Сложность вычислений
Лекция 3: Ещё один метод доказательства нижних оценок для схем ограниченной глубины

Дмитрий Ицыксон

ПОМИ РАН

24 февраля 2010

В прошлый раз

- Мы рассматривали схемы из $\neg$ и $\bigvee$, $\bigwedge$ неограниченной входной степени.
- Доказали: схема константной глубины, решающая *Parity* имеет суперполиномиальный размер.
- Доказательство проходит для любой функции, которая не обращается в константу при подстановке значений части переменным.
- А если разрешить использовать в схеме $\bigoplus$?

Сегодня

- $MOD_p(x_1, x_2, \ldots, x_n) = \begin{cases} 0, & x_1 + x_2 + \cdots + x_n = 0 \bmod p \\ 1, & \text{иначе} \end{cases}$
- Теорема. (Разборов, Смоленский) Если $p, q \in \mathbb{P}$, $p \neq q$, то любая схема константной глубины из $\neg, \bigvee, \bigwedge, MOD_p$, вычисляющая MOD_q, имеет экспоненциальный размер.
- Для простоты считаем: $q = 2, p = 3$.

План доказательства

1. Приблизить схему C размера S многочленом от n переменных:
   - Степень многочлена $\leq \sqrt{n}/2$
   - Значение многочлена совпадает со значениями C на доле $1 - S/2^{n^c}$ входов.
2. Показать, что многочлен степени $\leq \sqrt{n}/2$ не может совпадать с MOD_2 более, чем на $\frac{49}{50}$ доле входов.
3. Следствие: $S \geq 2^{n^c}/50$.

Приближение многочленами

- Гейт g на глубине h мы приближаем многочленом $\tilde{g}(x_1, x_2, \ldots, x_n)$ над полем $\mathbb{Z}_3$ степени l^h ($l > 2$ — выберем позже).
- Требуем, чтобы на $\{0,1\}^n$ значения были бы из $\{0,1\}$. (Достаточно возвести в квадрат).
- Если g — это вход схемы, то $\tilde{g} = x_i$.
- Если $g = \neg f$, то $\tilde{g} = 1 - \tilde{f}$.
- Если $g = MOD_3(f_1, f_2, \ldots, f_k)$, то $\tilde{g} = (\tilde{f}_1 + \tilde{f}_2 + \cdots + \tilde{f}_k)^2$. Степень $2l^h < l^{h+1}$.
- Если $g = \bigwedge_{i=1}^{k} f_i$, то хочется приблизить так: $\tilde{g} = \prod_{i=1}^{k} \tilde{f}_i$. Но степень увеличивается в k раз!!!

Приближение $\bigwedge$ и $\bigvee$

- Опишем приближение для $\bigvee$ (для $\bigwedge$ — аналогично по правилам де Моргана)
- $g = \bigvee_{i=1}^{k} f_i$.
- Выберем случайное подмножество $A \subseteq \{1, 2, \ldots, k\}$.
  - Если $\bigvee_{i=1}^{k} f_i = 1$, то $\Pr[(\sum_{i \in A} f_i)^2 = 1] \geq \frac{1}{2}$.
  - Если $\bigvee_{i=1}^{k} f_i = 0$, то $\Pr[(\sum_{i \in A} f_i)^2 = 0] = 1$.
- Выберем случайные $A_1, A_2, \ldots, A_{l/2} \subseteq \{1, 2, \ldots, k\}$.
- $\tilde{g} = 1 - \prod_{j=1}^{l/2}(1 - (\sum_{i \in A_j} \tilde{f}_i)^2)$, $\deg \tilde{g} \leq \frac{l}{2} 2 (l)^{h-1} = l^h$.
- $\forall x \Pr_r[\text{ошибка}] < 1/2^{\frac{l}{2}} \implies \Pr_{x,r}[\text{ошибка}] < 1/2^{\frac{l}{2}} \implies \exists r \Pr_x[\text{ошибка}] < 1/2^{\frac{l}{2}}$.
- Ошибка на схеме размера S: $\leq S/2^{\frac{l}{2}}$
- $l = (\sqrt{n}/2)^{1/d}$: полином степени $\sqrt{n}/2$, ошибка: $S/2^{n^{1/(2d)}/2^{1+1/d}}$

