# Дерандомизация: основные результаты и подходы
# Лекция 4: Псевдослучайные генераторы.

Дмитрий Ицыксон

ПОМИ РАН

22-ое декабря 2006

# Псевдослучайное множество

## Определение.

Множество $P \subseteq \{0,1\}^r$ называется псевдослучайным для класса множеств $C \subseteq 2^{\{0,1\}^r}$ с вероятностью ошибки $\epsilon$, если для любого $S \in C$.

$$|P_{x \in P}\{x \in S\} - P_{x \in \{0,1\}^r}\{x \in S\}| \leq \frac{\epsilon}{2}$$

## Определение.

Множество $P \subseteq \{0,1\}^r$ называется псевдослучайным для схем размера $r$, для любой схемы $A$ размера $r$

$$|P_{x \in P}\{A(x) = 1\} - P_{x \in \{0,1\}^r}\{A(x) = 1\}| \leq \frac{\epsilon}{2}$$

# Результат

## Теорема

Если существует язык $L \in \mathbf{EXP}$, схемная сложность которого суперполиномиальная, тогда $\mathbf{BPP} \subseteq \mathbf{DTime}(2^{O(n^\epsilon)})$ для всех $\epsilon > 0$.

# План доказательства

## Лемма 1

Пусть $s(n)$ — суперполиномиальная функция. Пусть мы умеем за время $2^{O(n^c)}$ строить таблицу истинности функции $f : \{0,1\}^n \to \{0,1\}$, такой что любая схема размера не более $s(n)$ правильно вычисляет функцию $f$ на не более, чем $\frac{1}{2} + \frac{1}{s(n)}$ доле входов. Тогда для любого $\epsilon > 0$ за время $2^{O(n^\epsilon)}$ построить псевдослучайное множество для схем размера $n$ с ошибкой $1/10$.

# План доказательства

## Лемма 2

Пусть $s(n)$ — суперполиномиальная функция. Пусть мы умеем за время $2^{O(n^c)}$ строить таблицу истинности функции $f : \{0,1\}^n \to \{0,1\}$, такой что любая схема размера не более $s(n)$ не вычисляет функцию $f$. Тогда за время $2^{O(n^c)}$ можно построить таблицу истинности функции $f : \{0,1\}^n \to \{0,1\}$, такой что любая схема размера не более $s'(n)$ правильно вычисляет функцию $f$ на не более, чем $\frac{1}{n^2}$ доле входов. $s'(n)$ — другая суперполиномиальная функция.

# План доказательства

## Лемма 3

Пусть $s'(n)$ — суперполиномиальная функция. Пусть мы умеем за время $2^{O(n^c)}$ строить таблицу истинности функции $f : \{0,1\}^n \to \{0,1\}$, такой что любая схема размера не более $s'(n)$ правильно вычисляет функцию $f$ на не более, чем $\frac{1}{n^2}$ доле входов. Тогда за время $2^{O(n^c)}$ можно построить таблицу истинности функции $f : \{0,1\}^n \to \{0,1\}$, такой что любая схема размера не более $s''(n)$ правильно вычисляет функцию $f$ на не более, чем $\frac{1}{2} + \frac{1}{s(n)}$ доле входов. $s''(n)$ — другая суперполиномиальная функция.

# Предсказатель

## Определение

Функция $f$ называется $\varepsilon$-предсказателем для распределения $D$, если для случайного элемента $x$, полученного по распределению $D$, $P\{f(x_1, x_2, \ldots x_{i-1}) = x_i\} \geq \frac{1}{2} + \varepsilon$.

## Лемма

Если множество $S \subseteq \{0,1\}^m$ не является $\varepsilon$-псевдослучайным для схем размера $m$, то для равномерного распределения на множестве $S$ существует $\frac{\varepsilon}{2m}$-предсказатель — схема размера $m$.

## Доказательство

Гибридный метод.

# Дизайн Nisan-Wigderson

## Дизайн

$S_1, S_2, \ldots, S_m$ — $s$-элементные подмножества $\{1, 2, \ldots n\}$. Для любых $i \neq j$, $|S_i \cap S_j| \leq l$.

## Лемма

Для любых параметров $m$ и $n$ существует явный дизайн с параметрами: $(n^m, n^2, n, m)$.

# Доказательство Леммы 1

Пусть $\epsilon' = \epsilon/c$. Зафиксируем дизайн $S_1, S_2, \dots S_n$ с параметрами $(n, n^{2\epsilon'}, n^{\epsilon'}, \log n)$. Определим множество $P = \{v_y\}_{y \in \{0,1\}^{n^{2\epsilon'}}}$. Определим $v_y = f(y_{S_1}) f(y_{S_2}) \dots f(y_{S_n})$.
Пусть это не псевдослучайное множество для схем размера $n$ с ошибкой $\frac{1}{10}$. Значит есть предсказатель для бита с номером $i$ от $v_i$ с вероятностью $\frac{1}{20(n+1)}$.
Заморозим все биты кроме битов $S_i$. $|S_i \cap S_j| \leq \log n$. Значит, таблица истинности $f(y_{S_j})$ — полиномиального размера от $n$. Далее вычисляем $f(y_{S_1}), \dots, f(y_{S_{i-1}})$ по табличкам. А предсказатель нам с вероятностью больше $\frac{1}{2} + \frac{1}{20(n+1)}$ даст $f(y_{S_i})$. $|Y_{S_i}| = n^{\epsilon'}$.