Структурная теория сложности

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

ПОМИ РАН

23 ноября 2008 г.

Доказательство леммы с прошлой лекции

For $\delta < 1/3$, f is not δ-close to a linear function $\Rightarrow$

$$\Pr_{y,z}\{f(y+z) \neq f(y)+f(z)\} > \delta/2.$$

Доказательство леммы с прошлой лекции

Для $\delta < 1/3$, если

$$\Pr_{y,z}\{f(y+z) = f(y) + f(z)\} \geq 1 - \delta/2,$$

то f является δ-близкой к линейной.

Вот она эта линейная:

$$\tilde{f}(x) = \operatorname*{maj}_r (f(x+r) + f(r)).$$

Пусть $p_x = \Pr_r\{\tilde{f}(x) = f(x+r) + f(r)\}$.

По построению $p_x \geq 1/2$. Покажем, что $p_x \geq 1 - \delta$.

$$\begin{aligned} \Pr_{r,s}\{f(x+r) + f(s) \neq f(x+r+s)\} &\leq \delta/2, \\ \Pr_{r,s}\{f(r) + f(x+s) \neq f(x+r+s)\} &\leq \delta/2, \text{ т.е.} \end{aligned}$$

$$1-\delta \leq \Pr_{r,s}\{f(x+r)+f(s) = f(x+s)+f(r)\} = \sum_{b=0}^{1}(\Pr_r\{f(x+r)+f(s) = b\})^2 =$$

$$p_x^2 + (1-p_x)^2 \leq p_x^2 + p_x(1-p_x) = p_x.$$

Доказательство леммы с прошлой лекции

Для $\delta < 1/3$, если

$$\Pr_{y,z}\{f(y+z) = f(y) + f(z)\} \geq 1 - \delta/2,$$

то f является δ-близкой к линейной.

Вот она эта линейная:

$$\tilde{f}(x) = \operatorname*{maj}_r (f(x+r) + f(r)).$$

Итак, $\Pr_r\{\tilde{f}(x) \neq f(x+r) + f(r)\} < \delta$.

- линейность:

$$\begin{aligned}
\Pr_r\{\underline{\tilde{f}(x) + \tilde{f}(y)} + f(r) &\neq f(x+r) + \tilde{f}(y)\} < \delta, \\
\Pr_r\{\underline{f(x+r) + \tilde{f}(y)} &\neq f(x+y+r)\} < \delta, \\
\Pr_r\{f(x+y+r) &\neq \underline{\tilde{f}(x+y)} + f(r)\} < \delta,
\end{aligned}$$

т.е. $\Pr_r\{\tilde{f}(x+y) = \tilde{f}(x) + \tilde{f}(y)\} > 0$, т.е. $= 1$.

Доказательство леммы с прошлой лекции

Для $\delta < 1/3$, если

$$\Pr_{y,z}\{f(y+z) = f(y) + f(z)\} \geq 1 - \delta/2,$$

то f является δ-близкой к линейной.

Вот она эта линейная:

$$\tilde{f}(x) = \operatorname*{maj}_r (f(x+r) + f(r)).$$

Итак, $\Pr_r\{\tilde{f}(x) \neq f(x+r) + f(r)\} < \delta$.

- линейность:

$$\begin{array}{rcl} \Pr_r\{\underline{\tilde{f}(x) + \tilde{f}(y)} + f(r) & \neq & f(x+r) + \tilde{f}(y)\} < \delta, \\ \Pr_r\{\underline{f(x+r) + \tilde{f}(y)} & \neq & f(x+y+r)\} < \delta, \\ \Pr_r\{f(x+y+r) & \neq & \underline{\tilde{f}(x+y)} + f(r)\} < \delta, \end{array}$$

  т.е. $\Pr_r\{\tilde{f}(x+y) = \tilde{f}(x) + \tilde{f}(y)\} > 0$, т.е. $= 1$.

