ZLOŻONOŚĆ OBLICZENIOWA - WYK. 5

1. Język parzystości PARITY: język tych słów na alfabetem binarnym, w których jest parzysta liczba jedynek.

   Fakt: PARITY$\in \mathbf{NC}^1$. **L**atwy obwód zliczający jedynki modulo 2.

   Twierdzenie: PARITY$\notin \mathbf{AC}^0$.

   Dowód: Rozważmy ciało $\mathbb{Z}_3 = \{-1, 0, 1\}$ i wielomiany nad nim. Wielomian n zmiennych $p : \mathbb{Z}_3^n \to \mathbb{Z}$ nazywamy *słusznym* jeśli dla argumentów z $\{0,1\}^n$ daje wyniki w $\{0,1\}$. Taki wielomian definiuje funkcję boolowską z n zmiennych. *Stopień całkowity* wielomianu p to maksymalna suma wykładników w jakimś jednomianie w p.

   Ustalmy głębokość $d \in \mathbb{N}$. Pokażemy, że PARITY nie da się rozpoznać (nawet niejednorodnym) ciągiem wielomianów głębokości d i rozmiarze wielomianowym. Ogólna idea jest taka: każdy obwód da się przybliżyć słusznym wielomianem niskiego stopnia, a funkcji parzystości nie da się przybliżyć żadnym wielomianem niskiego stopnia.

   Formalnie, pokażemy dwa lematy:

   Lemat 1: Dla dowolnej liczby naturalnej $t > 0$, dla odpowiednio dużych n, dla każdego obwodu C o n bramkach wejściowych i o głębokości d istnieje słuszny wielomian p o n zmiennych, o stopniu całkowitym $(2t)^d$, który daje wyniki różne od C na co najwyżej $\frac{|C|}{2^t}2^n$ zestawach danych wejściowych. ($|C|$ to liczba bramek w C.)

   Użyjemy tego lematu, podstawiając $t = \frac{1}{2}\sqrt[2d]{n}$. Dostaniemy wtedy, że każdy obwód C da się przybliżyć wielomianem stopnia $\sqrt{n}$, który różni się od C na co najwyżej

   $$\frac{|C|}{\sqrt{2}^{\sqrt[2d]{n}}}2^n$$

   zestawach danych wejściowych. Jeśli $|C|$ jest wielomianowe względem n, to powyższy ułamek dąży do 0. To nam da oczekiwany wynik dzięki drugiemu lematowi:

   Lemat 2: Dla odpowiednio dużych n, każdy wielomian n zmiennych stopnia całkowitego $\sqrt{n}$ różni się od funkcji parzystości na co najmniej $\frac{1}{100}2^n$ zestawach danych wejściowych.

   Z obu lematów dostajemy, że ewentualny obwód głębokości d rozpoznający funkcję parzystości musi mieć $\Omega(\sqrt{2}^{\sqrt[2d]{n}})$ bramek, czyli więcej niż wielomianowo wiele.

   Teraz udowodnimy lematy.

   Dowód Lematu 1: Ustalmy n, t i obwód C głębokości d. Załóżmy bez utraty ogólności, że C występują tylko bramki OR i NOT.

   Z każdą bramką obwodu C wiążemy (słuszny) wielomian n zmiennych $x_1, \ldots, x_n$, przez indukcję po poziomie bramki, tak by obliczał wartość C na możliwie wielu zestawach danych wejściowych.

Dla i-tej bramki wejściowej, bierzemy wielomian x_i. To zawsze oblicza właściwą wartość.

Dla bramki typu NOT, jeśli dla jej argumentu ustaliliśmy wielomian p, bierzemy wielomian $1-p$.To oblicza właściwą wartość wszędzie tam gdzie p oblicza właściwą wartość.

