Релятивизуемые и нерелятивизуемые теоремы полиномиальной теории алгоритмов

Н.К. Верещагин

Начиная с работы Бейкера, Гилла и Соловея [5] в теории вычислительной сложности был доказан ряд результатов, состоящих в отделении различных релятивизованных классов сложности или несуществовании в таких классах полных языков. При этом все результаты такого сорта по существу были основаны на получении нижних оценок для разрешающих деревьев специального вида или машин с полилогарифмическим ограничением на время работы. Возникает вопрос: являются ли эти методы доказательства "релятивизованных" результатов универсальными? Первая часть настоящей работы как раз и состоит в том, что предлагается общая модель, в которой утверждения об универсальности такого рода можно сформулировать и доказать в виде удобных критериев. Эти критерии позволяют получить в качестве простых следствий некоторых известных результатов о булевских разрешающих деревьях некоторые новые "релятивизованные" результаты, а также новые доказательства некоторых старых результатов. Вторая часть работы состоит в применении найденных общих критериев к большому числу частных случаев. Например, для большого числа ранее изучавшихзся в литературе классов полностью описаны все релятивизуемые включения между этими классами.

1. Введение

Большинство теорем общей теории алгоритмов, как известно, релятивизуется. Это значит, что для любого языка A теорема останется верной, если в качестве модели вычисления взять машину Тьюринга с оракулом A. В полиномиальной теории алгоритмов это не так. В 1975 году в работе [5] были построены такие оракулы A, B, что $\mathbf{P}^A \neq \mathbf{NP}^A$, $\mathbf{P}^B = \mathbf{NP}^B$. Хотя до сих пор неизвестно, какое из двух утверждений $\mathbf{P} \neq \mathbf{NP}$, $\mathbf{P} = \mathbf{NP}$ истинно, ни то ни другое утверждение не релятивизуется. После работы [5] было получено много результатов следующего вида: для некоторых пар сложностных классов, зависящих от оракула C, K_1^C, K_2^C, доказывалось, что существуют оракулы A и B, для которых $K_1^A \neq K_2^A$, $K_1^B = K_2^B$. Многие интересные классы лежат между $\mathbf{P}$ и $\mathbf{PSPACE}$, для таких классов в качестве второго

оракула можно всегда брать оракул B из [5], потому что для него на самом деле верно $\mathbf{P}^B = \mathbf{PSPACE}^B$.

В 1989 году впервые появились нерелятивизуемые теоремы, первая из них — теорема из работы [18]: $\mathbf{PH} \subseteq \mathbf{IP}$. Как было доказано ранее в работе [8], $\exists A\ \mathbf{Co\text{-}NP}^A \not\subseteq \mathbf{IP}^A$.

Все известные доказательства результатов типа $\exists A\ K_1^A \neq K_2^A$ (фактически доказывается $\exists A\ K_1^A \not\subseteq K_2^A$ или наоборот) устроены следующим образом: имеется общая "диагональная" часть — построение оракула по шагам — и специфическая комбинаторная часть, обеспечивающая возможность выполнения каждого шага. Первый результат данной работы — формализация этого разделения: теорема 3.1 из параграфа 3 заключает в себе общую диагональную часть всех таких доказательств. В этой же теореме указано какое специфическое комбинаторное утверждение нужно доказывать в каждом конкретном случае.

В литературе появлялись также теоремы типа: "существует оракул A, для которого класс K^A не содержит полной по Карпу (или по Куку) проблемы". Первой известной автору работой такого типа является работа [23], в которой доказано, что существует оракул A, для которого $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ не имеет полной по Карпу (т.е. относительно A-полиномиальной m-сводимости) проблемы и такой оракул A, для которого R^A не имеет полной по Карпу проблемы.

Все вышесказанное о доказательствах типа $\exists A\ K_1^A \not\subseteq K_2^A$ относится и к доказательствам отсутствия полных проблем. В параграфе 4 доказывается теорема 4.1, заключающая в себе диагональную часть таких доказательств.

Как теорема 3.1, так и теорема 4.1, являются критериями: теорема 3.1 — того, что

$$\forall A\ K_1^A \subseteq K_2^A, \tag{1}$$

теорема 2 — того, что

$$\forall A\ (K_2^A \text{ имеет полную по Карпу проблему для } K_1^A). \tag{2}$$

Неформально, критерии состоят в следующем. Пусть K — некоторый сложностной класс. Обозначим через KLOGS "напарник" класса K, полученный заменой всех полиномов, входящих в определение K, на полиномы от логарифма и заменой проблем разрешения (т.е. языков) на проблемы отделения. Тогда (1) эквивалентно абсолютному включению $K_1\text{LOGS} \subseteq K_2\text{LOGS}$, а (2) истинно тогда и только тогда, когда K_2LOGS содержит язык полный для K_1LOGS. Анализ доказательств релятивизуемых утверждений типа (1) (например, $\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2$ из [24]) показывает, что более естественная формулировка этих утверждений имеет как раз вид $K_1\text{LOGS} \subseteq K_2\text{LOGS}$.

Аналогичные критерии существуют и для теорем еще двух видов

$$\forall A\ (K_2^A \text{ содержит полную по Куку проблему для } K_1^A), \tag{3}$$

$$\forall A\ (\forall L_1 \in K_1^A \exists L_2 \in K_2^A : L_1 \text{ сводится по Куку к } L_2), \tag{4}$$

т.е., «K_1^A сводится по Куку к K_2^A».

Эти критерии сформулированы и доказаны в параграфах 5, 6.

Новый взгляд на релятивизуемые теоремы четырех указанных видов делает психологически и технически более простым решение конкретных проблем типа (1)–(4).

В параграфах 7, 8 и 9 для многих известных из литературы классов K_1, K_2 между **P** и **PSPACE**, к которым применимы критерии параграфов 3–6, выясняется, какое из двух утверждений — (1) или отрицание (1) — имеет место, или это неизвестно, и аналогично для утверждений типа (2), (3), (4). При этом получены некоторые новые положительные и отрицательные результаты этого типа (положительными результатами мы называем утверждения типа (1)–(4)). Некоторое количество проблем этого типа остаются открытыми.

2. Основные определения и обозначения

Множество всех слов в алфавите Σ будем обозначать Σ^*. Через $\mathbf{B}$ обозначим $\{0,1\}$.

Проблемой отделения будем называть произвольную функцию из $\mathbf{B}^*$ в множество $\{0,1,*\}$. Содержательно, проблема отделения F состоит в том, что требуется отделить множество $\{x \mid F(x)=1\}$ от множества $\{x \mid F(x)=0\}$. Через $D(F)$ обозначим множество $\{x \in \mathbf{B}^* \mid F(x) \neq *\}$.

Язык $L \subseteq \mathbf{B}^*$ будем отождествлять с его характеристической функцией, обозначаемой той же буквой

$$L(x) = \begin{cases} 1 & \text{при } x \in L \\ 0 & \text{при } x \notin L. \end{cases}$$

Таким образом, любой язык — это проблема отделения.

Длину слова x обозначим $|x|$.

Через $\log n$ обозначим функцию $\lceil \log_2 n \rceil$ и положим $\log(0)=0$. Функции вида $p(\log n)$, где p — некоторый полином, будем называть полилогарифмами. Выражения $\mathrm{poly}(n)$, $\mathrm{polylog}(n)$ будут означать некоторый полином и, соответственно, полилогарифм от n.

Мы будем изучать сложностные классы, определяемые машинами Тьюринга, время работы которых ограничено полилогарифмом от длины входа. Поскольку обычная машина Тьюринга за полилогарифмическое время может прочитать только начало исходного слова полилогарифмической длины, мы, будем применять модель, которая обычно используется при сильных ограничениях на время. Исходное данное в этой модели дается машине как оракул, точнее, машина кроме рабочей ленты имеет еще одну ленту (будем называть ее входной), на которой сначала записана длина исходного слова x.[1]

[1] Если не указано противное, будем всегда считать, что натуральные числа даются

Машина в любой момент вычисления может «задать вопрос вида '$x(i) =$?'», т.е. может записать на входной ленте число $i \leq |x|$ и в ответ получает на этой ленте i-ый символ x — $x(i)$. Время записи i входит в общее время работы, время записи $x(i)$ считается равным 1. (Эквивалентная с точностью до увеличения времени на polylog($|x|$) модель получится, если машина не знает $|x|$ и на вопрос '$x(i) =$?' с $i > |x|$ получает ответ «?».) Если ограничение на время полиномиально, то разница между новой и старой моделью пропадает. Через $M(x)$ будем обозначать результат работы M на исходном слове x.

Наша ближайшая цель — дать определение полилогарифмического напарника сложностного класса. Сначала, в качестве примера, мы определим полилогарифмические напарники трех известных сложностных классов **P**, **NP**, **R**, а затем дадим определение полилогарифмического напарника в общем виде. Полилогарифмический напарник — это некоторый класс проблем отделения. Если K — это обозначение некоторого сложностного класса, принятое в литературе, то полилогарифмический напарник класса K мы будем обозначать через KLOGS, например, **PLOGS**, **NPLOGS**, **RLOGS**.

Итак, пусть F — проблема отделения. Тогда по определению $F \in$ **PLOGS**, если если существует детерминированная машина Тьюринга, работающая время, ограниченное полилогарифмом от длины входа такая, что для всех $\alpha \in D(F)$ выполнено $M(\alpha) = F(\alpha)$.

Полилогарифмической недетерминированной машиной назовем недетерминированную машину Тьюринга, время работы которой на всех возможных путях вычисления на входе α ограничено polylog($|\alpha|$). По определению $F \in$ **NPLOGS**, если существует полилогарифмическая недетерминированная машина M, такая, что если $F(\alpha) = 1$, то существует допускающее вычисление M на α, а если $F(\alpha) = 0$, то не существует допускающего вычисления M на α.

Вероятностной полилогарифмической машиной называется вероятностная машина Тьюринга M, время вычисления которой на входе α при всех значениях случайного датчика не превосходит polylog($|\alpha|$). По определению $F \in$ **RLOGS**, если существует полилогарифмическая вероятностная машина M такая, что если $F(\alpha) = 1$, то Prob$[M(\alpha) = 1] > \frac{2}{3}$, и если $F(\alpha) = 0$, то Prob$[M(\alpha) = 1] = 0$ (если $F(\alpha) = *$, то вероятность может быть любой).

Перейдем к формализации понятия полилогарифмического напарника. Для этого нам понадобится фиксировать некоторую общую схему, по которой определяется большинство сложностных классов между **P** и **PSPACE**.

С этой целью рассмотрим определения двух конкретных сложностных классов **NP** и **BPP** в удобном для нас виде.

2.1. $L \in$ **NP** $\Longleftrightarrow$ существуют полиномиально вычислимая функция s :

машине и выдаются машиной в двоичной записи. И вообще мы отождествим натуральные числа с двоичными словами: натуральное число n отождествим с двоичной записью числа $n + 1$ без старшей единицы.

$\mathbf{B}^* \to \mathbf{N}$ и полиномиальный предикат $P(x,i)$ такие, что $x \in L \Leftrightarrow \exists i \le s(x) : P(x,i)$,

2.2. $L \in \mathbf{BPP} \Longleftrightarrow$ существуют такая полиномиально вычислимая функция $s : \mathbf{B}^* \to \mathbf{N}$ и такой полиномиальный предикат $P(x,i)$, что если $x \in L$, то частное $\frac{|\{i \in \mathbf{N}(1 \le i \le |x|, P(x,i)\}|}{s(x)}$ больше $\frac{2}{3}$, а если $x \notin L$, то это частное меньше $\frac{1}{3}$.

Если в обоих определениях обозначить через $f(x)$ последовательность значений предиката $P(x,i)$ при $i \le s(x)$, то в обоих определениях принадлежность x к L определяется через некоторое свойство слова $f(x)$, причем любой символ слова $f(x)$ можно вычислить за полиномиальное от $|x|$ время. Это обстоятельство приводит нас к следующим определениям.

Пусть f функция из $\mathbf{B}^*$ в $\mathbf{B}^*$, а $t : \mathbf{N} \to \mathbf{N}$.

Определение 2.1. Функция f слабовычислима за время t, если

1) функция $x \mapsto |f(x)|$ вычислима за время $t(|x|)$.

2)двухместный частичный предикат $P(x,i) =$ ($i-$ый бит слова $f(x)$) вычисляется некоторой машиной M, которая при всех $x \in \mathbf{B}^*$ и всех $i \le |f(x)|$ работает время, не превосходящее $t(|x|)$.

Функции, слабовычислимые за время $\mathrm{poly}(n)$, $\mathrm{polylog}(n)$, $2^{O(n)}$ будем называть соответственно слабополиномиальными, слабополилогарифмическими, слабоэкспоненциальными. Слабополиномиальной будет, например, функция $f(x) = 0^{2^{|x|}}$ (через 0^n обозначаем подряд n нулей), а слабополилогарифмической — например, функция $f(x) = x$.

Оба определения 2.1, 2.2 имеют следующий вид. Фиксируется некоторая проблема отделения F и объявляется, что язык L принадлежит классу, если существует слабополиномиальная функция f такая, что для всех $x \in \mathbf{B}^* L(x) = F(f(x))$. Обозначим определенный таким образом класс через $\mathrm{POLY}(F)$. Например, для класса $\mathbf{NP}$ в качестве F надо взять проблему отделения

$$F_{\mathbf{NP}}(\alpha) = \begin{cases} 1, & \text{если } \exists i \le |\alpha| \ \alpha(i) = 1, \\ 0, & \text{иначе,} \end{cases}$$

а для класса $\mathbf{BPP}$ в качестве F надо взять проблему отделения

$$F_{\mathbf{BPP}}(\alpha) = \begin{cases} 0, & \text{если } \#_1(\alpha) < \frac{1}{3}|\alpha|, \\ 1, & \text{если } \#_1|\alpha| > \frac{2}{3}|\alpha|, \\ *, & \text{иначе,} \end{cases}$$

где $\#_1(x)$ обозначает количество единиц в двоичном слове x.

Можно проверить, что классы $\mathbf{P}$, $\mathbf{NP}$, $\mathbf{R}$, $\mathbf{BPP}$, $\mathbf{UP}$, $\mathbf{FewP}$, Σ_k, $\oplus\mathbf{P}$, $\mathbf{PP}$, $\mathbf{PSPACE}$, $\mathbf{MA}$, $\mathbf{AM}$, $\mathbf{IP}$ (с открытыми бросаниями костей) имеют вид $\mathrm{POLY}(F)$.

Определим на множестве $\{0,1,*\}$ отношение частичного порядка $<$, положив $* < 0$, $* < 1$. Определим $\mathrm{LOGS}(F)$ как класс таких проблем отделения G , что для некоторой слабополигорафмической функции f выполнено

$\forall \alpha \in \mathbf{B}^* G(\alpha) \leq F(f(\alpha))$, а $\mathrm{LOG}(F)$ как класс всех языков из $\mathrm{LOGS}(F)$. Класс $\mathrm{LOGS}(F)$ и есть по определению полилогарифмический напарник класса $\mathrm{POLY}(F)$. Точнее, проблема отделения F задает сразу пару — класс $\mathrm{POLY}(F)$ и его полилогарифмический напарник $\mathrm{LOGS}(F)$ (как мы увидим в дальнейшем, класс $\mathrm{LOGS}(F)$ не определяется однозначно классом $\mathrm{POLY}(F)$).

Перейдем к релятивизованным классам. Оракулом называется произвольный язык. Машиной с оракулом называется машина Тьюринга, имеющая дополнительную ленту, называемую оракульной, на которой имеется читающе-записывающая головка. Будем считать, что эта головка может записывать только 0 и 1. Если машина приходит в некоторое выделенное состояние, то содержимое оракульной ленты от первой ячейки до той ячейки, где находится головка, воспринимается как вопрос к оракулу и на оракульной ленте за единицу времени появляется «ответ оракула»— 0 или 1 в той ячейке, где находится головка. Время записи вопроса входит в общее время. Пусть M машина с оракулом, а $A \subseteq \mathbf{B}^*$. Обозначим $M^A(x)$ результат работы M на x, а $t_{M^A}(x)$ — время работы M на x, если в качестве ответа оракула на вопрос z дается $A(z)$. Машина M называется полиномиальной (экспоненциальной), если существует полином q (соответственно константа c) такой, что для всех $x \in \mathbf{B}^*$ и всех $A \subseteq \mathbf{B}^*$ $t_{M^A}(x) \leq q(|x|)$ (соответственно, $t_{M^A}(x) \leq 2^{c|x|+c}$). Функция f называется полиномиальной (экспоненциальной) относительно A, если существует полиномиальная (соответственно, экспоненциальная) машина M с оракулом такая, что $\forall x\ f(x) = M^A(x)$ (т.е., M^A вычисляет f).

Пусть A некоторый оракул. Для того, чтобы дать общее определение релятивизованного оракулом A класса, связанного с проблемой отделения F — класса, который мы обозначим $\mathrm{POLY}^A(F)$ — определим понятие слабой вычислимости относительно оракула. Для этого в определении слабой вычислимости в пункте 2) заменим машину M на машину M с оракулом A, а в пункте 1) разрешим функции $|f(x)|$ быть вычислимой за время $t(|x|)$ на машине с оракулом A

Определение 2.2. $\mathrm{POLY}^A(F)$ — это класс таких языков L, что для некоторой слабополиномиальной относительно A функции f выполнено $\forall x \in \mathbf{B}^* L(x) = F(f(x))$.

3. Критерий релятивизуемого включения полиномиальных сложностных классов

Теорема этого параграфа утверждает, что полиномиальный сложностной класс языков K_1 включен в полиномиальный сложностной класс языков K_2 во всех релятивизованных мирах, если выполняется включение (абсолютное) их полилогарифмических напарников. Эта теорема верна для всех

классов вида $\mathrm{POLY}(F)$ при следующем ограничении на F.

Назовем проблему отделения F невырожденной, если выполнены условия

3.1. Существует слабополиномиальная функция $f : \mathbf{N} \to \mathbf{B}^*$ такая, что $|f(n)| = n$ и $F(f(n)) \neq *$ для всех $n \in \mathbf{N}$.

3.2. Существуют два слова, обозначим их $zero_F$, one_F, такие, что $F(zero_F) = 0$, $F(one_F) = 1$.

Заметим, что проблемы отделения, задающие все конкретные классы, перечисленные выше, невырождены.

Теорема 3.1. *Для невырожденных проблем отделения следующие условия эквивалентны*

3.3. $\mathrm{LOGS}(F) \subseteq \mathrm{LOGS}(G)$

3.4. $F \in \mathrm{LOGS}(G)$

3.5. *Для всех* $A \subseteq \mathbf{B}^*$ $\mathrm{POLY}^A(F) \subseteq \mathrm{POLY}^A(G)$

Если F — язык, то все условия эквивалентны условию

3.6. $\mathrm{LOG}(F) \subseteq \mathrm{LOG}(G)$.

Доказательство. Очевидно, что 3.3 $\Longrightarrow$ 3.4. Докажем, что 3.4$\Longrightarrow$3.3. Пусть $F \in \mathrm{LOGS}(G)$, $F(\alpha) \leq G(g(\alpha))$, где g — слабо-полилогарифмическая функция. Докажем, что $\mathrm{LOGS}(F) \subseteq \mathrm{LOGS}(G)$. Пусть $H \in \mathrm{LOGS}(F)$, $H(\alpha) \leq F(f(\alpha))$, где f — слабополилогарифмическая функция. Тогда $H(\alpha) \leq G(g(f(\alpha)))$. Нетрудно проверить, что $g(f(\alpha))$ слабополилогарифмическая функция, следовательно $H \in \mathrm{LOGS}(G)$.

Далее, из 3.3 очевидно следует 3.6, и, если F — язык, то из 3.6 следует 3.4.

Докажем, что из 3.4 следует 3.5. Пусть f такая слабополилогарифмическая функция, что $F(\alpha) \leq G(f(\alpha))$. Пусть $A \subseteq \mathbf{B}^*$ и $L \in \mathrm{POLY}^A(F)$. Тогда для некоторой слабополиномиальной относительно A функции g выполнено $L(x) = F(g(x))$. Значит $L(x) = G(f(g(x)))$. Легко проверить, что функция $f(g(x))$ слабополиномиальна относительно A. Следовательно, $L \in \mathrm{POLY}^A(G)$.

Докажем, что если 3.4 не выполнено, то и 3.5 не выполнено. Пусть $F \notin \mathrm{LOGS}(G)$. Значит, для любой проблемы отделения $H \in \mathrm{LOGS}(G)$ найдется такое $\alpha \in \mathbf{B}^*$, что $F(\alpha) \not\leq H(\alpha)$. Докажем, что, более того, существует бесконечно много $\alpha \in \mathbf{B}^*$, таких, что $F(\alpha) \not\leq H(\alpha)$. Допустим противное: существуют такое n и такая слабополилогарифмическая функция f, что для всех $\alpha \in \mathbf{B}^*$ из $|\alpha| > n$ следует $F(\alpha) \leq G(f(\alpha))$. Тогда функция

$$f_1(\alpha) = \begin{cases} f(\alpha), & \text{при } |\alpha| > n, \\ zero_G, & \text{при } |\alpha| \leq n,\ F(\alpha) = 0 \\ one_G, & \text{иначе.} \end{cases}$$

слабополилогарифмична и $F(\alpha) \leq G(f_1(\alpha))$ для всех $\alpha \in \mathbf{B}^*$.

