TIN 100 Základy přenosu a zpracování informace **zima 2015/2016**

3. domácí úlohy - samoopravné kódy

do 26. dubna 2016

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

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. V Reed-Solomonově kódu se zpráva $m = m_1 m_2 \cdots m_k \in GF[q]$ interpretuje jako koeficienty polynomu $p_m(x)$ a kódem pro m je $(p_m(\alpha_1), \ldots, p_m(\alpha_n))$. Ukažte, že pokud m přiřadíme polynom $p'_m(x)$ stupně nejvýše $k-1$ takový, že $p'_m(\alpha_i) = m_i$, pro $i = 1, \ldots, k$, a $(p'_m(\alpha_1), p'_m(\alpha_2), \ldots, p'_m(\alpha_n))$ prohlásíme za kód m, pak dostaneme opět Reed-Solomonův kód. Nalezněte generující matici takového kódu.

Úloha 4. Vezměme si neorientovaný graf $G = (V, E)$ na m vrcholech s n hranami. Podmnožiny hran tohoto grafu lze reprezentovat pomocí vektorů z $\{0,1\}^n$, kde každá souřadnice je přiřazená jedné hraně a udává, zda tam daná hrana je nebo není. Definujme si kód $C_{\text{cut}} \subseteq \{0,1\}^n$ vektorů, které reprezentují řezy v G, tj. množiny hran $F \subseteq E$ takové, že $F = \{\{u,v\},\ u \in S \;\&\; v \notin S\}$ pro nějakou množinu $S \subseteq V$.

a) Ukažte, že C_{cut} je lineární kód.

b) Ukažte, že pokud umíme pro libovolné $x \in \{0,1\}^n$ efektivně nalézt nejbližší kódové slovo z C_{cut}, pak umíme též efektivně nalézt největší řez v G. Hledání největšího řezu v G je takzvaný problém MAX-CUT, který je NP-těžký.