САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

Ицыксон Дмитрий Михайлович

СЛОЖНОСТЬ В СРЕДНЕМ СЛУЧАЕ ВЕРОЯТНОСТНЫХ ВЫЧИСЛЕНИЙ С ОГРАНИЧЕННОЙ ОШИБКОЙ

01.01.06 — математическая логика, алгебра и теория чисел

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
кандидата физико-математических наук

Санкт-Петербург
2009

Работа выполнена в лаборатории математической логики Учреждения Российской академии наук Санкт-Петербургского отделения Математического института им. В. А. Стеклова РАН

Научный руководитель:	кандидат физико-математических наук, доцент Гирш Эдуард Алексеевич
Официальные оппоненты:	доктор физико-математических наук, профессор Верещагин Николай Константинович (Московский государственный университет имени М.В. Ломоносова)
	кандидат физико-математических наук Вяткина Кира Вадимовна (Санкт-Петербургский государственный университет)
Ведущая организация:	Вычислительный центр им. А. А. Дородницына РАН

Защита диссертации состоится “28” декабря 2009 г. в 17 час. на заседании совета Д 212.232.29 по защите докторских и кандидатских диссертаций при Санкт-Петербургском государственном университете по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, 27, ауд. 311 (помещение ПОМИ РАН).

Адрес диссертационного совета: 198504, Санкт-Петербург, Ст. Петергоф, Университетский пр. д. 28.

С диссертацией можно ознакомиться в Научной библиотеке им. М. Горького Санкт-Петербургского государственного университета по адресу: 199034, Санкт-Петербург, Университетская наб., 7/9.

Автореферат разослан “ ” 2009 г.

Ученый секретарь
диссертационного совета,
доктор физ.-мат. наук, профессор Нежинский В. М.

Общая характеристика работы

Актуальность темы. Интерес к вероятностным алгоритмам с ограниченной ошибкой возрос в 1970-х годах, когда Соловэй и Штрассен опубликовали эффективный вероятностный алгоритм проверки числа на простоту. В те же годы Гилл дал определение классу сложности **BPP**, состоящему из языков, которые могут быть распознаны за полиномиальное время вероятностными алгоритмами с ограниченной ошибкой. Долгое время задача проверки числа на простоту была самым ярким примером задачи, которая эффективно решается вероятностными алгоритмами, но не решается детерминированными. Однако в 2002 году Агравал, Каял и Саксена предложили детерминированный полиномиальный по времени тест числа на простоту.

Неизвестно, совпадают ли классы **P** и **BPP**. Полиномиальный алгоритм проверки числа на простоту и результаты современных исследований о связи существования явных труднорешаемых задач и дерандомизации (работы Нисана, Вигдерсона и др. 1994–2003 гг.) дают основание для выдвижения гипотезы $\mathbf{P} = \mathbf{BPP}$ (в частности, из существования булевой функции, которая вычислима за время 2^{cn}, но не вычислима с помощью схем размера меньше, чем $2^{\epsilon n}$, следует, что $\mathbf{P} = \mathbf{BPP}$).

P и **BPP** — это классы задач, которые можно эффективно решать на практике. Для определения понятия надежности криптографического протокола нужно понимать, что значит, что задачу (взлом протокола) невозможно эффективно решать на практике. Из того, что задача не лежит в классе **BPP**, еще не следует, что эту задачу нельзя эффективно решать на практике. Вполне возможно, что для каждой длины входа есть ровно один вход, для которого задача сложна, а для всех остальных входов задача является простой. Именно для нужд криптографии в конце 1980-х годов Левиным и Гуревичем были сформулированы основные понятия теории сложности в среднем случае.

