

Сложность пропозициональных доказательств

Эдуард Алексеевич Гирш

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

ПОМИ РАН

7 октября 2010 г.

Непересекающиеся NP-пары

- ▶ Пара (A, B) множеств $A, B \in \mathbf{NP}$ т.ч. $A \cap B = \emptyset$.
- ▶ Задача — **разделить** A и B :
по x решить, что верно: $x \in A$ или $x \in B$
(если ни то, ни другое, ответить что угодно).

Непересекающиеся NP-пары

- ▶ Пара (A, B) множеств $A, B \in \mathbf{NP}$ т.ч. $A \cap B = \emptyset$.
- ▶ Задача — **разделить** A и B :
по x решить, что верно: $x \in A$ или $x \in B$
(если ни то, ни другое, ответить что угодно).
- ▶ Если $A = \overline{B}$, это вопрос о языке из $\mathbf{NP} \cap \mathbf{co-NP}$.

Непересекающиеся NP-пары

- ▶ Пара (A, B) множеств $A, B \in \mathbf{NP}$ т.ч. $A \cap B = \emptyset$.
- ▶ Задача — **разделить** A и B :
по x решить, что верно: $x \in A$ или $x \in B$
(если ни то, ни другое, ответить что угодно).
- ▶ Если $A = \overline{B}$, это вопрос о языке из $\mathbf{NP} \cap \mathbf{co-NP}$.
- ▶ Сведение $(A, B) \rightarrow (C, D)$:
полиномиально вычислимая f , т.ч. $f(A) \subseteq C$, $f(B) \subseteq D$.
- ▶ \exists полные пары?..

Непересекающиеся NP-пары

- ▶ Пара (A, B) множеств $A, B \in \mathbf{NP}$ т.ч. $A \cap B = \emptyset$.
- ▶ Задача — **разделить** A и B :
по x решить, что верно: $x \in A$ или $x \in B$
(если ни то, ни другое, ответить что угодно).
- ▶ Если $A = \overline{B}$, это вопрос о языке из $\mathbf{NP} \cap \mathbf{co-NP}$.
- ▶ Сведение $(A, B) \rightarrow (C, D)$:
полиномиально вычислимая f , т.ч. $f(A) \subseteq C$, $f(B) \subseteq D$.
- ▶ \exists полные пары?..
- ▶ \exists полная $\implies \exists$ полная (A, B) с **NP**-полными A, B .

Откуда берутся NP-пары

Пример (NP-пара криптосистемы)

$A = \{\text{коды } 0\},$

$B = \{\text{коды } 1\}.$

Не должна быть разделима за полиномиальное время!

Откуда берутся NP-пары

Пример (NP-пара криптосистемы)

$$A = \{\text{коды } 0\},$$

$$B = \{\text{коды } 1\}.$$

Не должна быть разделима за полиномиальное время!

Пример (Каноническая NP-пара...)

... для системы док-в Π для $\overline{\text{SAT}}$.

$$\text{SAT}_* = \{(F, 1^t) \mid F \in \text{SAT}\},$$

$$\text{REF}_\Pi = \{(F, 1^t) \mid F \in \overline{\text{SAT}}, \exists \Pi\text{-док-во размера } \leq t \text{ для } F\}.$$

Откуда берутся NP-пары

Пример (NP-пара криптосистемы)

$A = \{\text{коды } 0\},$

$B = \{\text{коды } 1\}.$

Не должна быть разделима за полиномиальное время!

Пример (Каноническая NP-пара...)

... для системы док-в Π для $\overline{\text{SAT}}$.

$\text{SAT}_* = \{(F, 1^t) \mid F \in \text{SAT}\},$

$\text{REF}_\Pi = \{(F, 1^t) \mid F \in \overline{\text{SAT}}, \exists \Pi\text{-док-во размера } \leq t \text{ для } F\}.$

Разделимость — слабая автоматизируемость!

Определение

Π **автоматизируема**, если док-ва можно найти за полиномиальное время от длины кратчайшего.

Π **слабо автоматизируема**, если Π' автоматизируема, где $\Pi' \leq \Pi$.

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Моделирование систем vs сводимость **NP**-пар

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая **NP**-пара опт. системы док-в — полная.

