Úlohy ke cvičení (+ pár definic)

Definice. Nechť $\mathbb{F}_2$ značí dvojprvkové těleso (s prvky 0 a 1). Dále $\mathbb{F}_2^n$ značí standardní vektorový prostor dimenze n nad $\mathbb{F}_2$. Vektorům z $\mathbb{F}_2^n$ budeme říkat slova délky n (např. vektor $(0,1,0,1,0)$ ztotožňujeme se slovem 01010). *Binárním kódem délky n* rozumíme libovolnou množinu slov $C \subseteq \mathbb{F}_2^n$. *Velikost kódu* je počet jeho slov, tj. $|C|$.

Nechť x a y jsou dvě slova z $\mathbb{F}_2^n$. *(Hammingova) vzdálenost* x a y, značená $d(x,y)$ je počet souřadnic, ve kterých se x a y liší. *Vzdálenost* binárního kódu C je minimum z hodnot $d(c_1,c_2)$, kde $c_1, c_2 \in C$, $c_1 \neq c_2$.

Binární kód C je *lineární*, pokud C je lineární podprostor $\mathbb{F}_2^n$. *Váhou* slova $x \in \mathbb{F}_2^n$ rozumíme počet jeho nenulových souřadnic.

Příklad 1. *Dokažte, že Hammingova vzdálenost je metrika, tedy že pro libovolné $x, y, z \in \mathbb{F}_2^n$ platí*

(i) $d(x,y) = 0$, *právě když* $x = y$,

(ii) $d(x,y) = d(y,x)$ *a*

(iii) $d(x,y) + d(y,z) \geq d(x,z)$.

Příklad 2. *Nechť C je lineární kód. Dokažte, že vzdálenost C je rovna minimální váze nenulového slova $c \in C$.*

Příklad 3. *Binární lineární kód C délky n, dimenze k a vzdálenosti d se nazývá $[n,k,d]$-kód.*

(i) Pro přirozené n najděte (jediný možný) $[n,n,1]$-kód.

(ii) Pro přirozené n najděte nějaký $[n,n-1,2]$-kód.

(iii) Určete parametry lineárního binárního kódu generovaného slovy 1110000, 1001100, 1000011 *a* 0101010 *(všechny lineární kombinace těchto slov do kódu také patří).*

Definice. Nechť $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ jsou dvě slova z $\mathbb{F}_2^n$. Jejich *skalárním součinem* rozumíme hodnotu

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

(Počítáme nad $\mathbb{F}_2$!)

Je-li C lineární kód, potom *duální kód* k C je kód

$$C^\perp := \{x \in \mathbb{F}_2^n : \langle x, y \rangle = 0\}.$$

Příklad 4. *Nechť C je binární lineární kód délky n.*

(i) Dokažte, že $C^\perp$ je binární lineární kód.

(ii) Dokažte, že $\dim C + \dim C^\perp = n$.

Příklad 5. *Nechť C je binární lineární k generovaný slovy* 11000, 10011, 01110 *a* 11101. *Určete $C^\perp$.*

Příklad 6. *Nechť m je přirozené číslo. Najděte kód C délky $2m$ takový, že $C = C^\perp$.*

Úlohy ke cvičení (+ pár definic)

Definice. Nechť $\mathbb{F}_2$ značí dvojprvkové těleso (s prvky 0 a 1). Dále $\mathbb{F}_2^n$ značí standardní vektorový prostor dimenze n nad $\mathbb{F}_2$. Vektorům z $\mathbb{F}_2^n$ budeme říkat slova délky n (např. vektor $(0,1,0,1,0)$ ztotožňujeme se slovem 01010). *Binárním kódem délky n* rozumíme libovolnou množinu slov $C \subseteq \mathbb{F}_2^n$. *Velikost kódu* je počet jeho slov, tj. $|C|$.

Nechť x a y jsou dvě slova z $\mathbb{F}_2^n$. *(Hammingova) vzdálenost* x a y, značená $d(x,y)$ je počet souřadnic, ve kterých se x a y liší. *Vzdálenost* binárního kódu C je minimum z hodnot $d(c_1,c_2)$, kde $c_1, c_2 \in C$, $c_1 \neq c_2$.

Binární kód C je *lineární*, pokud C je lineární podprostor $\mathbb{F}_2^n$. *Váhou* slova $x \in \mathbb{F}_2^n$ rozumíme počet jeho nenulových souřadnic.

Příklad 1. *Dokažte, že Hammingova vzdálenost je metrika, tedy že pro libovolné $x, y, z \in \mathbb{F}_2^n$ platí*

(i) $d(x,y) = 0$, *právě když* $x = y$,

(ii) $d(x,y) = d(y,x)$ *a*

(iii) $d(x,y) + d(y,z) \geq d(x,z)$.

Příklad 2. *Nechť C je lineární kód. Dokažte, že vzdálenost C je rovna minimální váze nenulového slova $c \in C$.*

Příklad 3. *Binární lineární kód C délky n, dimenze k a vzdálenosti d se nazývá $[n,k,d]$-kód.*

(i) Pro přirozené n najděte (jediný možný) $[n,n,1]$-kód.

(ii) Pro přirozené n najděte nějaký $[n,n-1,2]$-kód.

(iii) Určete parametry lineárního binárního kódu generovaného slovy 1110000, 1001100, 1000011 *a* 0101010 *(všechny lineární kombinace těchto slov do kódu také patří).*

Definice. Nechť $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ jsou dvě slova z $\mathbb{F}_2^n$. Jejich *skalárním součinem* rozumíme hodnotu

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

(Počítáme nad $\mathbb{F}_2$!)

Je-li C lineární kód, potom *duální kód* k C je kód

$$C^\perp := \{x \in \mathbb{F}_2^n : \langle x, y \rangle = 0\}.$$

Příklad 4. *Nechť C je binární lineární kód délky n.*

(i) Dokažte, že $C^\perp$ je binární lineární kód.

(ii) Dokažte, že $\dim C + \dim C^\perp = n$.

Příklad 5. *Nechť C je binární lineární k generovaný slovy* 11000, 10011, 01110 *a* 11101. *Určete $C^\perp$.*

Příklad 6. *Nechť m je přirozené číslo. Najděte kód C délky $2m$ takový, že $C = C^\perp$.*