В теории сложности в среднем случае массовые вычислительные за-

дачи рассматриваются вместе с распределением на входах (индивидуальных задачах). Задачи, снабженные распределением, мы называем распределенными задачами. Мы рассматриваем полиномиально моделируемые распределения, т.е. такие, которые могут быть порождены за полиномиальное время с использованием равномерного распределения. Первое определение понятия полиномиального в среднем случае алгоритма дал Левин в 1986 году. Левин также доказал полноту в среднем случае задачи о замощении. Если задача о замощении может быть решена за полиномиальное в среднем время, то и все **NP**-задачи с полиномиально моделируемыми распределениями могут быть решены за полиномиальное в среднем время. Позже было доказано, что следующие распределенные задачи тоже являются полными в среднем случае: задача об ограниченной остановке машины Тьюринга, задача Поста (Гуревич, 1991), задача декомпозиции матрицы (Басс, Гуревич, 1995) и др.

Пусть Σ — конечный алфавит, мы рассматриваем функции действующие из Σ^* в Σ^*, где Σ^* — это множество конечных слов в алфавите Σ. Мы называем функцию f односторонней, если ее легко вычислить, но трудно обратить. Обычно принято считать, что функция легко вычислима, если она вычислима за полиномиальное время. Есть несколько подходов для определения трудности обращения функции.

Криптографически односторонняя функция. Полиномиально вычислимая функция называется криптографически слабо односторонней, если для некоторой положительной константы c каждый вероятностный полиномиальный по времени алгоритм ошибается при обращении этой функции с вероятностью (по входам и случайным битам алгоритма) не менее $\frac{1}{n^c}$ для всех достаточно больших длин входов. Неизвестно никаких разумных предположений о сложностных классах, из которых следовало бы существование криптографических односторонних функций.

Односторонняя в среднем случае функция. Есть два способа определить трудность обращения функции на языке сложности в среднем случае в зависимости от того, где задано полиномиально моделируемое распре-

деление. Если задача обращения функции f с полиномиально моделируемым распределением на *входах* f не решается никаким полиномиальным в среднем случае вероятностным алгоритмом с ограниченной ошибкой, то функцию f будем называть односторонней в среднем случае.

Если задача обращения функции f с полиномиально моделируемым распределением на *выходах* (образах) f не решается никаким полиномиальным в среднем случае вероятностным алгоритмом с ограниченной ошибкой, то говорят, что задача обращения f — это трудная в среднем случае задача. Существование трудных в среднем случае задач эквивалентно $(\mathbf{NP}, \mathbf{PSamp}) \not\subseteq \mathbf{AvgBPP}$, где $(\mathbf{NP}, \mathbf{PSamp})$ — это множество задач из $\mathbf{NP}$ с полиномиально моделируемыми распределениями, а $\mathbf{AvgBPP}$ — это множество распределенных задач, решаемых за полиномиальное в среднем время вероятностными алгоритмами с ограниченной ошибкой.

Из существования односторонних в среднем случае функций следует существование трудных в среднем случае задач, поскольку полиномиально моделируемое распределение на входах функции порождает полиномиально моделируемое распределение на выходах функции. Из существования криптографических односторонних функций следует существование односторонних в среднем функций, из чего следует существование трудных в среднем задач, что влечет $(\mathbf{NP}, \mathbf{PSamp}) \not\subseteq \mathbf{AvgBPP}$. Следует ли из $(\mathbf{NP}, \mathbf{PSamp}) \not\subseteq \mathbf{AvgBPP}$ существование криптографических односторонних функций, является важнейшим открытым вопросом. Следует ли из $(\mathbf{NP}, \mathbf{PSamp}) \not\subseteq \mathbf{AvgBPP}$ существование односторонних в среднем случае функций, также является открытым вопросом. Можно показать (Левин, 2003), что если существует трудная в среднем задача обращения функции, сохраняющей длину, с равномерным распределением, то существует и односторонняя в среднем функция (эти два условия столь сильные, что их не получается удовлетворить, основываясь ни на одной из известных полных задач в классе $(\mathbf{NP}, \mathbf{PSamp})$).