- δ-близость: если $\Pr_x\{f(x) \neq \tilde{f}(x)\} > \delta$, а (по построению) $\Pr_r\{\tilde{f}(x) = f(x+r) + f(r)\} \geq 1/2$, то $\Pr_{x,r}\{f(x) \neq f(x+r) + f(r)\} > \delta/2$, противоречие.

Constraint Satisfaction Problems

Теорема (PCP Theorem)

$\mathbf{NP} = \mathbf{PCP}(O(\log n), O(1))$.

Теорема (Переформулировка PCP Theorem)

$\exists \rho < 1$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f : \{0,1\}^* \mapsto \{3\text{–КНФ}\}$ т.ч.

$$
\begin{aligned}
x \in L &\Rightarrow f(x) \text{ выполнима,} \\
x \notin L &\Rightarrow \text{нельзя выполнить даже долю } \rho \text{ клозов } f(x).
\end{aligned}
$$

Constraint Satisfaction Problems

Обобщение SAT — задача q–$\mathtt{CSP}_W$: даны клозы вида

$$C_i = (\underbrace{X \in [1\,..\,n]^q}_{\text{переменные}},\ \underbrace{c_i\colon [1\,..\,W]^q \to \{0,1\}}_{\text{таблица истинности}});$$

найти присваивание $A\colon [1\,..\,n] \to [1\,..\,W]$,
выполняющее все клозы: $\forall i\ c_i(A(X_1)\ldots, A(X_q)) = 1$.

Теорема (Ещё переформулировка PCP Theorem)

$\exists \rho < 1$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f\colon \{0,1\}^* \mapsto$ инд. задачи q–$\mathtt{CSP}_W$ т.ч.

$$\begin{aligned} x \in L &\Rightarrow f(x) \text{ выполнима,} \\ x \notin L &\Rightarrow \text{нельзя выполнить даже долю } \rho \text{ клозов } f(x). \end{aligned}$$

Стратегия доказательства PCP Theorem

Теорема

$\exists \delta > 0$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f : \{0,1\}^* \mapsto$ инд. задачи q–CSP_W т.ч.

$$x \in L \quad \Rightarrow \quad f(x) \text{ выполнима},$$

$$x \notin L \quad \Rightarrow \quad \text{нельзя выполнить даже долю } 1-\delta \text{ клозов } f(x).$$

- δ-невыполнимые формулы: не выполнить даже долю $1-\delta$ клозов;
- δ-сведéние изменяет задачу q–CSP_W так, что
  - размер увеличивается линейно;
  - невыполнимые получаются δ-невыполнимые;
  - новые q' и W' зависят только от q и W.

Стратегия доказательства PCP Theorem

Теорема

$\exists \delta > 0$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f : \{0,1\}^* \mapsto$ инд. задачи q–CSP_W т.ч.

$$x \in L \quad \Rightarrow \quad f(x) \text{ выполнима},$$

$$x \notin L \quad \Rightarrow \quad \text{нельзя выполнить даже долю } 1-\delta \text{ клозов } f(x).$$

- δ-невыполнимые формулы: не выполнить даже долю $1-\delta$ клозов;
- δ-сведéние изменяет задачу q–CSP_W так, что
  - размер увеличивается линейно;
  - невыполнимые получаются δ-невыполнимые;
  - новые q' и W' зависят только от q и W.
- Для доказательства достаточно построить сведéние, которое по формулам, у которых уже нельзя выполнить даже долю δ, строит те, у которых нельзя 2δ.

Стратегия доказательства PCP Theorem

Теорема

$\exists \delta > 0$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f : \{0,1\}^* \mapsto$ инд. задачи q–CSP_W т.ч.

$$x \in L \quad \Rightarrow \quad f(x) \text{ выполнима},$$

$$x \notin L \quad \Rightarrow \quad \text{нельзя выполнить даже долю } 1-\delta \text{ клозов } f(x).$$