Зафиксируем удобный способ кодирования пар слов. Пусть $x \in \mathbf{B}^*$. Обозначим $\bar{x}$ результат удвоения всех битов x и приписывания 01 в конце (например, $\overline{001} = 00001101$). Очевидно за полиномиальное время по слову $\bar{x}y$ можно найти x и y и по слову u выяснить имеет ли оно вид $\bar{x}y$. Обозначим для любого оракула A и любого $n \in \mathbf{N}$ через A_n слово длины n, i-ый бит которого равен $A(\bar{n}i)$ [2]

Мы определим оракул A так, чтобы язык $L^A = \{n | F(A_n) = 1\}$ принадлежал $\mathrm{POLY}^A(F) \setminus \mathrm{POLY}^A(G)$. Чтобы обеспечить $L^A \in \mathrm{POLY}^A(F)$ мы добьемся, чтобы было выполнено условие (глобальное)

(G) $\quad \forall n \in \mathbf{N}\ F(A_n) \neq *$.

Тогда $L^A(n) = F(A_n)$ для всех n и поскольку функция $h(n) = A_n$ слабополиномиальна относительно A мы получим $L^A \in \mathrm{POLY}^A(F)$.

Перенумеруем все слабо полиномиальные относительно оракула функции. Это означает, что нумеруются все пары машин, входящих в определение 2. Обозначим i-ую функцию через $f_i^A(x)$ (оракул A является вторым аргументом функции). Возьмем такой полиномиально разрешимый язык E, что $F(E_n) \neq *$ для всех $n \in \mathbf{N}$. Такой язык существует в силу невырожденности F. Сначала положим $A = E$, удовлетворив тем самым требование (G). Затем мы выполним счетное число шагов $i = 1, 2, \ldots$. На i-ом шаге мы изменим A на конечном множестве слов так, чтобы стало выполнено требование (локальное)

(L_i) $\quad \exists n \in \mathbf{N}\ F(A_n) \neq G(f_i^A(n))$,

и при этом не испортим свойства (G).

В конце i-го шага мы зафиксируем все слова, обеспечивающие выполнение (L_i), и все слова, на которых оракул был изменен. На более поздних шагах мы не будем менять значение A на зафиксированных словах. Таким образом, после выполнения счетного числа шагов, будет корректно определен некоторый оракул A, для которого выполнены условия (G) и (L_i), $i \in \mathbf{N}$. Для этого оракула A, очевидно, будет выполнено $L^A \in \mathrm{POLY}^A(F) \setminus \mathrm{POLY}^A(G)$.

Теперь опишем шаг i. Пусть A — оракул, построенный к этому шагу (с некоторым конечным множеством зафиксированных слов). Пусть $\alpha \in \mathbf{B}^*$ и $|\alpha| = n$. Обозначим $A[\alpha]$ оракул, полученный из A заменой A_n на α, т.е.

$$A[\alpha](u) = \begin{cases} A(u), & \text{если } u \text{ не имеет вида } \bar{n}i,\ i \leq n, \\ \alpha(i), & \text{если } u = \bar{n}i, \text{ где } i \leq n. \end{cases}$$

Положим $H(\alpha) = G(f_i^{A[\alpha]}(|\alpha|))$.

Поскольку A полиномиально разрешим (т.к. A получен из E конечным изменением), функция $\alpha \mapsto f_i^{A[\alpha]}(|\alpha|)$ слабополилогарифмическая, а значит $H \in \mathrm{LOGS}(G)$. Следовательно, существует бесконечно много $\alpha \in \mathbf{B}^*$, для

[2] Напомним, что мы отождествляем натуральные числа и слова в алфавите $\mathbf{B}$.

которых $F(\alpha) \not\leq H(\alpha)$. Значит, существует такое $\alpha \in \mathbf{B}^*$, что $F(\alpha) \not\leq H(\alpha)$ и ни одно из слов вида $\overline{|\alpha|}i$, $i \leq |\alpha|$ не зафиксировано. Выберем одно такое слово α и заменим A на $A[\alpha]$. Тем самым будет выполнено (L_i) при $n = |\alpha|$, поскольку $F(A_n) = F(\alpha) \not\leq H(\alpha) = G(f_i^A(n))$.

Слово $f_i^A(n)$ зависит лишь от значения A на некотором конечном множестве. Зафиксируем все слова этого множества и все слова вида $\bar{n}i$, $i \leq n$. Требование (G) не нарушено, поскольку $F(A_n) = F(\alpha_0)$ и $F(\alpha_0) \neq *$ (т.к. $F(\alpha_0) \not\leq H(\alpha_0)$, а $*$ - наименьший элемент в $\{0, 1, *\}$). Импликация 3.5$\Longrightarrow$ 3.4 доказана. Теорема доказана. □

Замечание 3.0. Для всех сложностных классов вида $\mathrm{POLY}(F)$, известных из литературы, в качестве функции f в определении класса $\mathrm{POLY}(F)$ достаточно рассматривать такие слабополиномиальные функции, что $|f(x)| = 2^{\mathrm{poly}(|x|)}$ (т.е. при таком ограничении объем класса $\mathrm{POLY}(F)$ не изменится). Более того, для всех этих классов определяющая класс проблема отделения F обладает следующим свойством ($*$). Определим проблему отделения $\bar{F}$ равенством

$$\bar{F}(\alpha) = \begin{cases} F(\alpha), & \text{если } |\alpha| \text{ имеет вид } 2^k,\ k \in \mathbf{N} \\ *, & \text{иначе.} \end{cases}$$

Свойство ($*$) состоит в том, что $F \in \mathrm{LOGS}(\bar{F})$ (и, следовательно, по теореме 3.1 $\mathrm{POLY}^A(\bar{F}) = \mathrm{POLY}^A(F)$ для всех A).

Если проблема отделения F, обладает этим свойством, то условия 3.3, 3.4, 3.5 эквивалентны условию

3.7. $\mathrm{EXP}^A(F) \subseteq \mathrm{EXP}^A(G)$ для всех A,

где $\mathrm{EXP}^A(H)$ — это по определению класс всех таких языков L, что $L(x) = H(g(x))$ для некоторой слабоэкспоненциальной относительно A функции g.

Действительно, 3.4$\Longrightarrow$ 3.7, поскольку, если $f(\alpha)$ — слабополилогарифмическая функция, а $g(x)$ — слабоэкспоненциальная относительно A функция, то $f(g(x))$ тоже слабоэкспоненциальная относительно A функция (т.к. $\mathrm{polylog}(2^{2^{O(n)}}) = 2^{O(n)}$. Обратно, докажем 3.7$\Longrightarrow$ 3.4. Ясно, что, если F удовлетворяет условию ($*$) и не удовлетворяет условию 3.4, то $\bar{F} \notin \mathrm{LOGS}(G)$. Поэтому, повторив рассуждение из доказательства импликации 3.4$\Longrightarrow$3.5, можно построить такой оракул A, что язык $L^A = \{n \mid F(A_{2^n}) = 1\}$ принадлежит $\mathrm{EXP}^A(F) \setminus \mathrm{EXP}^A(G)$.

Отображение, сопоставляющее оракулу A класс $\mathrm{POLY}^A(F)$, назовем многообразием, порожденным F. Вообще, любое отображение, сопоставляющее каждому оракулу $A \subseteq \mathbf{B}^*$ класс языков, назовем многообразием. Для семейства проблем отделения $\mathcal{F}$ определим многообразие $\mathrm{POLY}^A(\mathcal{F}) = \bigcup_{F \in \mathcal{F}} \mathrm{POLY}^A(F)$. Положим $\mathrm{LOGS}(\mathcal{F}) = \bigcup_{F \in \mathcal{F}} \mathrm{LOGS}(F)$.

Легко видеть, что теорема 3.1 обобщается на семейства проблем отделения.

Следствие 3.2. *Если семейства $\mathcal{F}$, $\mathcal{G}$ состоят из невырожденных проблем отделения, то условия*

3.8. $\mathrm{LOGS}(\mathcal{F}) \subseteq \mathrm{LOGS}(\mathcal{G})$

3.9. $\mathrm{POLY}^A(\mathcal{F}) \subseteq \mathrm{POLY}^A(\mathcal{G})$ *для всех* A.

эквивалентны.

Многообразия вида $\mathrm{POLY}^A(\mathcal{F})$, где $\mathcal{F}$ — семейство невырожденных проблем отделения, назовем порождаемыми, а если $\mathcal{F}$ одноэлементно, то однопорождаемыми.

Следствие 3.2, в частности, означает, что по порождаемому многообразию порождающее семейство восстанавливается однозначно с точностью до слабополилогарифмической эквивалентности:

$$(\forall A\ \mathrm{POLY}^A(\mathcal{F}) = \mathrm{POLY}^A(\mathcal{G})) \leftrightarrow \mathrm{LOGS}(\mathcal{F}) = \mathrm{LOGS}(\mathcal{G}).$$

Для абсолютных классов это не так: существуют проблемы отделения F_1 и F_2 такие, что $\mathrm{POLY}(F_1) = \mathrm{POLY}(F_2)$ и $\mathrm{LOGS}(F_1) \neq \mathrm{LOGS}(F_2)$. Другими словами, существует нерелятивизуемое утверждение вида $\mathrm{POLY}(F_1) = \mathrm{POLY}(F_2)$, а именно $\mathbf{IP} = \mathbf{PSPACE}$ (результат [18, 22]). Оба класса могут быть определены по нашей схеме, что будет показано в параграфе 7.

Рассмотрим один пример применения теоремы 3.1, восходящий, по существу, к работе [5]. Требуется доказать, что $\exists A\ \mathbf{P}^A \neq \mathbf{NP}^A$. Для этого достаточно доказать, что $F_{\mathbf{NP}} \notin \mathbf{PLOG}$. То есть, за полилогарифмическое от $|\alpha|$ время нельзя выяснить, есть ли в α хотя бы одна единица. Допустим, существует полилогарифмическая машина M, распознающая наличие 1. Запустим M на слове из одних нулей длины n, большей, чем время работы M на словах длины n. Такое n существует поскольку $n - \mathrm{polylog}(n) \to +\infty$. Машина должна выдать 0. Но поскольку M спросила не все биты α, можно обмануть ее, изменив неспрошенный бит на 1.

В этом рассуждении используется только то, что машина может спросить полилогарифмическое от $|\alpha|$ количество битов α, время же работы M может быть любым. Именно это обстоятельство делает возможным получать отрицательные оракульные результаты типа $\exists A\ K_1^A \not\subseteq K_2^A$. То есть, если в определении полилогарифмической машины ограничить только количество спрошенных битов и полученный таким образом из $\mathrm{LOGS}(G)$ класс обозначить $\mathrm{n.u.LOGS}(G)$, то для доказательства $\exists A\ \mathrm{POLY}^A(F) \not\subseteq \mathrm{POLY}^A(G)$ достаточно доказать $F \notin \mathrm{n.u.LOGS}(G)$, поскольку $\mathrm{n.u.LOGS}(G) \supseteq \mathrm{LOGS}(G)$. Рассуждения, связанные с количеством вопросов, являются обычно чисто комбинаторными.

Дадим формальное определение класса $\mathrm{n.u.LOGS}(F)$. Для этого введем новую модель вычислений, которую будем называть неравномерной.

Неравномерная модель определяется с помощью известных в литературе булевских разрешающих деревьев. Пусть $x_1, \ldots, x_n$ — булевские переменные, а M — некоторое множество.

Назовем $(M, x_1, \ldots, x_n)$-деревом конечное дерево с корнем и двоичным ветвлением, листья которого помечены элементами M, внутренние вершины помечены переменными из $\{x_1, \ldots, x_n\}$, и для каждой внутренней вершины одно ребро, исходящее из нее помечено единицей, а другое — нулем. $(M, x_1, \ldots, x_n)$-дерево T вычисляет функцию $f : \mathbf{B}^n \to M$ определяемую следующим образом. $f(x_1 \ldots x_n)$ равно пометке того листа, в который мы придем, если начиная с корня будем продвигаться вверх по ребру, помеченному значением той переменной, которой помечена вершина, в которой мы находимся. Будем эту функцию обозначать тем же символом, что и дерево, т.е. $f(x_1 \ldots x_n)$ обозначать $T(x_1 \ldots x_n)$. Сложность дерева будет определяться его высотой.

Скажем, что частичная функция $f : \mathbf{B}^n \to M$ вычислима за t вопросов, если существует $(M, x_1, \ldots, x_n)$-дерево T высоты $\leq t$ такое, что функция $T(x_1, \ldots, x_n)$ продолжает функцию $f(x_1 \ldots x_n)$. Изменим в определении 2.1 слабовычислимой функции понятие вычислимости за время $t(|x|)$ на понятие вычислимости за $t(|x|)$ вопросов. Полученное понятие назовем неравномерной слабовычислимостью за время $t(n)$.

Определение 3.3. Класс n.u.LOGS(G) — это класс таких проблем отделения F, что $F(\alpha) \leq G(f(\alpha))$ для некоторой неравномерно слабополилогарифмической функции f и всех $\alpha \in \mathbf{B}^*$.

Ясно, что LOGS$(G) \subseteq$ n.u.LOGS(F), и мы получаем из теоремы 3.1 очевидное

Следствие 3.3. *Если выполнено*

$$F \notin \text{n.u.LOGS}(G), \tag{5}$$

то выполнено и отрицание 3.5.

Утверждение (5) и есть то комбинаторное утверждение, которое доказывается всякий раз, когда надо доказать, что

$$\exists A \ \text{POLY}^A(F) \not\subseteq \text{POLY}^A(G).$$

4. Критерий релятивизуемого существования m-полной проблемы

Будем полиномиальную m-сводимость (сводимость Карпа) обозначать $\leq_m^p$. Если машина, вычисляющая сводящую функцию, имеет доступ к оракулу $A \subseteq \mathbf{B}^*$, то полученную сводимость обозначим $\leq_m^{p,A}$. Пусть $\leq$ — некоторая сводимость. Скажем, что проблема отделения H $\leq$-трудна для класса проблем отделения K, если любая проблема отделения из K $\leq$-сводится к H. При этом, если $H \in K$, то скажем, что H полна в K. Класс K_1 назовем $\leq$-полным для класса K_2, если K_1 содержит $\leq$-трудную проблему для K_2.

Следующая теорема, являющаяся критерием того, что класс $\mathrm{POLY}^A(G) \leq_m^{p,A}$-полон для класса $\mathrm{POLY}^A(F)$ при всех A, выглядит более естественной, если на проблемах отделения ввести слабополилогарифмическую сводимость $\preceq_m^l$. Именно, определим, что $F \preceq_m^l G$, если $F \in \mathrm{LOGS}(G)$, т.е. в качестве сводящих функций берутся слабополилогарифмические функции. Легко видеть, что сводимость $\preceq_m^l$ рефлексивна и транзитивна и что проблема F $\preceq_m^l$-полна в классе $\mathrm{LOGS}(F)$. Скажем, что проблема отделения G является решением проблемы отделения F, если $F(x) \leq G(x)$ при всех $x \in \mathbf{B}^*$.

Теорема 4.1. *Если проблема отделения F удовлетворяет условию 3.1, а проблема отделения G удовлетворяет условию 3.2, то следующие условия эквивалентны*

4.1. $\mathrm{LOG}(G)$ $\preceq_m^l$*-полон для* $\mathrm{LOGS}(F)$

4.2. *F имеет решение в* $\mathrm{LOG}(G)$

4.3. *Для всех $A \subseteq \mathbf{B}^*$ класс* $\mathrm{POLY}^A(G) \leq_m^{p,A}$*-полон для* $\mathrm{POLY}^A(F)$.

Если F — язык, то эти условия эквивалентны условию

4.4. $\mathrm{LOG}(G)$ $\preceq_m^l$*-полон для* $\mathrm{LOG}(F)$.

Доказательство. Докажем 4.1$\Longrightarrow$ 4.2. Пусть любая проблема отделения из $\mathrm{LOGS}(F)$ $\preceq_m^l$-сводится к $H \in \mathrm{LOGS}(G)$. Тогда $F \preceq_m^l H$. Пусть $g : \mathbf{B}^* \to \mathbf{B}^*$ — сводящая функция. Язык $H(g(\alpha))$ продолжает F и принадлежит $\mathrm{LOG}(G)$.

Докажем 4.2$\Longrightarrow$ 4.1. Пусть $H \in \mathrm{LOG}(G)$ продолжает F. Тогда H $\preceq_m^l$-полон для $\mathrm{LOGS}(F)$, поскольку F $\preceq_m^l$-полон для $\mathrm{LOGS}(F)$.

Из 4.1 очевидно следует 4.4. Импликация 4.4$\Longrightarrow$ 4.2 в случае, если F — язык, доказывается точно так же, как 4.1$\Longrightarrow$ 4.2, поскольку $F \in \mathrm{LOG}(F)$.

Докажем 4.2$\Longrightarrow$ 4.3.

Пусть F имеет всюду определенное продолжение $H \in \mathrm{LOG}(G)$. Пусть $A \subseteq \mathbf{B}^*$. По теореме 3.1 $\mathrm{POLY}^A(F) \subseteq \mathrm{POLY}^A(H) \subseteq \mathrm{POLY}^A(G)$. Поэтому достаточно доказать, что $\mathrm{POLY}^A(H) \leq_m^{p,A}$-полон для $\mathrm{POLY}^A(F)$. На самом деле, мы докажем, что в $\mathrm{POLY}^A(H)$ есть $\leq_m^p$-полный язык. Перенумеруем все слабополиномиальные относительно A функции $g_0^A, g_1^A, g_2^A, \ldots$ Положим $L_i^A(x) = H(g_i^A(x))$. По определению, $\mathrm{POLY}^A(H) = \{L_i^A \mid i \in \mathbf{N}\}$.

Пусть $p_i(|x|)$ — полином, ограничивающий время слабого вычисления функции $g_i^A(x)$ по $\bar{i}\bar{x}$. Мы докажем, что существует слабополиномиальная относительно A функция, f^A такая, что $\forall i \in \mathbf{N}\ \forall x \in \mathbf{B}^*\ f^A(\bar{i}\bar{x}0^{p_i(|x|)}) = g_i^A(x)$. Допустим, у нас уже есть такая функция. Тогда положим $L^A(u) = H(f^A(u))$. По своему определению $L^A \in \mathrm{POLY}^A(H)$. С другой стороны $L^A \leq_m^p$-полон в $\mathrm{POLY}^A(H)$, поскольку для каждого $i \in \mathbf{N}$ функция $x \mapsto \bar{i}\bar{x}0^{p_i(|x|)}$ полиномиальна и сводит L_i^A к L^A.

Функцию f^A можно определить так. Пусть M^A — машина, вычисляющая по $\bar{i}\bar{x}$ длину $g_i^A(x)$, а N^A — машина, вычисляющая по $\bar{i}\bar{x}j$ j-ый бит слова $g_i^A(x)$. Тогда длина слова $f^A(w)$ вычисляется такой машиной $\bar{M}^A$: определяем имеет ли w вид $\bar{i}\bar{x}0^t$, и если нет, то выдаем 0. Иначе находим i, x, и t и запускаем M^A на $\bar{i}\bar{x}$ и если за время $\leq t$ машина M^A даст ответ, то выдаем этот ответ, а иначе выдаем 0. Далее, j-ый бит слова $f^A(w)$ вычисляется следующей машиной $\bar{N}^A$: сначала запускаем $\bar{M}^A$ на w, пусть n — ее результат. Если $n = 0$, то выдаем, скажем 0. Иначе находим такие i, x и t, что $w = \bar{i}\bar{x}0^t$, и запускаем $N^A(\bar{i}\bar{x}j)$; если за время $\leq t$ машина N^A даст ответ, то выдаем этот ответ. Иначе выдаем 0.

Докажем, что если 4.2 неверно, то и 4.3 неверно. Пусть F не имеет продолжения в $\mathrm{LOG}(G)$. Построим оракул A, для которого $\mathrm{POLY}^A(G)$ не имеет $\leq_m^{p,A}$-трудного языка для $\mathrm{POLY}^A(F)$. Перенумеруем все слабополиномиальные относительно оракула A (еще не построенного) функции $f_0^A, f_1^A, \ldots, f_i^A, \ldots$ и все $\leq_m^{p,A}$-сводящие функции m_0^A, m_1^A, ..., m_j^A, ... (т.е. все полиномиальные относительно A функции типа $\mathbf{B}^* \to \mathbf{B}^*$). Пусть $A \subseteq \mathbf{B}^*$. Назовем i-ым компонентом A язык $A^i = \{x \mid \bar{i}x \in A\}$ и обозначим $L_i(A) = \{n \mid F((A^i)_n) = 1\}$. Напомним, что для $C \subseteq \mathbf{B}^*$, C_n обозначает слово длины n, j-ый бит которого равен $C(\bar{n}j)$. Ясно, что достаточно построить такой оракул A, что для всех $i \in \mathbf{N}$ выполнено одно из двух условий:

1) $G(f_i^A(y)) = *$ при некотором $y \in \mathbf{B}^*$;

2) Язык $L_i(A)$ принадлежит $\mathrm{POLY}^A(F)$ и не $\leq_m^{p,A}$-сводится к проблеме отделения $G(f_i^A(y))$.

