TIN 085 - Vybrané kapitoly z výpočetní složitosti I **zima 2007/2008**

3. domácí úlohy

Vzorové řešení

16. prosince 2007

1. Sestrojte co největší kód s relativní minimální vzdáleností 2/3 a co největší kód s relativní minimální vzdáleností 3/5.

   Řešení: Například$C_{2/3} = \{000, 011, 110, 101\}$ a $C_{3/5} = \{111\,000\,000\,0, 000\,111\,000\,0, 000\,000\,111\,0, 110\ 110\ 110\ 1, 011\ 011\ 011\ 1, 101\ 101\ 101\ 1\}$. Velikost těchto kódů je optimální, což plyne z Plotkinovy meze.

2. Nechť $p_1, p_2, \ldots, p_n$ jsou různá prvočísla mezi n^2 a $2n^2$. Položme $N = p_1 \cdot p_2 \cdots p_k$, pro nějaké $k < n$. Pro číslo $0 \le M < N$, definujme jako jeho kód $E(M) = \langle M \bmod p_1, M \bmod p_2, \ldots, M \bmod p_n\rangle$. Co můžeme říci o kódu $C = \{E(M), 0 \le M < N\}$? (Můžete použít Čínskou větu o zbytcích, která říká, že pro po dvou nesoudělná celá kladná čísla $m_1, m_2, \ldots, m_\ell$ a dvě navzájem různé čísla $0 \le x, y < m_1 \cdot m_2 \cdots m_\ell$, $\langle x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_\ell\rangle \ne \langle y \bmod m_1, y \bmod m_2, \ldots, y \bmod m_\ell\rangle$.)

   Řešení: (Podle Martina Sudy) Vezměme $0 \le M < M' < N$. Nechť $E(M)$ a $E(M')$ se shoduje v souřadnicích $i_1, i_2, \ldots, i_\ell$. Zřejmě $p_{i_1} \cdot p_{i_2} \cdots p_{i_\ell}$ musí být menší nebo rovno M', jinak podle Čínské věty o zbytcích by $M = M'$. Vzhledem k výběru prvočísel p_i, $n^\ell < p_{i_1} \cdot p_{i_2} \cdots p_{i_\ell} \le M' < N < (2n)^k$. Odsud dostaváme $\ell \log n < k(1 + \log n)$. Tedy minimální vzdálenost tohoto kódu je alespoň $n - k - \frac{k}{\log n}$.

   Pokud bychom věděli, že $p_1 < p_2 \ldots < p_n$, úloha by byla jednodušší a minimální vzdálenost kódu by byla $n - k + 1$.

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 $\Delta(m, m') = 1$, $r_m(x) \ne r_{m'}(x)$. (*Hint:* Použijte faktu, že každý polynom se dá rozložit jednoznačne na součin ireducibilních polynomů. *Ireducibilní polynom* je takový, který se nedá rozložit na součin dvou polynomů stupně alespoň 1.)

   (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, $r_m(x) \ne r_{m'}(x)$.

   (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, $r_m(x) \ne r_{m'}(x)$. Ukažte, že každé takové $q(x)$ je násobkem polynomu $x + 1$.

   (d) existuje polynom $q(x)$ takový, že $q(x)$ nedělí žádný z polynomů $x^i + 1$, pro $1 \le i \le 2^{n-3}$. (*Hint:* Použijte početní argument.)

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

   (f) existuje polynom $q(x)$ takový, že pro $k < 2^{n-4}$ a pro každé dvě zprávy $m, m' \in \{0,1\}^k$ takové, že $\Delta(m, m') \le 3$, $r_m(x) \ne r_{m'}(x)$.

   Řešení: Rozebereme pouze případ (d), neboť ostatní byly v podstatě přímočaré.

   (d) Jak si někteří povšimli, x^n splňuje zadaní úlohy, avšak nelze jej použít v bodě (e) a (f). Rádi bychom tedy polynom $q(x)$ takový, že $q(0) = 1$. Nejsem si jist, zda zadání je splnitelné v takovém případě s uvedenými parametry, ale s drobnou změnou se tvrzení pravdivé stane (důkaz, který jsem měl původně rozmyšlen, byl chybný, ale dá se upravit na správný). Polynom $x^i + 1$ má nejvýše i různých ireducibilních dělitelů. Tedy polynomy $x^i + 1$, pro $1 \le i \le 2^{n'}$, mají dohromady nejvýše $2^{2n' - 1}$ různých ireducibilních dělitelů. Nyní využijeme známého faktu, že ireducibilních polynomů stupně n nad tělesem $GF[q]$ je alespoň $\frac{1}{n}\left(q^n - q^{1+n/2}\right)$. Zvolíme-li $n' < \frac{1}{2}(n - \log_2 n)$, pak musí existovat ireducibilní polynom stupně n, který nedělí žádný z polynomů x^i+1, pro $1 \leq i \leq 2^{\frac{n}{2}-\log n}$. Meze v případě (e) a (f) by měly být příslušně upraveny.