На правах рукописи

Ицыксон Дмитрий Михайлович

Нижние оценки и вопросы оптимальности для систем доказательств

01.01.06 — математическая логика, алгебра и теория чисел

Автореферат
диссертации на соискание ученой степени
доктора физико-математических наук

Санкт-Петербург
2022

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

Официальные оппоненты: **Верещагин Николай Константинович**,
доктор физико-математических наук,
профессор,
Московский государственный университет
им. М.В. Ломоносова, профессор

Григорьев Дмитрий Юрьевич
доктор физико-математических наук

Разборов Александр Александрович
доктор физико-математических наук,
чл.-корр. РАН,
Математический институт им. В. А. Стеклова
РАН, главный научный сотрудник

Ведущая организация: Федеральное государственное автономное
образовательное учреждение высшего
образования «Уральский федеральный
университет имени первого Президента
России Б.Н. Ельцина»

Защита диссертации состоится “ ” 2022 г. в на заседании совета Д 002.202.02 по защите докторских и кандидатских диссертаций при Санкт-Петербургском отделении Математического института им. В. А. Стеклова Российской академии наук по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, 27, ауд. 311.

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

Автореферат разослан “ ” 2022 г.

Телефон для справок: +7 (812) 312-40-58.

Ученый секретарь
диссертационного совета,
доктор физ.-мат. наук Пономаренко И. Н.

Актуальность темы

Программа Кука-Рекхау. Сложность пропозициональных доказательств — это раздел теории сложности вычислений, в котором изучаются системы доказательств для языка невыполнимых формул в КНФ (UNSAT). Понятие системы доказательств определяется для каждого языка (т.е. для подмножества множества строк над некоторым конечным алфавитом). Доказываемые утверждения имеют вид «строка x принадлежит языку L». Системой доказательств для языка L называется полиномиальный по времени алгоритм Π, который получает на вход пару строк (x, w); строка x — это строка, принадлежность которой языку L мы пытаемся доказать, а w — кандидат на роль доказательства. Неформально, алгоритм Π проверяет доказательство на корректность. Формально, должны выполняться два следующих свойства:

1. (Корректность) Если $\Pi(x, w) = 1$, то $x \in L$.
2. (Полнота) Для каждого $x \in L$ существует такая строка w, что $\Pi(x, w) = 1$.

Система доказательств Π для языка L называется полиномиально ограниченной, если существует такой полином p, что для любой строки $x \in L$ найдется строка w длины не более $p(|x|)$, что $\Pi(x, w) = 1$. Нетрудно видеть, что класс NP состоит в точности из языков, для которых существует полиномиально ограниченная система доказательств. Класс coNP состоит из языков, дополнение которых лежит в классе NP; известно, что язык UNSAT, состоящий из невыполнимых пропозициональных формул в КНФ, является полным в классе coNP. Вопрос о равенстве классов coNP и NP открыт, основная гипотеза состоит в том, что эти два класса не равны. Стоит отметить, что из NP $\neq$ coNP следует P $\neq$ NP, а вопрос о равенстве классов P и NP является одним из самых известных открытых математических проблем, в частности, этот вопрос включен в список проблем тысячелетия институтом Клэя. Классы NP и coNP различаются тогда и только тогда, когда язык UNSAT не имеет полиномиально

ограниченных систем доказательств. Кук и Рекхау [26] предложили программу по доказательству различности классов NP и coNP, которая состоит в том, чтобы рассматривать различные системы доказательств для UNSAT и находить для каждой из них трудное семейство невыполнимых формул, т.е. такое, для которого в этой системе нет доказательств полиномиального размера. Находя трудные формулы во все более и более сильных системах доказательств, мы будем постепенно приближаться к доказательству NP $\neq$ coNP. Для многих важных пропозициональных систем доказательств суперполиномиальные нижние оценки все еще не доказаны, однако исследование сложности систем доказательств оказало существенное влияние на другие области исследования.

Алгоритмы для задачи выполнимости. Программа Кука и Рекхау предлагает больше, чем просто программу по доказательству NP $\neq$ coNP. Действительно, даже если будет доказано, что NP $\neq$ coNP, то из этого не следует, что для каждой конкретной системы доказательств легко найти трудные формулы. Теория сложности пропозициональных доказательств имеет огромное влияние на разработку алгоритмов для задачи выполнимости булевой формулы SAT. Каждый алгоритм для задачи SAT задает систему доказательств для языка UNSAT: доказательством невыполнимости формулы ϕ в этой системе является протокол работы алгоритма на формуле ϕ. Системы доказательств, изучаемые в теории сложности пропозициональных доказательств, лежат в основе основных алгоритмов для задачи выполнимости. Первые практические реализации алгоритмов для SAT были основаны на подходе, предложенным Дэвисом, Путнамом, Ловелэндом и Логеманом [29] [28] (по инициалам авторов этот подход называют DPLL), этот подход соответствует древовидной резолюции. Практически все самые быстрые современные алгоритмы для SAT используют подход CDCL (Conflict-Driven Clause Learning), этот подход соответствует резолюционным доказательствам общего вида [21]. Алгоритмам, основанным на линейном и полуопределенном программировании, соответствуют полуалгебраические системы

доказательств; алгоритмам, основанным на базисе Гребнера [25], соответствуют алгебраические системы доказательств; алгоритмам, основанным на OBDD (ordered binary decision diagram) [16; 43], соответствуют системы доказательств, оперирующие OBDD [20]. Из нижних оценок на сложность вывода в системе доказательств следуют нижние оценки на время работы алгоритма, соответствующего этой системе доказательств.

