На правах рукописи

Соколов Дмитрий Олегович

Сложность решения задачи выполнимости булевых формул алгоритмами, основанными на расщеплении

01.01.06 — математическая логика, алгебра и теория чисел

01.01.09 — дискретная математика и математическая кибернетика

Автореферат

диссертации на соискание ученой степени

кандидата физико-математических наук

Санкт-Петербург — 2014

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

Научные руководители:

Гирш Эдуард Алексеевич

доктор физико-математических наук, доцент, ведущий научный сотрудник лаборатории математической логики ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук

Ицыксон Дмитрий Михайлович

кандидат физико-математических наук, старший научный сотрудник лаборатории математической логики ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук

Официальные оппоненты:

Райгородский Андрей Михайлович

доктор физико-математических наук

профессор ФГОУ ВПО "Московский Государственный Университет им. М.В. Ломоносова"

Шень Александр Ханьевич

кандидат физико-математических наук

старший научный сотрудник лаборатории № 1 им. М.С. Пинскера ФГБУН Института проблем передачи информации им. А.А. Харкевича Российской академии наук

Ведущая организация: ФГАОУВПО "Казанский (Приволжский) федеральный университет"

Защита состоится «4» марта 2015 г. в 17:00 на заседании диссертационного совета Д002.202.02 в ФГБУН Санкт-Петербургском отделении Математического института им. В. А. Стеклова Российской академии наук по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, 27, к. 311.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук, http://www.pdmi.ras.ru/

Автореферат разослан «____» _____ 2015 г.

Ученый секретарь
диссертационного совета, д. ф.-м. н. А. В. Малютин

Общая характеристика работы

Актуальность темы. Задача выполнимости булевых (пропозициональных) формул (SAT) — это задача нахождения по булевой формуле такой подстановки значений переменным, что при применении данной подстановки формула обращается в тождественную истину. Если такая подстановка существует, то формула называется выполнимой; если же нет, то функция, задаваемая данной формулой, является тождественной ложью, и формула является невыполнимой.

SAT — одна из первых задач, для которых была доказана **NP**-полнота (теорема Кука-Левина (1973)). Это означает, что любая задача из класса **NP**, который включает в себя широкий круг естественных задач, возникающих на практике, сводится к задаче выполнимости булевых формул. Таким образом существование эффективного алгоритма для SAT (как и доказательство его отсутствия) эквивалентно одной из центральных задач теории сложности о равенстве между классами **P** и **NP**, и таких алгоритмов в настоящее время не известно.

Несмотря на это, формулы, возникающие на практике, успешно решаются при помощи SAT-солверов (программ для решения задачи выполнимости). Одним из основных подходов к решению задачи выполнимости пропозициональных формул являются DPLL-алгоритмы (названы в честь авторов: Davis, Putnam, Logemann и Loveland), основанные на методе расщепления. DPLL-алгоритм — рекурсивный алгоритм, который на вход получает формулу ϕ, затем запускает процедуру **A**, которая выбирает переменную x, после этого алгоритм запускает процедуру **B** для выбора константы c, затем рекурсивно вызывает себя на формуле $\Phi[x := c]$, если был найден выполняющий набор, то выдает его, иначе возвращает результат запуска алгоритма на формуле $\Phi[x := 1 - c]$. Рекурсивные вызовы прекращаются, когда формула становится тривиальной. Таким образом, алгоритм расщепления определяется

правилами упрощения и двумя эвристиками: эвристика **A** выбирает переменную, а эвристика **B** выбирает, какое значение переменной будет проверено раньше.

