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

3. domácí úlohy

do 17. prosince 2010

Úloha 1. 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.

Úloha 2. Zaveďme si následující *permutační vzdálenost:* slovo x má vzdálenost od slova y nejvýše d, pokud lze x získat z y s užitím nejvýše d přesunů souřadnic, kde každý přesun spočívá v tom, že symbol z x vyjmeme a přesuneme ho na jinou pozici. Vzdáleností x od y je nejmenší d takové, že x má od y vzdálenost nejvýše d. Např. $\Delta_{\text{perm}}(01101101, 10110110) = 1$ a $\Delta_{\text{perm}}(000, 010) = \infty$.

a) Pro která x, y, z platí $\Delta_{\text{perm}}(x,y) + \Delta_{\text{perm}}(y,z) \leq \Delta_{\text{perm}}(x,z)$.

b) Pro $x \in \{0,1\}^n$ nalezněte rozumné odhady pro $\text{Vol}_{2,\text{perm}}(x,d)$, kde

$$\text{Vol}_{2,\text{perm}}(x,d) = |\{y \in \{0,1\}^n;\ \Delta_{\text{perm}}(x,y) \leq d\}|\,,$$

když $d = \sqrt{n}$ a když $d = \delta n$ pro nějakou konstantu $0 < \delta < 1$.

Přirozeným způsobem můžeme zadefinovat samoopravné kódy pro permutační vzdálenost. Řekneme, že kód $C \subseteq \{0,1\}^n$ detekuje d permutačních chyb, když pro každé $x \in C$, žádné slovo v C nemá permutační vzdálenost od x menší než $d+1$.

c) Existují takové kódy s konstantní relativní vzdáleností a konstantním ratem? Pokud ano, tak nějaký navrhněte.

Úloha 3. Nechť n je kladné celé číslo. Zkonstruujme následující kód: nechť zpráva M je matice z $GF[2]^{n\times n}$. Její zakódování je M společně s paritou každého řádku, paritou každého sloupce a paritou těchto parit (tedy matice (vektor) z $GF[2]^{(n+1)^2}$). Kolik chyb tento kód umí opravit? Jak chyby opravovat?

Úloha 4. *Čínská věta o zbytcích* říká, že pro po dvou nesoudělná celá kladná čísla $m_1, m_2, \ldots, m_\ell$ a dvě navzájem různé čísla $0 \leq x, y < m_1 \cdot m_2 \cdots m_\ell$,

$$\langle x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_\ell\rangle \neq \langle y \bmod m_1, y \bmod m_2, \ldots, y \bmod m_\ell\rangle\,.$$

a) Dokažte Čínskou větu o zbytcích.

Nechť $p_1 < p_2 < \cdots < p_n$ 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 $0 \leq M < N$, definujme jako jeho kód

$$E(M) = \langle M \bmod p_1, M \bmod p_2, \ldots, M \bmod p_n\rangle\,.$$

b) Určete a zdůvodněte parametry kódu $C = \{E(M),\ 0 \leq M < N\}$.