# Доказательства с ошибками

Э.Гирш

по материалам совместных работ
с Д.Ицыксоном, И.Монаховым, В.Николаенко и А.Смалем

- Классические системы и процедуры поиска доказательств.
- Вероятностные . . .
- Эвристические (“физические”) . . .

# Системы доказательств

## Определение

Система доказательств для $L$ — полиномиальная по времени процедура проверки $V$, т.ч. $f \in L \iff \exists \pi \; V(f, \pi) = 1$.

Процедура поиска доказательств (аксептор) для $L$ — частный случай системы доказательств:

- $A(f)$ на $f \in L$ останавливается, есть протокол;
- $A(f)$ на $f \notin L$ зацикливается.

## Факт

**NP** $=$ **co-NP** $\iff$ существует система доказательств, в которой у каждой тавтологии логики высказываний есть доказательство полиномиальной длины (полиномиально ограниченная система).

# Сводимости между системами

## Определение

Система $S$ моделирует систему $W$ (пишем $S \leq W$) $\iff$
$S$-док-ва не длиннее $W$-док-в (с точностью до полинома $p$): $\forall f \in L$

$$|\text{кратчайшее } S\text{-док-во } f| \leq p(|\text{кратчайшее } W\text{-док-во } f|).$$

## Определение (конструктивный вариант)

. . . $p$-моделирует $(\leq_p)$ . . . $\iff$ по $W$-док-ву размера $s$ можно за полиномиальное время построить $S$-док-во размера $\leq p(s)$.

## Определение

($p$-)оптимальная система доказательств — наименьший элемент относительно $\leq$ $(\leq_p)$.

«А был ли мальчик?..»

# Оптимальные аксепторы

## Определение

$A$ — оптимальный аксептор для $L$ $\iff$
$\forall A'$ имеется полином $p$, т.ч. $\forall f \in L \qquad \mathrm{time}_A(f) \le p(\mathrm{time}_{A'}(f) + |f|)$.

## Теорема (Krajíček, Pudlák, 1989; Messner. . . )

Для языка пропозициональных тавтологий (и не только. . . ):
$\exists$ $p$-оптимальная система док-в $\iff$ $\exists$ оптимальный аксептор.

"Наивный" перечислительный подход:

запустить параллельно первые $n$ алгоритмов

- $A_1(f)$,
  . . .
- $A_n(f)$,

и выдать 1, как только один из них выдаст 1.

Проблема: как отличить "правильные" алгоритмы?

# Вероятностные алгоритмы

## . . . и вероятностно проверяемые доказательства

Вероятностный алгоритм — использует датчик случайных чисел, для каждого входа вероятность ошибки $< \frac{1}{4}$.

### Лемма (Schwartz-Zippel)

Пусть $p(\vec{x}) \in \mathbb{F}[x_1, \ldots, x_n]$, $p \not\equiv 0$.
Выберем $r_1, \ldots, r_n$ независимо, равновероятно из $S \subseteq \mathbb{F}$.
Тогда

$$\Pr\{p(\vec{r}) = 0\} \leq \frac{\deg p}{|S|}.$$

**“Теорема:”** многочлен $p$ не очень большой степени можно представить в виде формулы некоторого вида.
**“Доказательство:”** формула $\Phi$ этого вида.
**Проверка:** $\Phi(\vec{r}) - p(\vec{r}) = 0$ в случайных точках $\vec{r}$.

# Неизоморфизм графов

$\mathrm{GNI} = \{(G_1, G_2) \mid G_1 \not\simeq G_2, |V(G_1)| = |V(G_2)|\}$,

- $n$ — количество вершин,
- $G^\pi$ — результат перестановки вершин $V(G)$ при помощи $\pi \in \mathfrak{S}_n$.