- δ-невыполнимые формулы: не выполнить даже долю $1-\delta$ клозов;
- δ-сведéние изменяет задачу q–CSP_W так, что
  - размер увеличивается линейно;
  - невыполнимые получаются δ-невыполнимые;
  - новые q' и W' зависят только от q и W.
- Для доказательства достаточно построить сведéние, которое по формулам, у которых уже нельзя выполнить даже долю δ, строит те, у которых нельзя 2δ.
- Два сведения:
  1. $\delta \mapsto \ell\delta, \qquad q' = 2, \qquad W' = O(1), \qquad \ell$ — любая константа.
  2. $\delta \mapsto \delta/3, \qquad q' = O(1), \qquad W' = 2.$

Стратегия доказательства PCP Theorem

Теорема

$\exists \delta > 0$ т.ч. $\forall L \in \mathbf{NP}$ имеется полин. $f : \{0,1\}^* \mapsto$ инд. задачи q–CSP_W т.ч.

$$x \in L \quad \Rightarrow \quad f(x) \text{ выполнима},$$

$$x \notin L \quad \Rightarrow \quad \text{нельзя выполнить даже долю } 1-\delta \text{ клозов } f(x).$$

- δ-невыполнимые формулы: не выполнить даже долю $1-\delta$ клозов;
- δ-сведéние изменяет задачу q–CSP_W так, что
  - размер увеличивается линейно;
  - невыполнимые получаются δ-невыполнимые;
  - новые q' и W' зависят только от q и W.
- Для доказательства достаточно построить сведéние, которое по формулам, у которых уже нельзя выполнить даже долю δ, строит те, у которых нельзя 2δ.
- Два сведения:
  1. $\delta \mapsto \ell\delta, \qquad q' = 2, \qquad W' = O(1), \qquad \ell$ — любая константа.
  2. $\delta \mapsto \delta/3, \qquad q' = O(1), \qquad W' = 2.$
  3. . . . и нулевое сведение, чтобы подготовить формулу к первому.

Нулевое сведение: $q' = 2$ и кое-что ещё

- $q' = 2$, $W' = 2^q$:
  - доп. переменные $y_i \sim$
    присваивание переменным клоза C_i, удовлетворяющее его.
  - клозы $D_{ij}(y_i, X_j) \sim$
    y_i действительно удовлетворяет C_i и согласовано со значением X_j.

Нулевое сведение: $q' = 2$ и кое-что ещё

- $q' = 2$, $W' = 2^q$:
  - доп. переменные $y_i \sim$
    присваивание переменным клоза C_i, удовлетворяющее его.
  - клозы $D_{ij}(y_i, X_j) \sim$
    y_i действительно удовлетворяет C_i и согласовано со значением X_j.
- Граф зависимостей CSP-формулы (с кратными рёбрами и петлями):
  - вершины $\sim$ переменные;
  - $C_i = (X, c_i)$, $X_i, X_j \in X \Rightarrow$ добавляем ребро $\{X_i, X_j\}$,
  - также добавим некоторые петли.

Нулевое сведение: $q' = 2$ и кое-что ещё

- $q' = 2$, $W' = 2^q$:
  - доп. переменные $y_i \sim$
    присваивание переменным клоза C_i, удовлетворяющее его.
  - клозы $D_{ij}(y_i, X_j) \sim$
    y_i действительно удовлетворяет C_i и согласовано со значением X_j.
- Граф зависимостей CSP-формулы (с кратными рёбрами и петлями):
  - вершины $\sim$ переменные;
  - $C_i = (X, c_i)$, $X_i, X_j \in X \Rightarrow$ добавляем ребро $\{X_i, X_j\}$,
  - также добавим некоторые петли.
  - Сделаем граф d-регулярным ($\forall v \ \deg v = d$):
    - уменьшим степень: $X_i \mapsto X_i^{(1)}, \ldots, X_i^{(k)}$;
    - увеличим степень: добавим петли (причём будем считать, что в каждой вершине не менее половины рёбер — петли).