Первое условие имеет локальный характер, обозначим его (L_i^1). Для выполнения второго условия достаточно выполнения одного глобального условия

(G_i) $\quad F((A^i)_n) \neq *$ при всех $n \in \mathbf{N}$

и счетного числа локальных условий

(L_{ij}^2) $\quad \exists n \in \mathbf{N}\ F((A^i)_n) \neq G(f_i^A(m_j^A(1^n))), j \in \mathbf{N}$.

Итак, мы построим оракул, для которого для всех пар $(i,j) \in \mathbf{N}^2$ выполнено (L_i^1) или $(\mathrm{G}_i)\&(\mathrm{L}_{ij}^2)$. Сначала определим оракул A так, чтобы он был полиномиально разрешим и чтобы для всех i было выполнено условие (G_i). Затем мы фиксируем некоторый пересчет множества $\mathbf{N}^2$ и выполним счетное число шагов, занумерованных парами (i,j). На шаге (i,j) конечными изменениями i-го компонента A будем добиваться выполнения условия (L_i^1) или условия (L_{ij}^2). При этом, если для некоторого i хотя бы для одного j на шаге (i,j) мы выполним условие (L_i^1), то в дальнейшем можно не выполнять шаги вида (i,j'). Истинности локальных условий мы будем добиваться конечными изменениями A и фиксированием значения A на конечном множестве слов. Процесс будет устроен таким образом, что если ни разу не удалось выполнить (L_i^1), то будет выполнено условие (G_i) и для всех j — условие (L_{ij}^2).

Шаг (i,j). Пусть A — оракул построенный к этому шагу (с некоторым конечным множеством зафиксированных слов). Рассмотрим два случая.

I случай: можно изменить i-ый компонент A на незафиксированных словах так, чтобы удовлетворить условие (L_i^1). Ясно, что для этого можно выполнить лишь конечное число изменений. Выполним их и зафиксируем эти изменения и остальные слова, гарантирующие выполнение этого условия. Поскольку при $i' \neq i$ $A^{i'}$ не было изменено, все истинные условия $(\mathrm{G}_{i'})$ не нарушились.

II случай: при любых изменениях i-го компонента A на незафиксированных словах условие (L_i^1) не выполнено. Пусть $\alpha \in \mathbf{B}^*$. Пусть $B \subseteq \mathbf{B}^*$ такой язык, что $B^{i'} = A^{i'}$ при $i' \neq i$ и $B^i = (A^i)[\alpha]$ ($C[\alpha]$ — обозначение из доказательства теоремы 1). Обозначим B через $A[\alpha, i]$. Рассмотрим язык

$$H = \{\alpha \in \mathbf{B}^* \mid G(f_i^{A[\alpha,i]}(m_j^{A[\alpha,i]}(|\alpha|))) = 1\}.$$

Докажем, что $H \in \mathrm{LOG}(G)$. По условию случая, при достаточно больших α, $G(f_i^{A[\alpha,i]}(y)) \neq *$ при всех $y \in \mathbf{B}^*$, в частности $G(f_i^{A[\alpha,i]}(m_j^{A[\alpha,i]}(|\alpha|))) \neq *$ при достаточно длинных α. Кроме того, A полиномиально разрешим (т.к. получен конечными изменениями из полиномиально разрешимого языка), а значит функция $\alpha \mapsto f_i^{A[\alpha,i]}(m_j^{A[\alpha,i]}(|\alpha|))$ слабополилогарифмична. Из этих двух утверждений и невырожденности G следует $H \in \mathrm{LOG}(G)$. Поэтому существует бесконечно много таких α, что $F(\alpha) \not\leq H(\alpha)$. Выберем любое такое α , что $F(\alpha) \not\leq H(\alpha)$ и что изменение, нужное для переделывания A в $A[\alpha, i]$, не затрагивает значения A на зафиксированных словах. Тогда при $n = |\alpha|$ мы имеем

$$F(((A[\alpha,i])^i)_n) = F(\alpha) \not\leq H(\alpha) = G(f_i^{A[\alpha,i]}(m_j^{A[\alpha,i]}(n))).$$

Заменим A на $A[\alpha, i]$ и зафиксируем все слова в A, от которых зависит $f_i^A(m_j^A(n))$, а также все слова вида $\bar{i}\bar{n}j$, $j \leq n$. Этим мы добьемся выполненности (L_{ij}^2). При этом условие (G_i) не нарушилось, поскольку $F(\alpha) \neq *$. Поскольку изменен только i-й компонент, остальные условия $(\mathrm{G}_{i'})$ нарушиться не могли.

Импликация 4.3$\Longrightarrow$ 4.2 доказана. Теорема доказана. □

Следствие 4.2. *Если F язык, то класс* $\mathrm{POLY}^A(F)$ *содержит $\leq_m^p$-полный язык.*

Замечание 4.0. Как видно из доказательства, в условии 4.3 сводимость $\leq_m^{p,A}$ можно заменить на $\leq_m^p$.

Замечание 4.0. Если имеется не более чем счетное количество пар проблем отделения F_i, G_i таких, что F_i не имеет продолжения в $\mathrm{LOG}(G_i)$, то, как видно из доказательства, можно построить один оракул A, для которого для всех i, $\mathrm{POLY}^A(G_i)$ не $\leq_m^{p,A}$-полон для $\mathrm{POLY}^A(F_i)$. Для этого для

каждого i в A нужно выделить свое счетное число компонент $A^{i,j} = \{x \in \mathbf{B}^* \mid \overline{ij}x \in A\}, j \in \mathbf{N}$. То же самое верно и для теоремы 3.1 и последующих теорем 5.1, 6.1. Ясно также, что можно совмещать и отрицательные результаты разных типов: например, построить такой оракул A, что для одного семейства пар F_i, G_i $\mathrm{POLY}^A(F_i) \not\subseteq \mathrm{POLY}^A(G_i)$ при всех i, а для другого семейства H_j, J_j, $\mathrm{POLY}^A(H_j)$ не $\leq_m^{p,A}$-полон для $\mathrm{POLY}^A(J_j)$ при всех j (если, конечно, этого можно добиться по отдельности).

Следствие 4.3. *Если для невырожденных F, G выполнено*

$$F \text{ не имеет продолжений в классе } \mathrm{n.u.LOGS}(G), \tag{6}$$

то существует такой оракул $A \subseteq \mathbf{B}^*$, что $\mathrm{POLY}^A(G)$ не $\leq_m^{p,A}$-полон для $\mathrm{POLY}^A(F)$.

Утверждение 6 и есть то комбинаторное утверждение, которое всегда доказывается в теоремах вида: $\exists A$ $\mathrm{POLY}^A(G)$ не $\leq_m^{p,A}$-полон для $\mathrm{POLY}^A(F)$.

Пример. Как будет видно из параграфа 9, $\mathrm{n.u.LOG}(F_{\mathbf{BPP}}) = \mathbf{n.u.PLOG}$, и поскольку, скажем, проблема отделения $F_{\mathbf{R}}$, задающая класс $\mathbf{R}$, не имеет продолжения в $\mathbf{n.u.PLOG}$, существует A, для которого $\mathbf{BPP}^A$ не имеет $\leq_m^{p,A}$-полного языка для $\mathbf{R}^A$.

Замечание 4.0. Если заменить в теореме 4.1 проблемы отделения F, G на счетные множества невырожденных проблем отделения $\mathcal{F}$, $\mathcal{G}$, то импликация 4.3$\Longrightarrow$ 4.1 останется очевидно верной. Обратная импликация будет верна, если усилить 4.1, потребовав равномерную сводимость всех проблем отделения из $\mathcal{F}$ к какой-нибудь одной проблеме отделения H из $\mathrm{LOG}(\mathcal{G})$. То есть, если потребовать существование вычислимой функции $f(i, \alpha)$, которая при любом фиксированном i слабополилогарифмична и сводит i-ую проблему отделения из $\mathcal{F}$ к H.

5. Критерий релятивизуемой сводимости по Тьюрингу одного класса к другому

Полиномиальную тьюрингову сводимость (сводимость Кука) обозначим $\leq_T^p$, а полиномиальную относительно $A \subseteq \mathbf{B}^*$ тьюрингову сводимость обозначим $\leq_T^{p,A}$. Напомним, что $L_1 \leq_T^{p,A} L_2$, если существует полиномиальная машина M с двумя оракулами A и L_2, распознающая L_1.

Пусть $\leq$ — некоторая сводимость. Скажем, что класс K_1 $\leq$-сводится к классу K_2 (обозначение: $K_1 \leq K_2$), если $\forall L_1 \in K_1\ \exists L_2 \in K_2 \quad L_1 \leq L_2$.

Чтобы сформулировать теорему, дающую критерий того, что $K_1 \leq_T^{p,A} K_2$ при всех оракулах A, определим слабополилогарифмическую тьюрингову сводимость на проблемах отделения, ослабляющую слабополилогарифмическую m-сводимость.

Скажем, что проблема отделения F слабополилогарифмически T-сводится к проблеме отделения G (обозначение: $F \preceq^l_T G$), если существует такая полиномиальная машина Тьюринга M с оракулом и существует такая функция $f : \mathbf{B}^* \times \mathbf{B}^* \to \mathbf{B}^*$, что значение $f(y,\alpha)$ слабовычислимо за время $\mathrm{poly}(|y| + \log|\alpha|)$ и для всех $\alpha \in D(F)$ выполнено

1) $G(f(y,\alpha)) \neq *$ для всех $y \in \mathbf{B}^*$ и

2) $F(\alpha) = M^{G(f(\cdot,\alpha))}(|\alpha|)$,

где $G(f(\cdot,\alpha))$ обозначает язык $\{y \in \mathbf{B}^* \mid G(f(y,\alpha)) = 1\}$.

Будем называть пару $\langle M, f\rangle$ сводящей парой. Результат, выдаваемый M при работе на входе $|\alpha|$ с оракулом $G(f(\cdot,\alpha))$ обозначим $\langle M, f\rangle^G(\alpha)$. Заметим, что если существует пара $\langle M, f\rangle$, для которой условия 1) и 2) выполнены для всех $\alpha \in D(F)$ за исключением конечного числа, то все равно $F \preceq^l_T G$.

Очевидно, что отношение $\preceq^l_T$ рефлексивно и транзитивно. Ясно, что $F \preceq^l_m G \Longrightarrow F \preceq^l_T G$.

Теорема 5.1. *Если F удовлетворяет 3.1, а G удовлетворяет 3.2, то следующие условия эквивалентны:*

5.1. $\mathrm{LOGS}(F) \preceq^l_T \mathrm{LOGS}(G)$

5.2. $F \preceq^l_T G$

5.3. *Для любого $A \subseteq \mathbf{B}^*$* $\mathrm{POLY}^A(F) \leq^{p,A}_T \mathrm{POLY}^A(G)$

Если F — язык, то все условия эквивалентны условию

5.4. $\mathrm{LOG}(F) \preceq^l_T \mathrm{LOG}(G)$.

Доказательство. Эквивалентность 5.1 и 5.2 очевидна.

Очевидно, что если F — язык, то 5.4$\Longrightarrow$ 5.2. Обратно, пусть F — язык и $F \preceq^l_T G$. Докажем сначала, что $\{F\} \preceq^l_T \mathrm{LOG}(G)$. Пусть $\langle M, f\rangle$ — это пара, сводящая F к G. Пусть $l(n)$ — полилогарифм, ограничивающий длину вопросов M к оракулу при работе на входе $n \in \mathbf{N}$. Рассмотрим язык $H = \{\bar{x}\alpha \mid |x| \leq l(|\alpha|), G(f(x,\alpha)) = 1\}$. За время $\mathrm{polylog}(|\beta|)$ мы можем выяснить, имеет ли β вид $\bar{x}\alpha$, $|x| \leq l(|\alpha|)$. Поскольку $D(F) = \mathbf{B}^*$, мы имеем $G(f(x,\alpha)) \neq *$ для всех x, $\alpha \in \mathbf{B}^*$. Из этих двух утверждений следует $H \in \mathrm{LOG}(G)$. Положим $g(x,\alpha) = \bar{x}\alpha$. Ясно, что $g(x,\alpha)$ слабовычислимо за время $\mathrm{poly}(|x| + \log|\alpha|)$ и что пара $\langle M, g\rangle$ сводит F к H, а значит $\{F\} \preceq^l_T \mathrm{LOG}(G)$. Поскольку язык F $\preceq^l_m$-полон в $\mathrm{LOG}(F)$, мы получаем $\mathrm{LOG}(F) \preceq^l_T \mathrm{LOG}(G)$.

Докажем,что из 5.2 следует 5.3. Пусть $F \preceq^l_T G$, и пусть $\langle M, f\rangle$ — сводящая пара. Пусть A — произвольный оракул и L — любой язык из $\mathrm{POLY}^A(F)$. Обозначим g такую слабополиномиальную относительно A функцию, что $L(x) = F(g(x))$. Тогда $L(x) = M^{G(f(\cdot,g(x)))}(|g(x)|)$ для всех $x \in \mathbf{B}^*$. Поскольку функция $|g(x)|$ полиномиально вычислима относительно A, язык

$L \leq_T^{p,A}$-сводится к языку $\{\bar{y}g(x) \mid G(f(y,g(x))) = 1\}$, который принадлежит $\mathrm{POLY}^A(G)$, поскольку $G(f(y,g(x))) \neq *$ для всех $x, y \in \mathbf{B}^*$ и функция $\bar{y}x \mapsto f(y,g(x))$ слабополиномиальна относительно A.

Докажем, что 5.2$\Longrightarrow$5.3. Пусть $F \not\preceq_T^l G$. Докажем, что выполнено 5.3. Заметим, что в условии 5.3 сводимость $\leq_T^{p,A}$ можно заменить на $\leq_T^p$. Действительно, если язык $L_1 \leq_T^{p,A}$-сводится к языку L из $\mathrm{POLY}^A(G)$, то L_1 $\leq_T^p$-сводится к языку $L \oplus A = \{0x \mid x \in L\} \cup \{1x \mid x \in A\}$, который принадлежит $\mathrm{POLY}^A(G)$ в силу того, что G удовлетворяет условию 3.2.

Ясно, что достаточно построить такой оракул A, что выполнены два условия:

(G) $\forall n A\_n \in D(F)$

(L) Язык $\{n \mid F(A_n) = 1\}$ не $\leq_T^p$-сводится ни к одному языку из $\mathrm{POLY}^A(G)$.

Перенумеруем все $\leq_T^p$-сводящие машины M_1^B, M_2^B,..., M_j^B,... (B — тот язык, к которому M_j сводит). Перенумеруем все слабополиномиальные относительно A функции $f_1^A(x)$, $f_2^A(x)$,..., $f_i^A(x)$,... Мы добьемся, чтобы для всех $i, j \in \mathbf{N}$ было выполнено

(L_{ij}) $\quad \exists n \in \mathbf{N}\ F(A_n) \neq M_j^{G(f_i^A(\cdot))}(n) \vee \exists y G(f_i^A(y)) = *$.

Сначала сделаем A равным такому полиномиально разрешимому языку, что выполнено условие (G). Выполним счетное число шагов с номерами $(i,j) \in \mathbf{N}^2$.

Шаг (i,j). Пусть A — оракул, определенный к этому шагу. Рассмотрим два случая. Назовем $\alpha \in \mathbf{B}^*$ свободным, если ни одно слово вида $\overline{|\alpha|}k, k \leq |\alpha|$ не зафиксировано. Ясно, что не свободных α лишь конечное число.

1-й случай. Существуют такое свободное $\alpha \in D(F)$ и такое $y \in \mathbf{B}^*$, что $F(\alpha) \neq *$ и $G(f_i^{A[\alpha]}(y)) = *$. Тогда заменяем A на $A[\alpha]$ и проводим конечное число фиксирований, закрепляющих выполнение (L_{ij}). Заметим, что при этом (G) не испортится.

2-й случай. Для всех свободных $\alpha \in D(F) G(f_i^{A[\alpha]}(y)) \neq *$ при всех $y \in \mathbf{B}^*$.

Докажем, что существует свободное $\alpha \in D(F)$ такое, что $F(\alpha) \neq M_j^{G(f_i^{A[\alpha]}(\cdot))}(|\alpha|)$. Допустим противное: для всех свободных $\alpha \in D(F)$ выполнено $F(\alpha) = M_j^{G(f_i^{A[\alpha]}(\cdot))}(|\alpha|)$. Функция $g(y,\alpha) = f_i^{A[\alpha]}(y)$ слабовычислима за время $\mathrm{poly}(|y| + \log|\alpha|)$ и для пары $\langle M, g\rangle$ выполнены условия 1) и 2) из определения сводимости $\preceq_T^l$ для всех свободных $\alpha \in D(F)$. Следовательно, $F \preceq_T^l G$ вопреки предположению.

Дальше рассуждаем, как в теореме 3.1. □

6. Критерий релятивизуемого существования полной по Тьюрингу проблемы

Теорема 6.1. *Для невырожденых проблем отделения F, G следующие условия эквивалентны:*

6.1. $\mathrm{LOG}(G)$ *$\preceq^l_T$-полон для* $\mathrm{LOGS}(F)$.

6.2. $\mathrm{LOG}(G)$ *содержит язык, к которому* $\preceq^l_T$*-сводится* F.

6.3. $\mathrm{POLY}^A(G)$ *$\leq^{p,A}_T$-полон для* $\mathrm{POLY}^A(F)$ *для любого* $A \subseteq \mathbf{B}^*$.

Если F *язык, то эти условия эквивалентны условию*

6.4. $\mathrm{LOG}(G)$ *$\preceq^l_T$-полон для* $\mathrm{LOG}(F)$.

Доказательство. Эквивалентность 6.1 и 6.2, а также эквивалентность этих условий 6.4 в случае, если F — язык, очевидна.

Докажем, что 6.2$\Longrightarrow$ 6.3. Пусть $F \preceq^l_T H \in \mathrm{LOG}(G)$. Если H не удовлетворяет условию 3.2, то $F \in \mathbf{PLOG}$ и утверждение 6.3 очевидно. Иначе, по теореме 4.1 для любого оракула A класс $\mathrm{POLY}^A(H)$ содержит $\leq^p_m$-полный язык и по теореме 5.1 $\mathrm{POLY}^A(F) \leq^{p,A}_T \mathrm{POLY}^A(H)$, следовательно класс $\mathrm{POLY}^A(G) \leq^{p,A}_T$-полон для класса $\mathrm{POLY}^A(F)$.

Докажем, что 6.3 влечет 6.2. Как и в теореме 6.1, в пункте 6.3 сводимость $\leq^{p,A}_T$ можно заменить на сводимость $\leq^p_T$.

Допустим 6.2 неверно, т.е. F не $\preceq^l_T$-сводится ни к какому языку из $\mathrm{LOG}(G)$.

Построим такой оракул A, что $\mathrm{POLY}^A(G)$ не содержит $\leq^p_T$-полного языка для $\mathrm{POLY}^A(F)$. Перенумеруем все слабополиномиальные относительно A функции $f^A_0(y)$, $f^A_1(y)$,..., $f^A_i(y)$,... Представим A как сумму компонент $A^i = \{x \mid \overline{i}x \in A\}$. Ясно, что было бы достаточно, если бы для всех $i \in \mathbf{N}$ было выполнено одно из двух:

1) (L^1_i) $G(f^A_i(y)) = *$ при некотором $y \in \mathbf{B}^*$,

2) Язык $L_i(A) = \{n \mid F(A^i_n) = 1\}$ принадлежит $\mathrm{POLY}^A(F)$ и не $\leq^p_T$-сводится к проблеме отделения $G(f^A_i(y))$.

Перенумеруем все полиномиальные машины с обычным оракулом ($\leq^p_T$-сводящие машины) M^L_0, M^L_1,..., M^L_j, ...

Для выполнения условия 2) достаточно выполнить условие

(G_i) $\quad \forall n\ F(A^i_n) \neq *$,

и счетное число условий

(L^2_{ij}) $\quad \exists n \in \mathbf{N}\ F(A^i_n) \neq M^{G(f^A_i(\cdot))}_j(n)$.

Будем действовать так же, как в доказательстве теоремы 4.1. Приведем только различия.