На данный момент для класса $\mathbf{BPP}$ неизвестно ни теоремы об иерархии по времени, ни полных задач относительно детерминированных сведе-

ний. Основное препятствие — это отсутствие вычислимой нумерации вероятностных машин, которые удовлетворяют условию ограниченной ошибки. Отметим, что если $\mathbf{P} = \mathbf{BPP}$, то класс $\mathbf{BPP}$ содержит полный язык (подойдет любой язык из класс $\mathbf{P}$). Однако существует такой оракул A, что в классе $\mathbf{BPP}^A$ нет полных языков (Хартманис, Хемачандра, 1986). Из существования полной задачи в классе $\mathbf{BPP}$ следует существование иерархии по времени (Барак, 2002). Лучший результат, связанный с иерархией по времени, суперполиномиальный: $\mathbf{BPTime}[n^{\log n}] \subsetneq \mathbf{BPTime}[2^{n^\epsilon}]$ (Карпинский, Вербек, 1987). Однако, мы не можем доказать, например, что $\mathbf{BPTime}[n] \subsetneq \mathbf{BPTime}[n^{100 \log n}]$.

Первый прогресс в исследовании структурных свойств вероятностных классов сложности — это теорема об иерархии по времени для вычислений с несколькими битами неравномерной подсказки (Барак, 2002; Фортноу, Сансанам, 2004), последние результаты включают иерархию по времени для классов всего с одним битом подсказки: $\mathbf{BPP}/1$ (Фортноу, Сансанам, 2004), $\mathbf{ZPP}/1, \mathbf{MA}/1$ и т.д. (Мелкебек, Первышев, 2007). Однако, понятие подсказки, используемое в этих результатах нестандартное, поскольку машины могут нарушать условие ограниченности ошибки, если подсказка неправильная. В случае, если использовать классическое определение подсказки, то существование иерархии по времени остается открытым вопросом, так как оно эквивалентно иерархии по времени без подсказки. Другим результатом в этой области стало доказательство иерархии по времени для эвристических вероятностных алгоритмов с ограниченной ошибкой (эвристические алгоритмы могут ошибаться на маленькой доле входов). Иерархия по времени в классе $\mathbf{Heur}_{\frac{1}{n^c}}\mathbf{BPP}$ (с равномерным распределением) была доказана в (Фортноу, Сансанам, 2004), доказательство было существенно упрощено в (Первышев, 2007). Однако, в этих результатах алгоритмы не только могут давать неверный ответ, но и нарушают условие ограниченности ошибки на малой доле входов. Возможность выдавать неверный ответ помогает и в построении полных объектов, например, существует полная криптосистема с открытым ключом, если декодирую-

щий алгоритм может ошибаться с маленькой вероятностью (Харник и др., 2005).

В 2000-м году Голдрейх предложил функцию, основанную на графах-расширителях, и выдвинул гипотезу, что эта функция является односторонней. Предложенная функция имеет n двоичных входов и n двоичных выходов. Каждый выход функции зависит только от каких-то d входов и вычисляется по ним с помощью заданного d-местного предиката. Голдрейх предлагал использовать графы со свойством расширения в качестве графа зависимостей и случайный d-местный предикат. Функция, предложенная Голдрейхом, имеет некоторое сходство с псевдослучайным генератором Нисана-Вигдерсона.

Одним из практических подходов к обращению односторонних функций является использование современных программ, решающих задачу выполнимости булевой формулы. Практически все реально используемые алгоритмы для задачи выполнимости булевой формулы основаны на методе расщепления (по инициалам авторов (Дэвис, Путнам, 1960), (Дэвис, Логеман, Ловеленд, 1962) такие алгоритмы называют DPLL алгоритмами).