Подсистемы $AC^0[2]$**-Frege.** Важнейшим открытым вопросом в теории сложности доказательств является получение суперполиномиальных нижних оценок в системах Фреге и расширенной системе Фреге. Системы Фреге эквивалентны классическим логическим исчислениям высказываний (например, гильбертовскому исчислению высказываний или секвенциальной системе с правилом сечения). Вывод в системе Фреге — это последовательность пропозициональных формул (а в расширенной системе Фреге — последовательность булевых схем). Поэтому вопрос о нижних оценках в системах Фреге и расширенной системе Фреге часто сравнивают с вопросом получения суперполиномиальных нижних оценок на формульную и схемную сложность явных булевых функций. Эти вопросы имеют и сходства, и различия. Оба эти вопроса давно являются открытыми и, кажется, что мы все еще далеки от решения этих вопросов. Есть некоторые косвенные аргументы в пользу того, что вопрос из сложности доказательств сложнее вопроса из схемной сложности. Например, известно, что существует булева функция, которая требует экспоненциальной схемной сложности, это можно показать с помощью подсчета количества булевых функций и маленьких булевых схем. Однако для системы Фреге даже вопрос существования трудной формулы является открытым. Экспоненциальная нижняя оценка на сложность вычисления функции четности схемами константной глубины была доказана в начале 1980-х [17; 32]. Аналогичный результат для подсистемы Фреге, оперирующей формулами, глубина которых ограничена константой, был доказан Айтаем только в 1994 году [18]. Разборов и Смоленский в 1987 году доказали нижнюю оценку для схем кон-

стантной глубины, в базисе которых кроме отрицаний, дизъюнкций и конъюнкций есть операция MOD_p [14; 47]. Однако аналогичный вопрос для систем Фреге константной глубины, которые оперируют формулами, использующими MOD_p (такую систему мы будем обозначать $\mathrm{AC}^0[p]$-Frege), до сих пор является открытым даже для $p = 2$.

Система доказательств $\mathrm{Res}(\oplus)$ [37; 12] является расширением резолюционной системы доказательств, эта система оперирует дизъюнкциями линейных равенств над $\mathbb{F}_2$, с помощью которых выводится противоречие из дизъюнктов исходных формул. Если же рассмотреть $\mathrm{Res}(\oplus)$ как систему доказательств для языка тавтологий в ДНФ, то она становится подсистемой системы $\mathrm{AC}^0[2]$-Frege, которая оперирует дизъюнкциями конъюнкций линейных равенств над $\mathbb{F}_2$. При этом недавний результат Басса, Ководжичека и Здановского [23] утверждает, что доказательства в системе $\mathrm{AC}^0[2]$-Frege могут быть промоделированы с квазиполиномиальным увеличением во фрагменте системы $\mathrm{AC}^0[2]$-Frege, оперирующем дизъюнкциями конъюнкций полиномиальных равенств логарифмической степени над $\mathbb{F}_2$. Однако суперполиномиальные нижние оценки неизвестны даже на размер вывода в системе $\mathrm{Res}(\oplus)$. Доказательство суперполиномиальных нижних оценок в этой системе доказательств является важнейшим шагом к доказательству нижних оценок в системе $\mathrm{AC}^0[2]$-Frege.

Метод монотонной интерполяции. Связь между сложностью пропозициональных доказательств и схемной сложностью булевых функций можно увидеть и в методах доказательства нижних оценок. Метод монотонной интерполяции позволяет сводить вопрос доказательства нижних оценок в некоторых системах доказательств к вопросу о доказательстве нижних оценок для монотонных булевых и вещественных схем [31; 36; 39; 44]. Недавний результат Гарга, Геса, Камата и Соколова [34] показывает и обратную связь: из нижних оценок на сложность вывода в резолюционной системе доказательств можно получить нижние оценки на монотонные схемы.

Семантические системы доказательств. Часто системы доказательств оперируют предикатами, которыми записываются промежуточные утверждения в выводе (proof lines). В резолюционной системе доказательств эти предикаты являются дизъюнктами (дизъюнкциями литералов), в системе секущие плоскости (cutting planes или CP) используемые предикаты — это линейные неравенства с целыми коэффициентами и булевыми переменными. В системе доказательств исчисление полиномов (polynomial calculus или PC) предикаты — это полиномиальные равенства над некоторым полем с булевыми переменными. Семантическая система доказательств определяется множеством предикатов, которые она может использовать. Доказательство невыполнимости формулы ϕ в КНФ в семантической системе доказательств — это последовательность предикатов, которая заканчивается тождественно ложным предикатом, при этом каждый предикат в этой последовательности либо эквивалентен дизъюнкту формулы ϕ, либо является семантическим следствием двух предикатов, идущих ранее. Семантические системы доказательств необязательно являются системами доказательств, поскольку проверка семантического следствия может быть сложной задачей для некоторых видов предикатов. Например, можно проверить за полиномиальное время семантическое следствие для дизъюнктов, но для линейных неравенств с целыми коэффициентами над булевыми переменными проверка семантического следствия NP-трудна [30]. Часто семантические системы доказательств являются более сильными, чем обычные, поэтому доказательство нижних оценок для семантических систем — это более сложная задача.

Системы доказательств, оперирующие OBDD**.** Метод монотонной интерполяции в изложении Крайчека [39] позволяет доказывать экспоненциальные нижние оценки для многих семантических систем доказательств, в которых предикаты обладают специальным свойством. А именно, этот метод работает для семантических систем, в которых значение предиката можно вычислить с небольшой коммуникацией. Одними из самых выразительных способов зада-

ний предикатов, для которых этот метод работает, — это OBDD (упорядоченные бинарные диаграммы решений). OBDD — это способ представления булевой функции, в котором с одной стороны многие важные функции имеют короткое представление, а с другой стороны есть эффективные алгоритмы вычисления бинарных операций, проверки выполнимости и т.д. Семантическая система доказательств, в которой предикаты записаны в виде OBDD [20] с одинаковым порядком на переменных, является довольно мощной, в частности она моделирует систему доказательств CP* (секущие плоскости с полиномиально ограниченными коэффициентами), имеет короткие доказательства для невыполнимых линейных систем над полем $\mathbb{F}_2$. Кроме того, корректность вывода в этой семантической системе можно проверить за полиномиальное время. Нижняя оценка в этой системе доказательств была получена Крайчеком [38] с помощью комбинации двух идей: сначала применяется метод монотонной интерполяции и доказывается нижняя оценка для какого-то одного порядка для переменных, затем строится преобразование, которое из формулы, которая требует большого доказательства в одном порядке, делает формулу, которая сложна для любых порядков. Ограничением этой системы доказательств является то, что порядки переменных во всех OBDD, которые используются в выводе, являются одними и теми же. Важный вопрос для исследований — изучить систему доказательств, в которой можно использовать разные порядки в разных OBDD. Делает ли возможность использования разных порядков систему доказательств сильнее? Можно ли доказать нижнюю оценку для системы доказательств, когда используются разные порядки? Существуют алгоритмы для задачи SAT, которые соответствуют подсистемам систем доказательств, оперирующих OBDD [16; 43]. Можно ли доказать нижнюю оценку на время работы таких алгоритмов, если у них будет возможность динамически менять порядок в OBDD?

