УДК 510.52

О.В.Вербіцький

ПРО ЙМОВІРНІСНУ ІЄРАРХІЮ МІЖ КЛАСАМИ P І NP

Ми розглядаємо модель обчислень, запропоновану в [1]. Нехай M — це машина Тюрінга із п'ятьма стрічками. Три з них є стандартними: вхідна, робоча і вихідна. На початку своєї роботи машина M зчитує із вхідної стрічки двійкове слово w, довжина якого позначається n. Після виконання на робочій стрічці стандартних операцій згідно з програмою, M записує на вихідній стрічці результат, що є символом 0 або 1. На четвертій стрічці записане "випадкове" слово r довжини $O(\log n)$. Вважається, що кожен біт цього слова є 1 або 0 з однаковою ймовірністю. На п'ятій стрічці записане слово u, що інтерпретується як доведення належності слова w до деякої множини. В ході роботи машині M дозволяється прочитати слово r повністю, а також щонайбільше k символів слова u, вибір яких машиною M може залежати від слова r. k є деякою натуральною константою. Час роботи M на вході w не повинен перевищувати $n^{O(1)}$.

Результат роботи машини M на вході w, випадковому слові r і доведенні u записуємо як $M(w,r,u)$.

Говоримо, що машина M розпізнає мову $L \subseteq \{0,1\}^*$ з ймовірністю помилки ϵ, $\epsilon \in (0,1)$, за умов:

(1) Якщо $w \in L$, то існує u таке, що $\mathbf{P}[M(w,r,u)=1] = 1$, де ймовірність береться за розподілом r.

(2) Якщо $w \notin L$, то для будь-якого u $\mathbf{P}[M(w,r,u)=1] < \epsilon$.

Через $PCP_\epsilon(O(\log n), k)$ позначаємо клас мов, які розпізнаються за допомогою описаної моделі.

Робота виконана за підтримки Міжнародного Наукового Фонду, грант MQT 300.

Нагадаємо, що клас P [NP] об'єднує всі мови, які розпізнаються [недетермінованими] машинами Тюрінга за час, обмежений поліномом від довжини входу. Як легко бачити, для будь-якого ϵ і k маємо $P \subseteq PCP_\epsilon(O(\log n), k) \subseteq NP$.

У [2] доведено, що $NP = PCP_{\epsilon_1}(O(\log n), K)$ для деяких $\epsilon_1 \in (0,1)$ і $K \in \mathbb{N}$. У цій роботі ми вказуємо, що аналогічний факт має місце і для класу P.

Теорема. *Для будь-якого $k \in \mathbb{N}$ і $\epsilon \leq 2^{-k}$,*

$$PCP_\epsilon(O(\log n), k) = P.$$

Доведення. Припустимо $L \in PCP_\epsilon(O(\log n), k)$, де $\epsilon \leq 2^{-k}$, тобто L розпізнає деяка машина M у розумінні пунктів (1) і (2). Необхідно описати поліноміальний алгоритм A, який за словом w визначав би, належить воно L, чи ні.

Булеву функцію $f_{w,r}(x_1, \ldots, x_l)$ задамо так. Вважаємо, що значення l достатньо велике, і змінні $x_1, \ldots, x_l$ позначають біти слова u. Означимо $f_{w,r}(x_1, \ldots, x_l) = M(w, r, x_1, \ldots, x_l)$. Оскільки r має довжину $O(\log n)$, всього маємо $N = n^{O(1)}$ функцій. Зауважимо, що $f_{w,r}$ залежить щонайбільше від k змінних, решта змінних фіктивні. Позначимо через $C_{w,r}$ диз'юнктивну нормальну форму функції $f_{w,r}$. Вона складається із не більш як 2^k кон'юнкцій $C_{w,r,j}$. Множину кон'юнкцій $C_{w,r,j}$ для всіх можливих r і $j \leq 2^k$ позначимо через $\mathcal{C}_w$. Перший крок роботи алгоритму A на вході w — це конструювання $\mathcal{C}_w$.

