TIN 086 Vybrané kapitoly z výpočetní složitosti II léto 2013/2014

2. domácí úlohy - Booleovské obvody

do 30. dubna 2014

Úloha 1. Cílem tohoto cvičení je sestrojit polynomiálně velkou monotóní formuli pro $\mathrm{MAJ}_n(x_1, \ldots, x_n)$ tedy funkci, která se vyhodnotí na jedničku právě tehdy, když vetšina jejích vstupních bitů je jednička.

a) Nalezněte monotóní formuli pro $\mathrm{MAJ}_3(x_1, x_2, x_3)$, tedy formuli sestávající pouze z binárních spojek AND a OR.

b) Nechť C je obvod (nebo formule) se vstupy $r_1, \ldots, r_m$ takový, že pro náhodně zvolený vstup z $\{0,1\}^m$, obvod je jedna s pravděpodobností $\frac{1}{2}+p$, kde p je reálné číslo mezi 0 a 1/2. Označme jako q pravděpodobnost, že obvod dá nulu. Ukažte, že pokud $p \leq 1/4$, pak pravděpodobnost, že $\mathrm{MAJ}_3(C_1, C_2, C_3)$ dá jedničku na náhodném vstupu, je alespoň $\frac{1}{2} + \frac{5}{4}p$. Zde $\mathrm{MAJ}_3(C_1, C_2, C_3)$ je obvod počítající MAJ_3 tří kopií obvodu C s nezávislými vstupy.

c) Pokračování z předchozího bodu. Ukažte, že pokud $p > 1/4$, pak pravděpodobnost, že $\mathrm{MAJ}_3(C_1, C_2, C_3)$ dá nulu na náhodném vstupu, je nejvýše $\frac{3}{4}q$.

d) Ukažte, že existuje konstanta c taková, že úplný ternární strom hloubky $c \log n$ sestávající ze spojek MAJ_3, kde každý list bere svou hodnotu z některého vhodně zvoleného vstupního bitu $x_1, \ldots, x_n$, počítá $\mathrm{MAJ}_n(x_1, \ldots, x_n)$. (*Hint:* Ukažte, že pokud si zafixujeme nějaký vstup $x_1, \ldots, x_n$ a jednotlivé vstupní bity přiřadíme listům náhodně, pak pravděpodobnost, že tento strom se vyhodnotí na hodnotu jinou než $\mathrm{MAJ}_n(x_1, \ldots, x_n)$ je menší než 2^{-n}.)

Úloha 2. Nechť $f : \{0,1\}^n \to \{0,1\}$ je libovolná funkce. Nechť C je nejmenší obvod pro tuto funkci sestávající z binárních spojek AND, OR a unárního NOT. Ukažte, že f lze počítat obvodem stejného typu a velikosti nejvýše dvakrát větší, než je velikost obvodu C, který však obsahuje nejvýše n spojek NOT.

Úloha 3. Nechť $f : \{0,1\}^n \to \{0,1\}$ je libovolná funkce. Nechť C je nejmenší obvod pro tuto funkci sestávající z binárních spojek AND, OR a unárního NOT. Ukažte, že f lze počítat obvodem stejného typu a velikosti nejvýše polynomiálně větší, než je velikost obvodu C, který však obsahuje nejvýše $O(\log n)$ spojek NOT. (*Hint:* Sestrojte obvod, který obsahuje $O(\log n)$ spojek NOT a který pro vstup $x_1, x_2, \ldots, x_n$ spočítá $\mathrm{NOT}(x_1), \mathrm{NOT}(x_2), \ldots, \mathrm{NOT}(x_n)$.)

Úloha 4. Ukažte, že pro každou booleovskou funkci $f : \{0,1\}^n \to \{0,1\}$ existuje obvod hloubky nejvýše pět sestávající pouze z hradel MOD-6 neomezeného stupně. MOD-m na vstupu $x_1, \ldots, x_n \in \{0,1\}$ je jedna, právě když $\sum_{i=1}^{n} x_i$ není dělitelné m. Jak velké obvody jsou potřeba? Dokažte dolní i horní odhady. (*Hint:* Ukažte, že každou funkci $f : \{-1,1\}^n \to \{0,1\}$ lze reprezentovat polynomem v proměnných $x_1, \ldots, x_n$ nad konečným tříprvkovým tělesem GF_3. Pro $x_1, \ldots, x_n \in \{-1,1\}$ ukažte souvislost mezi počítáním $x_1 \cdot x_2 \cdots x_n$ a počítáním MOD-2.)