Сложность цейтинских формул. Кроме доказательства нижних оценок важным вопросом является сравнение двух систем друг с другом. Для сравнения систем доказательств используются канони-

ческие семейства формул, обычно эти формулы кодируют простые комбинаторные утверждения. Самым популярным семейством формул является так называемый принцип Дирихле PHP_n^m (pigeonhole principle), который утверждает, что при $m > n$ невозможно разместить m кроликов по n клеткам так, чтобы каждый кролик попал хотя бы в одну клетку и в каждой клетке сидел не более чем один кролик. Другое важное семейство формул, которое используют как базовое для сравнения пропозициональных систем доказательств, — это семейство цейтинских формул. Каждая цейтинская формула строится по неориентированному графу $G(V, E)$ и функции пометок $c : V \to \{0, 1\}$, каждому ребру $e \in E$ соответствует переменная x_e. Цейтинская формула $\mathsf{T}(G, c)$ [15] представляет из себя конъюнкцию условий четности для каждой вершины $v \in V$: сумма по модулю 2 переменных x_e по всем ребрам, инцидентным вершине v, равняется $c(v)$. Известно, что цейтинская формула $\mathsf{T}(G, c)$ выполнима тогда и только тогда, когда для каждой компоненты связности сумма пометок четна [48]. Сложность цейтинской формулы зависит от графа, для некоторых графов формула простая для почти всех систем доказательств. Невыполнимые цейтинские формулы, основанные на специфических графах (обычно требуется, чтобы граф был экспандером, иногда рассматривают граф клетчатой сетки $n \times n$), являются трудными формулами во многих системах доказательств [13; 22; 27; 35; 48]. Интересно получить оценку сложности вывода цейтинской формулы в разных системах доказательств для произвольного графа, выразив ее через структурные свойства графа.

Оптимальные системы доказательств и алгоритмы. Если следовать программе Кука и Рекхау, то чтобы доказать $\mathrm{NP} \neq \mathrm{coNP}$, нужно доказать суперполиномиальную нижнюю оценку во всех пропозициональных системах доказательств. Система доказательств Π для языка L называется p-оптимальной, если для любой другой системы доказательств Ψ существует полиномиальный алгоритм, который отображает Ψ-доказательства в Π-доказательства. Если бы p-оптимальная система доказательств для языка UNSAT существова-

ла, то для доказательства NP $\neq$ coNP достаточно было бы доказать экспоненциальную нижнюю оценку только для одной p-оптимальной системы доказательств. Из существования p-оптимальной системы доказательств следует существование самой трудной для разделения дизъюнктной NP-пары [45; 46].

Аксептором для языка L называется алгоритм, который принимает все строки из языка и не останавливается на всех остальных строках. Аксепторами обладают все рекурсивно перечислимые языки. В 1989 году Крайчек и Пудлак [40] доказали, что существование p-оптимальной системы доказательств для языка UNSAT эквивалентно существованию оптимального аксептора (оптимальный аксептор на всех строчках языка работает не более, чем в полином раз дольше, чем любой другой аксептор). В 1999 году Месснер обобщил [42] этот результат на большой класс языков (все языки, которые устойчивы относительно дописывания наполнителя (padding)). Неизвестно ни одного нетривиального примера языка из класса NP $\cup$ coNP, для которого бы существовал оптимальный аксептор. Интересно рассмотреть проблему существования оптимального аксептора, если немного ослабить требование на алгоритмы и перейти к эвристическим алгоритмам, которым можно ошибаться на небольшой доле входов. Существует ли оптимальный эвристический аксептор для какого-нибудь языка из класса coNP?

Цели работы

1. Атсериас, Колайтис и Варди [20] предложили систему доказательств, основанную на OBDD, в которой невыполнимость формулы ϕ в КНФ доказывается с помощью вывода тождественно ложной OBDD из OBDD, представляющих дизъюнкты формулы ϕ, по одному из следующих правил: 1) правило конъюнкции ($\wedge$), 2) правило проекции ($\exists$), 3) правило ослабления (weakening). Конкретная система доказательств использует свой поднабор правил, который указывается в скобках при обозначении системы доказательств; поскольку правило проекции является частным

случаем правила ослабления, то его можно не указывать, если есть правило ослабления. Агуйре и Варди [16] предложили подход к задаче о пропозициональной выполнимости, основанный на OBDD и символьной элиминации квантора существования. По аналогии с системами доказательств, алгоритмы, основанные на этом подходе, мы будем обозначать как OBDD($\wedge, \exists$) алгоритмы. Известно, что по представлению булевой функции f в виде OBDD и перестановке переменных π можно получить представление функции f в порядке π за время, полиномиальное относительно размера исходной OBDD и размера минимальной OBDD в порядке π [41]. Это наблюдение позволяет добавить в системы доказательств и алгоритмы, оперирующие OBDD, правило смены порядка (reordering). Первая цель настоящей работы связана со следующими вопросами о системах доказательств и алгоритмах, основанных на OBDD и использующими правило смены порядка.

