TIN 085 Vybrané kapitoly z výpočetní složitosti I **zima 2010/2011**

1. domácí úlohy

do 29. října 2010

Úloha 1. Nechť G_1 a G_2 jsou generující matice kódů s parametry $[n_1, k, d_1]_q$ a $[n_2, k, d_2]_q$. Určete a zdůvodněte, jaké kódy generují následující matice

a)

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$$

b)

$$\begin{pmatrix} G_1 & G_2 \end{pmatrix}$$

c)

$$G_1 \otimes G_2 = \begin{pmatrix} a_{1,1}G_2 & a_{1,2}G_2 & \cdots & a_{1,n_1}G_2 \\ a_{2,1}G_2 & a_{2,2}G_2 & \cdots & a_{2,n_1}G_2 \\ \cdots & \cdots & \cdots & \cdots \\ a_{k,1}G_2 & a_{k,2}G_2 & \cdots & a_{k,n_1}G_2 \end{pmatrix}.$$

Zde

$$G_1 = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n_1} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n_1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k,1} & a_{k,2} & \cdots & a_{k,n_1} \end{pmatrix}$$

a $a_{i.i}G_2$ je matice G_2 vynásobená po složkách skalárem $a_{i,i}$.

Úloha 2. Nechť H je kontrolní matice lineárního kódu C nad $GF[2]$ generovaného $k \times n$ maticí G, to jest $\{y \in \{0,1\}^n,\, yH = 0\} = \{bG,\, b \in \{0,1\}^k\}$. Ukažte, že C má minimální vzdálenost d právě tehdy, když každých $d-1$ řádků matice H je lineárně nezávislých a existuje d řádků matice H, které jsou lineárně závislé. Platí toto tvrzení i pro jiná tělesa než $GF[2]$? ($GF[2]$ je dvouprvkové těleso s prvky 0 a 1 a počítáním $\bmod 2$.)

Úloha 3. Na přednášce jsme ukázali, že pro $0 < p < 1$ je $Vol_2(n, pn) \leq 2^{H(p)n}$.

a) Ukažte, že $\frac{2^{H(p)n}}{n+1} \leq Vol_2(n, pn)$.

b) Nalezněte (*rozumný*) dolní a horní odhad pro velikost $Vol_q(n, pn)$, tedy pro velikost Hammingovské koule o poloměru pn v prostoru $\{0, \ldots, q-1\}^n$.

Úloha 4. Ukažte, že pro všechna n lze vektory z $\{0,1\}^n$ uspořádat do posloupnosti $v_1, v_2, \ldots, v_{2^n-1}$ takové, že po sobě jdoucí vektory se liší právě v jedné pozici, to jest $\delta(v_i, v_{i+1}) = 1$ pro všechna $1 \leq i < 2^n$. (Tomuto uspořádání se říká *Grayův kód. Hint:* Použijte indukci.)

Úloha 5. Ukažte, že pro lineární binární kód $[n, k, d]_2$ platí

$$n \geq d_0 + d_1 + d_2 + \cdots + d_{k-2},$$

kde $d_0 = d$ a pro $i \geq 0$, $d_{i+1} = \lfloor (d_i + 1)/2 \rfloor$. $\lfloor \cdot \rfloor$ znamená zaokrouhlování dolů.