Елементи множини $\mathcal{C}_w$ перенумеруємо довільно: $\mathcal{C}_w = \{C_1, \ldots, C_m\}$, $m = n^{O(1)}$. Кожне C_i є кон'юнкцією щонайбільше k змінних $x_1, \ldots, x_l$ або їх заперечень. Далі слово u утотожнюється з набором значень істинності змінних $x_1, \ldots, x_l$. Зрозуміло, що будь-який набір u задовольняє не більше N кон'юнкцій із $\mathcal{C}_w$. Якщо $w \in L$, то за умовою (1) знайдеться u, що задовольняє саме N кон'юнкцій. Якщо $w \notin L$, то за умовою (2) будь-який набір значень істинності задовольняє менш як ϵN функцій $f_{w,r}$, а отже, менш як ϵN кон'юнкцій із $\mathcal{C}_w$.

Тепер вважаємо, що набір значень істинності u вибирається випадково. Позначимо через $e(\mathcal{C}_w)$ математичне сподівання кількості кон'юнкцій із $\mathcal{C}_w$, що задовольняються цим набором. Зважаючи на лінійність

математичного сподівання, маємо:

$$e(\mathcal{C}_w) = \mathbf{E}[\#\{i : C_i(u) = 1\}] = \mathbf{E}\left[\sum_{i=1}^{m} C_i(u)\right]$$
$$= \sum_{i=1}^{m} \mathbf{E}[C_i(u)] = \sum_{i=1}^{m} \mathbf{P}[C_i = 1].$$

Остання рівність має два наслідки. По-перше, вона показує, що $e(\mathcal{C}_w) \geq 2^{-k}m$. По-друге, оскільки кожна кон'юнкція C_i залежить від не більш як k змінних, ймовірність $\mathbf{P}[C_i(u) = 1]$ легко обчислюється. Отже, значення $e(\mathcal{C}_w)$ може бути обчислене за поліноміальний час. Другий крок алгоритму A полягає якраз в обчисленні величини $e(\mathcal{C}_w)$.

Згідно з вище викладеними міркуваннями, якщо $w \in L$, то $e(\mathcal{C}_w) \geq 2^{-k}m > 2^{-k}N$; якщо ж $w \notin L$, то $e(\mathcal{C}_w) < \epsilon N \leq 2^{-k}N$. Отже, завершальний крок алгоритму A такий: якщо $e(\mathcal{C}_w) > 2^{-k}N$, то робиться висновок, що $w \in L$, інакше — що $w \notin L$. Теорему доведено.

Отже, маємо таку картину:

$$P = PCP_{\epsilon_0}(O(\log n), K) \subseteq$$
$$\cdots \subseteq PCP_{\epsilon}(O(\log n), K) \subseteq \ldots$$
$$\subseteq PCP_{\epsilon_1}(O(\log n), K) = NP$$

для $\epsilon_0 \in (0, 2^{-K}]$ і $\epsilon \in (\epsilon_0, \epsilon_1)$. За припущення $P \neq NP$, залишається відкритим питання про кількість різних класів $PCP_{\epsilon}(O(\log n), K)$, $\epsilon \in (0,1)$, а також про співвідношення цієї ієрархії із іншими ієрархіями всередині класу NP, наприклад, із ієрархією обмеженого детермінізму.

Список літератури

1. S. Arora, S. Safra, *Probabilistic checking of proofs; a new characterization of NP*, Proc. 33rd IEEE Symp. on Foundations of Computer Science, IEEE Computer Soc. Press, Los Alamitos, CA, 1992, pp. 2–13.
2. S. Arora, C. Lund, R. Motwani, M. Sudan M. Szegedy, *Proof verification and hardness of approximation problems*, Proc. 33rd IEEE Symp. on Foundations of Computer Science, IEEE Computer Soc. Press, Los Alamitos, CA, 1992, pp. 14–23.