Известны экспоненциальные нижние оценки на время работы DPLL-алгоритмов на невыполнимых формулах, в частности, такие оценки следуют из оценок на размер резолюционных доказательств. В случае выполнимых формул суперполиномиальные нижние оценки на время работы всех возможных DPLL-алгоритмы повлекли бы за собой неравенство $\mathbf{P} \neq \mathbf{NP}$. Экспериментальные данные показывают, что современные `SAT`-солверы могут выдавать корректный результат за приемлемое время на значительно больших выполнимых формулах, чем на невыполнимых. Несмотря на важность задачи существует не так много работ, в которых доказываются нижние оценки на время работы DPLL-алгоритмов на выполнимых формулах. Для других алгоритмов — основанных на локальном поиске — экспоненциальные нижние оценки для выполнимых формул известны довольно давно — с работ Гирша (2000) и Алехновича и Бен-Сассона (2002), также некоторые оценки были доказаны в работах Николенко (2003) и Бима (и др.) (2001). В работе Алехновича, Гирша и Ицыксона (2005) дается экспоненциальная нижняя оценка для двух достаточно больших классов DPLL-алгоритмов — "близоруких" и "пьяных".

В работах Тревисана (и др.) (2009, 2014) и Ицыксона (2010) представлен "криптографический" взгляд на рассматриваемую проблему. 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 (из этого следует, что задача обращения функции лежит в классе **NP**). В 2000 году Голдрейх в своей работе предложил в качестве кандидата односторонней функции конструкцию, основанную на графах-экспандерах. Его конструкция принимает в качестве параметра двудольный

граф с n вершинами в каждой доле и степенью d каждой вершины в правой доле (где d — некоторая константа, не зависящая от n или функция, растущая не быстрее $O(\log(n))$), а также предикат $P : \{0,1\}^d \to \{0,1\}$. Для того, чтобы вычислить функцию на входе $x \in \{0,1\}^n$, сопоставим биты входа вершинам из левой доли графа, после чего пометим каждую вершину в правой доле значением предиката P, примененного к соседям вершины. Значением функции будет последовательность пометок вершин правой доли. В работе Трэвисана было замечено, что нижняя оценка для близоруких алгоритмов была доказана на формулах, которые кодируют задачу обращения функции Голдрейха с линейным предикатом. Однако линейная функция Голдрейха неинтересна с криптографической точки зрения, так как она быстро обращается при помощи метода Гаусса. Мотивацией в работе Трэвисана было доказательство нижней оценки для функции, которую, действительно трудно обратить. Как результат данной работы, была обобщена техника, разработанная в работе Алехновича, Гирша и Ицыксона для доказательства нижней оценки для близоруких алгоритмов, на нелинейные предикаты и доказана экспоненциальная нижняя оценка на среднее (по входам функции) время обращения функции Голдрейха с предикатом $x_1 \oplus x_2 \oplus \cdots \oplus x_{d-2} \oplus x_{d-1}x_d$ близорукими алгоритмами. Также было показано, что задача обращения функции Голдрейха с таким предикатом трудна для программы MiniSAT 2.0. Во всех перечисленных работах функция Голдрейха строится не явно, конструкция графа зависимостей вероятностная.

Все описанные нижние оценки на выполнимых формулах основаны на факте, что после нескольких шагов алгоритма формула станет трудной невыполнимой и алгоритм обойдет для нее все дерево расщепления. Однако, если разрешить алгоритму не просматривать некоторые ветви дерева, то никаких оценок не известно, в то время как такой подход кажется естественным для эвристических алгоритмов.

Формулы, которые кодируют невыполнимые системы линейных уравнений, сложны для DPLL-алгоритмов. В работе Алехновича, Гирша и Ицыксона показано, что выполнимые системы линейных уравнений также являются сложными примерами для близоруких и пьяных DPLL-алгоритмов. Естественное обобщение DPLL-алгоритмов, которое может помочь решать линейные системы уравнений — алгоритмы, в которых расщепление происходит по линейной комбинации переменных над полем $\mathbb{F}_2$. На текущий момент данные алгоритмы не исследованы, однако идеи подобного расщепления используются в теоретических алгоритмах для решения задачи выполнимости, в частности, в алгоритме Сето и Тамаки (2013).

