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

Vánoční série - 4. domácí úlohy

do zkoušky

Úloha 1. *How to share a secret.* Představte si, že máte skupinu n bankovních úředníků a chcete mezi ně rozdělit kód k trezoru tak, aby libovolná skupina k z nich mohla kód společně zrekonstruovat, ale aby žádná skupina méně než k z nich kód zrekonstruovat nemohla a neměla by o něm žádnou informaci (to jest z jim dostupné informace by kód mohl být stále ještě cokoliv.) Vytvořte takové schéma. V prvním přiblížení tedy chceme funkci $f : \{1, \ldots, N\} \times \{1, \ldots, R\} \to \{1, \ldots, N\}^n$ takovou, že z libovolných k složek $f(x, r)$ můžeme jednoznačně určit x, ale pokud známe pouze $k-1$ složek $f(x)$, x může být libovolné. Zde x je onen kód k trezoru a r je parametr, který bude zvolen náhodně a též bude utajen. Jak to souvisí se samoopravnými kódy?

Úloha 2. Uvažujme kód nad abecedou {-1,1}. Pro $u, v \in \{-1, 1\}^n$, jaký je vztah mezi hammingovou vzdáleností mezi u a v a skalárním součinem $\langle u, v\rangle = \Sigma_{i=1}^{n} u_i \cdot v_i$. Ukažte, že pokud $v_1, v_2, \ldots, v_k \in \mathbb{R}^n$ a $0 < \alpha$ jsou takové, že $\langle v_i, v_i\rangle = 1$ a $\langle v_i, v_j\rangle \leq -\alpha$ pro všechna $i \neq j$, pak $k \leq 1 + \frac{1}{\alpha}$. Odvoďte, že binární kód s relativní minimální vzdáleností $\delta = \frac{1}{2} + \epsilon$ má nejvýše $\frac{1}{2\epsilon} + 1$ kódových slov. (*Hint:* Podívejte se na $\langle z, z\rangle$, kde $z = \sum_{i=1}^{k} v_i$.)

Úloha 3. V této úloze se podíváme na tzv. CRC kódy (*Cyclic Redundancy Check*). Zvolme celá kladná čísla $n < k$ a polynom $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ nad $GF[2]$. CRC kód zprávy $m \in \{0, 1\}^k$ spočteme tímto způsobem: zadefinujeme polynom $p_m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \cdots + m_0$, kde $m = m_0 m_1 \cdots m_{k-1}$, a položme jako CRC kód zprávy m polynom $r_m(x)$ stupně nejvýše $n-1$, který je zbytkem při dělení polynomu $p_m(x)$ polynomem $q(x)$ nad $GF[2]$, tj. $p_m(x) = q(x) \cdot t_m(x) + r_m(x)$. Ukažte, že

a) pokud $q(0) = 1$, pak pro každé dvě zprávy $m, m' \in \{0, 1\}^k$ takové, že $\Delta(m, m') = 1$, $r_m(x) \neq r_{m'}(x)$. (*Hint:* Použijte faktu, že každý polynom se dá rozložit jednoznačne na součin ireducibilních polynomů.)

b) pokud $q(0) = 1$, pak pro každé dvě zprávy $m, m' \in \{0, 1\}^k$ takové, že m a m' se liší pouze ve skupině bitů navzájem vzdálených maximálně o $n-2$ pozic, $r_m(x) \neq r_{m'}(x)$.

c) pokud počet nenulových koeficientů polynomu $q(x)$ je sudý, pak pro každé dvě zprávy $m, m' \in \{0, 1\}^k$ takové, že $\Delta(m, m')$ je lichá, $r_m(x) \neq r_{m'}(x)$. Ukažte, že každé takové $q(x)$ je násobkem polynomu $x + 1$.

d) existuje polynom $q(x)$ takový, že $q(0) = 1$ a $q(x)$ nedělí žádný z polynomů $x^i + 1$, pro $1 \leq i \leq 2^{\frac{n}{2} - \log n}$. (*Hint:* Použijte fakt, že ireducibilních polynomů stupně n nad $GF[2]$ je alespoň $\frac{1}{n} \cdot \left(2^n - 2^{(n+2)/2}\right)$.)

e) existuje polynom $q(x)$ takový, že pro $k < 2^{\frac{n}{2} - 1 - \log n}$ a pro každé dvě zprávy $m, m' \in \{0, 1\}^k$ takové, že $\Delta(m, m') \leq 3$, $r_m(x) \neq r_{m'}(x)$.

f) S užitím CRC kódu sestrojte kód schopný opravit alespoň jednu chybu. Jaké další případné typy chyb bude umět váš kód detekovat.