Нулевое сведение: $q' = 2$ и кое-что ещё

- $q' = 2$, $W' = 2^q$:
  - доп. переменные $y_i \sim$
    присваивание переменным клоза C_i, удовлетворяющее его.
  - клозы $D_{ij}(y_i, X_j) \sim$
    y_i действительно удовлетворяет C_i и согласовано со значением X_j.
- Граф зависимостей CSP-формулы (с кратными рёбрами и петлями):
  - вершины $\sim$ переменные;
  - $C_i = (X, c_i)$, $X_i, X_j \in X \Rightarrow$ добавляем ребро $\{X_i, X_j\}$,
  - также добавим некоторые петли.
  - Сделаем граф d-регулярным ($\forall v \ \deg v = d$):
    - уменьшим степень: $X_i \mapsto X_i^{(1)}, \ldots, X_i^{(k)}$;
    - увеличим степень: добавим петли (причём будем считать, что в каждой вершине не менее половины рёбер — петли).
  - Сделаем из графа расширитель:
    - пусть G — расширитель с тем же числом вершин (что такое расширитель, используется в док-ве, которое мы приводить не будем; но это граф ограниченной степени).
    - новые клозы — фиктивные: рёбра из G.

Первое сведение: $\delta \mapsto \ell\delta$, $q \mapsto 2$

"Возводим 2–CSP_W формулу с d-регулярным графом в степень t":

- $W' = W^{d^{5t}}$;
- новые переменные $y_1, \ldots, y_n \in W'$;
- значение y_i кодирует значения всех X_j, достижимых из X_i за $\leq t + \sqrt{t}$ шагов;
- клозы $\sim \forall y, y'$, связанных путём длины $2t + 1$, для какого-то ребра (X_i, X_j) на этом пути с вершинами внутри шаров радиуса $\leq t + \sqrt{t}$ вокруг y, y', опровергается старый клоз $c(X_i, X_j)$, где значение X_i задано y, а значение X_j — y';
- δ увеличивается в $\frac{\sqrt{t}}{10^5 d W^4}$ раз (см. на доску).

Второе сведение: $\delta \mapsto \delta/3,\ W \mapsto 2$

- Переменные из W разделим на отдельные биты.
- Каждому старому клозу (от $2 \log W$ переменных) дадим **PCP**$(\mathrm{poly}(n), 1)$-доказательство, соответствующее вып. набору u.

Второе сведение: $\delta \mapsto \delta/3,\ W \mapsto 2$

- Переменные из W разделим на отдельные биты.
- Каждому старому клозу (от $2 \log W$ переменных) дадим $\mathbf{PCP}(\mathrm{poly}(n), 1)$-доказательство, соответствующее вып. набору u.
- Правда, этот u состоит из двух половинок и ещё доп. переменных для сведения старого клоза к квадратичным равенствам, т.к. набор для всех клозов дан наборами от W переменных: в частности, для одного клоза даны $\pi_1 = \mathrm{WH}(u_1)$, $\pi_2 = \mathrm{WH}(u_2)$.
- Поэтому нужен concatenation test (f — весь набор для клоза):

$$f(r \circ s \circ 0 \ldots 0) = \pi_1(r) + \pi_2(s).$$

Второе сведение: $\delta \mapsto \delta/3,\ W \mapsto 2$

- Переменные из W разделим на отдельные биты.
- Каждому старому клозу (от $2 \log W$ переменных) дадим $\mathbf{PCP}(\mathrm{poly}(n), 1)$-доказательство, соответствующее вып. набору u.
- Правда, этот u состоит из двух половинок и ещё доп. переменных для сведения старого клоза к квадратичным равенствам, т.к. набор для всех клозов дан наборами от W переменных: в частности, для одного клоза даны $\pi_1 = \mathrm{WH}(u_1)$, $\pi_2 = \mathrm{WH}(u_2)$.
- Поэтому нужен concatenation test (f — весь набор для клоза):

$$f(r \circ s \circ 0 \ldots 0) = \pi_1(r) + \pi_2(s).$$

- Вероятность ошибки $1/2 \Rightarrow$
если лишь $\delta/3$ новых не выполнены, $2\delta/3$ старых не выполнены.