Сложность вычислений
Лекция 12: Повышение трудности функции. Коды, исправляющие ошибки.

Дмитрий Ицыксон

ПОМИ РАН

28 апреля 2011

План

$$H^{\rho}_{avg}(f) = \max\{S \mid \forall C, |C| \le S \implies \Pr_{x \leftarrow U_n}[C(x) = f(x)] < \rho\}$$

$$H_{wrs}(f) = H^{1}_{avg},\ H_{avg}(f) = \max\left\{S \mid H^{\frac{1}{2}+\frac{1}{S}}_{avg}(f) \ge S\right\}$$

Цель: По f с большой $H_{wrs}(f)$ построить f' с большой $H^{1-\delta}_{avg}(f')$.

1. Локальное декодирование
2. Итог: дерандомизация

Локальный декодер

Определение. $E : \{0,1\}^n \to \{0,1\}^m$ — код. Локальным декодером для E, исправляющим ρ ошибок, называется вероятностный алгоритм D:

1. Который получает оракульный доступ к битам y, где $\Delta(y, E(x)) < \rho$
2. D работает $poly(\log m)$ шагов
3. $\Pr[D^y = x_j] \geq \frac{2}{3}$

Теорема. Существует код $E : \{0,1\}^N \to \{0,1\}^{N^C}$, где $C > 1$ — некоторая константа, что E вычислим за время $poly(N)$ и существует локальный декодер для E, который работает время $poly(\log N)$ и обрабатывает 0.01 долю ошибок.

Чем помогает локальный декодер?

- Пусть $f : \{0,1\}^n \to \{0,1\}$ — явная трудная функция $H_{wrs}(f) = S(n)$.
- Таблица истинности f — это строка из $\{0,1\}^N$, где $N = 2^n$.
- $E(f) \in \{0,1\}^{N^c}$ — это таблица истинности функции $g : \{0,1\}^{cn} \to \{0,1\}$.
- Пусть $H_{avg}^{1-\rho}(g) = S'(cn)$.
- Есть локальный декодер, который читает $E(f)$ с ρ ошибками, работает $(cn)^r$ шагов.
- По декодеру строим схему размера $(cn)^{2r} n^2 S'(cn)$, которая без ошибок вычисляет f.
- $S'(cn) \geq S(n)/poly(n)$
- Если $f \in \mathrm{E}$, то и $g \in \mathrm{E}$.

Дерандомизация

- Если $H_{wrs}(f) = S(n)$, то $H^{0.99}_{avg}(g) = S'(n) = S(n)/poly(n)$;
- Если $H^{\frac{1}{2}+\epsilon}_{avg}(h) \geq s$ и $\epsilon \leq \frac{1}{s}$, то $H_{avg}(h) \geq s$.
- По XOR-лемме $H^{\frac{1}{2}+\epsilon}_{avg}(g^{\oplus k}) \geq \frac{\epsilon^2}{poly(n)} S'(n)$, $\epsilon < 0.99^k$.
- $H_{avg}(g^{\oplus k}) \geq S''(n)$, если $\epsilon = \frac{1}{S''(n)} > 0.99^k$
- $S''(n) = poly(n)(S'(n))^{\frac{1}{3}}$
- $\frac{1}{S'} = \epsilon > 0.99^k$
- $k = O(\log S') = O(n)$, $g^{\oplus k} : \{0,1\}^{cn^2} \to \{0,1\}$.
- Если $H_{wrs}(f) \geq 2^{n_1^\epsilon}$, то
  $H_{wrs}(g^{\oplus k}) \geq 2^{n_2^\epsilon} \implies \mathbf{BPP} \subseteq \mathbf{QuasiP} = \mathbf{DTime}[2^{polylog(n)}]$.
- Если
  $H_{wrs}(f) \geq n^{\omega(1)} \implies \mathbf{BPP} \subseteq \mathbf{SUBEXP} = \cap_{\epsilon > 0}\mathbf{DTime}[2^{n^\epsilon}]$.

Локальное декодирование списокм

Определение. $E : \{0,1\}^n \to \{0,1\}^m$ — код. Локальным декодер списком для E, исправляющим ρ ошибок, называется вероятностный алгоритм D:

1. Который получает оракульный доступ к битам y, где $\Delta(y, E(x)) < \rho = 1$, $0 < \rho < 1$.
2. D получает $i_0, |i_0| = O(\log m)$.
3. D работает $poly(\log m)$ шагов
4. Для каждого x существует такой i_0, что $\Pr[D^y(i_0) = x_j] \geq \frac{2}{3}$

Теорема.

- $S(n) < 2^n$ — суперполиномиальная конструктивная по времени функция, $N = 2^n$
- $\exists$ код $E : \{0,1\}^N \to \{0,1\}^{N^C}$, $C > 1$ — некоторая константа, что E вычислим за время $poly(N)$, $\exists$ локальный декодер списком для E, который работает время $poly(S(n))$ и обрабатывает $\frac{1}{2} - \frac{1}{S(n)}$ долю ошибок.

Итог

Теорема. $f \in \mathrm{E}$, $H_{wrs}(f)(n) \geq S(n)$, $S(n)$ — конструктивная по времени неубывающая функция. Тогда $\exists g \in \mathrm{E}$ и $c, \epsilon > 0$, что $H_{avg}(g)(n) \geq S(n/c)^{\epsilon}$.