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая NP-пара опт. системы док-в — полная.

- ▶ Рассмотрим $(F, 1^t) \in \text{REF}_W$.
- ▶ Надо из $(F, 1^t)$, т.е. “есть Π_1 -док-во размера $\leq t$ ” сделать $(F, 1^s)$, т.е. “есть Π_2 -док-во размера $\leq s$ ”.

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая NP-пара опт. системы док-в — полная.

- ▶ Рассмотрим $(F, 1^t) \in \text{REF}_W$.
- ▶ Надо из $(F, 1^t)$, т.е. “есть Π_1 -док-во размера $\leq t$ ” сделать $(F, 1^s)$, т.е. “есть Π_2 -док-во размера $\leq s$ ”.
- ▶ $S \leq W \implies s$ полиномиально от t .
Этот полином p и используем: $(F, 1^t) \rightarrow (F, 1^{p(t)})$.

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая NP-пара опт. системы док-в — полная.

- ▶ Рассмотрим $(F, 1^t) \in \text{REF}_W$.
- ▶ Надо из $(F, 1^t)$, т.е. “есть Π_1 -док-во размера $\leq t$ ” сделать $(F, 1^s)$, т.е. “есть Π_2 -док-во размера $\leq s$ ”.
- ▶ $S \leq W \implies s$ полиномиально от t .
Этот полином p и используем: $(F, 1^t) \rightarrow (F, 1^{p(t)})$.
- ▶ Для $(F, 1^t) \in \text{SAT}_*$ изменения в 1^{\dots} несущественны.

Моделирование систем vs сводимость NP-пар

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая NP-пара опт. системы док-в — полная.

- ▶ Рассмотрим $(F, 1^t) \in \text{REF}_W$.
- ▶ Надо из $(F, 1^t)$, т.е. “есть Π_1 -док-во размера $\leq t$ ” сделать $(F, 1^s)$, т.е. “есть Π_2 -док-во размера $\leq s$ ”.
- ▶ $S \leq W \implies s$ полиномиально от t .
Этот полином p и используем: $(F, 1^t) \rightarrow (F, 1^{p(t)})$.
- ▶ Для $(F, 1^t) \in \text{SAT}_*$ изменения в 1^{\dots} несущественны.

Замечание

Обратной импликации нет (контрпример!).

Моделирование систем vs сводимость NP-пар

Теорема

$$S \leq W \implies (\text{SAT}_*, \text{REF}_W) \rightarrow (\text{SAT}_*, \text{REF}_S).$$

Каноническая NP-пара опт. системы док-в — полная.

- ▶ Рассмотрим $(F, 1^t) \in \text{REF}_W$.
- ▶ Надо из $(F, 1^t)$, т.е. “есть Π_1 -док-во размера $\leq t$ ” сделать $(F, 1^s)$, т.е. “есть Π_2 -док-во размера $\leq s$ ”.
- ▶ $S \leq W \implies s$ полиномиально от t .
Этот полином p и используем: $(F, 1^t) \rightarrow (F, 1^{p(t)})$.
- ▶ Для $(F, 1^t) \in \text{SAT}_*$ изменения в 1^{\dots} несущественны.

Замечание

Обратной импликации нет (контрпример!).

$$\text{CP}^2 = \text{CP} + \{a_{x,y} = x \wedge y \mid \text{для каждой пары старых переменных } x, y\}$$

Тавтологии о раскраске графа с кликой

В G нет n -клики $\vee G$ не раскрашиваем в $n - 1$ цвет,

Тавтологии о раскраске графа с кликой

В G нет n -клики $\vee G$ не раскрашиваем в $n - 1$ цвет,

т.е. \exists двух гомоморфизмов $K_n \xrightarrow{q} G \xrightarrow{r} K_{n-1}$.

Тавтологии о раскраске графа с кликой

В G нет n -клики $\vee G$ не раскрашиваем в $n - 1$ цвет,

т.е. \nexists двух гомоморфизмов $K_n \xrightarrow{q} G \xrightarrow{r} K_{n-1}$.

$G = (V, E)$, $|V| = m$, $p_{ij} \equiv (\{i, j\} \in E)$.

