TIN 085 - Vybrané kapitoly z výpočetní složitosti I **zima 2006/2007**

2. domácí úlohy - hrátky s hašováním

do 14. listopadu 2006

1. 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 $x \oplus y$ je xor x a y po složkách.

   (a) Ukažte, že když $|A| > \frac{3}{4}2^n$, pak existují vektory $r_1, r_2, \ldots, r_n \in \{0,1\}^n$ takové, že $\{0,1\}^n \subseteq \bigcup_{i \in \{1,\ldots,n\}} A \oplus r_i$. (Hint: Použijte náhodné vektory r_i.)

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

   (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. Rozmyslete si!)

2. Nechť $m, n > 1$ jsou celá čísla a $H \subseteq \{h : \{0,1\}^n \to \{0,1\}^m\}$ je 2-univerzální hašovací systém. Nechť $A \subseteq \{0,1\}^n$.

   (a) Pro $h \in H$ definujme množinu kolizí $C_h = \{(x_1, x_2) \in A^2; h(x_1) = h(x_2)\}$. Jaká je očekávaná velikost C_h, to jest $E_{h \in H}[|C_h|]$?

   (b) Dokažte, že když $2^m \geq 4|A|$, pak s pravděpodobností alespoň $1/2$ pro náhodné $h \in H$, alespoň polovina množiny A se zobrazí prostě při zobrazení h, to jest nekoliduje s jiným prvkem z A.

   (c) Dokažte, že když $2^m \geq |A|^2$, pak s pravděpodobností alespoň $1/2$ pro náhodné $h \in H$, množina A se zobrazí prostě při zobrazení h, to jest nenastává žádná kolize prvků z A. (Tomuto jevu se říká, že h *hašuje* A *perfektně*.)

3. Splnitelnost $SAT = \{\varphi; \varphi$ je splnitelná Booleovská formule$\}$ je dobře známý NP-úplný problém. O něco méně známý avšak taktéž NP-úplný je problém $SAT' = \{(\varphi, a, b, r); \varphi$ je Booleovská formule, pro kterou existuje splňující ohodnocení x, jenž zároveň splňuje $a \circ x \oplus b = r\}$. Zde $\circ$ je konvoluce definovaná během přednášky a vektory $a, b, r \in \{0,1\}^*$ jsou libovolné velikosti vhodné pro provedení konvoluce. Vektor x splňující dané vztahy je nazýván *svědek* pro (φ, a, b, r).

   Sestrojte pravděpodobnostní algoritmus, který dostane jako vstup Booleovskou formuli φ a zkonstruuje čtveřici (φ', a, b, r) takovou, že pokud φ není splnitelná, pak $(\varphi', a, b, r) \notin SAT'$ a pokud φ je splnitelná, pak s *rozumnou* pravděpodobností $(\varphi', a, b, r) \in SAT'$ a existuje právě jeden svědek pro (φ', a, b, r). Ukažte, že váš algoritmus splňuje toto zadání. (Hint: Použijte předchozí cvičení.)

   (Tomuto algoritmu se říká Valiant-Vazirani redukce ze SAT na $unique - SAT$. Ukazuje se tak, že rozpoznávat mezi formulí, která nemá žádné splnitelné ohodnocení a která má právě jedno splnitelné ohodnocení, je v principu skoro stejně těžké jako rozhodovat SAT. Rozmyslete si.)