Систематическое изучение вопросов, связанных с системами доказательств для пропозициональной логики, в частности, вопроса о длине минимального доказательства в различных системах, началось с работы Кука и Рекоу (1979). Интерес к этим вопросам обусловлен, в частности, тем, что пропозициональная система доказательств — это недетерминированный алгоритм, который определяет, является ли булева формула тавтологией (или невыполнимой формулой), таким образом неравенство $\mathbf{NP} \neq \mathbf{co\text{-}NP}$ влечет существование трудных примеров для всех систем доказательств. Следующий план иногда называют программой Кука: доказывать суперполиномиальные нижние оценки для все более сильных систем доказательств, пока не удастся развить методы, позволяющие обобщить результаты на произвольную систему доказательств.

Как было указано выше, для резолюционной системы доказательств существуют экспоненциальные нижние оценки. Однако, если разрешить вместо переменных использовать линейные комбинации над полем $\mathbb{F}_2$, соответствующим образом преобразовав операции резолюционной системы доказательств, то получившая система будет не слабее классической резолюции, и на текущий момент нижних оценок на нее не известно. Также, как работа

DPLL-алгоритмов тесно связана, с резолюционной системой доказательств, работа алгоритмов расщепления по линейным уравнениям тесно связана с указанным обобщением резолюционной системы доказательств. Похожие системы доказательств рассматриваются в работе Раза и Цемерета (2008), однако в их работе рассматриваются линейные уравнения над целыми числами, а не над полем $\mathbb{F}_2$.

Цели работы.

1. Получить явную конструкцию графа и предиката, для которых функция Голдрейха является криптографически устойчивой по отношению к близоруким DPLL-алгоритмам. Доказать нижнюю оценку на время обращения данной функции.

2. Предложить обобщение DPLL-алгоритмов, добавив эвристику отсечения ветвей. Построить трудные примеры и доказать нижнюю оценку на время работы данного обобщения.

3. Построить двудольный граф-экспандер с ограниченной степенью вершин и полным рангом матрицы смежности.

4. Предложить схему алгоритмов расщепления по линейным функциям над полем $\mathbb{F}_2$ для решения задачи выполнимости. Доказать нижние и верхние оценки для данных алгоритмов.

5. Описать системы доказательств, связанные с алгоритмами расщепления по линейным функциям. Доказать нижние оценки для полученных систем доказательств.

Научная новизна. Все результаты диссертации являются новыми.

Теоретическая и практическая ценность. Работа носит теоретический характер. Ее результаты могут быть использованы в структурной тео-

рии сложности и теории сложности в среднем для анализа алгоритмов, в теории сложности доказательств для получения оценок на различные системы доказательств. Конструкции графов-экспандеров могут быть использованы в различных областях дискретной математики и теории сложности.

Методы исследований. В работе используются методы теории сложности вычислений и доказательств, а также техника работы с графами-экспандерами. В частности, используются методы коммуникационной сложности, явные конструкции графов-экспандеров, строятся системы доказательств, используются методы расщепления.

Основные результаты.

1. Получена явная конструкция такого графа-экспандера и предиката, что с вероятностью, близкой к 1, близорукие DPLL алгоритмы работают экспоненциальное время на формулах, кодирующих задачу обращения функции Голдрейха, основанной на данном графе и предикате.

2. Получена явная конструкция семейства таких невыполнимых формул $\Phi^{(n)}$, что для любого близорукого DPLL-алгоритма с эвристикой отсечения ветвей существует такой явный ансамбль распределений на выполнимых формулах R_n, что данный алгоритм либо ошибается на 99% формул, сгенерированных согласно распределению R_n, либо работает экспоненциальное время на формуле $\Phi^{(n)}$.

3. Получена явная конструкция двудольных графов-экспандеров, с ограниченной степенью вершин в обоих долях и полным рангом матрицы смежности над полем $\mathbb{F}_2$.

