso velikost  $q$ . Nechť  $C$  je lineární kód s parametry  $[n, k, d]_q$ . Duálním kódem  $k$   $C$  je kód  $C^\perp = \{y \in \mathbb{F}_q^n : \langle x, y \rangle = 0, \text{ pro každé } x \in C\}$ , kde pro  $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n)$  je  $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ . Generující maticí kódu  $C$  je matice  $M \in \mathbb{F}_q^{k \times n}$ , která má za řádky vektory báze kódu  $C$ . Kontrolní maticí kódu  $C$  je matice  $M^\perp \in \mathbb{F}_q^{(n-k) \times n}$ , která je generující matice kódu  $C^\perp$ .

Hadamardovy kódy jsou tvořeny řádky a mínus řádky Hadamardovy matice, která je tvořena  $\pm 1$  a platí, že  $HH^T = nI_n$ . V našich úlohách budeme uvažovat bijekci  $z \mapsto -1 \rightarrow 1$  a  $1 \rightarrow 0$ .

**Příklad 1.** Dokažte, že Hammingova vzdálenost je na množině  $\Sigma^n$  metrikou.

*Řešení.* Musíme ověřit všechny čtyři axiomy metriky.

1. Nezápornost vzdálenosti je zřejmá.
2.  $d(x, y) = 0 \Leftrightarrow x = y$ , protože musí být stejné.
3. Symetrie je z definice zřejmá.
4. Trojúhelníková nerovnost  $d(x, z) \leq d(x, y) + d(y, z)$  platí, protože pokud se liší na  $i$ -té pozici  $x$  a  $z$ , tak se musí lišit  $y$  s  $x$  nebo  $z$  na té samé pozici.

□

**Příklad 2.** Nechť  $C$  je lineární kód s parametry  $[n, k, d]_q$ . Dokažte následující tvrzení.

- Platí  $C^\perp = \{y \in \mathbb{F}_q^n : My = 0\}$ , kde  $M$  je generující maticí kódu  $C$ .
- Duální kód  $C^\perp$  je lineárním kódem s délkou slov  $n$  a s dimenzí  $n - k$ . Speciálně platí  $\dim(C) + \dim(C^\perp) = n$ .
- Platí  $(C^\perp)^\perp = C$ .
- Platí  $C = \{x \in \mathbb{F}_q^n : M^\perp x = 0\}$ , kde  $M^\perp$  je kontrolní maticí kódu  $C$ .

*Řešení.* Musíme ověřit všechny čtyři axiomy metriky.

- Jelikož kód pro každé  $y \in C^\perp$  má skalární součin s každým  $x \in C$  rovný nule. Pak stačí, pokud má skalární součin rovný nule s bázi daného prostoru.
- Podle a) víme, že  $C^\perp = \{y \in \mathbb{F}_q^n : My = 0\}$ . Uvažme  $f : \mathbb{F}_q^n \rightarrow F_q^k$  lineární zobrazení určené maticí  $M$ , neboli  $f(y) = My$ . Potom z linearity víme, že  $\dim(\text{Ker}(f)) + \dim(\text{Im}(f)) = n$  (v řeči matic máme  $\text{Im}(f) = S(M)$ ,  $\dim(S(M)) = \text{rank}(M)$  a  $\text{Ker}(f) = \text{Ker}(M)$ ). Z  $C^\perp = \{y \in \mathbb{F}_q^n : My = 0\}$  máme  $\text{Ker}(f) = C^\perp$  a tedy  $C^\perp$  je vektorovým prostorem nad  $\mathbb{F}_q$  a je tedy i lineárním kódem slov délky  $n$ . Také  $\dim(C^\perp) + \dim(\text{Im}(f)) = n$ . Protože  $M$  má rank rovný  $k$ , pak je  $\dim(\text{Im}(f)) = k = \dim(C)$  a tedy skutečně  $\dim(C) + \dim(C^\perp) = n$ .

---

\*Informace o cvičení naleznete na <http://kam.mff.cuni.cz/~fila/>

- Platí, že  $C \subseteq (C^\perp)^\perp$ , protože každý vektor z  $C$  je z definice  $C^\perp$  kolmý na každý vektor z  $C^\perp$ .  
Podle části b) pro lineární kód  $C^\perp$  víme, že  $\dim(C^\perp)^\perp = n - \dim(C^\perp) = k$ . Jelikož mají  $(C^\perp)^\perp$  a  $C$  stejnou dimenzi a jeden je vektorový podprostor druhého, pak jde o stejné prostory a  $(C^\perp)^\perp = C$ .
- Z c) víme, že  $(C^\perp)^\perp = C$ . Zároveň z a) víme, že  $(C^\perp)^\perp = \{y \in \mathbb{F}_q^n : M^\perp y = 0\}$  a tedy  $C = \{y \in \mathbb{F}_q^n : M^\perp y = 0\}$ .

