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

2. domácí úlohy

do 13. května 2010

Úloha 1. Nechť A a B jsou dva izomorfní jazyky to jest takové, že A je převeditelné na B v polynomiálním čase (logaritmickém prostoru) a B je převeditelné na A. Ukažte, že pokud A má *instance checker* pak jej má i B.

Úloha 2. Ukažte, že $QBF = \{\psi, \psi$ je pravdivá kvantifikovaná formule$\}$ má *instance checker*. Ukažte, že každý PSPACE-úplný problém má *instance checker*. (*Hint:* Využijte interaktivní protokoly.)

Úloha 3. *Čínská věta o zbytcích:* Nechť $p_1, p_2, \ldots, p_k$ jsou různá prvočísla. Pro každá dvě čísla $0 \leq a < b < p_1 \cdot p_2 \cdots p_k$, $(a \bmod p_1, a \bmod p_2, \ldots, a \bmod p_k) \neq (b \bmod p_1, b \bmod p_2, \ldots, b \bmod p_k)$. Dokažte. (*Hint:* $(a + b) \bmod p = (a \bmod p) + (b \bmod p) \bmod p$ a $ab \bmod p = (a \bmod p)(b \bmod p) \bmod p$.)

Pozn.: Obecnější formulace věty požaduje pouze $p_1, p_2, \ldots, p_k$ navzájem nesoudělná kladná celá čísla.

Úloha 4. Mějme dvě *multi*-množiny $X, Y \subseteq \{1, \ldots, m\}$ velikosti nejvýše n, pro celá čísla $n, m \geq 1$. (V *multi-množině* se mohou prvky opakovat.) Pro celé číslo $x > 0$ definujme $h(x) = (n + 1)^x$ a pro multi-množinu $X = \{x_1, x_2, \ldots, x_\ell\}$ definujme $h(X) = \sum_{i=1}^{\ell} h(x_i)$. Ukažte, že pro dostatečně velké k, pokud $X \neq Y$, pak pro náhodné prvočíslo $p \in \{2, \ldots, k\}$ platí $h(X) \bmod p \neq h(Y) \bmod p$ s pravděpodobností alespoň $1/2$. Jak velké musí být k?

Úloha 5. S použitím předchozího sestrojte *instance checker* pro třídění, to jest pro funkci $SORT : \{1, \ldots, n^{10}\}^n \to \{1, \ldots, n^{10}\}^n$, která vrací setříděné vektory. Jaká je časová složitost takového *instance checkeru*, pokud aritmetické operace (plus, minus, krát, celočíselné dělení) s čísly do polynomiální velikosti stojí konstantu času.