Для невыполнимых формул нижние оценки на время работы алгоритмов расщепления следуют из нижних оценок на размер резолюционных доказательств (Цейтин, 1968). Невыполнимые формулы, основанные на псевдослучайных генераторах Нисана-Вигдерсона, используются для доказательства нижних оценок в различных пропозициональных системах доказательств (Алехнович и др., 2000). Но формулы, получающиеся из задач обращения односторонних функций, обычно являются выполнимыми. Вполне возможно, что расщепляющие алгоритмы быстро работают на выполнимых формулах. Если никак не ограничивать эвристики выбора переменной для расщепления и значения, которое рассматривается первым, то доказательство экспоненциальной нижней оценки на время работы расщепляющих алгоритмов на выполнимых формулах означало бы, что $\mathbf{P} \neq \mathbf{NP}$.

В работе (Дж. Кук и др., 2009) изучается сложность обращения функции Голдрейха, основанной на предикате $x_1 \oplus x_2 \oplus \cdots \oplus x_{d-2} \oplus x_{d-1}x_d$. Для

«близоруких» алгоритмов, основанных на расщеплении доказывается экспоненциальная нижняя оценка на среднюю сложность обращения таких функций. В «близоруких» алгоритмах эвристики выбора переменной и выбора значения, которое будет рассматриваться первым, в таких алгоритмах ограничены тем, что они могут за каждый шаг прочитать лишь маленькую часть строки, на которой функция обращается. Также было показано, что задача обращения функции Голдрейха с таким предикатом трудна для программ MiniSAT 2.0. Вопрос о экспоненциальных нижних оценках на время обращения функций Голдрейха «пьяными» алгоритмами оставлен открытым в (Дж. Кук и др., 2009). В классе «пьяных» алгоритмов эвристика выбора переменной ничем не ограничена и может быть даже невычислимой, а эвристика выбора значения, которое будет подставлено первым, ограничено достаточно сильно: значение выбирается равновероятно случайным образом.

Цели работы.

1. Установить связь между существованием криптографически односторонних функций и односторонних в среднем случае функций.

2. Построить распределенную задачу, которая является полной в классе $(\mathbf{AvgBPP}, \mathbf{PSamp})$ относительно детерминированных сведений.

3. Доказать теорему об иерархии по времени в классе $(\mathbf{AvgBPP}, \mathbf{PSamp})$.

4. Сравнить класс сложности **AvgP** с классами **P** и **EXP**, сравнить класс **AvgBPP** с классами **BPP** и **BPEXP**.

5. Построить трудные выполнимые формулы для «пьяных» алгоритмов, которые основаны на трудных невыполнимых формулах.

6. Получить нижнюю оценку на среднее время обращения функции Голдрейха, основанной на нелинейном предикате, «пьяными» алгоритмами.

Общая методика работы. В работе используются методы теории сложности вычислений. Для доказательства нижней оценки на среднее время обращения функции Голдрейха используются методы теории сложности доказательств и техника работы с графами-расширителями.

Основные результаты.

1. Доказано существование функций, которые являются криптографически односторонними для бесконечного числа длин входов, в предположении о существовании сохраняющей длину функции, которую невозможно обратить полиномиальным в среднем случае вероятностным алгоритмом с ограниченной ошибкой при полиномиально моделируемом распределении на входах функции.

2. Построена распределенная задача, которая является полной в классе $(\mathbf{AvgBPP}, \mathbf{PSamp})$.

3. Доказана теорема об иерархии по времени в классе $(\mathbf{AvgBPP}, \mathbf{PSamp})$.

4. Доказаны включения (для полиномиально моделируемых распределений): $\mathbf{P} \subsetneq \mathbf{AvgP} \subseteq \mathbf{HeurP} \subsetneq \mathbf{EXP}$ и $\mathbf{BPP} \subsetneq \mathbf{AvgBPP} \subseteq \mathbf{HeurBPP} \subsetneq \mathbf{BPEXP}$.

5. Построены трудные выполнимые формулы для «пьяных» алгоритмов, которые основаны на трудных невыполнимых формулах.

