WYKŁAD

25.05.2015

Dowody naturalne

Alexander Razborov, Steven Rudich

Nagroda w 2007 roku, artykuł z roku 1997

Razborov i Rudich pokazali, że pewnego typu metodami najprawdopodobniej nie da się pokazać, że $P \neq NP$ (o ile to jest prawda). Ale zacznijmy historię od początku.

Najpierw zabierano się do pokazywania, że $P \neq NP$ poprzez metodę zwaną diagonalizacją. Chodzi o to, żeby zrobić maszynę w NP, która będzie się różnić ~~na~~ na pewnych wejściach od każdej maszyny w P. Okazuje się jednak, że takie podejście się relatywizuje. To znaczy nie jest istotne, czy badamy maszyny w P i NP bez wyroczni, czy też z jakąś wyrocznią L, tzn. P^L, NP^L.

W 1975 roku Baker, Gill i Solovay pokazali, że istnieją języki K, L t. że $P^K \neq NP^K$ oraz $P^L = NP^L$. A zatem ~~to~~ metoda diagonalizacji nie pokaże ani, że $P = NP$ (bo $P^K \neq NP^K$) ani, że $P \neq NP$ (bo $P^L = NP^L$).

Wtedy ludzie przerzucili się na obwody. No bo tu wydawało się że jest większa szansa żeby coś pokazać.

Spójrzmy na przykładowe pyskiego dowodu faktu, że PARITY $\notin AC^0$ pokazanego w 1987 przez Razborova i Smolenskiego.

Opowiem tylko ideę.

AC^0 to obwody o stałej głębokości, PARITY$(x_1, \ldots, x_n) = 1 \iff$ liczba $x_i = 1$ jest parzysta

Pomysł jest taki, żeby przybliżać funkcje $f: \{0,1\}^n \to \{0,1\}$ wielomianami n zmiennych. Te wielomiany będą nad $\mathbb{Z}^3 = \{0,1,-1\}$.

Okazuje się, że każda funkcja $f \in AC^0$ daje się „dobrze" (tzn. na większości wejść ok) przybliżyć wielomianem niskiego stopnia.

Z drugiej strony pokazuje się, że PARITY nie daje się dobrze przybliżyć żadnym wielomianem niskiego stopnia.

Szczegóły tu pominiemy, chociaż warto to sobie przeczytać jak ktoś jest zainteresowany.

Powiedzmy to teraz nieco inaczej. Niech F_n to zbiór funkcji $f: \{0,1\}^n \to \{0,1\}$.

W dowodzie powyżej użyty był zbiór $C_n \subseteq F_n$, gdzie

$C_n = \{ f \in F_n$ t.że nie daje się dobrze przybliżyć wielomianem małego stopnia $\}$

Mamy:

- PARITY $\in C_n$
- C_n jest użyteczne przeciwko AC^0, tzn. gdy $f \in C_n$, to $f \notin AC^0$.

Na trochę podobnej zasadzie ludzie próbowali dowodzić, że $P \neq NP$.

Pomysł był taki, żeby:

- zdefiniować pewną miarę ~~dla~~ μ skomplikowania funkcji ~~f~~ z F_n
- pokazać, że dla każdej funkcji $f \in P/poly$, czyli obliczalnej przez obwód wielomianowej wielkości $\mu(f)$ jest mała
- pokazać, że $\mu(SAT)$ jest duża.

Razborov i Rudich pokazali, że dowód idący tym tropem najprawdopodobniej nie zadziała. ~~Dlatego~~ Może nie należy tak na to patrzeć, a bardziej w stylu, że żeby zadziałał, to musi spełniać pewne dodatkowe warunki. R. i R. zdefiniowali klasę dowodów naturalnych. Pokazali, że wszystkie dotychczasowe dowody były naturalne albo naturalizowalne (~przerobialne na naturalne). Pokazali też, że dowody naturalne nie pokażą, że $P \neq NP$ przy założeniu, że istnieją generatory pseudolosowe, w co ludzie mocno wierzą.

