TIN 086 Vybrané kapitoly z výpočetní složitosti II **léto 2009/2010**

1. domácí úlohy

do 22. dubna 2010

Úloha 1. Vezměme si interaktivní protokol, ve kterém bude ověřovatel deterministický. Ukažte, že jazyky rozpoznávané s využitím takovýchto ověřovatelů budou patřit do NP.

Úloha 2. Nechť n, k jsou celá kladná čísla, $x \in \{0,1\}^n$ a $a \in \{0,1\}^{n+k-1}$ jsou vektory. Zaveďme následující operaci $c = a \circ x$, kde výsledný vektor c je z $\{0,1\}^k$ a splňuje $c_i = \sum_{j=1}^{n} x_j \cdot a_{j+i-1}$, pro $i = 1, \ldots, k$. (Všechny operace jsou modulo 2.) Pro vektory $a \in \{0,1\}^{n+k-1}$ a $b \in \{0,1\}^k$, nechť $h_{a,b} : \{0,1\}^n \to \{0,1\}^k$ je funkce daná předpisem $h_{a,b}(x) = a \circ x \oplus b$, kde $\oplus$ je sčítání po složkách modulo 2. Ukažte, že pro pevné $x_1, x_2 \in \{0,1\}^n$ a $y_1, y_2 \in \{0,1\}^k$, $\Pr_{a,b}[h_{a,b}(x_1) = y_1 \ \& \ h_{a,b}(x_2) = y_2] = 2^{-2k}$, kde pravděpodobnost je brána pro náhodně zvolená $a \in \{0,1\}^{n+k-1}$ a $b \in \{0,1\}^k$. (Jinými slovy, $\{h_{a,b};\ a \in \{0,1\}^{n+k-1},\ b \in \{0,1\}^k\}$ je *2-univerzální hašovací systém*.)

Úloha 3. Sestrojte interaktivní protokol s konstantním počtem kol pro následující problémy.

a) Ověřovatel dostane Booleovskou formuli ϕ a číslo K, které je mocninou dvojky menší než počet všech možných ohodnocení ϕ. Za pomoci dokazovatele má rozhodnout, zda počet splňujících ohodnocení formule ϕ je K. Pokud je počet splňujících ohodnocení skutečně K, pak by ověřovatel měl přijmout s pravděpodobností alespoň $3/4$. Pokud je počet splňujících ohodnocení ϕ menší než $K/2$, pak by měl ověřovatel odmítnout s pravděpodobností alespoň $1/2$ ať mu dokazovatel nalhává cokoliv.

b) To samé jako v (a), ale K nemusí být mocnina dvojky a v případě, že je počet splňujících ohodnocení ϕ menší než $K/2$, pak by měl ověřovatel odmítnout s pravděpodobností alespoň $3/4$.

Úloha 4. Nechť $n > 1$ je celé číslo a $A \subseteq \{0,1\}^n$. Pro vektor $x \in \{0,1\}^n$, označme jako $A \oplus x = \{x \oplus y; y \in A\}$, kde $\oplus$ je sčítání po složkách modulo 2.

a) Ukažte, že když $|A| > \frac{1}{10}2^n$, pak existují vektory $r_1, r_2, \ldots, r_{10n} \in \{0,1\}^n$ takové, že $\{0,1\}^n \subseteq \bigcup_{i \in \{1,\ldots,10n\}} A \oplus r_i$. (*Hint:* Použijte náhodné vektory r_i. Připomeňme, že $1 - x < \mathrm{e}^{-x}$ pro všechna reálná čísla x.)

b) Ukažte, že když $|A| < 2^n/10n$, pak pro každou $10n$-tici vektorů $r_1, r_2, \ldots, r_{10n} \in \{0,1\}^n$ existuje $x \in \{0,1\}^n \setminus \bigcup_{i \in \{1,\ldots,10n\}} A \oplus r_i$.

Poznámka na okraj: Toto je podstata důkazu, že $BPP \subseteq \Sigma_2 = NP^{NP}$. Pro daný vstup w se za množinu A berou náhodné řetízky, na kterých BPP algoritmus odpoví 1.

Úloha 5. S užitím předchozí úlohy sestrojte tříkolový interaktivní protokol pro Grafový neizomorfismus, ve kterém ověřovatel posílá pouze svoje náhodné bity a ve kterém ověřovatel přijme s pravděpodobností jedna, pokud jsou zadané grafy neizomorfní.