Шаг i, j:

Случай II. При любых изменениях A^i на незафиксированных словах $G(f^A_i(y)) \neq *$ при всех $y \in \mathbf{B}^*$. Назовем $\alpha \in \mathbf{B}^*$ свободным, если ни одно слово в A^i вида $\overline{|\alpha|}j$, $j \leq |\alpha|$ не зафиксировано. Очевидно достаточно доказать, что существует свободное $\alpha \in D(F)$ такое, что $F(\alpha) \neq M^{G(f^{A^{[\alpha,i]}}_i(\cdot))}_j(|\alpha|)$. Допустим противное. Пусть $l(n)$ — полилогарифм, ограничивающий длину

вопросов машины M к оракулу при работе на входе n. Возьмем язык

$$H = \{\bar{y}\alpha : |y| \le l(|\alpha|),\ G(f_i^{A[\alpha,i]}(y)) = 1\}$$

и функцию $g(y,\alpha) = \bar{y}\alpha$. Поскольку для всех свободных α и всех $y \in \mathbf{B}^*, G(f_i^{A[\alpha,i]}(y)) \neq *$, язык H принадлежит $\mathrm{LOG}(G)$. Для пары $\langle M_j, g\rangle$ выполнены условия 1) и 2) определения $\preceq_T^l$-сводимости F к H для всех свободных $\alpha \in \mathbf{B}^*$. Следовательно, $F \preceq_T^l H$ вопреки условию. □

Следствие 6.2. *Если* $F \not\preceq_T^l$ n.u.$\mathrm{LOG}(G)$, *то существует оракул* A, *для которого* $\mathrm{POLY}^A(G)$ *не* $\le_T^{p,A}$*-полон для* $\mathrm{POLY}^A(F)$.

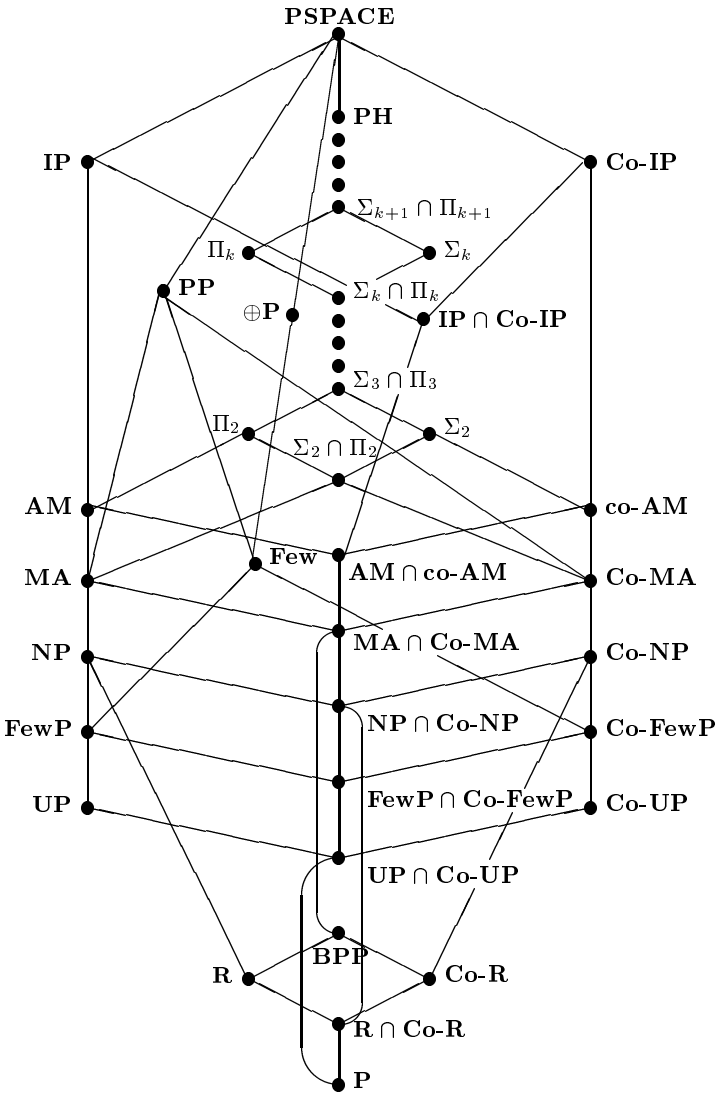
Замечание 6.0. Пусть K_1,K_2 классы языков, A некоторый язык. Как замечено в [3], если K_2 замкнут относительно $\le_T^{p,A}$-сводимости, то $K_2 \le_T^{p,A}$-полон для K_1 тогда и только тогда, когда $K_2 \le_m^p$-полон для K_1. Действительно, если к языку $L \in K_2$ $\le_T^{p,A}$-сводится любой язык из K_1, то к языку $L_1 = \{\bar{i}\bar{x}0^t \mid M_i^{A,L}$ на входе x выдает результат 1 за время $\le t\}$ (M_0, M_1, ... — нумерация $\le_T^{p,A}$-сводящих машин) $\le_m^p$-сводится любой язык из K_1. С другой стороны $L_1 \le_T^{p,A} L$, следовательно, $L_1 \in K_2$.

7. Релятивизуемые включения конкретных сложностных классов

В этом параграфе мы рассмотрим наиболее распространенные в литературе порождаемые многообразия между $\mathbf{P}^A$ и $\mathbf{PSPACE}^A$ (исключение составляет многообразие $\mathbf{Few}^A$, про которое автору неизвестно, порождаемо ли оно). Как уже отмечалось в Замечании 3, все конкретные известные из литературы классы можно задавать с помощью проблем отделения, не равных $*$ только на словах длины 2^n, $n \in \mathbf{N}$. Чтобы упростить обозначения будем далее рассматривать только такие проблемы отделения. Обозначим $\mathbf{F}_n = \mathbf{B}^{2^n}$, $\mathbf{F} = \bigcup_{i=0}^{\infty} \mathbf{F}_n$ и будем нумеровать символы слова $\alpha \in \mathbf{F}_n$ не числами от 1 до 2^n, а словами длины n из нулей и единиц. Для слова α из $\mathbf{F}$ обозначим $\|\alpha\| = \log_2 |\alpha|$. Будем придерживаться далее следующего правила: если конкретная проблема отделения определяется только на некотором множестве слов $A \subseteq \mathbf{B}^*$, то на словах из $\mathbf{B}^* \setminus A$ она считается равной $*$.

На рисунке 1 показаны все известные включения этих многообразий (многообразие K_1^A включено в K_2^A, если $\forall A\ K_1^A \subseteq K_2^A$), т.е. все известные релятивизуемые включения. Ребра соединяют меньший класс с большим, причем больший класс расположен выше.

Рис. 1. Релятивизуемые включения сложностных классов



Пояснения к рисунку

1. $\mathbf{UP}^A$ — это класс, определяемый проблемой отделения

$$F_{\mathbf{UP}}(\alpha) = \begin{cases} 1, & \text{если } \#_1(\alpha) = 1, \\ 0, & \text{если } \#_1(\alpha) = 0, \\ *, & \text{иначе.} \end{cases}$$

2. $\mathbf{FewP}^A \rightleftharpoons \mathrm{POLY}^A(\mathcal{F})$, где $\mathcal{F}$ состоит из проблем отделения F вида

$$F(\alpha) = \begin{cases} 1, & \text{если } 0 < \#_1(\alpha) \le p(\|\alpha\|), \\ 0, & \text{если } \#_1(\alpha) = 0, \\ *, & \text{иначе,} \end{cases}$$

где p — некоторый полином.

3. $\mathbf{Few}^A$ — это класс, определенный в работе [7], следующим образом:

Язык L принадлежит $\mathbf{Few}^A$, если существуют слабополиномиальная относительно A функция f^A, полином q и полиномиальный относительно A предикат $\mathbf{R}^A$ на $\mathbf{B}^* \times \mathbf{N}$ такие, что $L(x) = \mathbf{R}^A(x, \#_1 f^A(x))$ и $\#_1(f^A(x)) \le q(|x|)$. Неизвестно, является ли многообразие $\mathbf{Few}^A$ порождаемым.

4. $\oplus\mathbf{P}^A \rightleftharpoons \mathrm{POLY}^A(\mathrm{PARITY})$, где

$$\mathrm{PARITY}(\alpha) = \begin{cases} 0, & \text{если } \#_1(\alpha) \text{ четно,} \\ 1, & \text{иначе.} \end{cases}$$

5. $\mathbf{AM}^A$ — сокращение для класса $\mathbf{AM}[2]^A$. Класс $\mathbf{AM}^A$ порождается следующей проблемой отделения $F_{\mathbf{AM}}$. Пусть $\mathrm{M}_d x \in M.P(x)$ означает, что $|\{x \in M : P(x)\}| > d \cdot |M|$. Тогда для $\alpha \in \mathbf{F}_{2n}$

$$F_{\mathbf{AM}}(\alpha) = \begin{cases} 1, & \text{если } \mathrm{M}_{2/3} u \in \mathbf{B}^n \ \exists v \in \mathbf{B}^n \ \alpha(uv) = 1, \\ 0, & \text{если } \mathrm{M}_{2/3} u \in \mathbf{B}^n \ \forall v \in \mathbf{B}^n \ \alpha(uv) = 0, \\ *, & \text{иначе,} \end{cases}$$

где uv обозначает конкатенацию слов u и v. Обозначим $\mathrm{LOGS}(F_{\mathbf{AM}})$ через **AMLOGS**.

6. $\mathbf{MA}^A$ — класс, порождаемый проблемой отделения

$$F_{\mathbf{MA}}(\alpha) = \begin{cases} 1, & \text{если } \exists u \in \mathbf{B}^n \ \mathrm{M}_{2/3} v \in \mathbf{B}^n \ \alpha(uv) = 1, \\ 0, & \text{если } \forall u \in \mathbf{B}^n \ \mathrm{M}_{2/3} v \in \mathbf{B}^n \ \alpha(uv) = 0, \\ *, & \text{иначе,} \end{cases}$$

при $\alpha \in \mathbf{F}_{2n}$.

7. Докажем, что многообразие $\mathbf{PSPACE}^A$ имеет вид $\mathrm{POLY}^A(F)$.

Известно, что любой язык L из $\mathbf{PSPACE}^A$ представим в виде
$L = \{x \mid \exists y_1 \in \mathbf{B}^n \ \forall y_2 \in \mathbf{B}^n \cdots Q y_n \in \mathbf{B}^n P^A(x, y_1 y_2 \cdots y_n)$, где $n = p(|x|)\}$,

где $P^A(x,u)$ некоторый полиномиальный относительно A предикат, а $p(m)$ — некоторый полином. И обратное тоже верно. Пользуясь этим, возьмем проблему отделения

$$F_{\mathbf{PSPACE}}(\alpha) = \begin{cases} 1, & \text{если для неко орого } n \in \mathbf{N} \text{ вып лнено} \\ & \|\alpha\| = n^2 \text{ и } \exists y_1 \in \mathbf{B}^n\ \forall y_2 \in \mathbf{B}^n \cdots Q y_n \in \mathbf{B}^n\ \alpha(y_1 y_2 \cdots y_n) = 1 \\ 0, & \text{иначе.} \end{cases}$$

Ясно, что $\mathrm{POLY}^A(F_{\mathbf{PSPACE}}) = \mathbf{PSPACE}^A$, а $\mathrm{LOG}(F_{\mathbf{PSPACE}})$ — класс языков, распознаваемых на полилогарифмической зоне.

8. Докажем, что многообразие $\mathbf{IP}^A$ имеет вид $\mathrm{POLY}^A(F)$.

Возьмем проблему отделения $F_{\mathbf{IP}}$, которая на словах $\alpha \in \mathbf{F}$ нормы $2n^2$ определена следующим образом

$$F_{\mathbf{IP}}(\alpha) = \begin{cases} 1, & \text{если } \exists P : \mathbf{B}^* \to \mathbf{B}^n\ \ \mathrm{Prob}[\alpha(r_1 r_2 \cdots r_n P(r_1) P(r_1 r_2) \cdots P(r_1 r_2 \cdots r_n)) = 1] > \frac{2}{3}, \\ 0, & \text{если } \forall P : \mathbf{B}^* \to \mathbf{B}^n\ \ \mathrm{Prob}[\alpha(r_1 r_2 \cdots r_n P(r_1) P(r_1 r_2) \cdots P(r_1 r_2 \cdots r_n)) = 1] < \frac{1}{3}, \\ *, & \text{иначе,} \end{cases}$$

(вероятность берется по равномерному распределению на $r_1 \cdots r_n$).

Тогда $\mathrm{POLY}^A(F_{\mathbf{IP}}) = \mathbf{IP}^A$, если $\mathbf{IP}^A$ определять по [4], т.е. считать, что все результаты бросаний Проверяющего известны Доказывающему.

Чтобы стал ясен содержательный смысл определения $F_{\mathbf{IP}}$, напомним определение $\mathbf{IP}^A$ по [4] в удобном для нас виде. Проверяющим назовем любую пару $V = (q, Q)$, где Q — полиномиально вычислимый предикат на $\mathbf{B}^* \times \mathbf{B}^* \times \mathbf{B}^*$, а $q : \mathbf{N} \to \mathbf{N}$ — полином. Доказывающим назовем любую функцию $P : \mathbf{B}^* \to \mathbf{B}^*$. Пусть $x \in \mathbf{B}^*$, $|x| = m$. Для каждой последовательности $r_1,\ldots,r_{q(m)}$ слов длины $q(m)$ (длина последовательности равна длине слова в последовательности) определим ответ (P, V) на x при результатах бросаний $r_1,\ldots,r_{q(m)}$ следующим образом. Определим для каждого $i \le q(m)$

$$p_i = P(r_1 \cdots r_i).$$

Положим ответ равным $Q(x, r_1 \cdots r_{q(m)}, p_1 \cdots p_{q(m)})$, если длины всех слов p_i равны $q(m)$ и нулю иначе. Обозначим ответ через $(P,V)(x)_{r_1 \cdots r_{q(m)}}$. Тогда язык L принадлежит $\mathbf{IP}$, если существует Проверяющий V со следующим свойством:

$$\forall x \in L\ \exists P\ \ \mathrm{Prob}[(P,V)(x)_{r_1 \cdots r_{q(|x|)}} = 1] > \frac{2}{3}$$
$$\forall x \notin L\ \forall P\ \ \mathrm{Prob}[(P,V)(x)_{r_1 \cdots r_{q(|x|)}} = 0] > \frac{2}{3},$$

где вероятность берется по равномерному распределению на $r_1 \cdots r_{q(|x|)}$.

Для определения $\mathbf{IP}^A$ нужно релятивизовать Проверяющего.

Определение проблемы отделения $F_{\mathbf{IP}}$ согласовано с определением **IP** так: $n = q(m)$ — количество раундов, а $\alpha(r_1 \cdots r_n P(r_1) \cdots P(r_1 \cdots r_n))$ есть $Q(x, r_1 \cdots r_n, p_1 \cdots p_n)$ — ответ (P,V) на x.

Определение **IP** с секретным датчиком случайных чисел по [10] не укладывается в нашу схему. Однако, как доказано в [11], оба определения эквивалентны и доказательство релятивизуется.

Языки из $\mathrm{LOG}(F_{\mathbf{IP}})$ — это языки, распознаваемые полилогарифмическим Проверяющим. Обозначим $\mathrm{LOG}(F_{\mathbf{IP}})$ через **IPLOG**.

9. О классах вида Co-K^A и $K^A \cap$ Co-K^A.

Заметим, что если многообразие K^A (одно)порождаемое, то и многообразие Co-$K^A = \{\mathbf{B}^* \setminus L : L \in K^A\}$ (одно)порождаемое. Если K_1^A, K_2^A однопорождаемые многообразия, $K_i^A = \mathrm{POLY}^A(F_i)$, $i = 1, 2$, то и многообразие $K_1^A \cap K_2^A$ однопорождаемо проблемой отделения

$$F(\alpha) = \begin{cases} 1, & \text{если } \alpha = \overline{|\alpha_1|}\alpha_1\alpha_2, \text{ где } F_1(\alpha_1) = F_2(\alpha_2) = 1, \\ 0, & \text{если } \alpha = \overline{|\alpha_1|}\alpha_1\alpha_2, \text{ где } F_1(\alpha_1) = F_2(\alpha_2) = 0, \\ *, & \text{если } \alpha \text{ не имеет такого вида.} \end{cases}$$

Кроме этого, для проблемы отделения F очевидно выполнено $\mathrm{LOG}(F) = \mathrm{LOG}(F_1) \cap \mathrm{LOG}(F_2)$, $\mathrm{LOGS}(F) = \mathrm{LOGS}(F_1) \cap \mathrm{LOGS}(F_2)$, $\mathrm{EXP}^A(F) = \mathrm{EXP}^A(F_1) \cap \mathrm{EXP}^A(F_2)$.

Исторические ссылки. Нетривиальные включения, показанные на Рис. fig1 доказаны следующими авторами.

1) $\mathbf{MA}^A \subseteq \Sigma_2^A \cap \Pi_2^A$ легко следует из результата Гача [24] $\mathbf{BPP}^A \subseteq \Sigma_2^A \cap \Pi_2^A$. Именно, в [24] построена проблема отделения $G(\alpha)$, продолжающая $F_{\mathbf{BPP}}$ такая, что

$$G(\alpha) = 1 \Longleftrightarrow \forall y \in \mathbf{B}^{p(\|\alpha\|)}\ \exists z \in \mathbf{B}^{p(\|\alpha\|)} Q(\alpha, y, z) \tag{7}$$

где p — некоторый полином, а Q — некоторый полилогарифмический предикат (т.е. $G \in \Pi_2\mathrm{LOG}$).

2) $\mathbf{AM}^A \subseteq \Pi_2^A$ следует из этого же результата Гача. Причем для этого включения важно, что в (7.1) предикат $Q(\alpha, y, z)$ монотонен по α (т.е. если α' получается из α заменой некоторых нулей на 1, то $Q(\alpha, y, z) \Longrightarrow Q(\alpha', y, z)$).

3) $\mathbf{MA}^A \subseteq \mathbf{AM}^A$ доказано в [4].

4) $\mathbf{Few}^A \subseteq \oplus\mathbf{P}^A$ доказано в [7].

5) Включение $\mathbf{MA}^A \subseteq \mathbf{PP}^A$ доказывается довольно просто. Кроме того, оно легко следует из известного результата [17]: $\mathbf{PP}^{\mathbf{BPP}} = \mathbf{PP}$ поскольку $\mathbf{MA} \subseteq \mathbf{NP}^{\mathbf{BPP}} \subseteq \mathbf{PP}^{\mathbf{BPP}} = \mathbf{PP}$.

6) Включение $\mathbf{Few}^A \subseteq \Sigma_2^A \cap \Pi_2^A$ следует из того, что $\forall A\ \mathbf{Few}^A \leq_T^p \mathbf{NP}^A$, что достаточно хорошо известно и довольно просто. Докажем для полноты эту сводимость.

Как отмечалось, достаточно доказать, что $\forall A\ \mathbf{Few}^A \leq_T^{p,A} \mathbf{NP}^A$. Фиксируем $A \subseteq \mathbf{B}^*$. Пусть $L \in \mathbf{Few}^A$, и пусть L задается полиномами p, q и полиномиальными предикатами R^A, Q^A, т.е.

$$L(x) = R^A(x, |\{y \in \mathbf{B}^{p(|x|)} : Q^A(x,y)\}|),$$
$$|\{y \in \mathbf{B}^{p(|x|)} : Q^A(x,y)\}| \le q(|x|).$$

Докажем, что имея в качестве оракула $\mathbf{NP}^A$-полный язык, можно за полиномиальное время по x найти $|\{y \in \mathbf{B}^{p(|x|)} : Q^A(x,y)\}|$. Для этого сначала выясняем, существует ли такое множество $M \subseteq \mathbf{B}^{p(|x|)}$ мощности ровно $q(|x|)$, что $\forall y \in M$ выполнено $Q^A(x,y)$. Это можно узнать, задав вопрос к $\mathbf{NP}^A$-полному языку (поскольку $|M|$ полиномиально). Если такое M существует, то $|\{y \in \mathbf{B}^{p(|x|)} : Q^A(x,y)\}| = q(|x|)$. Если нет, то спрашиваем, существует ли $M \subseteq \mathbf{B}^{p(|x|)}$ мощности $q(|x|) - 1$ такое, что $\forall y \in M\ Q(x,y)$. И т.д. $q(|x|)$ раз.

7) Включение $\mathbf{Few}^A \subseteq \mathbf{PP}^A$ доказано в работе [17].

Все ли истинные включения указаны на рисунке? Мы утверждаем, что все истинные включения указаны. Истинность этого следует из следующих утверждений, в которых перечисляются все такие пары классов K_1, K_2, что

$$K_1 \not\subseteq K_2 \text{ и } \forall K_1'(K_1' < K_1 \Longrightarrow K_2' \le K_2),\ \forall K_2'\ (K_2 < K_2' \Longrightarrow K_1 \le K_2'),$$

где $<$ — отношение строгой достижимости по ребрам на рисунке.