6. Доказана нижняя оценка на среднее время обращения функции Голдрейха «пьяными» алгоритмами, где функция Голдрейха основана на случайном графе и предикате $x_1 \oplus \ldots x_{d-k} \oplus Q(x_{d-k+1} \ldots x_d)$, где $k+1 < \frac{d}{4}$, а Q — произвольный предикат.

Научная новизна. Все результаты, представленные в диссертации, являются новыми.

Практическая и теоретическая ценность. Работа носит теоретический характер. Результаты работы могут быть использованы для изу-

чения структурной сложности семантических классов, для установления новых связей между существованием криптографических примитивов и понятиями теории сложности вычислений.

Апробация работы. Основные результаты были доложены на следующих конференциях и семинарах: международная конференция International Colloquium on Automata, Languages and Programming (ICALP 2004), Финляндия, 2004; международная школа Estonian Winter School in Computer Science (EWSCS 2005), Эстония, 2005; международная конференция Workshop on Computational, Descriptive and Proof Complexity, and Algorithms, Россия, 2007; международная конференция Workshop on Logic, Language, Information and Computation (WoLLIC 2008), Великобритания, 2008; международная школа Estonian Winter School in Computer Science (EWSCS 2009), Эстония, 2009; российско-австрийский семинар Логика конечного и бесконечного, Австрия, 2009; международный симпозиум International Computer Science Symposium in Russia (CSR 2009), Россия, 2009.

Результаты, лежащие в основе диссертации, неоднократно докладывались на семинаре ПОМИ РАН. Два доклада были признаны лучшими на студенческих школах EWSCS 2005 и EWSCS 2009. Работа, содержащая результаты диссертации, удостоена третьей премии в номинации «аспиранты» на конкурсе молодых математиков Фонда Эйлера. Статья на конференции CSR 2009 получила премию за лучшую студенческую статью.

Публикации результатов. Основные результаты диссертации опубликованы в пяти работах [1-5]. В работах [1, 4] соискателю принадлежит доказательство того, что при модификации с помощью наполнителя функция, которая не обращается за полиномиальное в среднем случае время, превращается в криптографически одностороннюю. Конструкция модификации с помощью наполнителя получена совместно с Э. А. Гиршем. В работе [2] соискателю принадлежит доказательство экспоненциальной нижней оценки на время работы «пьяных» алгоритмов на выполнимых формулах, доказательство нижней оценки для «близоруких» алгоритмов

принадлежит соавторам. Работы [1,2] опубликованы в изданиях, входящих в список рекомендованных Высшей аттестационной комиссией.

Структура и объем диссертации. Диссертация объемом 93 страницы состоит из введения и четырех основных глав, разбитых на разделы и подразделы. Список цитируемой литературы состоит из 44 наименований.

Содержание работы

Во **введении** обсуждаются рассматриваемые в диссертации задачи и состояние исследований в области, формулируются основные результаты, описывается структура диссертации.

В **первой главе** даются определения основных понятий, используемых в диссертации. В **первом разделе** даны определения ансамбля распределений и распределенных задач распознавания и распределенных **NP**-задач поиска. Во **втором разделе** даны определения того, что значит, что алгоритм работает полиномиальное в среднем время по Левину и по Импальяццо. Для вероятностных алгоритмов с ограниченной ошибкой приведено доказательство эквивалентности этих определений.

Согласно Левину, алгоритм работает полиномиальное в среднем случае время, если существует такое положительное число ϵ, что математическое ожидание функции $T^{\epsilon}(x)$ по всем входам x длины n есть $O(n)$, где $T(x)$ — это время работы алгоритма на входе x. Эквивалентное определение дал Импальяццо в 1995 году; согласно ему, вычислительная задача решается за полиномиальное в среднем время, если для нее существует алгоритм с двумя параметрами x (вход) и δ (вероятность ответа «не знаю»), время работы которого ограничено полиномом относительно $\frac{|x|}{\delta}$ и который отвечает «не знаю» с вероятностью не больше δ (в противном случае он выдает правильный ответ).