$\mathrm{SelfCorrect}_{A,N}$ исправляет ошибки в любом аксепторе для GNI:

- Запустить параллельно $N+1$ копий $A$ для случайных $\pi_{ij} \in \mathfrak{S}_n$:
  - $A({G_1}^{\pi_{11}}, {G_1}^{\pi_{12}})$
  - $A({G_1}^{\pi_{21}}, {G_1}^{\pi_{22}})$
  - $\ldots$
  - $A({G_1}^{\pi_{N1}}, {G_1}^{\pi_{N2}})$
  - $A({G_1}^{\pi_{N+1,1}}, {G_2}^{\pi_{N+1,2}})$
- Выдать 1, если последняя копия выдала 1 быстрее всех; иначе — зациклиться.

## Лемма

1. Если $G_1 \simeq G_2$, то $\Pr[\text{выдать 1}] \leq \frac{1}{N+1}$.
2. Если $G_1 \not\simeq G_2$ и $A$ ошибается с вероятностью $\leq \frac{1}{2^n}$, то $\Pr[\text{выдать 1 не слишком медленнее } A] \geq 1 - \frac{N+1}{2^n}$.

# Оптимальный аксептор для неизоморфизма графов

Алгоритм $Opt(G_1, G_2)$:

- Запустить параллельно:
  - $A_1(G_1, G_2)$ (полный перебор),
  - 3 экземпляра $\text{SelfCorrect}_{A_2,30n}(G_1, G_2)$,
  - 3 экземпляра $\text{SelfCorrect}_{A_3,30n}(G_1, G_2)$,
  - ...
  - 3 экземпляра $\text{SelfCorrect}_{A_n,30n}(G_1, G_2)$.
- Выдать 1, как только один из процессов выдаст 1.

## Лемма (корректность)

Если $G_1 \simeq G_2$, то $\Pr[Opt(G_1, G_2) = 1] \leq \frac{3n}{30n+1} < \frac{1}{10}$.

## Лемма (эффективность)

Для любого аксептора $A$ для GNI $\exists$ полином $p$, т.ч. $\forall (G_1, G_2) \in GNI,\ \text{time}_{Opt}(G_1, G_2) \leq p\left(\max_{\pi,\sigma \in \mathfrak{S}_n}[\text{time}_A(G_1^\pi, G_2^\sigma)]\right)$, где time — медианное время.

# Эвристические системы доказательств и аксепторы

Пусть $D$ — распределение на нетеоремах (т.е. на $\overline{L}$);
$D_n$ — распределение на $\overline{L} \cap \{0,1\}^n$.

## Определение

Эвр. система док-в для $(L, D)$ — это полиномиальный алгоритм $\Pi$, т.ч.

(полнота) $\forall f \in L\ \forall d \in \mathbb{N}\ \exists w \quad \Pr\{\Pi(f, w, d) = 1\} > \frac{1}{2}$.

(Такое $w$ — $\Pi$-доказательство.)

(корректность) $D\left\{g \colon \exists w\ \Pr\{\Pi(g, w, d) = 1\} > \frac{1}{4}\right\} < \frac{1}{d}$.

## Определение

Эвр. аксептор $A$ для $(L, D)$:

(полнота) $\forall f \in L\ \forall d \in \mathbb{N} \quad A(f, d) = 1$.

(корректность) $D\left\{g \colon \Pr\{A(g, d) = 1\} > \frac{1}{4}\right\} < \frac{1}{d}$.

Если $A(g, d) \neq 1$, он зацикливается.

# Оптимальный эвристический аксептор

## Определение

$A$ — оптимальный эвр. аксептор для $L \iff \forall A'$ имеются полиномы $p$,$q$, т.ч. $\forall f \in L \qquad \mathrm{time}_A(f, d) \leq \max_{d' \leq q(f,d)} p(\mathrm{time}_{A'}(f, d') + |f| + d)$.

Пусть $D$ — polynomial-time samplable.

Оптимальный эвр. аксептор $U(x, d)$:

- Параллельно для всех $i \leq n$:
  1. Запустить $A_i(x, d')$; пусть его время $T_i$.
  2. Проверить корректность $A_i$:
     повторить много раз
     - $r \leftarrow D_n$,
     - если $A_i(r, d') = 1$ за $T_i$ шагов слишком часто, поставить крестик;

     и убедиться, что крестиков мало.
  3. Ответить “1”.