- Доказать экспоненциальную нижнюю оценку на класс OBDD($\wedge, \exists,$ reordering) алгоритмов, которые могут динамически менять порядок переменных в OBDD.
- Доказать нижние оценки на сложность вывода цейтинских формул и принципа Дирихле в системе доказательств OBDD($\wedge,$ reordering).
- В работе [20] было замечено, что существует такой порядок переменных, в котором принцип раскрашиваемости клики (семейство формул, кодирующих существование в графе клики размера k и возможность правильно раскрасить граф в $k-1$ цвет) требует экспоненциальных OBDD($\wedge,$ weakening) доказательств. Выяснить, существует ли порядок переменных, в котором эти формулы имеют полиномиальное по размеру доказательство.
- Выяснить, делает ли добавление правила смены порядка систему доказательств сильнее.

- Сравнить между собой все пары систем доказательств из списка: Res, CP*, OBDD($\wedge$), OBDD($\wedge$, weakening), OBDD($\wedge$, reordering), OBDD($\wedge$, weakening, reordering).
- Доказать суперполиномиальную нижнюю оценку на размер вывода в семантических системах доказательств 1-NBP($\wedge$), которая обобщает систему OBDD($\wedge$, reordering) и оперирует произвольными однопроходными недетерминированными программами (1-NBP). Усилить этот результат до системы 1-NBP($\wedge, \exists_k$), в которой число переменных, к которым разрешается применить правило проекции, не превосходит k.

2. Вторая цель состоит в выяснении сложности цейтинских формул в зависимости от структурных свойств графа:
   - невыполнимых цейтинских формул в системе доказательств OBDD($\wedge$, reordering) с точностью до квазиполинома;
   - невыполнимых цейтинских формул в системе Фреге глубины d с точностью до квазиполинома;
   - невыполнимых цейтинских формул в регулярной резолюции с точностью до логарифмического множителя в экспоненте;
   - вычисления выполнимых цейтинских формул однопроходными ветвящимися программами.

3. Третья цель — исследовать сложность вывода в подсистемах системы доказательств Res($\oplus$).
   - Выяснить сложность вывода принципа Дирихле в древовидной системе Res($\oplus$).
   - Пусть Res($\oplus; \leqslant k$) обозначает подсистему системы Res($\oplus$), в которой в каждой дизъюнкции линейных уравнений не более k уравнений зависят от одной переменной. Промоделировать Res($\oplus; \leqslant k$) в системах OBDD($\wedge$, weakening) и PCR. Такие моделирования повлекут нижние оценки на сложность вывода в системе Res($\oplus; \leqslant k$).

- Доказать нижнюю оценку на сложность DPLL($\oplus$) алгоритмов на выполнимых формулах, которые расщепляются по линейной форме, при этом значение линейной формы выбирается случайным образом.

4. Четвертая цель — изучить вопрос о существовании оптимального аксептора для ослабленных требований на модели вычислений.

   - Построить оптимальный аксептор в классе вероятностных эвристических аксепторов.
   - Построить оптимальный эвристический детерминированный алгоритм для нетривиального языка.
   - Построить оптимальный в среднем случае вероятностный аксептор для языка пар неизоморфных графов GNI.

Научная новизна

Все основные результаты диссертации являются новыми. В диссертации впервые изучены системы доказательств, основанные на OBDD, использующие правило смена порядка; предложены новые методы, позволяющие доказывать нижние оценки в этих системах. Впервые получена нижняя оценка на сложность вывода цейтинских формул, выраженная через древесную ширину графа. В диссертация введена новая мера на графах, компонентная ширина, значение которой находится между путевой шириной и древесной шириной графа. Впервые получены нетривиальные конструкции оптимальных эвристических и вероятностных аксепторов.

Теоретическая и практическая ценность

Работа носит теоретический характер. Результаты работы могут быть использованы в исследованиях по теории сложности вычислений и теории сложности пропозициональных доказательств. Введенная в

работе мера на графах (компонентная ширина) может быть использована в теории графов. Результаты о системах доказательств и алгоритмов, основанных на OBDD, могут быть использованы при разработке алгоритмов для задачи выполнимости булевых формул.

Методы исследования

В работе используются методы теории сложности вычислений, теории сложности доказательств, коммуникационная сложность, методы и понятия теории графов.

Положения, выносимые на защиту

1. Результаты про системы доказательств, основанных на OBDD.

   - Доказана экспоненциальная нижняя оценки на сложность вывода в системе OBDD($\wedge$, reordering) принципа Дирихле PHP_n^{n+1}.
   - Построено полиномиальное по размеру доказательство принципа раскрашиваемости клики в системе доказательств OBDD($\wedge$, weakening).
   - Доказано, что система доказательств OBDD($\wedge$, weakening, reordering) строго сильнее системы доказательств OBDD($\wedge$, weakening). Получено сравнение каждой пары из следующих систем доказательств Res, CP^*, OBDD($\wedge$), OBDD($\wedge$, weakening), OBDD($\wedge$, reordering), OBDD($\wedge$, weakening, reordering), см. рис. 1.
   - Доказана экспоненциальная нижняя оценка на сложность вывода цейтинских формул и формул, кодирующих существование совершенного паросочетания, построенных по алгебраическому экспандеру в семантической системе доказательств 1-NBP($\wedge$).

- Доказана экспоненциальная нижняя оценка на сложность вывода в семантической системе доказательств 1-NBP$(\wedge, \exists_{cn})$ для некоторой константы c, где n — число переменных формул. Система доказательств 1-NBP$(\wedge, \exists_k)$ является подсистемой 1-NBP$(\wedge, \exists)$, в которой в любом выводе разрешается применять правило проекции к не более чем k переменным.
- Построено семейство выполнимых формул, на котором любой OBDD$(\wedge, \exists, \text{reordering})$ алгоритм работает экспоненциальное число шагов.

2. Результаты о сложности цейтинских формул.