4. Построена модель алгоритмов расщепления с расщеплением по линейным комбинациям переменных. Доказана полиномиальная верхняя оценка на время работы таких алгоритмов на формулах, кодирующих линейные системы уравнений. Доказана экспоненциальная нижняя

оценка на данную модель для 2-кратных цейтинских формул.

5. Описана система доказательств Res-Lin и Sem-Lin. Доказана их эквивалентность и семантическая полнота. Получена конструкция по дереву расщеплений древовидного доказательства в системе Res-Lin. Доказана экспоненциальная нижняя оценка на древовидные системы Res-Lin и Sem-Lin на 2-кратных цейтинских формулах.

Апробация работы. Результаты диссертационной работы были изложены на следующих конференциях и семинарах.

1. Международная конференция "The 6th International Computer Science Symposium in Russia" (Санкт-Петербург, CSR 2011).

2. Санкт-Петербургский городской семинар по дискретной математике.

3. Международная конференция "First Russian-Finnish Symposium on Discrete Mathematics" (Санкт-Петербург, RuFiDim 2011).

4. Колмогоровский семинар (Москва, 2011).

5. Международная конференция "The 22nd International Symposium on Algorithms and Computation" (Йокогама, ISAAC 2011).

6. Семинар по математической логике математического института города Прага (Прага, 2013).

7. Международный симпозиум "Franco-Russian workshop on Algorithms, complexity and applications" (Москва, 2013).

8. Международный симпозиум "Proof Complexity" (Вена, PC 2014).

9. Международная конференция "Mathematical Foundations of Computer Science 2014 - 39th International Symposium" (Будапешт, MFCS 2014).

Публикации. Основные результаты диссертации опубликованы в рецензируемых научных изданиях — [1], [2], [3], [4].

Работы [1]-[4] написаны в соавторстве. В работе [2] диссертанту принадлежат: конструкция графа-экспандера, достаточного для создания почти биективной функции Голдрейха (раздел 3); оценка на число прообразов функции Голдрейха после подстановок (леммы 5.6 и 5.7); реализация схемы доказательства, предложенной Ицыксоном в теоремах 5.1 и 5.2, эти же результаты приводятся в работе [1]. В работе [3] диссертанту принадлежат: конструкция по невыполнимой формуле семейства близоруких копий (лемма 3.1); упрощение понятия замыкания (раздел 4); доказательство свойств замыкания, предложенных Ицыксоном (предложение 4.1); конструкция экспандера с полным рангом матрицы смежности и ограниченной степенью вершин (лемма 5.1 и раздел 6); доказательство лемм 5.2 и 5.4, являющихся частью доказательства теоремы 5.1; доказательство, предложенной Ицыксоном теоремы о трудных распределениях на выполнимых формулах (теорема 5.3). В работе [4] диссертанту принадлежат: определение модели алгоритмов с расщеплением по линейным функциям, определение систем доказательств Res-Lin и Sem-Lin, результаты из раздела 4 о нижней оценке для 2-кратных цейтинских формул и результаты раздела 6 о системах доказательств Res-Lin и Sem-Lin.

Неупомянутые результаты работ принадлежат соавторам.

Структура и объем работы. Диссертация состоит из введения, четырех глав и списка литературы. Общий объем диссертации 88 страниц. Список литературы включает 51 наименование на 6 страницах.

Содержание работы

Во введении обсуждаются рассматриваемые в диссертации задачи, приводится обзор состояния исследований в области, формулируются основные

результаты диссертации, описывается структура диссертации.

В **первой главе** приведены основные определения и базовые теоремы, используемые в диссертации. В первом разделе дается определение систем доказательств: согласно Куку системой доказательств для языка L называется полиномиальный по времени алгоритм $\Pi : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$, для которого выполнены следующие свойства:

- (полнота) если $x \in L$, то существует такой y, что $\Pi(x, y) = 1$;
- (корректность) если существует такой y, что $\Pi(x, y) = 1$, то $x \in L$.

