ZLOŻONOŚĆ OBLICZENIOWA - WYK. 3

1. Niejednorodne modele obliczeń.

   Powiedzmy że P≠NP. To znaczy, że nie ma algorytmu, który szybko rozwiązuje wszystkie instancje problemu SAT. Ale może jest tak, że dla każdego n istnieje krótki algorytm, który szybko rozwiązuje wszystkie instancje rozmiaru n? Nawet jeśli taki algorytm trudno znaleźć, to i tak znaczyłoby to, że SAT jest w praktyce rozwiązywalny.

   Warto więc rozważać modele obliczeń, w których dla każdego n stosujemy inny algorytm. *Uwaga:* to jest subtelne, bo dla każdego n język instancji o tym rozmiarze jest regularny...

2. Modele obliczeń równoległych: co jeśli mamy do dyspozycji mnóstwo procesorów?

   Przykład: naiwny algorytm mnożenia macierzy zajmuje działa sekwencyjnie w n^3 krokach. Ale gdybyśmy mieli do dyspozycji n^2 procesorów, to dałoby się to zrobić w czasie liniowym. A gdyby procesorów było n^3, to nawet w czasie logarytmicznym (wykładnicze przyspieszenie!)

   Pytanie: Jakie algorytmy dają się dobrze zrównoleglać a jakie nie?

3. Obwody logiczne (boolowskie): inny model obliczeń

   - idea: liczenie funkcji boolowskich za pomocą bramek logicznych
   - intuicja: każda bramka to prosty procesor.

   Definicja: obwód logiczny o wejściu rozmiaru n to acykliczny graf skierowany, w którym:

   - jest $2n$ bramek (wierzchołków) o stopniu wejściowym 0, oznaczonych $x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n$ i nazywanych bramkami wejściowymi,
   - pozostałe bramki są oznaczone symbolami $\wedge$ albo $\vee$,
   - jedna z bramek, o stopniu wyjściowym 0, jest zaznaczona jako bramka wyjściowa.

   Obwód jest *binarny* jeśli każda bramka ma stopień wejściowy co najwyżej 2. (Stopnia wyjściowego nie ograniczamy.)

4. Obwód rzędu n liczy n-argumentową funkcję boolowską. *Przykład:* obwod dla binarnego XOR.

5. Definicja: język rozpoznawany przez ciąg obwodów. *Fakt:* każdy język jest rozpoznawalny jakimś ciągiem obwodów (o głębokości 2 i rozmiarze wykładniczym).

6. Miary złożoności:

   - głębokość obwodu

- liczba bramek B, liczba krawędzi K,
- rozmiar obwodu: $(B+K)\cdot \log B$ (długość reprezentacji obwodu; wyjaśnić reprezentację)

Pytanie: jakie języki są rozpoznawane obwodami o rozmiarze wielomianowym?

7. *Twierdzenie:* Każdy język rozstrzygalny w czasie $T(n)$ jest rozpoznawalny ciągiem obwodów $(C_n)_{n\in\mathbb{N}}$ o głębokości $\mathcal{O}(T(n))$ i liczbie bramek $\mathcal{O}(T(n)^2)$. Co więcej, obwód C_n jest obliczalny z M i n w czasie wielomianowym of $T(n)$.

   Dowód : (ze szczegółami w skrypcie Damiana Niwińskiego)

   - Załóżmy że maszyna M działa zawsze dokładnie w $T(n)$ krokach. Jeśli czasem działa szybciej, to rozważmy rozszerzone obliczenia, w których ostatnia konfiguracja jest powtarzana. Wszystkie konfiguracje są rozmiaru co najwyżej $T(n)$.
   - Z maszyny M tworzymy obwód o n wejściach i $T(n)$ warstwach: w warstwie i, bramki oznaczają "po i krokach, na pozycji j w konfiguracji jest bit 1". To można najłatwiej objaśnić przy początkowym założeniu, że bramki mogą przyjmować wartości z Γ lub $\Gamma\times Q$. Potem kodujemy to w bitach.

8. Implikacja odwrotna nie zachodzi: nad alfabetem unarnym dowolny język, także nierozstrzygalny, jest obliczalny ciągiem obwodów o rozmiarze i głębokości stałej. (Niejednorodność!)