1. $\exists A\ \mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A \not\subseteq \mathbf{BPP}^A$
2. $\exists A\ \mathbf{R}^A \cap \mathbf{Co\text{-}R}^A \not\subseteq \oplus\mathbf{P}^A$
3. $\exists A\ \mathbf{Co\text{-}UP}^A \not\subseteq \oplus\mathbf{IP}^A$
4. $\exists A\ \mathbf{FewP}^A \cap \mathbf{Co\text{-}FewP}^A \not\subseteq \mathbf{UP}^A$
5. $\exists A\ \mathbf{Co\text{-}R}^A \not\subseteq \mathbf{NP}^A$
6. $\exists A\ \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A \not\subseteq \mathbf{PH}^A$
7. $\exists A\ \mathbf{AM}^A \cap \mathbf{co\text{-}AM}^A \not\subseteq \mathbf{PP}^A$
8. $\exists A\ \mathbf{AM}^A \not\subseteq \Sigma_2^A$
9. $\exists A\ \mathbf{PP}^A \not\subseteq \mathbf{PH}^A$
10. $\exists A\ \oplus\mathbf{P}^A \not\subseteq \mathbf{PH}^A$
11. $\exists A\ \oplus\mathbf{P}^A \not\subseteq \mathbf{PP}^A$
12. $\exists A\ \Pi_k^A \not\subseteq \Sigma_k^A$ при $k \ge 3$

Сейчас мы докажем те утверждения из этого списка, доказательство которых не занимает слишком много места, и дадим ссылки на доказательства остальных.

1.

Теорема 7.1. $\exists A\ \mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A \not\subseteq \mathbf{BPP}^A$

Доказательство. Фиксируем некоторую удобную терминологию, которую мы будем использовать в этом и других доказательствах. Пусть $F \in \mathrm{LOGS}(G)$, т.е. для некоторой слабополилогарифмической функции f для всех $\alpha \in D(F)$ выполнено $F(\alpha) = G(f(\alpha))$. Для всех конкретных G, которые мы будем рассматривать, можно считать, что $\|f(\alpha)\|$ зависит только от $\|\alpha\|$ и равно некоторому полиному $p(\|\alpha\|)$ от $\|\alpha\|$. Пусть $P(\alpha, r)$ — полилогарифмический предикат, дающий r-ый бит слова $f(\alpha)$. Тогда слова r из $\mathbf{B}^{p(\|\alpha\|)}$ мы будем называть экспертами (для f и $\|\alpha\|$), а $P(\alpha, r)$ — мнением эксперта r об α.

Фиксируем некоторую машину M, вычисляющую по α, r, где $|r| = p(\|\alpha\|)$, за полилогарифмическое от $|\alpha|$ время значение $P(\alpha, r)$. Будем говорить, что эксперт r спрашивает об $\alpha(u)$ ($u \in \mathbf{B}^{\|\alpha\|}$), если M на входе α, r спрашивает u-ый бит α. Ясно, что для каждого α и $r \in \mathbf{B}^{p(\|\alpha\|)}$ существует не более $\mathrm{poly}(\|\alpha\|)$ таких $u \in \mathbf{B}^{\|\alpha\|}$, что r спрашивает об $\alpha(u)$. Весом u относительно α назовем долю тех экспертов $r \in \mathbf{B}^{p(\|\alpha\|)}$, которые спрашивают об $\alpha(u)$. Вес обозначим $w_\alpha(u)$. Если неясно о каких полиноме p и предикате P идет речь, то будем говорить о весе u относительно α для p, P. Нетрудно доказать общий факт, который мы будем неоднократно использовать: $\sum_{u \in \mathbf{B}^{\|\alpha\|}} w_\alpha(u) \leq q(\|\alpha\|)$, где q — полином, ограничивающий количество вопросов каждого эксперта $r \in \mathbf{B}^{p(\|\alpha\|)}$.

Итак, приступим к доказательству теоремы 7.1. По теореме 3.1, достаточно доказать, что проблема отделения

$$F(\alpha) = \begin{cases} 1, & \text{если } \alpha = \beta\gamma,\ \|\beta\| = \|\gamma\|,\ \#_1(\beta) = 1,\ \#_1(\gamma) = 0, \\ 0, & \text{если } \alpha = \beta\gamma,\ \|\beta\| = \|\gamma\|,\ \#_1(\beta) = 0,\ \#_1(\gamma) = 1, \\ *, & \text{иначе.} \end{cases}$$

не принадлежит **BPPLOGS** (очевидно, что $\mathrm{POLY}^A(F) = \mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A$).

Допустим противное: существуют полином p и полилогарифмический предикат P такие, что $\forall n\ \forall \beta, \gamma \in \mathbf{F}_n$

$$\#_1(\beta) = 1,\ \#_1(\gamma) = 0 \Rightarrow \mathrm{M}_{2/3} r \in \mathbf{B}^{p(n)} P(\beta\gamma, r) = 1$$
$$\#_1(\beta) = 0,\ \#_1(\gamma) = 1 \Rightarrow \mathrm{M}_{2/3} r \in \mathbf{B}^{p(n)} P(\beta\gamma, r) = 0$$

Возьмем в качестве β, γ слова β_0, γ_0 из одних нулей достаточно большой нормы n. Пусть (без ограничения общности) доля r таких, что $P(\beta_0\gamma_0, r) = 1$, больше или равна $1/2$. Будем считать, что биты первой половины β_0 слова $\beta_0\gamma_0$ нумеруются словами вида $0u$, $u \in \mathbf{B}^n$, а биты γ_0 словами вида $1u$. (Этого правила будем придерживаться и в дальнейшем.)

Пусть $k = \mathrm{poly}(n)$ ограничивает количество вопросов, задаваемых экспертами к $\beta_0\gamma_0$.

Тогда $\sum_{u \in \mathbf{B}^n} w_{\beta_0\gamma_0}(1u) \leq k$ поэтому существует такое $u_0 \in \mathbf{B}^n$, что $w_{\beta_0\gamma_0}(1u_0) \leq \frac{k}{2^n} < \frac{1}{6}$ (при достаточно большом n). Обозначим γ_1 слово, имеющее 1 на u_0-ом месте, а остальные — нули. Заменим слово $\beta_0\gamma_0$ на $\beta_0\gamma_1$. При такой замене менее $\frac{1}{6}$ экспертов изменят свое мнение, следовательно, доля r таких, что $P(\beta_0\gamma_1, r) = 1$, больше $\frac{1}{3}$. Поскольку $F(\beta_0\gamma_1) = 0$, получаем противоречие. □

2.

Теорема 7.2. $\exists A\ \mathbf{R}^A \cap \mathbf{Co\text{-}R}^A \not\subseteq \oplus\mathbf{P}^A$

Доказательство. Очевидно многообразие $\mathbf{R}^A \cap \mathbf{Co\text{-}R}^A$ порождается проблемой отделения F, определенной следующим образом: если $\gamma \in \mathbf{F}_1$,

то $F(\gamma) = *$, если $\gamma \in \mathbf{F}_{n+1}$, то обозначим α первую половину γ, а β — вторую. Тогда

$$F(\gamma) = \begin{cases} 0, & \text{если } \#_1(\alpha)=0,\ \#_1(\beta) \geq \frac{1}{2}|\beta|, \\ 1, & \text{если } \#_1(\alpha) \geq \frac{1}{2}|\alpha|,\ \#_1(\beta)=0, \\ *, & \text{иначе.} \end{cases}$$

По теореме 3.1 достаточно доказать, что $F \not\preceq^l_m$ PARITY. Допустим противное: для некоторого полинома p и полилогарифмического предиката P выполнено

$$\forall n\ \forall \gamma \in \mathbf{F}_{n+1}\ F(\gamma) \leq \sum_{r \in \mathbf{B}^{p(n)}} P(\gamma, r).$$

Знаки $\sum$, $+$ в данном доказательстве означают сложение по модулю 2.

Фиксируем достаточно большое n. Пусть $k = \mathrm{poly}(n)$ — количество вопросов к слову γ при вычислении $P(\gamma, r)$. Докажем, что для любого фиксированного $r \in \mathbf{B}^{p(n)}$ $P(\gamma, r)$ является многочленом степени $\leq k$ в поле вычетов по модулю 2 от переменных $\gamma(v), v \in \mathbf{B}^n$. Действительно,

$$P(\gamma, r) = \sum \prod_{i=1}^{k} (\gamma(v(b_1 \cdots b_{i-1}, r)) + b_i + 1),$$

где сумма берется по всем таким $b_1, \ldots, b_k \in \mathbf{B}$, что машина, вычисляющая $P(\gamma, r)$, выдает 1 при условии получения ответов $b_1, \ldots, b_k$ на вопросы к γ, а $v(b_1 \cdots b_i, r) \in \mathbf{B}^{n+1}$ — номер бита γ, о котором спрашивает машина, вычисляющая $P(\gamma, r)$, если ответы на предыдущие вопросы — $b_1 \ldots b_i$.

Из этого следует, что $\sum_{r \in \mathbf{B}^{p(n)}} P(\gamma, r)$ — многочлен степени $\leq k$ от переменных $\gamma(v)$. Обозначим этот многочлен Q. Разобьем переменные $\gamma(v), v \in \mathbf{B}^{n+1}$ на две группы — $\alpha(u), u \in \mathbf{B}^n$ и $\beta(u), u \in \mathbf{B}^n$, задающие соответствующие биты первой и второй половины γ.

Рассмотрим два случая

1й случай: свободный член Q равен нулю. Зафиксируем значения всех переменных $\beta(u)$ равными 0, зафиксируем также значение $\alpha(0^n)$ равным 0. Мы получили многочлен степени $\leq k = \mathrm{poly}(n)$, обозначим его R, от $2^n - 1$ переменной с нулевым свободным членом, который принимает значение 1, если среди значений переменных $\geq 2^{n-1}$ единиц. Выведем противоречие из существования такого многочлена. Рассмотрим множество A всех наборов значений переменных, содержащих ровно 2^{n-1} единиц. Мощность A равна $C^{2^{n-1}}_{2^n-1}$. Докажем, что это число нечетное. Мы будем использовать известный критерий нечетности числа C^l_m.

Лемма 7.2.1. C^l_m нечетно тогда и только тогда, когда любой бит двоичной записи m больше или равен соответствующего бита числа l.

Доказательство. Пусть $i = m - l$. Тогда $C^l_m = \frac{(i+l)!}{i!l!}$. Очевидно, что двойка входит в разложение числа $j!$ с показателем $[\frac{j}{2}] + [\frac{j}{4}] + \ldots$ Поэтому двойка

входит в C_m^l с показателем

$$([\tfrac{i+l}{2}] - [\tfrac{i}{2}] - [\tfrac{l}{2}]) + ([\tfrac{i+l}{4}] - [\tfrac{i}{4}] - [\tfrac{l}{4}]) + \dots$$

Каждая скобка очевидно неотрицательна. При этом $\left[\frac{i+l}{2^s}\right] - \left[\frac{i}{2^s}\right] - \left[\frac{l}{2^s}\right] = 0$ тогда и только тогда, когда при сложении младших s разрядов чисел i и l не происходит переноса в $s+1$ разряд. То есть, C_m^l нечетно, если при сложении i и l столбиком в двоичной системе ни разу не происходит перенос. Лемма доказана. □

По лемме $C_{2^n-1}^{2^{n-1}}$ нечетно. При каждом $\vec{a} \in A$ $R(\vec{a}) = 1$, поэтому $\sum_{\vec{a}\in A} R(\vec{a}) = 1$ ($\vec{a}$ — это кортеж длины $2^n - 1$ из 0 и 1). Возьмем любой моном T из R и докажем, что $\sum_{\vec{a}\in A} T(\vec{a}) = 0$, что даст противоречие. Поскольку свободного члена в R нет, T имеет вид $\alpha(u_1)\cdots\alpha(u_i)$, где $i \geq 1$, $i \leq k$ и $u_1, \dots, u_i$ различны. Докажем, что количество $\vec{a} \in A$, для которых $\forall j \leq i$ $\vec{a}(u_j) = 1$, четно. Очевидно, это количество равно $C_{2^n-1-i}^{2^{n-1}-i}$ (мы предполагаем, что $i < 2^{n-1}$; поскольку $i \leq k = \mathrm{poly}(n)$, при большом n это верно). Рассмотрим самый младший единичный разряд числа i, пусть его номер равен s. Тогда s-ый бит числа $2^n - 1 - i$ равен 0, а s-ый бит числа $2^{n-1} - i$ равен 1. Поэтому по лемме число $C_{2^n-1-i}^{2^{n-1}-i}$ четно.

Осталось рассмотреть второй случай. Он сводится к первому, поскольку можно к Q добавить 1 и положить все $\alpha(u)$ равными 0. Теорема доказана. □

3. $\forall A$ $\mathbf{Co\text{-}UP}^A \not\subseteq \mathbf{IP}^A$.

Это доказано в [8] (формально, там доказывается более слабое утверждение $\exists A$ Co-$\mathbf{NP}^A \not\subseteq \mathbf{IP}^A$). Ввиду простоты, приведем доказательство.

Теорема 7.3. *(Фортноу, Сипсер).* $\exists A$ $\mathbf{Co\text{-}UP}^A \not\subseteq \mathbf{IP}^A$.

Доказательство. По теореме 1 требуется доказать, что проблема отделения

$$F_{\mathbf{Co\text{-}UP}}(\alpha) = \begin{cases} 1, & \text{если } \#_1(\alpha) = 0, \\ 0, & \text{если } \#_1(\alpha) = 1, \\ *, & \text{иначе.} \end{cases}$$

не принадлежит **IPLOG**.

Допустим противное: существует полилогарифмический Проверяющий V такой, что

$$\#_1(\alpha) = 0 \Rightarrow \exists P \ \ \mathrm{Prob}[(P,V)(\alpha) = 1] > \frac{2}{3}$$
$$\#_1(\alpha) = 1 \Rightarrow \forall P \ \ \mathrm{Prob}[(P,V)(\alpha) = 1] < \frac{1}{3},$$

где $(P,V)(\alpha)$ означает ответ, выданный V после обмена сообщениями с P на исходном слове α.

Возьмем большое n и положим $\alpha_0 = 0^{2^n}$. Тогда, по предположению, существует Доказывающий P такой, что $\mathrm{Prob}[(P,V)(\alpha_0)=1] > \frac{2}{3}$.

Рассмотрим работу (P,V) на α_0. Показания случайных датчиков Проверяющего будем называть экспертами, а вопросы заданные Проверяющим к α_0 во время работы P,V на α_0 при показаниях датчиков, равных r, назовем вопросами эксперта r. Весом слова $u \in \mathbf{B}^n$ назовем долю экспертов, задающих вопрос об $\alpha_0(u)$. Очевидно, при большом n существует u с весом $< \frac{1}{3}$. Изменим u-й бит α_0; полученное слово обозначим α_1. Так как $\mathrm{Prob}[(P,V)(\alpha_0)=1] > \frac{2}{3}$, то $\mathrm{Prob}[(P,V)(\alpha_1)=1] > \frac{2}{3} - \frac{1}{3} = \frac{1}{3}$. А по условию требуется, чтобы последняя вероятность была $< \frac{1}{3}$. Противоречие. □

4. $\exists A\ \mathbf{FewP}^A \cap \mathbf{Co\text{-}FewP}^A \not\subseteq \mathbf{UP}^A$. В следующем параграфе мы докажем более сильное утверждение $\exists A\ \mathbf{FewP}^A \cap \mathbf{Co\text{-}FewP}^A \not\leq_T^{p,A} \mathbf{UP}^A$.

5.

Теорема 7.4. $\exists A\ \mathbf{Co\text{-}R}^A \not\subseteq \mathbf{NP}^A$

Доказательство. Допустим противное: существует такой полином p полилогарифмический предикат $P(\alpha, r)$, что $\forall \alpha \in \mathbf{F}$

$$\begin{aligned} \#_1(\alpha) = 0 \quad &\Rightarrow \quad \exists r \in \mathbf{B}^{p(\|\alpha\|)} P(\alpha, r) = 1 \\ \#_1(\alpha) > \frac{2}{3}|\alpha| \quad &\Rightarrow \quad \forall r \in \mathbf{B}^{p(\|\alpha\|)} P(\alpha, r) = 0 \end{aligned}$$

Найдем такое α, что $\#_1(\alpha) > \frac{2}{3}|\alpha|$ и $\exists r \in \mathbf{B}^{p(\|\alpha\|)} P(\alpha, r)$. Возьмем $\alpha_0 = 0^{2^n}$, где n достаточно большое. Тогда для некоторого $r_0 \in \mathbf{B}^{p(n)}$ выполнено $P(\alpha_0, r_0)$. Изменим все биты α_0, про которые в вычислении $P(\alpha_0, r_0)$ не задано вопроса. Получим искомое слово α. Теорема доказана. □

6. В [1] доказано, что $\exists A \quad \mathbf{IP}^A \not\subseteq \mathbf{PH}^A$. Сделав в доказательстве несущественные изменения, можно доказать, что существует такой оракул A, что $\mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A \not\subseteq \mathbf{PH}^A$.

7. $\exists A\ \mathbf{AM}^A \cap \mathbf{co\text{-}AM}^A \not\subseteq \mathbf{PP}^A$. Это доказано автором в [26].

8. $\exists A\ \mathbf{AM}^A \not\subseteq \Sigma_2^A$. Это доказано в [21].

9. $\exists A\ \mathbf{PP}^A \not\subseteq \mathbf{PH}^A$. Это следует из того, что функция $\mathrm{MAJORITY}(x_1, \ldots, x_n)$ не представима в виде

$$\bigvee_{i_1=1}^{2^{\mathrm{polylog}(n)}} \bigwedge_{i_2=1}^{2^{\mathrm{polylog}(n)}} \cdots \bigvee_{i_{2k-1}=1}^{2^{\mathrm{polylog}(n)}} \bigwedge_{i_{2k}=1}^{2^{\mathrm{polylog}(n)}} f_{i_1 \ldots i_{2k}}(x_1, \ldots, x_n),$$

где $f_{i_1 \cdots i_{2k}}(x_1, \ldots, x_n)$ — это переменная или отрицание переменной, ни для какого фиксированного $k \in \mathbf{N}$ ([9], [2], [27], [13]).

10. $\exists A\ \oplus \mathbf{P}^A \not\subseteq \mathbf{PH}^A$. Это доказано в [9], [2], [27], [13].

11. $\exists A\ \oplus \mathbf{P}^A \not\subseteq \mathbf{PP}^A$. Это следует из доказанного в работе [19]. утверждения, что $\mathrm{PARITY} \not\leq_m^l \mathrm{MAJORITY}$. В оракульном виде теорема впервые появилась в [6].

12. $\forall k \geq 3\ \exists A\ \Pi_k^A \not\subseteq \Sigma_k^A$. Первые сверхполиномиальные нижние оценки на размер Σ_k-схем, требуемых для вычисления Π_k-функций, были получены Сипсером. Необходимая для наших целей оценка $(2^{f(n)})$, где f растет выстрее любого полилогарифма, была получена в работе [13].

8. Тьюрингова сводимость сложностных классов

В этом параграфе мы приведем все известные релятивизуемые утверждения о сводимости по Тьюрингу одного сложностного класса к другому. Очевидно, что если $K_1 \subseteq K_2$, то $K_1 \leq_T^p K_2$, поэтому все включения рисунка 1 дают также и соответствующие сводимости, Перечислим остальные известные случаи $\leq_T^p$-сводимости.

1) Классы K и Co-K $\leq_T^p$-сводятся друг к другу

2) $\oplus\mathbf{P}^A \leq_T^p \mathbf{PP}^A$

3) $\mathbf{Few}^A \leq_T^p \mathbf{NP}^A$

4) $\mathbf{PH}^A \leq_T^p \mathbf{PP}^A$ Утверждение 1) очевидно. Утверждения 2) и 3) тоже довольно просты; утверждение 3) было доказано в параграфе 7, а утверждение 2) мы сейчас докажем. Утверждение 4) сложное, оно доказано в работе [25].

Теорема 8.1. $\oplus\mathbf{P}^A \leq_T^p \mathbf{PP}^A$ *для всех оракулов* A.

Доказательство. По теореме 5.1 достаточно доказать, что язык $\mathrm{PARITY}(\alpha)$ $\preceq_T^l$-сводится к языку

$$\mathrm{MAJORITY}(\alpha) = \begin{cases} 1, & \text{если } \#_1(\alpha) \geq \frac{1}{2}|\alpha|, \\ 0, & \text{иначе.} \end{cases}$$

При доказательстве того, что одна проблема F $\preceq_T^l$-сводится или не $\preceq_T^l$-сводится к другой проблеме G удобно представлять себе сводящую пару $\langle M, f\rangle$ как машину, работающую на исходном данном α так же, как M на входе $|\alpha|$, и задающую вопросы не к оракулу $G(f(\cdot,\alpha))$ а к оракулу G (в тот момент, когда M задает оракулу вопрос о его значении на слове y, эта новая машина задает G вопрос о значении на слове $f(y,\alpha)$). Определим пару $\langle M, f\rangle$, сводящую PARITY к MAJORITY, объяснив как работает эта новая машина.