Также в первом разделе определяется резолюционная система доказательств. Во втором разделе дается определение общей схемы алгоритмов расщепления (DPLL-алгоритмов). Алгоритм расщепления параметризован двумя *эвристиками* (процедурами):

- процедура **A**, которая по формуле в КНФ выдает переменную из этой формулы. Это переменная, по которой будет проводиться расщепление;
- процедура **B**, которая по формуле в КНФ и ее переменной выдает значение из $\{0,1\}$. Это значение, которое будет подставляться при расщеплении первым.

Алгоритм расщепления — это рекурсивный алгоритм, который получает на вход формулу φ и частичную подстановку ρ и работает следующим образом:

- Упростить φ с помощью правил упрощения (считаем, что правила упрощения меняют φ и ρ, причем все переменные, значения которых определяются подстановкой ρ, удаляются из формулы φ).
- Если формула стала пустой (т.е. все ее дизъюнкты выполнены подстановкой ρ), то выдать ρ. Если формула содержит пустой дизъюнкт (заведомо невыполнимый), то выдать «формула невыполнима».

- $j := \mathbf{A}(\varphi)$.
- $c := \mathbf{B}(\varphi, j)$.
- Запустить алгоритм рекурсивно на $(\varphi[x_j := c], \rho \cup \{x_j := c\})$; если алгоритм выдал подстановку, то выдать ее, в противном случае рекурсивно запустить на $(\varphi[x_j := 1 - c], \rho \cup \{x_j := 1 - c\})$; если рекурсивный вызов выдал подстановку, то выдать ее, иначе выдать «формула невыполнима».

Также во втором разделе первой главы определяются “пьяные” и “близорукие” DPLL-алгоритмы и показывается связь между алгоритмами расщепления и резолюционной системой доказательств. В третьем разделе дано определение функции Голдрейха и описано сведение задачи обращения функции к задаче выполнимости булевой формулы. В четвертом разделе дано определение графов-экспандеров и приведены примеры явных конструкций. В пятом разделе сформулировано понятие полиномиально моделируемого распределения на входах.

Вторая глава посвящена конструкции функции Голдрейха, обращение которой является трудной задачей для близоруких DPLL-алгоритмов. Предлагаемая функция Голдрейха имеет следующую структуру: она состоит из суммы линейной функции Голдрейха и нелинейной. Линейная функция нужна для того, чтобы DPLL-алгоритмам было сложно ее обратить, а нелинейная нужна для того, чтобы получившаяся функция не была бы тривиально обратимой. Во втором разделе мы берем линейную функцию Голдрейха, основанную на экспандере и немного модифицируем ее для того, чтобы она стала почти биективной. Затем в разделе 2 мы доказываем нижнюю оценку на время работы близоруких DPLL-алгоритмов на невыполнимых формулах, полученных путем модификации формул, кодирующих задачу обращения. В третьем разделе мы определяем понятие “умного близорукого” алгоритма,

который сильнее, чем просто "близорукий", и показываем, что для функции, построенной по методу, описанному в разделе 1 с большой вероятностью за первые несколько шагов текущая формула станет невыполнимой, и применяем доказанную оценку для невыполнимых формул. Результатом главы 2 является следующая теорема.

Теорема 1. Для любого $\epsilon > 0$ существует такая явная конструкция нелинейной функции Голдрейха f, что для любого "близорукого" алгоритма A, выполнено $\Pr\limits_{y,s}[t_A(\Phi_{f(x)=f(y)}) \geq 2^{\Omega(n)}] \geq 1 - 2^{-\Omega(\frac{n}{K})}$, где $t_A(x)$ — время работы алгоритма A на входе x, s — строка случайных битов, которые использует алгоритм A и $K = n^{1-\epsilon}$.

