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

2. domácí úlohy

do 19. listopadu 2010

Úloha 1. Dokažte:

a) Každý kód $C \subseteq \{0,1\}^n$ s minimální vzdáleností alespoň $\frac{3}{4}n$ má nejvýše dvě slova. Ukažte takový lineární kód.

b) Každý kód $C \subseteq \{0,1\}^n$ s minimální vzdáleností alespoň $\frac{2}{3}n$ má nejvýše čtyři slova. Ukažte takový lineární kód.

c) Sestrojte co největší kód $C \subseteq \{0,1\}^n$ s minimální vzdáleností alespoň $\frac{3}{5}n$.

Úloha 2. 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 $i = 1, \ldots, m$, 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 3. Uvažujme následující variantu Reed-Solomonových kódů. Nechť $\alpha_1, \alpha_2, \ldots, \alpha_n \in GF[q]$ jsou pevně zvolená. Pro zprávu $m = m_1 m_2 \cdots m_k \in GF[q]$ definujme polynom $p_m(x)$ jako

a) $p_m(x) = \sum_{i=1}^{k} m_{i-1} x^{3i}$,

b) $p_m(x) = \sum_{i=1}^{k} m_{i-1} x^{2i+\ell}$, kde ℓ je pevně zvolené přirozené číslo,

a kódem pro m je jako obvykle $(p_m(\alpha_1), p_m(\alpha_2), \ldots, p_m(\alpha_n))$. Jaký kód dostane v případě a) a b)? Uveďte jeho parametry.

Úloha 4. Nechť p je prvočíslo. S pomocí jednoznačnosti rozkladu čísel na prvočísla ukažte, že pro každé $m \in \{1, \ldots, p-1\}$ je funkce $f_m(x) = m \cdot x \bmod p$ bijekcí z $\{1, \ldots, p-1\}$ do $\{1, \ldots, p-1\}$. Odvoďtě, že $\{0, \ldots, p-1\}$ s počítáním modulo p je těleso, to jest především že existují inverzní prvky pro násobení. Podobná věta platí i o polynomech v proměnné x nad $GF[p]$, tedy každý monický polynom lze jednoznačně rozložit na součin monických ireducibilních polynomů. (Polynom je monický, pokud člen nejvyššího stupně má koeficient 1.) S pomocí tohoto faktu ukažte, že $\{p(x),\ p$ je polynom stupně nejvýše $k-1$ nad $GF[p]\}$ je těleso s operacemi sčítání a násobení modulo nějaký pevně zvolený ireducibilní polynom stupně k.