В **третьем разделе** даны определения классов распределенных задач поиска **FAvgP** и **FAvgBPP**. В **четвертом разделе** даны определения классов распределенных задач распознования $\mathbf{AvgP}, \mathbf{AvgBPP}$, $\mathbf{Avg}_{\delta(n)}\mathbf{P}$, $\mathbf{Avg}_{\delta(n)}\mathbf{BPP}$, $\mathbf{AvgTime}[g(n)]$,

AvgBPTime$[g(n)]$ и **AvgEXP**. В **пятом разделе** даны определения эвристических классов задач распознавания: **HeurP**, **HeurBPP**, **Heur**$_{\delta(n)}$**P**, **Heur**$_{\delta(n)}$**BPP**, **HeurTime**$[g(n)]$, **HeurBPTime**$[g(n)]$, **Avg**$_{\delta(n)}$**PTime**$[g(n)]$, **Avg**$_{\delta(n)}$**BPTime**$[g(n)]$, **Heur**$_{\delta(n)}$**PTime**$[g(n)]$, **Heur**$_{\delta(n)}$**BPTime**$[g(n)]$. В **шестом разделе** дано определение функций, криптографически односторонних для бесконечного числа длин входов. В **седьмом разделе** даны определения функции Голдрейха и двудольного граничного графа-расширителя, приведена теорема о существовании нужных графов-расширителей. В **восьмом разделе** приведено общее определение алгоритмов расщепления и дано определение «пьяных» алгоритмов расщепления.

Во **второй главе** приведен результат, показывающий, как из полиномиально вычислимой функции, которую не обратить полиномиальным в среднем вероятностным алгоритмом с ограниченной ошибкой, построить функцию, которая будет криптографически односторонней для бесконечного числа длин входов. В **первом разделе** приводятся детерминированные сведения «многие к одному» между распределенными задачами поиска и доказывается замкнутость классов **FAvgBPP** и **FAvgP** относительно этих сведений. Во **втором разделе** показывается, почему односторонняя в среднем случае функция не является автоматически слабой односторонней функцией, и приводится основная идея конструкции. Основная идея доказательства заключается в том, чтобы снабдить исходную функцию *наполнителем*. А именно, определяется новая функция $f_p(x, y)$ на парах строк, которая применяет f к своему первому аргументу и заменяет второй аргумент на строку $1^{|y|}$. В **третьем разделе** приводится конструкция со всеми деталями и доказывается теорема:

Теорема 1. *Если существует сохраняющая длину полиномиально вычислимая функция f, которая не может быть обращена за вероятностное (с ограниченной ошибкой) полиномиальное в среднем время с полиномиально моделируемым распределением на входах, то существует сохраня-*

ющая длину функция, которая является криптографической односторонней для бесконечного числа длин входов.

В **третьей главе** изучается структурные свойства класса **AvgBPP**. В **первом разделе** приводятся определения безошибочных и эвристических детерминированных сведений по Тьюрингу и доказывается замкнутость класса **AvgP** относительно безошибочных сведений и **HeurP** относительно эвристических сведений. Во **втором разделе** строится язык C и полиномиально моделируемое распределение R, для которых доказывается следующая теорема:

Теорема 2. *Задача* (C, R) *полна в классе* $(\mathbf{AvgBPP}, \mathbf{PSamp})$ *относительно детерминированных сведений по Тьюрингу.*

Следствием этой теоремы является то, что если задача (C, R) принадлежит классу $(\mathbf{AvgP}, \mathbf{PSamp})$ (или даже $(\mathbf{Avg}_{\frac{1}{n^c}}\mathbf{P}, \mathbf{PSamp})$), то $(\mathbf{AvgBPP}, \mathbf{PSamp})$ равняется $(\mathbf{AvgP}, \mathbf{PSamp})$. Аналогичное утверждение выполняется и для $(\mathbf{HeurBPP}, \mathbf{PSamp})$.