- Доказано, что для каждого связного графа $G(V, E)$ сложность вывода цейтинской формулы $\mathsf{T}(G, c)$ в системе доказательств OBDD$(\wedge, \text{reordering})$ не больше $O\left(|E||V|2^{\text{pw}(G)} + |\,\mathsf{T}(G, c)|^2\right)$ и не меньше $2^{\Omega\left(\text{tw}(G)^\lambda\right)}$, где $\text{tw}(G)$ — это древесная ширина графа G, $\text{pw}(G)$ — это путевая ширина G, а λ — это константа из теоремы о миноре-сетке (на сегодняшний день известно, что $\lambda \geq \frac{1}{10}$ [24]).
- Доказано, что существует такая константа K, что цейтинская формула, основанная на связном графе G, требует доказательств размера как минимум $2^{\text{tw}(G)^{\Omega(1/d)}}$ в системах Фреге глубины d для $d < \frac{K \log n}{\log \log n}$. Доказано, что для достаточно больших d формула $\mathsf{T}(G, c)$ имеет доказательство в системе Фреге глубины d размера $2^{\text{tw}(G)^{O(1/d)}}\text{poly}(|\,\mathsf{T}(G, c)|)$.
- Определена новая графовая мера, компонентная ширина (compw) и показано, что размер минимальной 1-NBP, вычисляющей выполнимую цейтинскую формулу $\mathsf{T}(G, c')$, основанную на графе $G(V, E)$, с точностью до полиномиального множителя равняется $2^{\text{compw}(G)}$. При этом выполняются следующие неравенства: $\Omega(\text{tw}(G)) \leq \text{compw}(G) \leq O(\text{tw}(G) \log(|V|))$.
- Доказано, что размер любого регулярного резолюционного опровержения цейтинской формулы $\mathsf{T}(G, c)$, построенной по связному графу $G(V, E)$, не меньше $2^{\Omega(\text{tw}(G)/\log|V|)}$.

Для графов константной степени известная верхняя оценка $2^{O(\mathrm{tw}(G))}\mathrm{poly}(|V|)$ [19; 33].

3. Результаты о сложности вывода в подсистемах системы $\mathrm{Res}(\oplus)$.

   - Доказано, что при $m > n$ размер любого древовидного $\mathrm{Res}(\oplus)$ опровержения принципа Дирихле PHP_n^m как минимум $2^{\lfloor n/2 \rfloor}$.
   - Доказано, что если существует $\mathrm{Res}(\oplus; \leqslant k)$ доказательство формулы ϕ длины m, то существует $\mathrm{OBDD}(\wedge, \mathrm{weakening})$ доказательство размера $2^{2k+1}(n+2)^2 m$, где n — число переменных в формуле ϕ.
   - Доказано, что если существует $\mathrm{Res}(\oplus; \leqslant \delta n)$ доказательство формулы ϕ размера S, где n — число переменных в формуле ϕ и $\delta \in (0, \frac{1}{4})$, то существует PCR доказательство (Polynomial Calculus Resolution) размера $2^{H(2\delta)n}\mathrm{poly}(n)S$, где $H(p)$ — это бинарная энтропия.
   - Рассмотрен класс $\mathrm{DPLL}(\oplus)$ алгоритмов, которые выбирают линейную комбинацию для расщепления произвольным образом, а значение, которое будет исследоваться первым, случайно равновероятно. Для этого класса построено семейство выполнимых формул F_n размера $\mathrm{poly}(n)$, обладающих таким свойством, что любой алгоритм из рассматриваемого класса с вероятностью $1 - 2^{-\Omega(n)}$ работает на формуле F_n как минимум $2^{\Omega(n)}$ шагов.

4. Результаты об эвристических аксепторах и системах доказательств.

   - Распределенной задачей доказательств (L, D) называется пара, состоящая из рекурсивно перечислимого языка L и полиномиально моделируемого распределения D на его дополнении. Вероятностный эвристический аксептор — это такой вероятностный алгоритм, который принимает с большой вероятностью все элементы языка и лишь малую долю согласно распределению D элементов дополнения. Доказано, что для

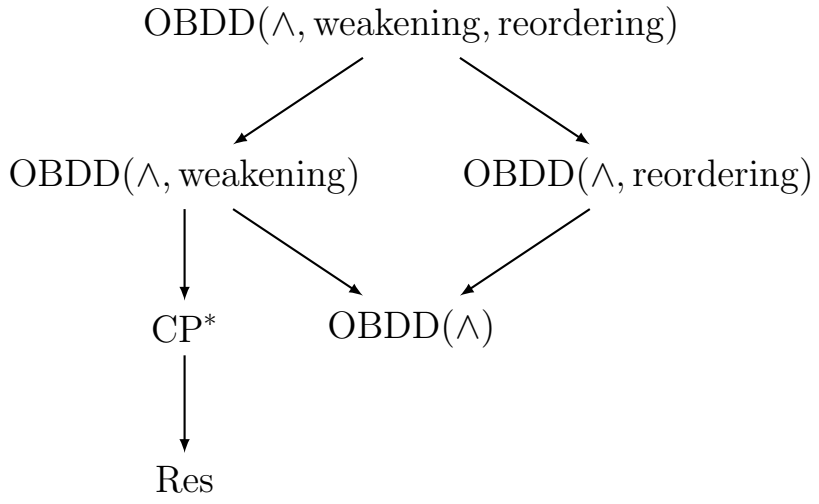

Рис. 1: Π_1 моделирует Π_2 тогда и только тогда, когда есть путь из Π_1 в Π_2 в графе.

каждой распределенной задачи доказательств (L, D) существует вероятностный эвристический аксептор, медианное время работы которого на элементах L оптимально с точностью до полиномиального множителя.

- Построен оптимальный детерминированный эвристический алгоритм для образа инъективной полиномиально вычислимой функции.

- Построен вероятностный аксептор для языка GNI, который оптимален с точностью до перестановки вершин во входном графе, т.е. его время работы на паре графов (G_1, G_2) не более чем в полином раз больше, чем медианное время работы любого другого аксептора, запущенного на входе $(\pi_1(G_1), \pi_2(G_2))$ для случайных перестановок π_1 и π_2.