Najpierw pokażemy pewną intuicję dotyczącą μ. Mianowicie, jeśli μ spełnia pewne dość naturalne własności oraz μ jest duża dla pewnej funkcji $f \in F_n$ (np. $\mu(SAT)$ duża), to μ jest też z dużym prawdopodobieństwem duża dla losowej funkcji.

Powiemy, że μ jest formalną miarą złożoności (ang. formal complexity measure) jeśli spełnia:

- $\mu(x_i) \leq 1$, $\mu(\overline{x_i}) \leq 1$
- $\mu(f * g) \leq \mu(f) + \mu(g)$ dla $* \in \{\vee, \wedge\}$

Intuicja jest taka: jeśli $f * g$ jest bardzo skomplikowana, ~~to~~ to ~~albo~~ f lub g powinna być dość skomplikowana.

~~[illegible]~~

Np. $\mu(f) =$ liczba zmiennych w najmniejszej formule dla f to jest formalna miara złożoności.

Ogólnie μ to jest coś jak ograniczenie dolne na złożoność ~~złożoności~~ funkcji.

Lemat

Jeśli istnieje funkcja $f \in F_n$ t. że $\mu(f) \geq c$, to przynajmniej $\frac{1}{4}$ wszystkich funkcji $g \in F_n$ spełnia $\mu(g) \geq \frac{c}{4}$.

D-d

Niech $g \in F_n$ będzie losową funkcją. Niech $h = f \oplus g$, wówczas $f = h \oplus g$. Innymi słowy $f = (\bar{h} \wedge g) \vee (h \wedge \bar{g})$, a więc $\mu(f) \leq \mu(g) + \mu(\bar{g}) + \mu(h) + \mu(\bar{h})$.

Przypuśćmy, że $|\underbrace{\{g : \mu(g) < \frac{c}{4}\}}_{S}| > \frac{3}{4}|F_n|$.

Skoro g była losowa, to $\bar{g}, h, \bar{h}$ też (choć nie są niezależne).

Zatem $\mathbb{P}(g, \bar{g}, h, \bar{h} \in S) = 1 - \mathbb{P}(\bigcup_{j \in g, \bar{g}, h, \bar{h}} j \in \bar{S}) \geq 1 - \sum_{j \in \{g, \bar{g}, h, \bar{h}\}} \mathbb{P}(j \in \bar{S}) >$
$> 1 - 4\frac{1}{4} = 0$.

Zatem istnieją $g, \bar{g}, h, \bar{h}$ t. że dla wszystkich $\mu(\cdot) < \frac{c}{4}$. Zatem $\mu(f) < c$, sprzeczność.

Teraz przejdziemy do zdefiniowania czym jest dowód naturalny.

Tak naprawdę będziemy się zajmować naturalnymi zbiorami funkcji.

Powiemy, że zbiór $C_n \subseteq F_n$ jest P-naturalną własnością użyteczną przeciw P/poly (w skrócie jest naturalny) jeśli:

- $|C_n| \geq 2^{-O(n)} |F_n|$ (duży)
- $f \in C_n \Rightarrow f \notin P/poly$ (użyteczny przeciw P/poly)
- pytanie, czy $f \in C_n$ jest obliczalne w czasie wielomianowym od reprezentacji f (czyli PTIME od 2^n) (P-naturalny) konstruktywny

Założenie 2 jest tu jasne. Zał. 1 jak pokazaliśmy wcześniej też jest dość naturalne (tu nawet mamy dużo bardziej luźne założenie). Założenie 3 po prostu jest konieczne do dowodu. Nie mamy jednak do tamtego czasu dawało się takiej konstruktywnej własności znaleźć w każdym dowodzie. Może jednak da się to jakoś obejść.

Teraz zmierzamy do pokazania, że istnienie naturalnej własności implikuje nieistnienie generatora pseudolosowego o odpowiedniej trudności.