▶ Каждая вершина клики отправлена в граф: $\sum_{i=1}^n q_{ki} \geq 1$.

▶ ... на своё персональное место: $\sum_{k=1}^m q_{ki} \leq 1$.

▶ ... и только на одно: $\sum_{i=1}^n q_{ki} \leq 1$.

▶ Между двумя вершинами клики есть ребро:

$$q_{ki} + q_{k',j} \leq p_{ij} + 1 \quad (k \neq k', i < j).$$

▶ Каждая вершина покрашена: $\sum_{\ell=1}^{m-1} r_{i\ell} \geq 1$.

▶ Корректность раскраски: $p_{ij} + r_{i\ell} + r_{j\ell} \leq 2 \quad (i < j)$.

Тавтологии о раскраске графа с кликой

В G нет n -клики $\vee G$ не раскрашиваем в $n - 1$ цвет,

т.е. \exists двух гомоморфизмов $K_n \xrightarrow{q} G \xrightarrow{r} K_{n-1}$.

$G = (V, E)$, $|V| = m$, $p_{ij} \equiv (\{i, j\} \in E)$.

▶ Каждая вершина клики отправлена в граф: $\sum_{i=1}^n q_{ki} \geq 1$.

▶ ... на своё персональное место: $\sum_{k=1}^m q_{ki} \leq 1$.

▶ ... и только на одно: $\sum_{i=1}^n q_{ki} \leq 1$.

▶ Между двумя вершинами клики есть ребро:

$$q_{ki} + q_{k',j} \leq p_{ij} + 1 \quad (k \neq k', i < j).$$

▶ Каждая вершина покрашена: $\sum_{\ell=1}^{m-1} r_{i\ell} \geq 1$.

▶ Корректность раскраски: $p_{ij} + r_{i\ell} + r_{j\ell} \leq 2 \quad (i < j)$.

Композиция q и r — принцип Дирихле!

Интерполяционная теорема (Craig)

Пропозициональный случай

Теорема

Если $A(\vec{x}, \vec{y}) \supset B(\vec{x}, \vec{z})$, то можно построить $C(\vec{x})$, т.ч.
 $A(\vec{x}, \vec{y}) \supset C(\vec{x})$ и $C(\vec{x}) \supset B(\vec{x}, \vec{z})$.

Размер C в общем случае экспоненциален!

Интерполяционная NP пара

Определение

$$I_b = \{(F_0, F_1, \pi) \mid \text{Vars}(F_0) \cap \text{Vars}(F_1) = \emptyset, \Pi(F_0 \vee F_1, \pi) = 1, F_b \notin \text{TAUT}\}.$$

Можно ли полиномиально разделить (I_0, I_1) ?

Определение

$$I_b = \{(F_0, F_1, \pi) \mid \text{Vars}(F_0) \cap \text{Vars}(F_1) = \emptyset, \Pi(F_0 \vee F_1, \pi) = 1, \\ F_b \notin \text{TAUT}\}.$$

Можно ли полиномиально разделить (I_0, I_1) ?

Можно ли по док-ву $G_0(\vec{x}, \vec{y}) \vee G_1(\vec{x}, \vec{z})$ построить схему $C: G_C(\vec{x}) \in \text{TAUT}$?

Интерполяционная NP пара

Определение

$$I_b = \{(F_0, F_1, \pi) \mid \text{Vars}(F_0) \cap \text{Vars}(F_1) = \emptyset, \Pi(F_0 \vee F_1, \pi) = 1, \\ F_b \notin \text{TAUT}\}.$$

Можно ли полиномиально разделить (I_0, I_1) ?

Можно ли по док-ву $G_0(\vec{x}, \vec{y}) \vee G_1(\vec{x}, \vec{z})$ построить схему C : $G_C(\vec{x}) \in \text{TAUT}$?

Определение

Reflection property: полиномиальные доказательства для

$$\Pi(F, \pi) \neq 1 \quad \vee \quad F[A] \neq 1,$$

где формула F , док-во π , набор A заданы векторами булевых переменных нужной длины.

Reflection $\implies (I_0, I_1) \sim (\text{SAT}_*, \text{REF}_\Pi)$.