ZŁO* — ćwiczenia 5

Obwody, twierdzenie Barringtona

Ćwiczenia oznaczone przez $\diamondsuit$ są z poprzednich ćwiczeń. Zrobimy je jeśli będą pomysły na sali. Ćwiczenia oznaczone przez $\spadesuit$ będziemy robić w miarę możliwości czasowych. Jeśli nie starczy czasu, to zostaną do przemyślenia w domu i następne ćwiczenia zaczniemy od wybranych z nich.

Zadania

Zadanie 1 ($\diamondsuit$). Język L nad alfabetem Σ nazwiemy definiowalnym w logice pierwszego rzędu jeśli istnieje formuła φ nad sygnaturą $\Sigma \cup \{<\}$ o następującej własności: jeśli dane słowo nad Σ rozważymy jako strukturę w której każdy $\sigma \in \Sigma$ jest interpretowany jako relacja unarna kodująca pozycje na których stoi σ, zaś relacja $<$ jest interpretowana jako relacja binarna kodująca porządek w słowie, to φ_L rozpoznaje dokładnie słowa z języka L. Wykaż, że każdy język definiowalny w logice pierwszego rzędu należy do AC^0.

Zadanie 2 ($\diamondsuit$). W tym zadaniu zajmujemy się obwodami z bramkami AND, OR, i NOT o nieograniczonym stopniu wejściowym. Przez *wielkość* obwodu rozumiemy sumaryczną liczbę drutów.

(a) Wykaż, że dla każdego $\varepsilon > 0$, dla dostatecznie dużych n istnieje funkcja $f\colon \{0,1\}^n \to \{0,1\}$, która nie ma obwodu wielkości co najwyżej $1000 \cdot \frac{2^n}{n^{1+\varepsilon}}$.

(b) Wykaż, że każda funkcja boolowska $f\colon \{0,1\}^n \to \{0,1\}$ ma obwód wielkości co najwyżej $1000 \cdot 2^n$.

(c) Wykaż, że każda funkcja boolowska $f\colon \{0,1\}^n \to \{0,1\}$ ma obwód używający co najwyżej $1000 \cdot \frac{2^n}{n}$ bramek.

(d) Wykaż, że każda funkcja boolowska $f\colon \{0,1\}^n \to \{0,1\}$ ma obwód wielkości co najwyżej $1000 \cdot \frac{2^n}{n}$.

Zadanie 3. Niech $t(n) \geqslant n$. Wykaż, że każdy język rozpoznawalny w czasie $t(n)$ da się rozpoznać przy pomocy obwodu wielkości $\mathrm{poly}(t(n))$, konstruowanego przez algorytm działający w pamięci $\mathcal{O}(\log t(n))$.

Zadanie 4. Wykaż, że $\mathsf{uniform\,NC} = \mathsf{uniform\,AC} \subseteq \mathsf{P}$.

Zadanie 5. Wykaż, że $\mathsf{uniform\,NC}^1 \subseteq \mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{uniform\,AC}^1$.

Branching program szerokości k, liczbie zmiennych boolowskich n, oraz długości m, to m-wyrazowy ciąg instrukcji postaci (i, f, g), gdzie:

- $i \in \{1, 2, \ldots, n\}$ to indeks zmiennej;
- $f, g\colon \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ to dowolne funkcje.

Bieg programu na boolowskich zmiennych $x_1, x_2, \ldots, x_n$ wygląda następująco. Program zaczyna w stanie 1, a następnie aplikuje kolejne instrukcje. Dla instrukcji (i, f, g), obecny stan q jest zmieniany na $f(q)$ lub $g(q)$, w zależności czy $x_i = 0$ czy $x_i = 1$. Program zwraca końcowy stan. Powiemy, że non-uniform ciąg programów $(P_n)_{n \in \mathbb{N}}$ rozpoznaje język L, jeśli $L \cap \{0,1\}^n$ obejmuje dokładnie te słowa $x_1 x_2 \ldots x_n$, na których program P_n zwraca stan 1. Klasa BWBP obejmuje języki rozpoznawalne przez non-uniform ciągi branching programów o stałej szerokości i wielomianowej długości.

Zadanie 6. Wykaż, że $\mathsf{BWBP} \subseteq \mathsf{NC}^1$.

Będziemy teraz pracowali nad grupą S_5, permutacji zbioru o 5 elementach. Element $g \in S_5$ jest 5-*cyklem* jeśli działa tranzytywnie na zbiorze.

Zadanie 7 (♠). Udowodnij, że w grupie S_5 są dwa 5-cykle g, h, że $[g, h] = ghg^{-1}h^{-1}$ też jest 5-cyklem.

Każdy branching program szerokości 5 zapuszczony na jakimś wejściu indukuje pewną funkcję $\{1, \ldots, 5\} \to \{1, \ldots, 5\}$. Ograniczymy się do programów zawsze indukujących jakąś permutacje z S_5. Dla danego obwodu C, powiemy, że branching program P *g-dobrze koduje* C, jeśli P zapuszczony na słowie w daje identyczność jeśli C nie akceptuje w, oraz g w przeciwnym przypadku.

Zadanie 8. Niech C będzie obwodem NC^1 kodującym formułę (każda nie-wejściowa bramka ma co najwyżej jeden drut wychodzący) używającą tylko bramek AND i NOT. Udowodnij przez indukcję po wysokości, że dla każdej bramki na d-tym poziomie od dołu, oraz dla każdego $g \in S_5$, istnieje branching program o długości co najwyżej 4^d, który g-dobrze koduje podformułę pod tą bramką.

Zadanie 9 (Twierdzenie Barringtona)**.** Skonkluduj, że $\mathsf{BWBP} = \mathsf{NC}^1$.