Generator pseudolosowy to $G_k: \{0,1\}^k \to \{0,1\}^{2k}$. Idea jest taka, że przerabia on losowe ciągi długości k na ciągi długości $2k$, które wyglądają jak losowe dla wystarczająco mocnych maszyn (obwodów).

Trudność generatora $H(G)$ to minimalny M taki, że istnieje obwód logiczny C o wielkości $\leq M$ taki, że

$$\left| \mathbb{P}(C(G_k(x)) = 1) - \mathbb{P}(C(y) = 1) \right| \geq \frac{1}{M},$$

gdzie x jest losowy z $\{0,1\}^k$, a y jest losowy z $\{0,1\}^{2k}$.

Wiemy, że istnieją generatory pseudolosowe o trudności 2^{n^ε} dla pewnego $\varepsilon > 0$ (np. kandydaci itd.).

<u>Tw.</u>

Jeśli istnieje własność naturalna, to nie ∃ istnieje żaden generator pseudolosowy o trudności 2^{n^ε}, $\varepsilon > 0$, który jest w $P/poly$.

<u>D-d</u>

Idea jest z grubsza taka, że taka własność naturalna ~~[illegible]~~ dostarczałaby obwód C, który jednak rozróżniałby $G_k(x)$ oraz y z dużym prawdopodobieństwem. To jest w zasadzie większość idei.

Pierwsza myśl jest taka, że nasza własność naturalna $C_n \subseteq F_n$ mówi coś o funkcjach, więc przerobimy generator G_k na generator funkcji. To jest konstrukcja, która już wcześniej była zrobiona, tu trochę zmodyfikowana.

Niech $G_k : \{0,1\}^k \to \{0,1\}^{2k}$ będzie w $P/poly$. Niech $n = \lceil k^\varepsilon \rceil$.

Skonstruujemy $F : \{0,1\}^k \to F_n$.

Niech ~~...~~ $G_0, G_1 : \{0,1\}^k \to \{0,1\}^k$ będą zwracały odpowiednio pierwszą i drugą połówkę G.

Teraz dla $y \in \{0,1\}^n$ definiujemy

$$G_y = G_{y_n} \circ G_{y_{n-1}} \circ \ldots \circ G_{y_2} \circ G_{y_1}.$$

Teraz niech $F(x)$, dla $x \in \{0,1\}^k$ będzie zdefiniowane jak

$F(x)\,(y)$ = pierwszy bit funkcji $G_y(x)$. $F(x)$ nazywa się pseudolosową funkcją.

Jest bardzo możliwe, że jest pokazane, że jeśli G ma dużą rozbieżność, to F też

Zauważmy, że $F(x)(y)$ jest obliczalne w $P/poly$.

A więc $\underset{x \in \{0,1\}^k}{\forall} F(x) \in F_n$, ale $F(x) \notin C_n$, bo $F \in C_n \Rightarrow F \notin P/poly$.

A zatem ~~...~~ dla losowego $x \in \{0,1\}^k$ zachodzi ~~$F(x)$~~

$$\mathbb{P}(F(x) \in C_n) = 0$$

Z drugiej strony niech $f \in F_n$ będzie losowa.

Z tego, że C_n jest duże mamy, że

$$\mathbb{P}(f \in C_n) \geq 2^{-O(n)}.$$

A więc $|\mathbb{P}(F(x) \in C_n) - \mathbb{P}(f \in C_n)| \geq 2^{-O(n)}$,

czyli obwód C_n rozróżnia $F(x)$ od losowego f z prawd. $\geq 2^{-O(n)} = 2^{-O(k^{\varepsilon})}$.

Teraz można stosunkowo łatwo pokazać, że to się przeniesie też na dowolny generator G. To znaczy wyciągając tego możemy też rozróżnić ze sporym prawdopodobieństwem $G(x)$ od y, gdzie $x \in \{0,1\}^k$, $y \in \{0,1\}^{2k}$ losowe.

Nie zrobimy tego, ale zajmuje $\underbrace{20}_{\text{łatwych}}$ linii w pracy R. i R.