Имея MAJORITY в качестве оракула, можно по α за время $\mathrm{polylog}(|\alpha|)$ найти $\#_1(\alpha)$ следующим образом. Пусть $|\alpha| = 2^k$. Сначала спрашиваем у MAJORITY, верно ли, что $\#_1(\alpha) \geq \frac{1}{2}|\alpha|$. Допустим это верно. Тогда выясняем, верно ли, что $\#_1(\alpha) \geq \frac{3}{4}|\alpha|$. Для этого берем слово β из $\frac{1}{2}|\alpha|$ нулей и спрашиваем верно ли, что $\#_1(\alpha\beta) \geq \frac{1}{2}|\alpha\beta|$. Нетрудно проверить, что это неравенство равносильно неравенству $\#_1(\alpha) \geq \frac{3}{4}|\alpha|$. После повторения

этого процесса k раз мы найдем $\#_1(\alpha)$. Теперь выдаем ответ 1 если $\#_1(\alpha)$ нечетно и 0, иначе. Теорема доказана. □

Таким образом картинка известных $\leq_T^p$-сводимостей выглядит так, как это показано на рисунке. Неизвестно, все ли имеющиеся утверждения о $\leq_T^{p,A}$-сводимости указаны на рисунке. Для того, чтобы доказать точность рисунка, необходимо и достаточно доказать следующие 14 утверждений.

1. $\exists A\ \mathbf{R}^A \cap \mathbf{Co\text{-}R}^A \not\leq_T^{p,A} \oplus\mathbf{P}^A$. Это следует из замкнутости класса $\oplus\mathbf{P}^A$ относительно $\leq_T^{p,A}$-сводимости и того, что $\exists A\ \mathbf{R}^A \cap \mathbf{Co\text{-}R}^A \not\subseteq \oplus\mathbf{P}^A$. Замкнутость $\oplus\mathbf{P}^A$ относительно $\leq_T^A$-сводимости доказана в работе [25].

2. $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A \not\leq_T^{p,A} \mathbf{BPP}^A$. Это верно и следует из того, что класс $\mathbf{BPP}^A$ замкнут относительно $\leq_T^{p,A}$-сводимости (при всех A), поэтому сводимость в данном случае эквивалентна включению, а в предыдущем параграфе было доказано, что существует оракул A, для которого $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A \not\subseteq \mathbf{BPP}^A$.

3. $\exists A\ \mathbf{FewP}^A \cap \mathbf{Co\text{-}FewP}^A \not\leq_T^{p,A} \mathbf{UP}^A$. Это верно и будет доказано в этом параграфе.

4. $\exists A\ \mathbf{R}^A \not\leq_T^{p,A} \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$. Это верно и следует из замкнутости $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ относительно $\leq_T^{p,A}$-сводимости и того, что $\exists A\ \mathbf{R}^A \not\subseteq \mathbf{Co\text{-}NP}^A$.

5. $\exists A\ \mathbf{UP}^A \not\leq_T^{p,A} \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A$. Это верно и следует из того, что $\mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A$ замкнут относительно $\leq_T^{p,A}$-сводимости и того, что $\exists A\ \mathbf{UP}^A \not\subseteq \mathbf{Co\text{-}IP}^A$.

6. $\exists A\ \Sigma_2^A \cap \Pi_2^A \not\leq_T^{p,A} \mathbf{IP}^A$. Это верно и будет доказано в параграфе 9.

7. $\exists A\ \mathbf{BPP}^A \not\leq_T^{p,A} \mathbf{NP}^A$. Это верно и будет доказано в параграфе 9.

8. $\exists A\ \oplus\mathbf{P}^A \not\leq_T^{p,A} \mathbf{PH}^A$. Это верно и следует из замкнутости класса $\mathbf{PH}^A$ относительно $\leq_T^{p,A}$-сводимости (замыкание Σ_k включено в Σ_{k+1}) и того, что $\exists A\ \oplus\mathbf{P}^A \not\subseteq \mathbf{PH}^A$.

9. $\exists A\ \mathbf{AM}^A \not\leq_T^{p,A} \Sigma_2^A \cap \Pi_2^A$. Это верно и следует из замкнутости $\Sigma_2^A \cap \Pi_2^A$ относительно $\leq_T^{p,A}$-сводимости и того, что $\exists A\ \mathbf{AM}^A \not\subseteq \Sigma_2^A$.

10. $\exists A\ \mathbf{AM}^A \cap \mathbf{co\text{-}AM}^A \not\leq_T^{p,A} \mathbf{MA}^A$. Это верно и доказано совместно Ан. А. Мучником и автором. Доказательство приводится в этом параграфе.

11. $\exists A\ \oplus\mathbf{P}^A \not\leq_T^{p,A} \mathbf{IP}^A$. Это верно и доказано в параграфе 9.

12. $\exists A\ \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A \not\leq_T^{p,A} \mathbf{PP}^A$. Верно ли это, неизвестно.

13. $\exists A\ \Sigma_k^A \cap \Pi_k^A \not\leq_T^{p,A} \Sigma_{k-1}^A$ $(k \geq 3)$. Верно ли это, неизвестно.

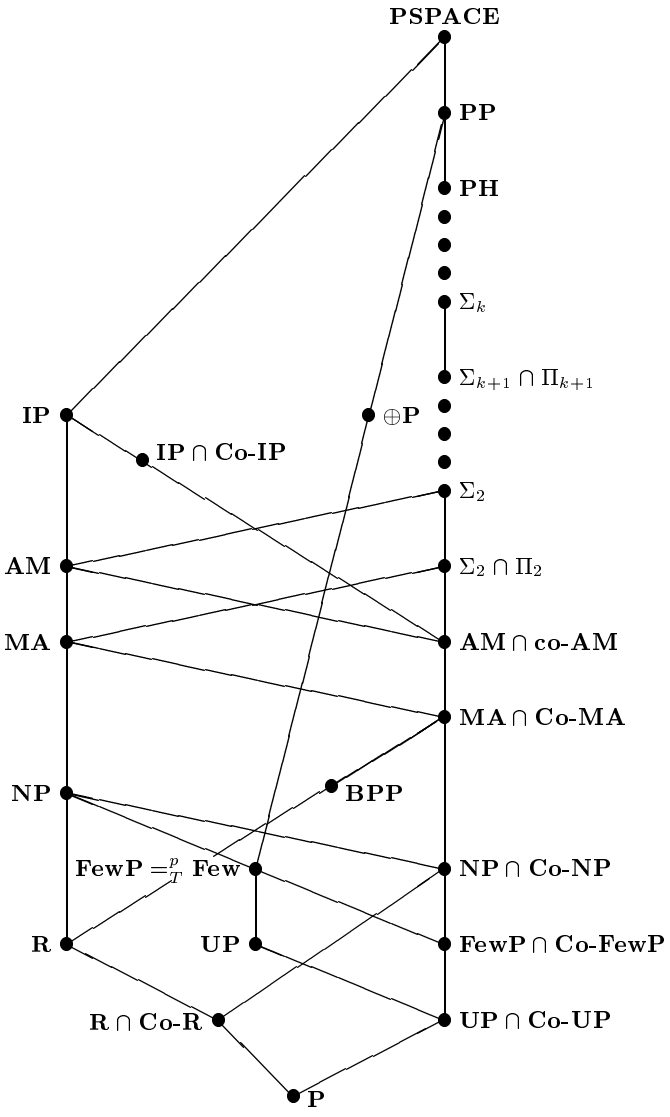
14. $\exists A\ \Sigma_k^A \not\leq_T^{p,A} \Sigma_k^A \cap \Pi_k^A$ $(k \geq 3)$. Это верно и следует из замкнутости класса $\Sigma_k^A \cap \Pi_k^A$ относительно $\leq_T^{p,A}$-сводимости и того, что $\exists A\ \Sigma_k^A \not\subseteq \Pi_k^A$.

15. $\exists A\ \mathbf{PH}^A \not\leq_T^{p,A} \Sigma_k^A$ $(k \geq 1)$. Это верно и следует из 14.

Сейчас мы докажем утверждения 3 и 10.

Теорема 8.2. *(Получена совместно с Ан. А. Мучником)* $\exists A\ \mathbf{AM}^A \cap \mathbf{co\text{-}AM}^A \not\leq_T^{p,A} \mathbf{MA}^A$.

Рис. 2. Тьюрингова сводимость сложностных классов



Доказательство. Рассмотрим проблему отделения F, определенную следующим образом. Для $\alpha = \beta\gamma$, где $\beta, \gamma \in \mathbf{F}_{2n}, n \in \mathbf{N}$

$$F(\alpha) = \begin{cases} 1, & \text{если } \mathrm{M}_{2/3}x \in \mathbf{B}^n\ \exists y \in \mathbf{B}^n\ \beta(xy) = 1, \\ & \qquad \mathrm{M}_{2/3}x \in \mathbf{B}^n\ \forall y \in \mathbf{B}^n\ \gamma(xy) = 0, \\ 0, & \text{если } \mathrm{M}_{2/3}x \in \mathbf{B}^n\ \forall y \in \mathbf{B}^n\ \beta(xy) = 0, \\ & \qquad \mathrm{M}_{2/3}x \in \mathbf{B}^n\ \exists y \in \mathbf{B}^n\ \gamma(xy) = 1, \\ *, & \text{иначе.} \end{cases}$$

По теореме 5.1 достаточно доказать, что F не $\preceq^l_T$-сводится к проблеме отделения $F_{\mathbf{MA}}$. Напомним, что $F_{\mathbf{MA}}(\beta) \neq *$ только если норма β четна, и при $\|\beta\| = 2k$

$$F_{\mathbf{MA}}(\beta) = \begin{cases} 1, & \text{если } \exists r \in \mathbf{B}^k\ \mathrm{M}_{2/3}s \in \mathbf{B}^k\ \beta(rs) = 1, \\ 0, & \text{если } \forall r \in \mathbf{B}^k\ \mathrm{M}_{2/3}s \in \mathbf{B}^k\ \beta(rs) = 0, \\ *, & \text{иначе.} \end{cases}$$

Для проблемы $F_{\mathbf{MA}}$ и всех остальных конкретных проблем G, рассматриваемых в работе, выполнено следующее. Для любой проблемы H, если $H \preceq^l_T G$, то существует сводящая пара $\langle M, f\rangle$ такая, что 1) количество вопросов M к оракулу на входе n не зависит от ответов оракула и равно некоторому полилогарифму от n и 2) для всех вопросов u, задаваемых M к своему оракулу B при работе на входе $|\alpha|$, длина слова $f(u, \alpha)$ одна и та же и зависит только от $|\alpha|$. То есть, при интерпретации $\langle M, f\rangle$ как одной машины, все вопросы, задаваемые ей к G на входе α, имеют одну длину, зависящую только от $|\alpha|$. Будем впредь считать, что сводящая пара $\langle M, f\rangle$ удовлетворяет условиям 1) и 2).

Допустим $F \preceq^l_T F_{\mathbf{MA}}$ посредством сводящей пары $\langle M, h\rangle$. Зафиксируем достаточно большое n (насколько большое будет видно в конце). Пусть φ — частичная функция из $\mathbf{B}^n$ в $\mathbf{B}^n$. Обозначим через $\bar\varphi$ слово длины 2^{2n}, кодирующее график φ. То есть, для $x, y \in \mathbf{B}^n, \bar\varphi(xy)$ равно 1, если $y = \varphi(x)$, и равно 0, иначе. Будем рассматривать в качестве аргументов проблемы отделения F слова вида $\bar\varphi\bar\psi$, где φ и ψ частичные функции из $\mathbf{B}^n$ в $\mathbf{B}^n$.

Пусть $m = \mathrm{poly}(n)$ — количество вопросов, задаваемых M к оракулу на входе 2^{2n+1}. Мы построим последовательность нулей и единиц $b_1, \ldots, b_m$, частичные функции $\varphi, \psi : \mathbf{B}^n \to \mathbf{B}^n$ и всюду определенные функции $f_0, g_0 : \mathbf{B}^n \to \mathbf{B}^n$ такие, что последовательность ответов оракула $F_{\mathbf{MA}}$ при работе (M, h) на входе $\bar f_0\bar\psi$ и на входе $\bar\varphi\bar g_0$ равна $b_1, \ldots, b_m$. Мощности областей определения φ и ψ будут ограничены полиномом от n, поэтому при большом n будет выполнено $|\mathrm{Dom}(\varphi)|, |\mathrm{Dom}(\psi)| < \frac{1}{3}2^n$. Очевидно, мы получим противоречие с тем, что (M, h) сводит F к $F_{\mathbf{MA}}$, поскольку $F(\bar f_0\bar\psi) = 1$, $F(\bar\varphi\bar g_0) = 0$.

Обозначим через $2k$ норму вопросов, задаваемых парой $\langle M, h\rangle$ к оракулу $F_{\mathbf{MA}}$ при работе на входах нормы $2n + 1$ ($k \in \mathbf{N}$, $k \leq \mathrm{poly}(n)$). Определим

на словах нормы $2k$ вспомогательную проблему отделения

$$G(\beta) = \begin{cases} 1, & \text{если } \exists r \in \mathbf{B}^k \ \mathrm{M}_{1/2} s \in \mathbf{B}^k \ \beta(rs) = 1, \\ 0, & \text{иначе.} \end{cases}$$

Очевидно, G продолжает $F_{\mathbf{MA}}$.

Возьмем произвольные функции $f, g : \mathbf{B}^n \to \mathbf{B}^n$. Запустим машину M на входе 2^{2n+1} с оракулом $G(h(\cdot, \bar{f}\bar{g}))$. Обозначим $e(f,g)$ последовательность ответов оракула. Поскольку длина $e(f,g)$ равна m, существует слово e_0 длины m такое, что для по крайней мере $\frac{1}{2^m}$ -ой доли всех пар (f,g) выполнено $e(f,g) = e_0$. Обозначим множество таких пар (f,g), что $e(f,g) = e_0$, через $\mathcal{K}$. Ясно, что для всех $(f,g) \in \mathcal{K}$ вопросы, задаваемые M к оракулу $G(h(\cdot, \bar{f}\bar{g}))$, будут одни и те же, обозначим их через $v_1, \ldots, v_m$. Пусть $P(\alpha, v, u)$ обозначает u-ый символ слова $h(v, \alpha)$, ($\alpha \in \mathbf{F}_{2n+1}$, $u \in \mathbf{B}^{2k}$. Обозначим биты e_0 через $b_1, \ldots, b_m$.

Для каждого $i \leq m$ такого, что $b_i = 1$, для всех $(f,g) \in \mathcal{K}$ найдется $r_i \in \mathbf{B}^k$ такое, что $\mathrm{M}_{1/2} s \in \mathbf{B}^k \ P(\bar{f}\bar{g}, v_i, r_i s) = 1$. Опять можно найти такое $\mathcal{K}' \subseteq \mathcal{K}$, что для всех i таких, что $b_i = 1$, для всех $(f,g) \in \mathcal{K}'$ это r_i одно и то же, и $\frac{|\mathcal{K}'|}{|\mathcal{K}|} \geq \frac{1}{2^{km}}$. Доля $\mathcal{K}'$ среди всех пар $\geq \frac{1}{2^{km+m}}$. Обозначим $\frac{1}{2^{km+m}}$ через ε. Будем представлять себе $\mathcal{K}'$ как плоское множество (площади $\geq \varepsilon$). Ясно, что существуют вертикальное сечение множества $\mathcal{K}'$ длины $\geq \varepsilon$ и горизонтальное сечение множества $\mathcal{K}'$ длины $\geq \varepsilon$. Т.е., существуют такие функции f_0, g_0 и семейства функций $\mathcal{F}'$ и $\mathcal{G}'$, что $|\mathcal{F}'| \geq \varepsilon 2^{(n \cdot 2^n)}$, $|\mathcal{G}'| \geq \varepsilon 2^{(n \cdot 2^n)}$, $\{f_0\} \times \mathcal{G}' \subseteq \mathcal{K}'$, $\mathcal{F}' \times \{g_0\} \subseteq \mathcal{K}'$.

Теперь определим частичную функцию φ и семейство $\mathcal{F}$ всюду определенных функций. Сначала положим $\varphi = \emptyset$, $\mathcal{F} = \mathcal{F}'$. Пусть $x, y \in \mathbf{B}^n$, обозначим *популярность*$_{\mathcal{F}}(x,y)$ долю тех $f \in \mathcal{F}$, для которых $f(x) = y$. Тогда мы делаем следующее. Пока существует хотя бы одна пара $(x,y) \in (\mathbf{B}^n \setminus \mathrm{Dom}(\varphi)) \times \mathbf{B}^n$ такая, что *популярность*$_{\mathcal{F}}(x,y) \geq 2^{-n+1}$, мы выбираем любую такую пару, доопределяем φ на x, положив $\varphi(x) = y$, и выбрасываем из $\mathcal{F}$ все функции f, для которых $f(x) \neq y$.

Получившиеся $\varphi, \mathcal{F}$ и суть искомые. Мы утверждаем, что они обладают следующими свойствами

1) $\mathcal{F} \subseteq \mathcal{F}'$,

2) все функции из $\mathcal{F}$ продолжают φ,

3) $\forall (x,y) \in (\mathbf{B}^n \setminus \mathrm{Dom}(\varphi)) \times \mathbf{B}^n$ популярность$_{\mathcal{F}}(x,y) < 2^{-n+1}$,

4) $|\mathrm{Dom}(\varphi)| \leq -\log_2(\text{доля } \mathcal{F}') \leq km + m = \mathrm{poly}(n)$.

Свойства 1)-3) очевидны. Докажем 4). При каждом доопределении φ на очередное x доля $\mathcal{F}$ среди всех функций, продолжающих φ, увеличивалась по крайней мере вдвое, поскольку количество элементов в $\mathcal{F}$ уменьшалось не более чем в 2^{n-1} раз, а количество функций, продолжающих φ уменьшалось ровно в 2^n раз. Поскольку доля не может стать больше 1, количество шагов доопределения не превосходит минус логарифма доли $\mathcal{F}'$ среди всех функций из $\mathbf{B}^n$ в $\mathbf{B}^n$.

Эту же процедуру применим к $\mathcal{G}'$ и получим $\mathcal{G}, \psi$.

Докажем, что для всех $i \le m$

$$F_{\mathbf{MA}}(h(v_i, \bar{\varphi}\bar{g}_0)) = b_i.$$

Возьмем произвольное $i \le m$. Рассмотрим два случая

1-й случай: $b_i = 1$. Тогда нам известно, что

$$\mathrm{M}_{1/2} s \in \mathbf{B}^k \ P(fg_0, v_i, r_i s) = 1 \qquad (+)$$

для всех $f \in \mathcal{F}$. По определению $\preceq_T^l$-сводимости, $F_{\mathbf{MA}}(h(v_i, \bar{\varphi}\bar{g}_0)) \ne *$ (если n настолько большое, что $|\operatorname{Dom}(\varphi)| < \frac{1}{3}2^n$). Допустим $F_{\mathbf{MA}}(h(v_i, \bar{\varphi}\bar{g}_0)) = 0$. Тогда

$$\mathrm{M}_{2/3} s \in \mathbf{B}^k \ P(\bar{\varphi}\bar{g}_0, v_i, r_i s) = 0. \qquad (++)$$

Пусть N — это машина, которая по $\alpha \in \mathbf{F}, v \in \mathbf{B}^*, u \in \mathbf{B}^{\|\alpha\|}$ за время $\mathrm{poly}(|v| + \|\alpha\|)$ вычисляет $P(\alpha, v, u)$. Если α имеет вид $\bar{\eta}\bar{\theta}$, где η, θ — частичные функции из $\mathbf{B}^n$ в $\mathbf{B}$, то вопросы, задаваемые N к α, являются вопросами о принадлежности пар $(x, y), x, y \in \mathbf{B}^n$ к графику η или θ, то есть имеют вид «$\eta(x) = y$?» и «$\theta(x) = y$?». Обозначим для $x, y \in \mathbf{B}^n$ через $w_{\varphi g_0}(x, y)$ долю тех $s \in \mathbf{B}^n$, для которых N на входе $(\bar{\varphi}\bar{g}_0, v_i, r_i s)$ задает вопрос «$\varphi(x) = y$?». Ясно, что $\sum_{x,y \in \mathbf{B}^n} w_{\varphi g_0}(x, y) \le \mathrm{poly}(n)$. Тогда для любой $f \in \mathcal{F}$ из $(+)$ и $(++)$ следует

$$\sum_{x \in \mathbf{B}^k \setminus \operatorname{Dom}\varphi} w_{\varphi g_0}(x, f(x)) \ge \frac{1}{6}, \text{ следовательно}$$

$$\frac{1}{|\mathcal{F}|} \sum_{f \in \mathcal{F},\ x \in \mathbf{B}^k \setminus \operatorname{Dom}\varphi} w_{\varphi g_0}(x, f(x)) \ge \frac{1}{6}.$$

Левую часть этого неравенства можно преобразовать так:

$$\frac{1}{|\mathcal{F}|} \sum_{f \in \mathcal{F},\ x \in \mathbf{B}^k \setminus \operatorname{Dom}\varphi} w_{\varphi g_0}(x, f(x)) =$$

$$= \sum_{x \in \mathbf{B}^k \setminus \operatorname{Dom}\varphi,\ y \in \mathbf{B}^k} w_{\varphi g_0}(x, y) \cdot \textit{популярность}_{\mathcal{F}}(x, y) \le$$

$$\le 2^{-n+1} \sum_{x \in \mathbf{B}^k \setminus \operatorname{Dom}\varphi,\ y \in \mathbf{B}^k} w_{\varphi g_0}(x, y) \le 2^{-n+1}\mathrm{poly(n)}.$$

При достаточно большом n мы получим противоречие $2^{-n+1}\mathrm{poly}(n) \ge \frac{1}{6}$.