Апробация работы

Результаты диссертации были представлены на следующих научных мероприятиях:

- 27th International Symposium on Theoretical Aspects of Computer Science (STACS 2010), Нанси, Франция, 2010 г.
- Workshop on postquanum cryptography, Санкт-Петербург, 2011 г.
- First Russian Finnish Symposium on Discrete Mathematics (RuFiDim-2011), Санкт-Петербург, 2011 г.
- Second Russian Finnish Symposium on Discrete Mathematics (RuFiDim-2012), Турку, Финляндия, 2012 г.
- Franco-Russion Workshop on Algorithms, Complexity and Applications, Москва, 2013 г.
- Workshop on Proof Complexity, Вена, Австрия, 2014 г.
- 39th International Symposium on Mathematical Foundations of Computer Science, Будапешт, Венгрия, 2014 г.
- Семинар Optimal algorithms and proofs, Дагштуль, Германия, 2014 г.
- Конференция Problems in Theoretical Computer Science, Москва, 2015 г.
- Workshop on proof complexity, Санкт-Петербург, 2016 г.
- Конференция Problems in Theoretical Computer Science, Москва, 2016 г.
- Семинар университета Турку, Финляндия, 2015-2016 гг.
- 34th International Symposium on Theoretical Aspects of Computer Science (STACS 2017), Ганновер, Германия, 2017 г.

- 42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017), Аалборг, Дания, 2017 г.
- Oberwolfach workshop «Proof Complexity and Beyond», Обервольфах, Германия, 2017 г.
- 33th Computational Complexity Conference (CCC 2018), Сан-Диего, США, 2018 г.
- Конференция День математики и механики, интернет видеоконференция: Екатеринбург, Новосибирск, Москва, Санкт-Петербург, 2018 г.
- Конференция Традиционная зимняя сессия МИАН–ПОМИ, посвященная теме «Математическая логика», Москва, МИАН, 2018 г.
- The 14th International Computer Science Symposium in Russia, Новосибирск, 2019 г.
- 44th International Symposium on Mathematical Foundations of Computer Science, Ахен, Германия, 2019 г.
- Конференция Problems in Theoretical Computer Science, Москва, 2019 г.
- Семинар Proof Complexity, Банф, Канада, 2020 г.

Публикации

Результаты диссертаций опубликованы в 12 статьях [1—12]; все статьи индексируются в библиографических базах Scopus и MathSciNet.

За исключением случаев, описанных ниже, из статей, написанных в соавторстве, в диссертацию включались результаты, полученные диссертантом лично.

Теорема 3.1 из статьи [8] была получена в неразрывном соавторстве с Э. А. Гиршем.

В работе [6] теорема 5.2 была сформулирована и доказана диссертантом, частный случай этой теоремы (для детерминированного эвристического аксептора) был ранее доказан диссертантом в соавторстве В. О. Николаенко, при этом идея доказательства этого частного случая принадлежит диссертанту.

Результаты из работы [7] были получены в неразрывном соавторстве с Э. А. Гиршем.

В работе [3] в теореме 17 Н. Галези предложил идею рассматривать топологические миноры вместо обычных в теореме о минорах, формулировка и доказательство теоремы 17 принадлежат диссертанту. Теорема 18 доказана в соавторстве с А. А. Софроновой и А. А. Рязановым, при этом диссертанту принадлежит постановка задачи, А. А. Софронова предложила использовать компактное представление функции четности в виде формулы, А. А. Рязанов предложил использовать древесное разбиение графов.

В работе [11] диссертанту принадлежит постановка задачи, общий план доказательства основного результата и формулировки промежуточных результатов, лемма 1.4 и теорема 3.1 были доказаны в неразрывном соавторстве с П. Ю. Смирновым и А. А. Рязановым. Теорема 1.8 была доказана в неразрывном соавторстве с Д. Г. Сагуновым.

В работе [10] теоремы 3.6 и 3.18 были доказаны в неразрывном соавторстве с А. А. Кнопом и Д. О. Соколовым. Теорема 5.2 была получена в неразрывном соавторстве с А. А. Кнопом.

В работе [2] автору принадлежит идея доказательства теоремы 8, а само доказательство получено в соавторстве с А. А. Кнопом и Д. О. Соколовым. Теорема 10 доказана в соавторстве с А. А. Кнопом.

В работе [1] в теореме 3.1 диссертанту принадлежит формулировка и план доказательства, само же доказательство получено в неразрывном соавторстве с Д. О. Соколовым, теорема 6.2 была доказана в соавторстве с А. А. Рязановым, однако идея доказательства была предложена диссертантом.

Статья [9] написана в соавторстве с А. А. Кнопом, при этом формулировка основного результата и идея доказательства принадлежит диссертанту.

Структура диссертации

Диссертация объемом 223 страницы состоит из введения и пяти основных глав, разбитых на разделы и подразделы. Список цитируемой литературы состоит из 122 наименований.

Содержание работы

Во **введении** диссертации дается общая характеристика работы, актуальность, постановка задачи, кратко описываются полученные результаты.

В **первой главе** диссертации определяются основные понятия, которые используются во всей диссертации и формулируются важные известные утверждения: алгебраические и реберные экспандеры, миноры графа, древесная и путевая ширина, теорема о миноре-сетке, ветвящиеся программы и их частные случаи (1-BP, 1-NBP, OBDD, деревья решений), пропозициональные формулы, формулы в КНФ, важные конкретные семейства формул (принцип Дирихле, принцип совершенного паросочетания, цейтинские формулы), системы доказательств, общие определения и конкретные системы: резолюция, секущие плоскости, системы Фреге.

Во **второй главе** диссертации изучаются системы доказательств и алгоритмы для задачи выполнимости, основанные на OBDD.

В разделе 2.1 определяются системы доказательств, основанные на OBDD, и дается обзор известных результатов.

В разделе 2.2 доказывается экспоненциальная нижняя оценка на сложность опровержения принципа Дирихле PHP_n^{n+1} в системе доказательств $\mathrm{OBDD}(\wedge, \mathrm{reordering})$.

