Вычислительно трудные задачи и дерандомизация
Лекция 12: Экстрактор из псевдослучайного генератора

Дмитрий Ицыксон

ПОМИ РАН

10 мая 2009

План

1. Экстрактор из псевдослучайного генератора
2. Что мы узнали и чего мы не узнали

Экстрактор из псевдослучайного генератора

- Мы строили по трудной функции псевдослучайный генератор.
- Конструкция пользовалась функцией как черным ящиком.
- По схеме, отличающей выход псевдослучайного генератора от равномерного распределения, можно построить схему, вычисляющую f.

Псевдослучайный генератор

Теорема. (Теорема Нисана-Вигдерсона, переформулировка)
Для любой правильной функции $S : \mathbb{N} \to \mathbb{N}$, $\exists c > 0$, алгоритмы G и R

- По функции $f : \{0,1\}^\ell \to \{0,1\}$ и строке $z \in \{0,1\}^{c\ell}$, алгоритм $G^f(z)$ работает время $2^{O(\ell)}$ и выдает строку длины $m = (S(\ell))^{1/c}$
- Если $h : \{0,1\}^m \to \{0,1\}$ функция, для которой $\left|\Pr[h(G^f(U_{c\ell})) = 1] - \Pr[h(U_m) = 1]\right| > \frac{1}{10}$, тогда существует подсказка a размера $S(\ell)^{1/4}$, что для всех x: $R^h(a,x) = f(x)$ и R работает время $S(\ell)^{1/4}$.

Экстрактор Тревисана

Лемма. $f \in \{0,1\}^n$, $z \in \{0,1\}^{c\ell}$, $\ell = \log n$. G — генератор из предыдущей теоремы. $f : \{0,1\}^\ell \to \{0,1\}$. Тогда $\mathrm{Ext}(f,z) \mapsto G^f(z)$ — это $(S(\ell), \frac{1}{5})$-экстрактор.

Доказательство. Пусть D — это (n,k)-источник, пусть h различает $\mathrm{Ext}(D, U_{c\ell})$ от U_m с вероятностью $\geq \frac{1}{10}$. С вероятностью $\geq \frac{1}{10}$ по $f \in D$ функция h отличает $G^f(U_{c\ell})$ от U_m. Назовем такие f плохими. Для каждой плохой функции есть подсказка a размера $S(l)^{1/4}$, что f вычислим $x \mapsto R^h(a,x)$. Значит, плохих f не больше, чем $2^{S(l)^{1/4}}$. Мера плохих f не превосходит $2^{^{1/4}}2^{-S(l)} << \frac{1}{10}$.

Краткое содержание курса

- Нижние оценки на схемную сложность
  1. Теорема Разборова о нижней оценке для монотонных схем
  2. Теорема Хастада о нижней оценки для схем ограниченной глубины
  3. Теорема Разборова-Смоленского: аппроксимация для схем ограниченной глубины
  4. Естественные доказательства
- Связь схемной сложности и дерандомизации
  1. Псевдослучайный генератор Нисана-Вигдерсона
  2. Повышение трудности функций: XOR-лемма Яо.
  3. Повышение трудности функций: коды, исправляющие ошибки.
- Дерандомизация
  1. Экономия случайных битов с помощью экспандеров
  2. Экстракторы
  3. Дерандомизация для вычислений, ограниченных по памяти
  4. Экстрактор Тревисана

Что не было рассказано в курсе?

- Hitting set генераторы.
- Дерандомизация при предположениях об алгоритмической сложности.
    - Если **BPP** $\neq$ **EXP**, тогда для любого языка из **BPP** существует детерминированный алгоритм, работающий время $2^{n^{o(1)}}$, который на бесконечном числе длин входа распознает язык на доле входов $1 - \frac{1}{n}$.
- Дерандомизация влечет нижние оценки для схем:
    - Если $ZeroP \in \mathbf{P}$, тогда либо **NEXP** $\not\subset$ **P**/**Poly**, либо $perm \notin AlgP/Poly$.
- И много-много других результатов...