В **третьей главе** класс DPLL-алгоритмов расширяется добавлением эвристику отсечения, которая может решить что ветвь дерева расщепления "бесперспективная" и не стоит ее просматривать. Цель данной главы — построение за полиномиальное время семейства таких невыполнимых формул $\Phi^{(n)}$, что для любых детерминированных эвристик $\mathbf{A}$ и $\mathbf{C}$ найдется такой полиномиально моделируемый ансамбль распределений R_n, что DPLL-алгоритм, основанный на эвристиках $\mathbf{A}, \mathbf{B}$ и $\mathbf{C}$ для некоторой эвристики $\mathbf{B}$ либо ошибается на 99% формул, сгенерированных согласно распределению R_n, либо работает экспоненциальное время на формуле $\Phi^{(n)}$.

В первом разделе дается формальное определение DPLL-алгоритмов с эвристикой отсечения ветвей. Во втором разделе для произвольной невыполнимой формулы Φ описывается достаточное свойство семейства выполнимых формул для доказательства искомой оценки, семейство формул, удовлетворяющее данному свойству назовем "система близоруких копий". В третьем разделе описывается вспомогательная конструкция замыкания. Данная конструкция является упрощением конструкции, предложенной Алехновичем и описанной в главе 2.

В четвертом разделе доказывается основная теорема данной главы.

Теорема 2. Существуют такой полиномиальный алгоритм, который выдает по n невыполнимую формулу $\Phi^{(n)}$, и такая константа $\delta > 0$, что для любого близорукого алгоритма с полиномиальными эвристиками $\mathbf{A}$ и $\mathbf{C}$ найдется такой полиномиально моделируемый ансамбль распределений R_n на выполнимых формулах, что если для некоторой эвристики $\mathbf{B}$ и некоторого $\epsilon > 0$ неравенство $\Pr\limits_{\phi \leftarrow R_n}[\mathcal{D}_{\mathbf{A},\mathbf{B},\mathbf{C}}(\phi) = 1] \geq 1 - \epsilon$ выполнено, то время работы алгоритма $\mathcal{D}_{\mathbf{A},\mathbf{B},\mathbf{C}}(\Phi^{(n)})$ не менее $(1-\epsilon)2^N$, где $N = min\{n^\delta, r/K\}$,$r = \Omega(n)$ и K — параметр близорукого алгоритма.

В первом параграфе данного раздела описывается конструкция семейства близоруких копий по формуле и алгоритму при помощи замыканий из раздела 3, данная конструкция основана на графах-экспандеров с дополнительными условиями, которая описана в разделе 5. Затем данная теорема обобщается с использованием стандартной техники и строится единое распределение, которое является трудным для всех алгоритмов. В конце раздела теорема 2 обобщается на случай трудных примеров, основанных на выполнимых формулах.

В пятом разделе описывается конструкция графов, необходимая для завершения доказательства из раздела 4.

Лемма 1. Для любого достаточно большого d и любого n существует явная конструкция $(r, d, 0.75d)$-экспандера с размерами долей $|X| = |Y| = n$, $r = \Omega(n)$ и со степенью вершин из доли X не более $20kd$, где k — достаточно большая константа.

В четвертой главе рассматривается обобщение DPLL-алгоритмов на случай, когда допускается расщепление по линейным комбинациям переменных над полем $\mathbb{F}_2$. В первом разделе главы дается формальное определение линейных деревьев расщеплений. Во втором разделе показывается, что при помощи линейных деревьев можно эффективно искать выполняющие наборы

для формул, кодирующих линейные системы уравнений. Заметим, что существуют такие системы линейных уравнений, для которых доказана нижняя оценка на время работы классических DPLL-алгоритмов. Также в разделе 2 показывается, что при помощи линейных деревьев расщеплений можно эффективно решать задачу выполнимости для формул, кодирующих существование совершенного паросочетания в графе с нечетным числом вершин.

В третьем разделе показывается связь между линейными деревьями расщеплений и коммуникационной сложностью задачи $Search_\phi$ — по подстановке значений переменным формулы ϕ найти опровергнутый дизъюнкт. Доказывается следующая теорема:

Теорема 3. Пусть ϕ — невыполнимая формула в КНФ и T — линейное дерево расщеплений для ϕ. Тогда для любого распределения переменных между участниками коммуникационного протокола верно следующее утверждение: $R^{pub}_{\frac{1}{3}}(Search_\phi) = O(\log(|T|)\log\log(|T|))$.