В разделе 2.3 доказывается, что тавтология раскрашиваемости клики имеет доказательство в системе $\mathrm{OBDD}(\wedge, \mathrm{weakening})$ полиномиального размера.

В разделе 2.4 доказывается, что добавление правила смены порядка делает системы доказательств, основанные на OBDD, строго сильнее.

В разделе 2.5 доказывается, что резолюционная система доказательств не моделирует OBDD($\wedge$), затем этот результат обобщается на систему секущие плоскости, также показывается, что система OBDD($\wedge$, weakening) не моделирует систему OBDD($\wedge$, reordering).

В разделе 2.6 определяются семантические системы доказательств, основанные на детерминированных и недетерминированных однопроходных ветвящихся программах, доказывается экспоненциальная нижняя оценка на сложность вывода в системе доказательств 1-NBP($\wedge$).

В разделе 2.7 доказываются верхние оценки на сложность вывода в системе доказательств 1-NBP($\wedge$).

В разделе 2.8 доказывается, что система доказательств 1-NBP($\wedge$) не моделирует древовидную резолюционную систему доказательств.

В разделе 2.9 доказывается экспоненциальная нижняя оценка в семантической системе доказательств 1-NBP($\wedge, \exists_{cn}$).

В разделе 2.10 доказываются полиномиальные верхние оценки на время работы OBDD($\wedge, \exists$) алгоритмов на цейтинских формулах, а также экспоненциальная нижняя оценка на время работы OBDD($\wedge, \exists$, reordering) алгоритмов.

В разделе 2.11 подводятся итоги по главе и формулируются открытые вопросы.

В **третьей главе** изучается сложность цейтинских формул в зависимости от свойств графа.

В разделе 3.1 дается обзор известных результатов про цейтинские формулы в различных системах доказательств.

В разделе 3.2 изучается сложность вычисления выполнимых цейтинских формул недетерминированными однопроходными ветвящимися программами. В подразделе 3.2.1 доказывается, что размер минимальной 1-NBP, вычисляющей выполнимую цейтинскую формулу, достигается на OBDD, в подразделе 3.2.2 вводится понятие компонентной ширины графа, а в подразделе 3.2.3 компонентная ширина оценивается через древесную ширину.

В разделе 3.3 доказываются нижние и верхние оценки на сложность вывода цейтинской формулы в системе доказательств OBDD($\wedge$, reordering) через древесную ширину графа.

В разделе 3.4 доказывается более точная оценка для регулярной резолюционной системы доказательств, определяется задача SearchVertex(G, c), которая состоит в том, что по набору значений переменных требуется найти вершину, в которой нарушается условие четности цейтинской формулы. В подразделе 3.4.1 определяются понятия хорошо структурированных ветвящихся программ, вычисляющих выполнимые цейтинские формулы и задачу SearchVertex(G, c). В подразделе 3.4.2 доказывается, что минимальные однопроходные ветвящиеся программы, вычисляющие задачу SearchVertex(G, c), являются хорошо структурированными. В подразделе 3.4.3 по однопроходной ветвящейся программе размера S для задачи SearchVertex(G, c) строится 1-BP, вычисляющая выполнимую цейтинскую формулу, размера $S^{O(\log |V|)}$.

В разделе 3.5 изучается сложность вывода цейтинских формул в системах Фреге ограниченной глубины. В подразделе 3.5.1 формулируется определение систем Фреге в виде игр Пудлака-Баса. В подразделе 3.5.2 доказывается нижняя оценка на сложность вывода цейтинских формул в системах Фреге ограниченной глубины. В подразделе 3.5.3 доказывается верхняя оценка на сложность вывода цейтинских формул в системах Фреге ограниченной глубины, которая точна с точностью до применения квазиполинома.

В разделе 3.6 подводятся итоги главы, упоминаются недавние результаты и формулируются открытые вопросы.

В **четвертой главе** изучаются подсистемы системы доказательств Res$(\oplus)$.

В разделе 4.1 дается определение системы доказательств Res$(\oplus)$, деревьев решений с линейными запросами и DPLL$(\oplus)$ алгоритмов, дается обзор известных результатов.

Раздел 4.2 посвящен древовидной версии Res$(\oplus)$, в подразделе 4.2.1 доказывается эквивалентность древовидной версии Res$(\oplus)$ и деревьев решений с линейными запросами. В подразделе 4.2.2 приводятся верхние оценки на сложность вывода в системе Res$(\oplus)$ для формул, кодирующих линейные системы уравнений над $\mathbb{F}_2$, и для принципа совершенного паросочетания для графов с нечетным числом вершин. В подразделе 4.2.3 доказывается экспоненциальная

нижняя оценка на древовидную сложность вывода принципа Дирихле PHP_n^m в системе $\mathrm{Res}(\oplus)$. В подразделе 4.2.4 доказывается нижняя оценка на время работы пьяных $\mathrm{DPLL}(\oplus)$ алгоритмов на семействе выполнимых формул.

В разделе 4.3 определяется подсистема $\mathrm{Res}(\oplus; \leqslant k)$, в подразделе 4.3.1 показывается, что линейные системы над $\mathbb{F}_2$ и принцип совершенного паросочетания для графов с нечетным числом вершин имеют полиномиального размера опровержения в системе $\mathrm{Res}(\oplus; \leqslant 2)$. В подразделе 4.3.2 доказывается, что $\mathrm{Res}(\oplus; \leqslant k)$ моделируется в системе $\mathrm{OBDD}(\wedge, \mathrm{weakening})$ с удлинением доказательства в 2^k раз и формулируется следствие о нижней оценке для принципа раскрашиваемости клики. В разделе 4.3.3 доказывается, что $\mathrm{Res}(\oplus; \leqslant k)$ моделируется в системе PCR (исчисление полиномов с резолюцией) с умеренно экспоненциальным раздуванием, в качестве следствия получается нижняя оценка на вывод функционального принципа Дирихле в этой системе доказательств.

В разделе 4.4 рассказывается о других исследованиях на близкие темы и формулируются открытые вопросы.