□

**Příklad 3.** *Nechť  $C$  je kód s parametry  $(n, k, 2t + 1)_2$  nad abecedou  $\{0, 1\}$ . Rozhodněte, jaké jsou parametry  $C'$ , který z  $C$  vznikne prodloužením každého kódového slova o jeden symbol určující paritu počtu jedniček v daném slově.*

*Řešení.* Nový kód bude mít první parametr  $n + 1$  a druhý parametr, protože je dimenze tedy i velikost stejná. Nyní nás zajímá minimální vzdálenost. Víme, že ke každému slovu se přidá jeden znak. Takže třetí parametr buď může zůstat stejný, nebo se zvednout o jedna.

Vezměme si libovolné dvě slova  $x, y$  s vzdáleností  $2t + 1$ . Nyní tedy víme, že rozdíl počtu jedniček je lichý, protože  $2t + 1$  je liché. To znamená, že i náš nový znak bude u obou slov rozdílný. Neboli máme kód s parametry  $(n + 1, k, 2t + 2)_2$ .

□

**Příklad 4.** *Uvažme kód obsahující všechna slova délky  $n \geq 2$  nad  $\{0, 1\}$  sudé váhy, neboli  $C = \{x = (x_1, \dots, x_n) \in \mathbb{F}_2^n : \sum_{i=1}^n x_i \equiv 0 \pmod{2}\}$ . Určete parametry tohoto kódu, ověřte, že je lineární a určete jeho duální kód  $C^\perp$ .*

*Řešení.* Snadno ověříme, že jde o lineární kód. Nulový vektor zde je. Pokud sečteme dvě kódová slova  $x$  a  $y$  z  $C$  s  $2k$  a  $2l$  jedničkami, pak máme tři možnosti. Na  $i$ -té pozici se sejdou dvě nuly, jedna jednička a jedna nula, nebo dvě jedničky. Chceme vědět, jaká je parita výsledného počtu jedniček. To bude rovno  $2k + 2l - 2 \cdot (\text{počet pozic, kde jsou jedničky v obou slovech})$ , což je znovu sudé číslo. Parametry jsou rovny  $(n, n - 1, 2)_2$ . První parametr je ze zadání. Druhý parametr plyne z toho, že počet slov se sudým počtem jedniček je  $2^{n-1}$ . Jelikož jde o lineární kód, tak stačí najít nejmenší nenulový vektor z  $C$ , což je vektor s dvěma jedničkami, proto je třetí parametr rovný dvěma.

Z Příkladu 2 víme, že duální kód má dimenzi 1. Víme, že nulový vektor i vektor samých jedniček v  $C^\perp$  jsou. Tím jsme našli celý  $C^\perp$ .

□

**Příklad 5.** *Dokažte, že Hadamardovy kódy (nad tělesem  $\mathbb{F}_2$  a naší bijekcí) vzniklé Sylvesterovou konstrukcí jsou lineární.*

*Řešení.* První řekněme, že  $1 \rightarrow 0$  a  $-1 \rightarrow 1$ . Potom víme, že první řádek je nulový vektor. Nyní už stačí ověřit, že pokud máme vektory  $u$  a  $v$ , pak je zde i součet. Budeme postupovat indukcí. Pro  $n = 1$  je to triviální. Nyní se podíváme na krok z  $n$  na  $2n$ . Začneme s řádky z matice  $H_{2n}$ . Libovolný řádek z prvních  $n$  je ve tvaru  $xx$  pro  $x \in H_n$ . Takže triviálně platí, že pokud  $x$  a  $y$  z  $H_n$ , máme  $xx + yy = (x + y)(x + y)$  je obsaženo v prvních řádcích  $H_{2n}$  z uzavřenosti  $H_n$ . Obdobně můžeme uvážit  $x(-x)$  z druhých  $n$  řádků a  $y(-y)$  z té samé množiny. Potom je zde i jejich suma  $(x + y)(-x - y) = (x + y)(x + y)$  což díky uzavřenosti  $H_n$  nalezneme i v  $H_{2n}$ . Třetí možnost je vzít  $xx$  z prvních  $n$  a  $y(-y)$  z druhých  $n$ . Potom máme  $(x + y)(x - y) = (x + y)(-(x + y))$  což v  $H_{2n}$  taky nalezneme.

□