Как следствие из данной теоремы доказывается нижняя оценка на линейное дерево расщеплений для 2-кратных цейтинских формул.

Теорема 4. За полиномиальное от n время можно построить граф $G(V,E)$ на n вершинах с максимальной степенью, ограниченной константой, и такую функцию $c : V \to \mathbb{F}_2$, что размер любого линейного дерева расщепления $TS^2_{(G,c)}$ по крайней мере $\Omega\left(2^{n^{1/3}/\log^3(n)}\right)$.

В разделе 4 приведено краткое доказательство нижней оценки на линейное дерево расщеплений для формул, кодирующих принцип Дирихле. В пятом разделе описываются системы доказательств Res-Lin и Sem-Lin, которые оперируют с линейными дизъюнктами — дизъюнкциями линейных уравнений. Показывается связь между линейными деревьями расщеплений и древовидной версией системы Res-Lin, таким образом нижние оценки на линейные деревья расщеплений переносятся на древовидную систему Res-Lin.

Затем в разделе 5 показывается эквивалентность систем Res-Lin и Sem-Lin, таким образом нижние оценки переносятся на древовидную версию системы Sem-Lin. В разделе 5.2 доказывается импликативная полнота систем Res-Lin и Sem-Lin, что позволяет перенести некоторые классические результаты, например, лемму о дедукции, на данные системы доказательств:

Теорема 5. Если линейный дизъюнкт C_0 семантически следует из $C_1, C_2, \ldots, C_k$, то C_0 может быть выведен из $C_1, C_2, \ldots, C_k$ в Res-Lin.

В разделе 5.3 доказывается, что система $R(lin)$, описанная в работе Раза и Цемерета (2008) моделирует системы Res-Lin и Sem-Lin.

Публикации автора по теме диссертации в рецензируемых научных изданиях:

1. Itsykson Dmitry, Sokolov Dmitry. The Complexity of Inversion of Explicit Goldreich's Function by DPLL Algorithms // Computer Science — Theory and Applications / под ред. Alexander Kulikov, Nikolay Vereshchagin. Springer Berlin Heidelberg, 2011. Т. 6651 из *Lecture Notes in Computer Science*. С. 134–147.

2. Ицыксон Дмитрий, Соколов Дмитрий. Сложность обращения явной функции Голдрейха DPLL алгоритмами // Записки научных семинаров ПОМИ. 2012. Т. 399. С. 88–108.

3. Itsykson Dmitry, Sokolov Dmitry. Lower Bounds for Myopic DPLL Algorithms with a Cut Heuristic // Algorithms and Computation / под ред. Takao Asano, Shin-ichi Nakano, Yoshio Okamoto [и др.]. Springer Berlin Heidelberg, 2011. Т. 7074 из *Lecture Notes in Computer Science*. С. 464–473.

4. Itsykson Dmitry, Sokolov Dmitry. Lower Bounds for Splittings by Linear Combinations // Mathematical Foundations of Computer Science 2014 / под

ред. Erzsébet Csuhaj-Varjú, Martin Dietzfelbinger, Zoltán Ésik. Springer Berlin Heidelberg, 2014. Т. 8635 из *Lecture Notes in Computer Science*. С. 372–383.

Другие публикации автора по теме диссертации:

5. Соколов Д. Нижние оценки на время работы DPLL алгоритмов с расщеплением по линейным функциям // Препринты ПОМИ РАН. Препринт 1/2014. 2014.

6. Itsykson Dmitry, Sokolov Dmitry. Lower bounds for myopic DPLL algorithms with a cut heuristic // Electronic Colloquium on Computational Complexity (ECCC). 2012. Т. 19. С. 141.