2-й случай $b_i = 0$. Тогда нам известно, что для всех $r \in \mathbf{B}^k$ для всех $f \in \mathcal{F}$ доля тех $s \in \mathbf{B}^k$, для которых $P(\bar{f}\bar{g}_0, v_i, rs) = 0$ меньше или равна $\frac{1}{2}$. Допустим $F_{\mathbf{MA}}(h(v_i, \bar{\varphi}\bar{g}_0)) = 1$, то есть найдется такое $r \in \mathbf{B}^k$, что

$$\mathrm{M}_{2/3} s \in \mathbf{B}^k \ P(\bar{\varphi}\bar{g}_0, v_i, rs) = 1$$

Тогда точно так же, как в первом случае мы получим противоречие.

Аналогично можно доказать, что $\forall i \leq m$

$$F_{\mathbf{MA}}(h(v_i, \bar{f}_0\bar{\psi})) = b_i.$$

Теорема доказана. □

Теорема 8.3. *Существует такой оракул A, что* $\mathbf{FewP}^A \cap \mathbf{Co\text{-}FewP}^A \not\leq_T^{p,A} \mathbf{UP}^A$.

Доказательство. Чтобы продемонстрировать метод, докажем сначала, что для некоторого оракула не выполнено включение. Определим проблему отделения F на словах $\beta\gamma$ с $\|\beta\| = \|\gamma\|$ так

$$F(\beta\gamma) = \begin{cases} 1, & \text{если } 1 \leq \#_1(\beta) \leq 2,\ \#_1(\gamma) = 0, \\ 0, & \text{если } 1 \leq \#_1(\gamma) \leq 2,\ \#_1(\beta) = 0, \\ *, & \text{иначе.} \end{cases}$$

По теореме 3.1, достаточно доказать, что $F \notin \mathbf{UPLOGS}$. Допустим противное: существует полином p и полилогарифмический предикат P такие, что

$$F(\beta\gamma) = 1 \Longrightarrow \exists! r \in \mathbf{B}^{p(\|\beta\|)}\ P(\beta\gamma, r) = 1$$
$$F(\beta\gamma) = 0 \Longrightarrow \forall r \in \mathbf{B}^{p(\|\beta\|)}\ P(\beta\gamma, r) = 0$$

Возьмем $\beta_0 = \gamma_0 = 0^{2^n}$, где n — достаточно большое натуральное число. Рассмотрим 2 случая

I случай: $\exists r \in \mathbf{B}^{p(n)}\ P(\beta_0\gamma_0, r) = 1$.

Выберем одного такого эксперта r_0, что $P(\beta_0\gamma_0, r_0) = 1$. При достаточно большом n существует такое $u \in \mathbf{B}^n$, что r_0 не спрашивает $\gamma_0(u)$. Сделав $\gamma_0(u)$ равным единице, получим противоречие.

II случай: $\forall r\ P(\beta_0\gamma_0, r) = 0$.

Докажем, что если n достаточно большое, то существует такое $\beta_1 \in \mathbf{F}_n$, что $\#_1(\beta_1) = 2$ и $|\{r \in \mathbf{B}^{p(n)} :\ P(\beta_1\gamma_0, r) = 1\}| \geq 2$. Для каждого $u \in \mathbf{B}^n$ обозначим β_0^u слово, в котором ровно одна 1 на u-ом месте. Для всех u $F(\beta_0^u\gamma_0) = 1$, следовательно, $\forall u \in \mathbf{B}^n\ \exists! r \in \mathbf{B}^{p(n)}\ P(\beta_0^u\gamma_0, r) = 1$. Обозначим это r через r_u. Определим 1-базу u как множество всех таких $v \in \mathbf{B}^n$, что эксперт r_u при работе на входе β_0^u спрашивает $\beta_0^u(v)$, а 0-базу u — как множество всех таких $v \in \mathbf{B}^n$, что эксперт r_u при работе на входе β_0 спрашивает $\beta_0(v)$. Обозначим базы соответственно $B_1(u)$ и $B_0(u)$.

Докажем, что при достаточно большом n существуют такие $u_1, u_2 \in \mathbf{B}^n$, что $u_1 \notin B_0(u_2) \cup B_1(u_2)$, $u_2 \notin B_1(u_1)$. Действительно, мощность базы ограничена полиномом от n, скажем $q(n)$. Возьмем случайные u_1, u_2 (независимые и равномерно распределенные). Мы имеем

$$\mathrm{Prob}[u_1 \in B_0(u_2)] \leq \frac{q(n)}{2^n},$$

$$\mathrm{Prob}[u_1 \in B_1(u_2)] \le \frac{q(n)}{2^n},$$
$$\mathrm{Prob}[u_2 \in B_1(u_1)] \le \frac{q(n)}{2^n}.$$

Поэтому с вероятностью близкой к 1 все три события не происходят.

Зафиксируем такие u_1, u_2, что $u_1 \notin B_0(u_2) \cup B_1(u_2)$, $u_2 \notin B_1(u_1)$. Определим β_1 следующим образом: $\beta_1(u_1) = \beta_1(u_2) = 1$ и $\beta_1(v) = 0$ при $v \neq u_1, u_2$. Тогда $\beta_1\gamma_0 \in D(F)$ и $P(\beta_1\gamma_0, r_{u_1}) = P(\beta_1\gamma_0, r_{u_2}) = 1$ (поскольку $u_2 \notin B_1(u_1)$, $u_1 \notin B_1(u_2)$). Кроме того, $r_{u_1} \neq r_{u_2}$ т.к. $P(\beta_0^{u_1}\gamma_0, r_{u_1}) = 1$, $P(\beta_0^{u_1}\gamma_0, r_{u_2}) = 0$ (поскольку $u_1 \notin B_0(u_2)$). Противоречие.

Теперь докажем, что $F \not\preceq_T^l F_{\mathbf{UP}}$. Напомним, что

$$F_{\mathbf{UP}}(\alpha) = \begin{cases} 1, & \text{если } \#_1(\alpha) = 1, \\ 0, & \text{если } \#_1(\alpha) = 0, \\ *, & \text{иначе.} \end{cases}$$

Допустим F сводится к $F_{\mathbf{UP}}$ посредством пары $\langle M, f\rangle$. По определению сводимости

$$\forall \alpha \in D(F)\ \forall e \in \mathbf{B}^*\ \#_1(f(e,\alpha)) \in \{0,1\} \qquad (+)$$

Зафиксируем $n \in \mathbf{N}$ и положим $\alpha_0 = 0^{2^{n+1}}$. Обозначим $D_1 = \{\alpha \in \mathbf{F}_{n+1} : \#_1(\alpha) = 1\}$. Ясно, что $D_1 \subseteq D(F)$. Мы построим множество $U \subseteq \mathbf{B}^{n+1}$ мощности poly(n) такое, что для всех α из D_1 равных нулю на U, последовательность ответов оракула $F_{\mathbf{UP}}$ при работе $\langle M, f\rangle$ на α одна и та же. Обозначим m — количество вопросов, задаваемых M к оракулу при работе на входе 2^{n+1}. Определим последовательность $b_1, \ldots, b_m$ нулей и единиц и последовательность $v_1, \ldots, v_m$ слов рекуррентным правилом: v_i — это вопрос, задаваемый машиной M к оракулу на входе 2^{n+1} при получении ответов $b_1, \ldots, b_{i-1}$ на предыдущие вопросы;

$$b_i = \begin{cases} 1, & \text{если } \#_1(f(v_i, \alpha_0)) \ge 1, \\ 0, & \text{иначе.} \end{cases}$$

Мы определим U так, чтобы для всех $\alpha \in D_1$, равных нулю на U, для всех i было выполнено $F_{\mathbf{UP}}(f(v_i, \alpha)) = b_i$. Множество U будет равно $\bigcup_{j=1} U_j$, где U_j будет обеспечивать выполнение указанного свойства для $i = j$.

Итак, зафиксируем $i \le m$ и построим U_i. По определению сводимости $\preceq_T^l$ существует машина N такая, что N на входе (α, v_i, r), где $|r| = \|f(v_i, \alpha)\|$, выдает r-ый бит слова $f(v_i, \alpha)$ за полилогарифмическое от $|\alpha|$ время.

Рассмотрим два случая

I случай: $b_i = 1$, т.е. $\#_1(f(v_i, \alpha_0)) \ge 1$. Выберем любое такое r, что $f(v_i, \alpha_0)(r) = 1$. Занесем в U_i все такие $u \in \mathbf{B}^n$, что в вычислении $N(\alpha_0, v_i, r)$ задается вопрос «$\alpha_0(u) =?$». Тогда для всех $\alpha \in \mathbf{F}_{n+1}$, равных нулю на U_i

будет выполнено $\#_1(f(v_i,\alpha)) \geq 1$, и в силу (+) для всех $\alpha \in D_1$, равных нулю на U_i, будет выполнено $\#_1(f(v_i,\alpha)) = 1$.

II случай: $\#_1(f(v_i,\alpha_0)) = 0$. Обозначим $\beta_0 = \gamma_0 = 0^{2^n}$. Вообще, будем использовать обозначения первой части доказательства. Докажем, что для всех $u \in \mathbf{B}^n$ за исключением полинома слов выполнено $\#_1(f(v_i,\beta_0^u\gamma_0)) = 0$. Обозначим множество u, для которых это не выполнено, через V. Докажем, что $|V| \leq 3q(n)$, где $q(n)$ — полином, ограничивающий количество вопросов вида «$\alpha_0(v) =?$» в вычислении $N(\alpha_0, v_i, r)$, при $|r| = \|f(v_i,\alpha_0)\|$. Допустим противное: $|V| > 3q(n)$. Для каждого $u \in V$ обозначим через r_u такое слово r, что r-ый бит слова $f(v_i,\beta_0^u\gamma_0)$ равен 1. Определим $B_0(u)$ (соответственно $B_1(u)$) как множество таких v, что в вычислении $N(\alpha_0, v_i, r_u)$ (соответственно, $N(\beta_0^u\gamma_0, v_i, r_u)$) задается вопрос «$\alpha_0(v) =?$» (соответственно, «$\beta_0^u\gamma_0(v) =?$»). Тогда для всех $u \in V$ выполнено $|B_0(u)|, |B_1(u)| \leq q(n)$. Поэтому для случайных независимых u_1, u_2, распределенных равномерно в V, вероятность события $[u_1 \notin B_0(u_2) \cup B_1(u_2), u_2 \notin B_1(u_1)]$ не меньше $1 - \frac{3q(n)}{|V|} > 0$. Как и в первой части доказательства строим слово β_1 ровно с двумя единицами такое, что $\#_1(f(v_i,\beta_1\gamma_0)) \geq 2$, что противоречит (+).

Заносим в U_i все слова из V. Аналогично поступаем со второй половиной слова α_0.

Если n настолько большое, что $2^n > |U|$, то в D_1 будут существовать два слова α_1, α_2 такие, что $F(\alpha_1) = 1$, $F(\alpha_2) = 0$ и α_1, α_2 равны нулю на U, следовательно, $\langle M, f\rangle^{F\mathbf{UP}}(\alpha_1) = \langle M, f\rangle^{F\mathbf{UP}}(\alpha_2)$. Противоречие. Теорема доказана. □

9. Наличие релятивизуемо полных языков в конкретных сложностных классах

Очевидные случаи существования $\leq_m^p$-полных языков следующие:

1) $\mathbf{P}^A$, $\mathbf{NP}^A$, $\mathbf{Co\text{-}NP}^A$, Σ_k^A, Π_k^A, $\mathbf{PSPACE}^A$ имеют $\leq_m^p$-полные языки,

2) $\oplus\mathbf{P}^A$ имеет $\leq_m^p$-полный язык,

3) $\mathbf{PP}^A$ имеет $\leq_m^p$-полный язык.

Все известные случаи релятивизуемого существования в одном классе языка, трудного для другого класса, получаются из указанных трех утверждений по следующим двум правилам:

класс K_2^A $\leq_m^{p,A}$-полон (или $\leq_m^p$-полон) для класса K_1^A, если существует класс K^A из списка $\mathbf{P}^A$, Σ_k^A, Π_k^A $(k \geq 1)$, $\oplus\mathbf{P}^A$, $\mathbf{PP}^A$, $\mathbf{PSPACE}^A$ такой, что $K_1^A \subseteq K^A \subseteq K_2^A$;

класс K_2^A $\leq_T^p$-полон для класса K_1^A, если существует класс K^A из списка $\mathbf{P}^A$, Σ_k^A, Π_k^A $(k \geq 1)$, $\oplus\mathbf{P}^A$, $\mathbf{PP}^A$, $\mathbf{PSPACE}^A$ такой, что $K_1^A \leq_T^p K^A \subseteq K_2^A$.

Сейчас мы приведем минимальный список отрицательных утверждений, которые необходимо и достаточно доказать для того, чтобы доказать, что отсутствуют другие релятивизуемые результаты о полноте для рассматри-

ваемых классов, кроме указанных. При этом мы будем учитывать следующее. Если $K_2^A \leq_m^{p,A}$-полон для K_1^A, то $K_1^A \subseteq K_2^A$ (поскольку все рассматриваемые классы замкнуты относительно $\leq_m^{p,A}$-сводимости). Поэтому, если доказано, что $\exists A\ K_1^A \not\subseteq K_2^A$, то доказано и что $\exists A\ K_2^A$ не $\leq_m^{p,A}$-полон для K_1^A. Аналогично, если $\exists A\ K_1^A \not\leq_T^{p,A} K_2^A$, то и $\exists A\ K_2^A$ не $\leq_T^{p,A}$-полон для K_1^A. Все доказываемые таким образом утверждения об отсутствии $\leq_m^{p,A}$- или $\leq_T^{p,A}$-трудных языков мы не будем включать в список. Список разделим на две части. В первой части перечислим случаи, когда неизвестно, имеет ли место релятивизуемая T-сводимость, во второй — все остальные.

Первая часть списка

1. $\exists A\ \mathbf{PP}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A$. Верно ли это, не известно. Поскольку $\mathbf{PP}^A$ имеет полный язык, это утверждение эквивалентно тому, что $\exists A\ \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A \not\leq_T^{p,A} \mathbf{PP}^A$.

2. $\exists A\ \Sigma_k^A$ не $\leq_T^{p,A}$-полон для $\Sigma_{k+1}^A \cap \Pi_{k+1}^A$. Верно ли это, неизвестно. Это утверждение эквивалентно тому, что $\exists A\ \Sigma_{k+1}^A \cap \Pi_{k+1}^A \not\leq_T^{p,A} \Sigma_k^A$.

Вторая часть списка

1. $\exists A\ \Sigma_k^A \cap \Pi_k^A$ не $\leq_T^{p,A}$-полон для $\Sigma_k^A \cap \Pi_k^A (k \geq 3)$. Верно ли это, неизвестно.

2. $\exists A\ \mathbf{IP}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{BPP}^A$. Это доказано автором совместно с Ан. А. Мучником. Доказательство приводится.

3. $\exists A\ \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{R}^A \cap \mathbf{Co\text{-}R}^A$. Это доказано в [16].

4. $\exists A\ \mathbf{IP}^A \cap \mathbf{Co\text{-}IP}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A$. Это доказано автором. Доказательство приводится.

5. $\exists A\ \Sigma_2^A \cap \Pi_2^A$ не $\leq_T^{p,A}$-полон для $\mathbf{BPP}^A$. Верно ли это, неизвестно.

6. $\exists A\ \mathbf{Few}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A$. Это верно. В [16] доказано, что для некоторого A $\mathbf{FewP}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A$. В настоящей работе доказано, что $\exists A\ \mathbf{Few}^A$ не $\leq_T^{p,A}$-полон для $\mathbf{UP}^A \cap \mathbf{Co\text{-}UP}^A$.

7. $\exists A\ \Sigma_2^A \cap \Pi_2^A$ не $\leq_T^{p,A}$-полон для $\mathbf{Few}^A$. Верно ли это, неизвестно.

Подчеркнем, что утверждения из списка являются максимально возможными утверждениями о неполноте. Немаксимальные утверждения доказывались и раньше. Именно, в [23] доказано, что $\exists A\ \mathbf{R}^A$ не имеет $\leq_m^{p,A}$-полного языка, в [16] этот результат усилен до $\leq_T^{p,A}$-сводимости; в [23] доказано, что $\exists A\ \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ не имеет $\leq_m^{p,A}$-полного языка, в [14] доказано, что $\exists A\ \mathbf{BPP}^A$ не имеет $\leq_m^{p,A}$-полного языка, в [3], [12], [15] эти два результата усилены до $\leq_T^{p,A}$-сводимости; в [14] доказано, что $\exists A\ \mathbf{UP}^A$ не имеет $\leq_m^{p,A}$-полного языка, в [16] этот результат усилен до $\leq_T^{p,A}$-сводимости.

Перейдем к доказательствам. Для результатов об отсутствии полных языков неравномерная модель вычислений, введенная в параграфе 3, играет еще большую роль. Ее применение основано на следующей лемме.

Лемма 9.1. *Если F, G невырожденные проблемы отделения такие, что*

9.1. $F \notin \mathbf{n.u.PLOGS}$, *и*

9.2. $\mathrm{n.u.LOGS}(G) = \mathbf{n.u.PLOG}$,

то существует оракул A, для которого класс $\mathrm{POLY}^A(G)$ *не* $\leq_T^{p,A}$*-полон для класса* $\mathrm{POLY}^A(F)$.

Доказательство. По теореме 6.1 достаточно доказать, что в $\mathrm{LOG}(G)$ нет языка, к которому $\preceq_T^l$-сводится F. Но такого языка нет даже в $\mathrm{n.u.LOG}(G)$, поскольку $\mathrm{n.u.LOGS}(G) = \mathbf{n.u.PLOG}$, следовательно, если бы $F \preceq_T^l H \in \mathrm{n.u.LOGS}(G)$, то F принадлежал бы **n.u.PLOGS** (поскольку **n.u.PLOGS** замкнут относительно $\preceq_T^l$-сводимости).

Утверждения 3, 4 легко следуют из леммы 9.1, теоремы 5.1 и следующей теоремы.

Теорема 9.1. $\mathbf{n.u.IPLOG} \cap \mathbf{Co\text{-}n.u.IPLOG} = \mathbf{n.u.PLOG}$.

Мы опускаем доказательство этой теоремы, поскольку оно получается простым обобщением доказательства результата Нисана [20], на нашем языке формулирующегося как $\mathbf{n.u.BPPLOG} = \mathbf{n.u.PLOG}$. Независимо теорема 12 доказана автором в первоначальной версии данной работы.

Подобным же способом доказывается утверждение 6. Формально, лемму 9.1 применить нельзя, поскольку $\mathbf{Few}^A$ не является порождаемым многообразием.

Теорема 9.2. *Если F невырожденная проблема отделения и* $F \notin \mathbf{n.u.PLOGS}$, *то существует оракул A, для которого* $\mathbf{Few}^A$ *не* $\leq_T^{p,A}$*-полон для* $\mathrm{POLY}^A(F)$.

Доказательство. Применяем диагональную конструкцию теоремы 5.1. Ясно, что достаточно доказать следующую лемму.

Лемма 9.2.1. Пусть $P(\alpha, r)$ предикат на $\mathbf{F} \times \mathbf{B}^*$, вычислимый за $\mathrm{poly}(\|\alpha\|, |r|)$ вопросов к α, а $p(n), q(n)$ полиномы такие, что $\forall \alpha \in \mathbf{F}\ |\{r \in \mathbf{B}^{p(\|\alpha\|)} : P(\alpha, r) = 1\}| \leq q(\|\alpha\|)$. Тогда функция

$$f(\alpha) = |\{r \in \mathbf{B}^{p(\|\alpha\|)} :\ P(\alpha, r) = 1\}|$$

неравномерно полилогарифмическая.

Доказательство. Пусть $\alpha \in \mathbf{F}_n$. Обозначим $m = p(n)$. Пусть $k = \mathrm{poly}(n)$ — количество вопросов к α, задаваемое при вычислении $P(\alpha, r)$ при $r \in \mathbf{B}^m$. Слова из $\mathbf{B}^m$ будем, как обычно, называть экспертами, и будем говорить, что эксперт r допускает α, если $P(\alpha, r) = 1$.