Jedyny problem to bramki typu OR. Rozważmy taką bramkę o arności k i załóżmy, że jej argumentom przypisano wielomiany $p_1, \ldots, p_k$. Można by przypisać jej wielomian

$$1 - \prod_{i=1}^{k}(1 - p_i).$$

Ten wielomian działa dobrze wszędzie tam gdzie $p_1, \ldots, p_i$ działają dobrze. Ma jednak za duży stopień: jeśli maksymalny stopień wielomianów p_i to s, to stopień nowego wielomianu to maksymalnie ks.

Podziałamy sprytniej. Wybierzmy *mądrze* t podzbiorów $S_1, \ldots, S_t \subseteq \{1, \ldots, k\}$. (Poniżej powiemy jak to zrobić mądrze.) Następnie rozważmy wielomiany:

$$q_i = \left(\sum_{j \in S_i} p_j\right)^2 \qquad\qquad p = 1 - \prod_{i=1}^{t}(1 - q_i).$$

Na początek proste fakty: po pierwsze, jeśli wszystkie p_i są słuszne, to wszystkie q_i i p też są słuszne. Po drugie, jeśli maksymalny stopień wielomianów p_i to s, to stopień wielomianu p to maksymalnie $2ts$. Z tego wypływa wniosek, że wielomian przypisany bramce wyjściowej obwodu C będzie miał stopień co najwyżej $(2t)^d$, jak w treści lematu.

Dla ustalonej bramki typu OR, w C ustalmy dowolny zestaw danych wejściowych dla C. Przy założeniu że wszystkie p_i dają właściwe wyniki dla tego zestawu danych, jakie jest prawdopodobieństwo, że dla losowo, niezależnie wybranych podzbiorów $S_1, \ldots, S_t$, wielomian p da właściwy wynik?

Jeśli wszystkie p_i dają wynik 0, to p też da wynik 0, czyli właściwy.

Jeśli któryś p_i daje wynik 1, to dla każdego podzbioru $S_i \subseteq \{1, \ldots, k\}$, wielomian q dla S_i daje wartość 1 jeśli w tym podzbiorze jest nieparzysta liczba (wielomianów z wartością) 1. Każdy niepusty zbiór X ma tyle samo podzbiorów o nieparzystym rozmiarze co o parzystym, więc prawdopodobieństwo, że dla losowego podzbioru S_i wielomian q_i (a więc i p) daje wartość 1, jest co najmniej $\frac{1}{2}$.

Jeżeli zbiory $S_1, \ldots, S_t$ wybierzemy losowo niezależnie, to prawdopodobieństwo, że wielomian p da niewłaściwy wynik (przy założeniu, że p_i dają właściwe wyniki) jest co najwyżej $\frac{1}{2^t}$.

To wszystko dzieje się dla każdego zestawu danych wejściowych dla C. Z tego wynika, że dla naszej bramki *istnieje* ustalony zestaw podzbiorów

$S_1, \ldots, S_t$ taki, że prawdopodobieństwo, że dla losowego zestawu danych wejściowych (wielomiany p_i dadzą właściwe wyniki a) wielomian p się pomyli, jest co najwyżej $\frac{1}{2^t}$. (To jest standardowy argument: skoro w macierzy, gdzie wiersze są indeksowane rodzinami $S_1, \ldots, S_t$ a kolumny – zestawami danych wejściowych, w każdej kolumnie jest dużo sukcesów, to w pewnym wierszu musi być dużo sukcesów.)

Ten ustalony zestaw podzbiorów $S_1, \ldots, S_t$ to właśnie ten *mądry* wybór, o którym mówiliśmy powyżej. Jeżeli dla każdej bramki wybierzemy mądrze, to każda bramka wprowadza co najwyżej $\frac{1}{2^t}2^n$ pomyłek, więc wielomian dla bramki wyjściowej myli się dla co najwyżej $\frac{|C|}{2^t}2^n$ zestawów danych wejściowych. To kończy dowód Lematu 1.

