TIN 086 Vybrané kapitoly z výpočetní složitosti II **léto 2007/2008**

4. domácí úlohy

do zkoušky

Úloha 1. Nechť $n, k, K \geq 1$ jsou celá čísla a $H \subseteq \{h : \{0,1\}^n \to \{0,1\}^k\}$ je 2-univerzální hašovací systém. Nechť $A \subseteq \{0,1\}^n$, kde $|A| \leq 2^{k-1}$ a $2^{k-2} \leq K \leq 2^{k-1}$.

a) Pro $h \in H$ definujme množinu kolizí $C_h = \{\{x_1, x_2\};\ x_1 \neq x_2 \in A \ \&\ h(x_1) = h(x_2)\}$. Jaká je očekávaná velikost C_h, to jest $\sum_{h \in H} |C_h|/|H|$?

b) Ukažte, že očekávaná velikost obrazu množiny A je alespoň $3|A|/4$, to jest $\sum_{h \in H} |h(A)|/|H| \geq 3|A|/4$.

c) Ukažte, že pokud $|A| = K$, pak pravděpodobnost, že pro náhodně zvolené $h \in H$, bude existovat $x \in A$ t.ž. $h(x) = 0^n$, je alespoň $\frac{3}{4} \cdot \frac{K}{2^{k-1}}$.

d) Ukažte, že pokud $|A| \leq K/2$, pak pravděpodobnost, že pro náhodně zvolené $h \in H$, bude existovat $x \in A$ t.ž. $h(x) = 0^n$, je menší než $\frac{1}{2} \cdot \frac{K}{2^{k-1}}$.

Úloha 2. 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 $3/4$.

(*Hint:* Použijte předchozí cvičení. Dále můžete použít Černovovu nerovnost, viz například shrnutí pravděpodobnosti dostupné na webové stránce přednášky.)

Úloha 3. Z přednášky známe interaktivní protokol pro neizomorfismus grafů, který pro svoji funkčnost vyžaduje, aby dokazovatel neznal náhodné bity ověřovatele. V tomto cvičení sestrojíme protokol pro neizomorfismus grafů, který dovoluje ověřovateli náhodné bity dokazovateli sdělit, aniž by mu tím pomohl ho podvést.

a) Pro grafy G_1 a G_2, označme jako $S = \{(H, \pi); H \simeq G_1$ nebo $H \simeq G_2$ a permutace π na vrcholech H splňuje $\pi(H) = H\}$. Jaká je velikost S pokud jsou G_1 a G_2 izomorfní a jaká je její velikost pokud izomorfní nejsou.

b) Sestrojte protokol pro neizomorfismus grafů, ve kterém jediná komunikace od ověřovatele k dokazovateli jsou náhodně vybrané bity.