Докажем, что задав не более $q(n) \cdot k^2$ вопросов к $\alpha \in \mathbf{F}_n$, можно найти всех экспертов, допускающих α.

Назовем сегментом любую частичную функцию $\varphi : \mathbf{B}^n \to \mathbf{B}$. Два сегмента согласованы, если они имеют общее продолжение. Каждый эксперт в

вычислении на входе $\alpha : \mathbf{B}^n \to \mathbf{B}$ спрашивает k битов α и тем самым находит некоторый сегмент с k-элементной областью определения, согласованный с α. Назовем этот сегмент информацией эксперта об α. Сертификатом эксперта r назовем информацию r о любом α, которое он допускает.

Способ по $\alpha \in \mathbf{F}_n$ найти всех экспертов, допускающих α, состоит в следующем. Выполним k шагов следующего вида.

Один шаг. Берем любое максимальное множество сертификатов с попарно непересекающимися областями определения. Обозначим это множество $\{\varphi_1, \ldots, \varphi_j\}$. Тогда $j \le q(n)$, поскольку существует $\beta \in \mathbf{F}_n$, согласованное со всеми $\varphi_1, \ldots, \varphi_j$, и $\varphi_1, \ldots, \varphi_j$ — сертификаты разных экспертов (поскольку разные сертификаты одного эксперта не согласованы, а значит их области пересекаются). Спрашиваем значение α на всех элементах из $\mathrm{Dom}(\varphi_1) \cup \cdots \cup \mathrm{Dom}(\varphi_j)$. Область любого сертификата φ пересекается с $\mathrm{Dom}(\varphi_1) \cup \cdots \cup \mathrm{Dom}(\varphi_j)$, а значит мы знаем значение α на хотя бы одном слове из $\mathrm{Dom}(\varphi)$. Теперь выбрасываем все сертификаты, не согласованные с полученной нами информацией об α, а из областей оставшихся сертификатов выбрасываем те $u \in \mathbf{B}^n$, для которых $\alpha(u)$ известно. Область каждого оставшегося сертификата уменьшилась. И самое главное: разные (оставшиеся) сертификаты одного эксперта опять не согласованы. Шаг закончен.

Поскольку после каждого шага непустые области оставшихся сертификатов уменьшаются, после выполнения k шагов все области оставшихся сертификатов станут пустыми. Поэтому оставшиеся сертификаты суть все сертификаты, согласованные с α. Те эксперты, некоторые сертификаты которых оказались согласованными с α, и суть допускающие α эксперты. Осталось заметить, что на каждом шаге мы спрашивали $\le q(n) \cdot k$ битов α. □

Теорема доказана. □

Утверждение 2 уже не может быть выведено из леммы 9.1, поскольку $\mathbf{n.u.IPLOG} \supseteq \mathbf{n.u.NPLOG} \supset \mathbf{n.u.PLOG}$.

Теорема 9.3. *(получена совместно с Ан.А.Мучником). Существует такой оракул A, что $\mathbf{IP}^A$ не $\le_T^{p,A}$-полон для $\mathbf{BPP}^A$.*

Мы докажем эту теорему вместе с недоказанными еще утверждениями предыдущего параграфа:

Теорема 9.4. $\exists A\ \mathbf{BPP}^A \not\le_T^{p,A} \mathbf{NP}^A$.

Теорема 9.5. $\exists A\ \oplus\mathbf{P}^A \not\le_T^{p,A} \mathbf{IP}^A$.

Теорема 9.6. $\exists A\ \Sigma_2^A \cap \Pi_2^A \not\le_T^{p,A} \mathbf{IP}^A$.

Доказательство теорем 14-17. Вообще говоря, теорема 9.4 следует из теоремы 9.3, поскольку $\mathbf{NP}^A$ содержит полную проблему и $\mathbf{NP}^A \subseteq \mathbf{IP}^A$. Тем

не менее, для лучшей иллюстрации метода мы начнем с доказательства теоремы 9.4. По теореме 6.1 достаточно доказать, что $F_{\mathbf{BPP}} \not\preceq^l_T F_{\mathbf{NP}}$.

Допустим $F_{\mathbf{BPP}} \preceq^l_T F_{\mathbf{NP}}$. Пусть $\langle M, f\rangle$ — сводящая пара. Фиксируем достаточно большое n. Обозначим $m = \mathrm{poly}(n)$ — количество вопросов M к оракулу на входе 2^n. Пусть $\alpha \in \mathbf{F}_n$. Обозначим через $e(\alpha)$ последовательность ответов оракула $F_{\mathbf{NP}}(f(\cdot,\alpha))$ при работе M на входе 2^n; по определению $e(\alpha) \in \mathbf{B}^m$. Возьмем $\alpha \in \mathbf{F}_n$ с лексикографически наибольшим $e(\alpha)$, обозначим это α через α_0, $e(\alpha_0)$ — через $e_0 = b^0_1 \cdots b^0_m$, а вопросы, задаваемые M к оракулу $F_{\mathbf{NP}}(f(\cdot,\alpha))$ — через $v_1, \ldots, v_m$. Пусть $v_{i_1}, \ldots, v_{i_k}$ — все те слова v_i, на которых значение оракула равно 1, т.е. $\#_1 f(v_i, \alpha_0) > 0$. Для каждого $j \le k$ зафиксируем одно такое слово t_j, что $f(v_{i_j}, \alpha_0)(t_j) = 1$. Пусть $q(n)$ — полином, ограничивающий время слабого вычисления функции $f(v_i, \alpha)$ для $\alpha \in \mathbf{F}_n$, $i \le m$. Очевидно, для каждого $j \le k$ можно зафиксировать значение α_0 на $q(n)$ словах так, что зафиксируется значение $f(v_{i_j}, \alpha_0)(t_j)$. Всего будет зафиксировано $\le mq(n) = \mathrm{poly}(n)$ значений. Теперь мы имеем: для любого $\alpha \in \mathbf{F}_n$, совпадающего с α_0 на зафиксированных словах для всех $i \le m$ таких, что $b^0_i = 1$, выполнено $F_{NP}(f(v_i, \alpha)) = 1$. Докажем, что, более того, для всех $\alpha \in \mathbf{F}_n$, совпадающих с α_0 на зафиксированных словах, выполнено $e(\alpha) = e(\alpha_0)$. Допустим противное, пусть α — контрпример. Обозначим $e(\alpha)$ через $b_1 \cdots b_m$. Пусть i наименьший такой номер, что $b^0_i \ne b^0_i$. Тогда поскольку вектор e_0 лексикографически наибольший среди всех векторов $e(\alpha)$, $\alpha \in \mathbf{F}_n$, мы имеем $b_i = 0$, $b^0_i = 1$. По доказанному, отсюда следует $F_{\mathbf{NP}}(f(v_i, \alpha)) = 1$. Но поскольку $b^0_1 \cdots b^0_{i-1} = b_1 \cdots b_{i-1}$, v_i есть i-ый вопрос к оракулу при работе M на входе 2^n с оракулом $F_{\mathbf{NP}}(f(\cdot,\alpha))$, а значит $F_{\mathbf{NP}}(f(v_i, \alpha)) = b_i$. Противоречие.

Из того, что $e(\alpha) = e(\alpha_0)$ следует $\langle M, f\rangle^{F_{\mathbf{NP}}}(\alpha) = \langle M, f\rangle^{F_{\mathbf{NP}}}(\alpha_0)$. Возьмем n таким большим, чтобы зафиксированных битов было меньше чем $\frac{1}{3}$ от общего числа. Положим α равным α_0 на зафиксированных битах, а на остальных определим единицей, если $\langle M, f\rangle^{F_{\mathbf{NP}}}(\alpha_0) = 0$, и нулем, иначе. Получим $F_{\mathbf{BPP}}(\alpha) \not\le \langle M, f\rangle^{F_{\mathbf{NP}}}(\alpha_0) = \langle M, f\rangle^{F_{\mathbf{NP}}}(\alpha)$. Теорема 9.4 доказана.

Докажем теорему 9.5. Поскольку PARITY — язык, по теореме 5.1 достаточно доказать, что PARITY $\not\preceq^l_T$ **IPLOG**. Допустим, что PARITY $\preceq^l_T$-сводится к некоторому языку из **IPLOG** посредством пары $\langle M, f\rangle$. Определим $\alpha_0, m, q(n), v_1, \ldots, v_m, e_0$ так же, как в предыдущем доказательстве. Поскольку $F \in$ **IPLOG** существует полилогарифмический Проверяющий V для F. Для каждого такого $i \le m$, что $b^0_i = 1$, фиксируем Доказывающего P_i такого, что $\mathrm{Prob}[(P_i, V)(f(v_i, \alpha_0)) = 1] > \frac{2}{3}$. Пусть N — машина, выдающая по α, v, t, где $|t| = \|f(v,\alpha)\|$, значение t-ого символа слова $f(v,\alpha)$ за время $\mathrm{poly}(\|\alpha\| + |v|)$. Пусть $x \in \mathbf{B}^n$, а $r = \mathrm{poly}(n)$ — максимальное количество вопросов вида «$\alpha_0(x) =?$», которое машина N задает при вычислении на входах вида α_0, v_i, t с $|t| = \|f(v_i, \alpha_0)\|$. Пусть $s = \mathrm{poly}(n)$ — максимальное количество вопросов «$\beta_0(t) =?$», которое может задать V при вычислении (P_i, V) значения $F(f(v_i, \alpha_0))$. Пусть $x \in \mathbf{B}^n$. Обозначим $w^i_{\alpha_0}(x)$ вероятность того, что существует $t \in \mathbf{B}^*$, $|t| = \|f(v_i, \alpha_0)\|$ такое, что в про-

цессе вычисления P_i и V на α_0 Проверяющий задаст вопрос «$f(v_i, \alpha_0)(t) =?$» и N в процессе вычисления на α_0, v_i, t задаст вопрос «$\alpha_0(x) =?$». Тогда $\sum_{i:b_i^0=1} \sum_{x \in \mathbf{B}^n} w^i_{\alpha_0}(x) \leq msr$, поэтому существует $x_0 \in \mathbf{B}^n$, для которого $\sum_{i:b_i^0=1} w^i_{\alpha_0}(x_0) \leq \frac{msr}{2^n} < \frac{1}{3}$ (при достаточно большом n). Изменим в $\alpha_0 x_0$-ый бит, обозначим полученное слово α. Докажем, что $e(\alpha) = e(\alpha_0)$, а значит $\langle M, f\rangle^F(\alpha) = \langle M, f\rangle^F(\alpha_0)$. Допустим $e(\alpha) \neq e(\alpha_0)$. Обозначим $e(\alpha) = b_1 \cdots b_m$ и возьмем наименьшее такое i, что $b_i \neq b_i^0$. Тогда $b_i = 0$, $b_i^0 = 1$. Значит $F(f(v_i, \alpha)) = 0$, следовательно

$\mathrm{Prob}[(P_i, V)(f(v_i, \alpha)) = 1] < \frac{1}{3}$, в то время, как

$\mathrm{Prob}[(P_i, V)(f(v_i, \alpha_0)) = 1] > \frac{2}{3}$. Следовательно $w^i_{\alpha_0}(x_0) > \frac{1}{3}$, поскольку α и α_0 отличаются только на x_0. Противоречие. Поскольку $\mathrm{PARITY}(\alpha) \neq \mathrm{PARITY}(\alpha_0)$, теорема доказана.

Теперь докажем теорему 9.3, т.е. что $F_{\mathbf{BPP}}$ не $\preceq^l_T$-сводится ни к какому языку F из **IPLOG**. Допустим противное $F_{\mathbf{BPP}} \preceq^l_T F \in \mathbf{IPLOG}$. Воспользуемся всеми обозначениями предыдущей теоремы. Пусть для определенности $\langle M, f\rangle^F(\alpha_0) = 1$. Тогда возьмем среди всех α с $e(\alpha) = e(\alpha_0)$ слово с наименьшим количеством 1, будем считать, что это и есть α_0. Если $\#_1(\alpha_0) < \frac{1}{3}2^n$, то уже получено противоречие. Если же $\#_1(\alpha_0) \geq \frac{1}{3}2^n$, то найдется $x_0 \in \mathbf{B}^n$ такой, что $\sum_{i:b_i^0=1} w^i_{\alpha_0}(x_0) \leq \frac{msr}{\frac{1}{3}2^n} < \frac{1}{3}$ и $\alpha_0(x_0) = 1$. Опять определим $\alpha : \alpha(x_0) = 0, \alpha(x) = \alpha_0(x)$ при $x \neq x_0$. Тогда $\#_1(\alpha) < \#_1(\alpha_0)$. Дальше, действуя так же, как и в предыдущем доказательстве, получаем $e(\alpha) = e(\alpha_0)$ вопреки минимальности количества единиц в α_0.

Теперь докажем теорему 17. Пусть α — произвольная частичная функция из $\mathbf{B}^n$ в $\mathbf{B}^n$. Как и в доказательстве теоремы 10 обозначим через $\bar{\alpha}$ график α ($\bar{\alpha} \in \mathbf{B}^{2^{2n}}$). Рассмотрим проблему отделения

$$F(\gamma) = \begin{cases} 1, & \text{если } \exists n \in \mathbf{N} : \gamma = \bar{\alpha}\bar{\beta}, \text{ где } \alpha \text{ и } \beta \text{ — такие частичные} \\ & \text{функции из } \mathbf{B}^n \text{ в } \mathbf{B}^n, \text{ что } \alpha \text{ всюду определена, } \beta \\ & \text{определена на всех аргументах, кроме одного,} \\ 0, & \text{если } \exists n \in \mathbf{N} : \gamma = \bar{\alpha}\bar{\beta}, \text{ где } \alpha \text{ и } \beta \text{ — такие частичные} \\ & \text{функции из } \mathbf{B}^n \text{ в } \mathbf{B}^n, \text{ что } \beta \text{ всюду определена, } \alpha \\ & \text{определена на всех аргументах, кроме одного,} \\ *, & \text{иначе.} \end{cases}$$

Через E_n обозначим $\{\gamma \in \mathbf{F}_{2n+1} \mid F(\gamma) \neq *\}$.

По теореме 6.1 достаточно доказать, что не существует $G \in \mathbf{IPLOGS}$ для которого $F \preceq^l_T G$. Допустим такая проблема отделения G существует. Обозначим сводящую пару $\langle M, f\rangle$. Фиксируем достаточно большое n. Используем обозначения предыдущих доказательств. Берем слово $\gamma \in E_n$ с лексикографически наибольшим $e(\gamma)$. Пусть α_0, β_0 — такие частичные функции, что $\gamma = \bar{\alpha}_0\bar{\beta}_0$. Пусть для определенности $F(\bar{\alpha}_0\bar{\beta}_0) = 1$, т.е. α_0 всюду определена. Пусть β_0 не определена на слове x_1. Фиксируем Проверяющего для решения проблемы отделения G. Введем подходящую нумерацию битов слова γ. Для $x, y \in \mathbf{B}^n$ будем считать $\gamma(0xy) = \bar{\alpha}_0(xy)$,

$\gamma(1xy) = \bar{\beta}_0(xy)$. Как и раньше, для каждого i такого, что $b_i^0 = 1$, вводим понятие веса $w^i_{\alpha_0\beta_0}(u)$ слова $u \in \mathbf{B}^{2n+1}$: $w^i_{\alpha_0\beta_0}(u)$ равно вероятности того, что существует $t \in \mathbf{B}^{\|f(v_i,\alpha_0)\|}$ такое, что V при работе в паре с P_i на входе $f(v_i, \alpha_0)$ задает вопрос «$f(v_i, \alpha_0)(t) =?$» и N на входе α_0, v_i, t задает вопрос «$\alpha_0(u) =?$». При достаточно большом n можно найти $x_0 \in \mathbf{B}^n$ такое, что $\sum_{i:b_i^0=1} w^i_{\alpha_0\beta_0}(0x_0\alpha_0(x_0)) < \frac{1}{6}$, и такое $y_1 \in \mathbf{B}^n$, что $\sum_{i:b_i^0=1} w^i_{\alpha_0\beta_0}(1x_1y_1) < \frac{1}{6}$.

Определим частичные функции α, β так:

$$\alpha(x) = \begin{cases} \alpha_0(x), & \text{при } x \neq x_0 \\ \text{неопределена}, & \text{при } x = x_0 \end{cases}$$

$$\beta(x) = \begin{cases} \beta_0(x), & \text{при } x \neq x_1, \\ y_1, & \text{при } x = x_1. \end{cases}$$

Тогда $e(\bar{\alpha}\bar{\beta}) = e(\bar{\alpha}_0\bar{\beta}_0)$ и $F(\bar{\alpha}\bar{\beta}) = 0$. Противоречие.

Литература

[1] W. Aiello, S. Goldwasser, and J. Hʀastad. On the power of interaction. In *27th Annual IEEE Symposium on Foundation of Computer Science*, pages 368–379, New York, 1986. IEEE.

[2] N. Ajtai. σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.

[3] K. Ambos-Spies. A note on complete problems for complexity classes. *Information Processing Letters*, 23:227–230, 1986.

[4] L. Babai. Trading group theory for randomness. In *17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[5] T. Baker, J. Gill, and R. Solovay. Relativization of P=?NP question. *SIAM Journal on Computing*, 4(4):431–442, 1975.

[6] C. H. Bennet and J. Gill. Relative to a random oracle P≠NP≠coNP with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

[7] J. Cai and L. Hemachandra. On the power of parity polynomial time. *Mathematical Systems Theory*, 23(2):95–106, 1990.

[8] L. Fortnow and M. Sipser. Are there interactive protocols for coNP languages? *Information Processing Letters*, 28:249–251, 1988.

[9] N. Furst, J. Saxe, and M. Sipser. Parity, circuits and the polynomial time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.

[10] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, 18:186–208, 1989.

[11] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In *18th Annual ACM Symposium on Theory of Computing*, pages 59–68, 1986.

[12] Y. Gurevich. Algebras of feasible functions. In *24th Annual IEEE Symposium on Foundation of Computer Science*, pages 210–214, 1983.

[13] J. Hrastad. Almost optimal lower bounds for small depth circuits. In *18th Annual ACM Symposium on Theory of Computing*, pages 6–20, 1986.

[14] J. Hartmanis and L. Hemachandra. Complexity classes without machines: On complete languahes for UP. *Theoretical Computer Science*, 58:129–142, 1988. Preliminary version appeared in: "International Colloquium on Automata, Languages and Programming", 1986. Lecture Notes in Computer Science, 1986, Vol. 226, pp. 123–135.).

[15] J. Hartmanis and N. Immerman. On complete problems for NP∪coNP. *International Colloquium on Automata, Languages and Programming, 1985. Lecture Notes in Computer Science*, 194:250–259, 1985.

[16] L. Hemaspaandra, S. Jain, and N. Vereshchagin. Banishing robust turing completeness. *International Journal on Foundations of Computer Science*, 4(3):245–265, 1993. Conference version appeared in: *Logic at TVER'92, Symposium on Logical Foundations of Computer Science, Lecture Notes in Computer Science,* 1992, vol. 620, pp. 186–197.

[17] J. Köbler and U. Shöning and S. Toda and J. Toran. Turing machines with few accepting computations and low sets for PP. In *Fourth Annual Conference on Structure in Complexity Theory*, 1989.

[18] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. The polynomial time hierarchy has interactive proofs. In *31th Annual IEEE Symposium on Foundation of Computer Science*, pages 2–10, 1990.

[19] M. Minsky and S. Papert. *Perceptrons.* MIT Press, Cambridge, MA, 1988. (Expanded edition, first edition appeared in 1967.).

[20] N. Nisan. Probabilistic versus deterministic decision trees and CREW PRAM complexity. In *21th Annual ACM Symposium on Theory of Computing*, pages 327–335, 1989.

[21] M. Santha. Relativized Arthur-Merlin versus Merlin-Arthur games. *Information and Computation*, 80:44–49, 1989.

[22] A. Shamir. IP=PSPACE. In *31th Annual IEEE Symposium on Foundation of Computer Science*, pages 11–15, 1990.

[23] M. Sipser. On relativizations and the existence of complete sets. *International Colloquium on Automata, Languages and Programming, 1982. Lecture Notes in Computer Science*, 140:523–531, 1982.

[24] M. Sipser. A complexity theoretic approach for randomness. In *15th Annual ACM Symposium on Theory of Computing*, pages 330–335, 1983.

[25] S. Toda. On the computational power of PP and $\oplus$P. In *30th Annual IEEE Symposium on Foundation of Computer Science*, pages 514–519, 1989.

[26] N. K. Vereshchagin. On the power of PP. In *7th Conference on Structure in Complexity Theory*, pages 138–143, 1992.

[27] A. Yao. Separating the polynomial hierarchy by oracles. In *26th Annual IEEE Symposium on Foundation of Computer Science*, pages 1–10, 1985.