Dowód Lematu 2: Ogólna idea jest taka: jeśli istnieje wielomian niskiego stopnia, który zgadza się z funkcją parzystości na dużym zbiorze S zestawów danych wejściowych, to dla każdej funkcji istnieje wielomian niskiego stopnia, który się z nią zgadza na tym samym zbiorze S. Wielomianów jest mało a funkcji dużo, więc zbiór S nie może być za duży.

Dla ustalonej liczby n, rozważmy n-argumentową funkcję $\pi : \{-1, 1\}^n \to \{-1, 1\}$:

$$\pi(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i.$$

Mamy zależność

$$\pi(x_1, \ldots, x_n) = \text{PARITY}(x_1 - 1, \ldots, x_n - 1) + 1$$

więc gdyby istniał wielomian zgodny z PARITY na jakimś zbiorze danych, to istniałby też wielomian tego samego stopnia zgodny z π na tym samym zbiorze.

Weźmy dowolny wielomian p o n zmiennych stopnia całkowitego $\sqrt{n}$. Niech $S \subseteq \{-1, 1\}^n$ będzie zbiorem tych wejść, dla których p zgadza się z π.

Dla każdej funkcji $f : S \to \mathbb{Z}_3$ istnieje wielomian, który zgadza się z f na zbiorze S:

$$p_f(x_1, \ldots, x_n) = \sum_{\vec{y} \in S} f(\vec{y}) \cdot \prod_{i=1}^{n} -(y_i x_i + 1)$$

Ten wielomian ma stopień całkowity n, czyli trochę dużo. Zbudujemy inny wielomian stopnia całkowitego $\frac{n}{2} + \sqrt{n}$ o tej samej własności.

W tym celu, dla dowolnego jednomianu $\prod_{i \in T} x_i$ w p_f dla $|T| > \frac{n}{2}$, zastąpmy go przez:

$$\prod_{i \in T} x_i = \prod_{i=1}^{n} x_i \cdot \prod_{i \notin T} x_i = p(\vec{x}) \cdot \prod_{i \notin T} x_i.$$

Ostatnia równość zachodzi na S, a ostatni wielomian jest stopnia co najwyżej $\frac{n}{2} + \sqrt{n}$.

Ile jest wielomianów stopnia całkowitego co najwyżej $\frac{n}{2} + \sqrt{n}$?

Na zbiorze $\{-1, 1\}^n$, w jednomianach trzeba rozważać potęg większych niż 1, bo $x^2 \equiv 1$. Dlatego *jedno*mianów n zmiennych stopnia co najwyżej $\frac{n}{2} + \sqrt{n}$ jest

$$\sum_{i=1}^{\frac{n}{2}+\sqrt{n}} \binom{n}{i} << 2^n$$

więc, dla odpowiednio dużych n, jest ich mniej niż $\frac{99}{100}2^n$. Z tego wynika, że *wielo*mianów jest mniej niż $3^{\frac{99}{100}2^n}$.

Z kolei funkcji $f : S \to \mathbb{Z}_3$ jest $3^{|S|}$, więc skoro dla każdej funkcji istnieje (inny) wielomian, to $|S| < \frac{99}{100}2^n$. To kończy dowód Lematu 2 i całego twierdzenia.

2. Pytanie: gdyby do $\mathbf{AC}^0$ dołączyć bramkę XOR, czy to wystarczyłoby do rozpoznania wszystkich języków regularnych?

   - klasa $\mathbf{AC}^0[m]$: to samo co $\mathbf{AC}^0$, ale z bramkami liczącymi jedynki modulo m.
   - fakt: jeśli $p \neq q$ są różnymi liczbami pierwszymi, to $\mathbf{AC}^0[p]$ nie potrafi liczyć modulo q.
   - problem: o $\mathbf{AC}^0[6]$ nie potrafimy nawet pokazać że jest ostro mniejsze od $\mathbf{NP}$.