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

1. domácí úlohy

do 27. března 2008

Nejprve připomene některé třídy jazyků a funkcí z přednášky.

- $L \in \Sigma_k$, pokud existuje jazyk $L' \in P$ a polynom q takový, že pro každé $x \in \{0,1\}^*$, $x \in L$ právě tehdy když $\exists w_1 \in \{0,1\}^{q(|x|)} \forall w_2 \in \{0,1\}^{q(|x|)} \cdots Q w_k \in \{0,1\}^{q(|x|)}$, $(x, w_1, w_2, \ldots, w_k) \in L'$. Zde Q označuje buď $\exists$ nebo $\forall$ v závislosti na paritě k.
- Π_k je definováno podobně jako Σ_k, pouze místo počátečního kvantifikátoru $\exists$ začneme kvantifikátorem $\forall$ a kvantifikátory dále střídáme.
- $PH = \bigcup_{k \geq 1} \Sigma_k$.
- $L \in PP$, pokud existuje jazyk $L' \in P$ a polynom q takový, že pro každé $x \in \{0,1\}^*$, $x \in L$ právě tehdy když pro ostrou většinu $w \in \{0,1\}^{q(|x|)}$, $(x, w) \in L'$.
- Funkce $f : \{0,1\}^* \to \mathbb{N}$ je v $\#P$, pokud existuje jazyk $L' \in P$ a polynom q takový, že pro každé $x \in \{0,1\}^*$, $f(x) = |\{w \in \{0,1\}^{q(|x|)};\ (x, w) \in L'\}|$.
- FP jsou funkce z $\{0,1\}^*$ do $\mathbb{N}$ počitatelné v polynomiálním čase.

Úloha 1. Dokažte, že pokud pro nějaké $k \geq 1$, $\Sigma_k = \Pi_k$, pak $PH = \Sigma_k$.

Úloha 2. Dokažte, že $PP = P$ právě tehdy, když $\#P = FP$.

Úloha 3. *Silně nedeterministický* Turingův stroj je nedeterministický Turingův stroj se třemi možnými výstupy - 0, 1 a NEVIM. Řekneme, že takový stroj přijímá jazyk L, pokud následující je pravda: pro všechna $x \in L$, všechny výpočty zkončí buď s výstupem 1 nebo NEVIM a alespoň jeden zkončí s výstupem 1, a pro všechna $x \notin L$, všechny výpočty zkončí buď s výstupem 0 nebo NEVIM a alespoň jeden zkončí s výstupem 0. Ukažte, že L je přijímán silně nedeterministickým Turingovým strojem právě tehdy, když je z $NP \cap co - NP$.

Úloha 4. 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.*)