TIN 085 Vybrané kapitoly z výpočetní složitosti I **zima 2015/2016**

2. domácí úlohy

do 14. prosince 2015

Úloha 1. Dokažte, že ke každé formuli φ velikosti m s proměnnými $x_1, \ldots, x_n$ a binarními spojkami AND a OR a unárním NOT existuje ekvivalentní formule ψ taková, že

a) její velikost je nejvýše m^5 a hloubka $5 \log m$.

b) používá spojku NOT pouze pro negaci proměnných a má stejný počet binárních spojek.

Úloha 2. Mějme graf G a v něm dva vrcholy s a t spojené cestou. Cílem tohoto cvičení je *izolovat* jednu cestu mezi s a t. Přiřaďme každé hraně náhodně celočíselnou délku z $\{1, \ldots, n^3\}$.

a) Nechť e je hrana v G. Ukažte, že pravděpodobnost, že nejkratší cesta mezi s a t, která jde přes e, a nejkratší cesta, která nejde přes e, mají stejnou délku, je nanejvýš $1/n^3$.

a) Ukažte, že pravděpodobnost, že nejkratší cesta mezi s a t je právě jedna, je alespoň $1 - 1/n$.

Úloha 3. 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 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.