Приближение MOD_2 многочленами

Теорема. Многочлен f из $\mathbb{Z}_3[x_1, x_2, \ldots, x_n]$ согласуется с MOD_2 на множестве $G' \subseteq \{0,1\}^n$. Если $\deg f \leq \sqrt{n}/2$, то $|G'| < \left(\frac{49}{50}\right) 2^n$

Доказательство.

- Замена переменных: $y_i = 1 + x_i \mod 3$. ($0 \to 1$, $1 \to -1$, $G' \to G \subseteq \{-1,1\}^n$, $f \to g$, $\deg g = \deg f \leq \sqrt{n}/2$)
- $$MOD_2(x_1, x_2, \ldots, x_n) = \begin{cases} 1 \implies \prod_{i=1}^{n} y_i = -1 \\ 0, \implies \prod_{i=1}^{n} y_i = 1 \end{cases}$$
- Итого, $g(y_1, y_2, \ldots, y_n)$ — это многочлен степени $\sqrt{n}/2$, который согласуется с $\prod_{i=1}^{n} y_i$ на G.

Приближение MOD_2 многочленами

- F_G — это множество всех функций из $G \to \{0, 1, -1\}$.
- $|F_G| = 3^{|G|}$.
- Достаточно показать: $|F_G| < 3^{(\frac{49}{50})2^n}$.

Лемма. Каждая функция $s \in F_G$ представляется в виде суммы мономов вида $a_I \prod_{i \in I} y_i$, где $|I| \leq \frac{n}{2} + \sqrt{n}/2$.

Доказательство.

- Представим s в виде многочлена.
- Поскольку входы из G, то $y_i^2 = 1$, т.е. s линеен по каждой переменной.
- Пусть в s есть моном $\prod_{i \in I} y_i$, в котором $|I| > n/2$.
- $\prod_{i \in I} y_i = \prod_{i=1}^{n} y_i \prod_{i \in [n] \setminus I} y_i = g(y) \prod_{i \in [n] \setminus I} y_i$.

Следствие. $|F_G| \leq 3^{\text{число мономов}} = 3^{C_n^1 + C_n^2 + \cdots + C_n^{\frac{n}{2} + \sqrt{n}/2}}$

Оценка $C_n^1 + C_n^2 + \cdots + C_n^{\frac{n}{2}+\sqrt{n}/2}$

Осталось показать, что $C_n^1 + C_n^2 + \cdots + C_n^{\frac{n}{2}+\sqrt{n}/2} < \left(\frac{49}{50}\right) 2^n$.

- Формула Стирлинга: $\sqrt{2 \cdot 3.14n}\left(\frac{n}{e}\right)^n < n! < \sqrt{2 \cdot 3.15n}\left(\frac{n}{e}\right)^n$
- $$C_n^{\frac{n}{2}} = \frac{n!}{\left(\frac{n}{2}!\right)^2} < \frac{\sqrt{2 \cdot 3.15n}\left(\frac{n}{e}\right)^n}{3.14n\left(\frac{n/2}{e}\right)^n} = \frac{2^n}{\sqrt{n/2}\frac{3.14}{\sqrt{3.15}}}$$
$$< \frac{2^n}{\sqrt{n\frac{3.12}{2}}} = \frac{2^n}{\sqrt{1.56n}}$$
- $C_n^1 + C_n^2 + \cdots + C_n^{\frac{n}{2}+\sqrt{n}/2} < 2^{n-1} + \frac{\sqrt{n}}{2} C_n^{n/2} < 2^n\left(\frac{1}{2} + \frac{1}{2\sqrt{1.56}}\right) < \left(\frac{49}{50}\right) 2^n$.