Построенное распределение R является не равномерным, а моделируемым искусственным образом. В **третьем разделе** дается интуитивный аргумент в пользу того, что для доказательства существования полной задачи с равномерным (или похожим на равномерное) распределением понадобится принципиально новая техника. Доказана следующая теорема:

Теорема 3. *Если существует полная задача в классе* $(\mathbf{AvgBPP}, \mathbf{PSamp})$ *относительно детерминированных сведений по Тьюрингу с плоским*[1] *распределением, то для всех языков* $L \in \mathbf{BPEXP}$ *распределенная задача* (L, U) *решается детерминированным алгоритмом с экспоненциальным в среднем случае временем, где* U *обозначает равномерное распределение.*

В **четвертом параграфе** доказывается теорема об иерархии по времени в классе $(\mathbf{AvgBPP}, \mathbf{PSamp})$.

[1]Распределение называется плоским, если вероятность любой строки x не превосходит $2^{|x|^\epsilon}$ для некоторого $\epsilon > 0$.

Теорема 4. *Для каждого $c \geq 1$ существует такой язык L и полиномиально моделируемое распределение D при котором $(L, D) \in$* **AvgBPP** *и $(L, D) \notin$* **AvgBPTime**$[n^c]$.

В **пятом параграфе** сравниваются классы **AvgP**, **AvgBPP**, **HeurP**, **HeurBPP** с их аналогами в наихудшем случае и показывается, что включения строгие. Доказывается теорема для детерминированных классов:

Теорема 5. *Выполняются следующие соотношения: 1)* $(\mathbf{P}, U) \subsetneq (\mathbf{AvgP}, U) \subseteq (\mathbf{HeurP}, U)$*; 2)* $(\mathbf{HeurP}, \mathbf{PSamp}) \subseteq (\mathbf{EXP}, \mathbf{PSamp})$*; 3) Существует такой язык $L_{EXP} \in$* **EXP**, *что для любого распределения $D \in$* **PSamp** *задача (L_{EXP}, D) не содержится в классе* $(\mathbf{HeurP}, \mathbf{PSamp})$.

Также доказывается аналогичная теорема для вероятностных классов:

Теорема 6. *Выполняются следующие соотношения 1)* $(\mathbf{BPP}, U) \subsetneq (\mathbf{AvgBPP}, U) \subseteq (\mathbf{HeurBPP}, U)$*; 2)* $(\mathbf{HeurBPP}, \mathbf{PSamp}) \subseteq (\mathbf{BPEXP}, \mathbf{PSamp})$*; 3) Существует язык $L \in$* **BPPEXP**, *что для любого распределения $D \in$* **PSamp** *задача (L, D) не содержится в классе* $(\mathbf{HeurBPP}, \mathbf{PSamp})$.

В **четвертой главе** изучаются «пьяные» алгоритмы расщепления и доказывается экспоненциальная нижняя оценка на время обращения функции Голдрейха пьяными алгоритмами в среднем случае. В **первом разделе** доказывается, что «пьяные» алгоритмы без существенной потери производительности могут не использовать правила упрощения: правило удаления единичного дизъюнкта и правило чистых литералов, показывается, что выполнимые цейтинские формулы могут быть решены «пьяными» алгоритмами за полиномиальное время. Во **втором разделе** рассказывается о связи алгоритмов расщепления с резолюционной системой доказательств и приводится известное предложение:

Предложение 1. *Время работы «пьяного» алгоритма на невыполнимой формуле не меньше, чем размер (количество дизъюнктов) кратчайшего древовидного резолюционного доказательства.*

В **третьем разделе** приводится доказательство экспоненциальной нижней оценки для «пьяных» алгоритмов в наихудшем случае. Приводится простой способ построения трудной выполнимой формулу из любой невыполнимой формулы, трудной для резолюций. В частности, с использованием трудных невыполнимых формул из статьи (Пудлак, Импальяццо, 2000) доказана следующая теорема:

