ZŁO* — ćwiczenia 13

Klasy z podpowiedzią

Klasa RP obejmuje problemy, dla których istnieje algorytm randomizowany, który każdą yes-instancję akceptuje z prawdopodobieństwem co najmniej 1/2, a każdą no-instancję zawsze odrzuca. Klasa PP obejmuje problemy, dla których istnieje algorytm randomizowany, który każdą yes-instancję akceptuje z prawdopodobieństwem co najmniej 1/2, a każdą no-instancję akceptuje z prawdopodobieństwem mniejszym niż 1/2. Klasa ZPP obejmuje problemy posiadające wielomianowy algorytm Las Vegas: algorytm używający randomizacji, który jest zawsze poprawny, ale którego czas działania ma wartość oczekiwaną ograniczoną wielomianowo.

Zadanie 1 ($\diamondsuit$)**.** Wykaż, że $\mathsf{NP} \subseteq \mathsf{PP}$.

Zadanie 2 ($\diamondsuit$)**.** Wykaż, że $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.

Niech A będzie klasą złożoności. Klasa A/poly obejmuje języki L, dla których istnieje ciąg słów $(\alpha_n)_{n\in\mathbb{N}}$ oraz algorytm $\mathcal{A}$ działający w klasie A o następujących własnościach:

- $|\alpha_n| \leqslant p(n)$ dla jakiegoś wielomianu $p(\cdot)$;
- $\mathcal{A}$ na wejściu $(x, \alpha_{|x|})$ rozstrzyga, czy $x \in L$.

Język L nazwiemy P-*selektywnym* jeśli istnieje wielomianowo obliczalna funkcja $f(x, y)$, gdzie $x, y \in \Sigma^\star$, taka, że jeśli $f(x, y) \in \{x, y\}$ dla każdych x, y, oraz jeśli $|\{x, y\} \cap L| = 1$, to $f(x, y)$ jest równe jedynemu elementowi w $\{x, y\} \cap L$. Klasę języków P-selektywnych nazwiemy Psel. Język L nazwiemy *rzadkim* jeśli dla każdego n mamy $|L \cap \Sigma^{\leqslant n}| \leqslant p(n)$, dla pewnego wielomianu p.

Zadanie 3. *Turniej* to graf skierowany D gdzie pomiędzy każdą parą wierzchołków u, v istnieje albo krawędź (u, v) albo (v, u). Zbiór X jest *dominujący* w D jeśli dla każdego wierzchołka u w D, $u \in X$ lub istnieje taki $x \in X$, że jest krawędź z x do u. Udowodnij, że Turniej na N wierzchołkach zawsze posiada zbiór dominujący wielkości co najwyżej $1 + \log_2 N$.

Zadanie 4. Udowodnij, że każdy język rzadki jest w P/poly.

Zadanie 5. Wykaż, że $\mathsf{Psel} \subseteq \mathsf{P/poly}$.

Zadanie 6. Wykaż, że jeśli istnieje język P-selektywny, który jest zarazem NP-zupełny, to $\mathsf{P} = \mathsf{NP}$.

Zadanie 7. Udowodnij, że jeśli istnieje NP-zupełny język rzadki, to $\mathsf{P} = \mathsf{NP}$.

Ustalmy $\Sigma = \{0, 1\}$. *OR-destylacją* języka $L \subseteq \Sigma^\star$ w język $R \subseteq \Sigma^\star$ nazwiemy algorytm, który:

- Bierze na wejściu dowolnie długi ciąg instancji $x_1, x_2, \ldots, x_t$.
- Działa w czasie wielomianowym od długości swojego wejścia.
- Zwraca jedną instancję y spełniającą $|y| \leqslant p(\max_{i=1,\ldots,t} |x_i|)$ dla pewnego wielomianu $p(\cdot)$, przy czym ma zachodzić, że $y \in R$ wtedy i tylko wtedy gdy $x_i \in L$ dla co najmniej jednego indeksu $i \in \{1, 2, \ldots, t\}$.

Inaczej mówiąc, OR-destylacja kompresuje wejściowe instancje w jedną, wielkości wielomianowej od maksimum z wielkości wejściowych instancji, zachowując logiczny OR odpowiedzi na wejściowe instancje.

Zadanie 8. Załóżmy, że mamy OR-destylację $\mathcal{A}$ z L w R; niech $p(\cdot)$ będzie ograniczeniem na wielkość wyjściowej instancji y. Rozważmy odpalanie $\mathcal{A}$ na t-krotkach słów długości co najwyżej k. Powiemy, że słowo x długości co najwyżej k jest *pokryte* przez słowo y długości co najwyżej $p(k)$, jeśli istnieje krotka $(x_1, x_2, \ldots, x_t)$ taka, że $\mathcal{A}(x_1, x_2, \ldots, x_t) = y$ oraz $x = x_i$ dla jakiegoś indeksu i. Udowodnij, że jeśli ustawimy $t \geqslant p(k) + 1$, to istnieje zawsze takie $y \in \Sigma^{\leqslant p(k)} \setminus R$, które pokrywa co najmniej połowę słów $x \in \Sigma^{\leqslant k} \setminus L$.

Zadanie 9. Wykaż, że przy założeniach poprzedniego zadania, w szczególności $t \geqslant p(k)+1$, istnieje podzbiór $S \subseteq \Sigma^{\leqslant p(k)} \setminus R$ wielkości $\mathrm{poly}(k)$, którego elementy w sumie pokrywają wszystkie elementy $\Sigma^{\leqslant k} \setminus L$.

Zadanie 10. Udowodnij, że jeśli język L posiada OR-destylację do jakiegokolwiek języka R (nawet nierozstrzygalnego), to $L \in \mathsf{coNP/poly}$. Wysnuj wniosek, że jeśli jakikolwiek NP-trudny język L posiada OR-destylację do jakiegokolwiek języka R, to $\mathsf{NP} \subseteq \mathsf{coNP/poly}$.