Теорема 7. *Для каждого $k \geq 3$ существует положительная константа $c_k = O(k^{-1/8})$, функция $f'(x) = \Omega(2^{x(1-c_k)})$ и последовательность выполнимых формул H_n в $(k+1)$-КНФ (H_n использует m переменных, где $n \leq m \leq n^2$) такие, что время работы любого «пьяного» алгоритма на входе H_n меньше $f'(n)$ с вероятностью не больше 2^{-n}.*

В **четвертом разделе** доказывается нижняя оценка для невыполнимых формул, кодирующих обращение функции Голдрейха.

В **пятом разделе** доказывается основной результат: экспоненциальная нижняя оценка на время обращения функции Голдрейха «пьяными» алгоритмами в среднем случае. В **первом подразделе** приводятся определения k-замыкания и множества Cl^k и доказывается оценка на размер k-замыкания. Во **втором подразделе** приводится описание надстройки над «пьяными» алгоритмами, которая не увеличивает время работы «пьяного» алгоритма на формулах, кодирующих задачу обращения функции Голдрейха, при которой алгоритм в течение линейного числа подстановок не совершает возвратов. В **третьем подразделе** оценивается количество решений уравнения $g(x) = g(y)$ для функции Голдрейха g, построенной по случайному графу. В **четвертом подразделе** доказывается основная теорема:

Теорема 8. *Пусть $P_d(x_1, x_2, \ldots, x_d) = x_1 \oplus \ldots x_{d-k} \oplus Q(x_{d-k+1}, \ldots, x_d)$, где Q — произвольный предикат, $k+1 < \frac{d}{4}$. Для достаточно больших d*

и для достаточно больших n случайный двудольный граф G обладает с вероятностью хотя бы 0.85 *следующим свойством: для любого «пьяного» алгоритма $\mathcal{A}$, $\Pr_{y \leftarrow U_n}\{\Pr\{t^{\mathcal{A}}_{\Phi_{g(x)=g(y)}} > 2^{\Omega(n)}\} > 1 - 2^{-\Omega(n)}\} > 0.9$, где g — это функция Голдрейха, построенная по предикату P_d и графу G, $t^{\mathcal{A}}_{\Phi}$ обозначает время работы алгоритма $\mathcal{A}$ на формуле Φ, а $\Phi_{g(x)=b}$ — это формула в КНФ, кодирующая равенство $g(x) = b$.*

Публикации автора по теме диссертации

Статьи в журналах, рекомендованных ВАК:

1. *Гирш Э.А., Ицыксон Д.М.* Бесконечно часто односторонняя функция, основанная на предположении о сложности в среднем // Алгебра и Анализ. 2009. Том 21, № 3. С. 130–144.

2. *Alekhnovich M., Hirsch E. A., Itsykson D.* Exponential Lower Bounds for the Running Time of DPLL Algorithms on Satisfiable Formulas // Journal of Automated Reasoning. 2005. Vol. 35, N. 1-3. P. 51–72.

Другие публикации:

3. *Ицыксон Д.М.* Нижняя оценка на среднее время обращения функции Голдрейха «пьяными» алгоритмами расщепления // Препринты ПОМИ РАН. 2009. № 3. С. 1–17.

4. *Hirsch E. A., Itsykson D. M.* An infinitely-often one-way function based on an average-case assumption // Proceedings of the 15th Workshop on Logic, Language, Information and Computation. Vol. 5110 of Lecture Notes in Computer Science. 2008. P. 208–217.

5. *Itsykson D. M.* Structural complexity of AvgBPP // Proceedings of the 4th International Computer Science Symposium in Russia, LNCS. Vol. 5675 of Lecture Notes in Computer Science. 2009. P. 155–166.