Пятая глава посвящена вопросу существования оптимальных аксепторов для разных моделей вычислений.

В разделе 5.1 приводится обзор результатов об оптимальных системах доказательств и оптимальных аксепторах.

В разделе 5.2 даются основные определения сложности в среднем: распределенные задачи, эвристические алгоритмы, распределенные задачи доказательств, эвристические аксепторы, определяется полиномиальная ограниченность и моделирование для эвристических алгоритмов и аксепторов.

В разделе 5.3 дается конструкция оптимального вероятностного эвристического аксептора для произвольной распределенной задачи доказательств (D, L), где L — это перечислимый язык, а D — полиномиально моделируемое распределение на дополнении L.

В разделе 5.4 рассматривается язык, состоящий из образа инъективной полиномиально вычислимой функции, увеличивающий длину входа на один бит, для этого языка и равномерного распределения строится оптимальный детерминированный эвристический алгоритм.

В разделе 5.5 рассматривается язык пар неизоморфных графов GNI, для него строится вероятностный аксептор с оптимальным в среднем медианным временем работы.

В разделе 5.6 обсуждается связь результатов главы с системами доказательств и формулируются открытые вопросы.

Публикации автора по теме диссертации

1. *Buss S.*, *Itsykson D.*, *Knop A.*, *Riazanov A.*, *Sokolov D.* Lower Bounds on OBDD Proofs with Several Orders // ACM Trans. Comput. Log. — 2021. — Т. 22, № 4. — 26:1—26:30.
2. *Buss S.*, *Itsykson D.*, *Knop A.*, *Sokolov D.* Reordering Rule Makes OBDD Proof Systems Stronger // 33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA. Т. 102 / под ред. R. A. Servedio. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. — 16:1—16:24. — (LIPIcs).
3. *Galesi N.*, *Itsykson D.*, *Riazanov A.*, *Sofronova A.* Bounded-Depth Frege Complexity of Tseitin Formulas for All Graphs // 44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany. Т. 138 / под ред. P. Rossmanith, P. Heggernes, J. Katoen. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. — 49:1—49:15. — (LIPIcs).
4. *Glinskih L.*, *Itsykson D.* On Tseitin Formulas, Read-Once Branching Programs and Treewidth // Theory Comput. Syst. — 2021. — Т. 65, № 3. — С. 613—633.
5. *Glinskih L.*, *Itsykson D.* Satisfiable Tseitin Formulas Are Hard for Nondeterministic Read-Once Branching Programs // 42nd International Symposium on Mathematical Foundations of Computer Science, MFCS 2017, August 21-25, 2017 - Aalborg, Denmark. Т. 83 / под ред. K. G. Larsen, H. L. Bodlaender, J. Raskin. — Schloss Dagstuhl - Leibniz-Zentrum fur Informatik, 2017. — 26:1—26:12. — (LIPIcs).

6. *Hirsch E. A.*, *Itsykson D. M.*, *Nikolaenko V. O.*, *Smal A. V.* Optimal heuristic algorithms for the image of an injective function // Зап. научн. сем. ПОМИ. — 2012. — Т. 399. — С. 15—31. — (Теория сложности вычислений. X).

7. *Hirsch E. A.*, *Itsykson D.* On an optimal randomized acceptor for graph nonisomorphism // Inf. Process. Lett. — 2012. — Т. 112, № 5. — С. 166—171.

8. *Hirsch E. A.*, *Itsykson D.*, *Monakhov I.*, *Smal A.* On Optimal Heuristic Randomized Semidecision Procedures,with Applications to Proof Complexity and Cryptography // Theory Comput. Syst. — 2012. — Т. 51, № 2. — С. 179—195.

9. *Itsykson D.*, *Knop A.* Hard Satisfiable Formulas for Splittings by Linear Combinations // Theory and Applications of Satisfiability Testing - SAT 2017 - 20th International Conference, Melbourne, VIC, Australia, August 28 - September 1, 2017, Proceedings. Т. 10491 / под ред. S. Gaspers, T. Walsh. — Springer, 2017. — С. 53—61. — (Lecture Notes in Computer Science).

10. *Itsykson D.*, *Knop A.*, *Romashchenko A. E.*, *Sokolov D.* On OBDD-based Algorithms and Proof Systems that Dynamically Change the order of Variables // J. Symb. Log. — 2020. — Т. 85, № 2. — С. 632—670.

11. *Itsykson D.*, *Riazanov A.*, *Sagunov D.*, *Smirnov P.* Near-Optimal Lower Bounds on Regular Resolution Refutations of Tseitin Formulas for All Constant-Degree Graphs // Comput. Complex. — 2021. — Т. 30, № 2. — С. 13.

12. *Itsykson D.*, *Sokolov D.* Resolution over linear equations modulo two // Ann. Pure Appl. Log. — 2020. — Т. 171, № 1.

Список литературы

13. *Ицыксон Д.*, *Кожевников А.* Нижние оценки на длину вывода цейтинских формул в статической системе доказательств Ловаса–

Схрайвера // Записки научных семинаров ПОМИ. — 2006. — Т. 340. — С. 10—32.

14. *Разборов А. А.* Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения // Математические заметки. — 1987. — Т. 41. — С. 598—607.

15. *Цейтин Г. С.* О сложности вывода в исчислении высказываний // Записки научных семинаров ЛОМИ / под ред. А. О. Слисенко. — 1968. — Т. 8. — С. 234—259. — (Исследования по конструктивной математике и математической логике II).

16. *Aguirre A. S. M.*, *Vardi M. Y.* Random 3-SAT and BDDs: The Plot Thickens Further // Principles and Practice of Constraint Programming - CP 2001, 7th International Conference, CP 2001, Paphos, Cyprus, November 26 - December 1, 2001, Proceedings. — 2001. — С. 121—136.

17. *Ajtai M.* $\sum_1^1$-Formulae on finite structures // Annals of Pure and Applied Logic. — 1983. — Т. 24, № 1. — С. 1—48. — ISSN 0168-0072.

18. *Ajtai M.* The Complexity of the Pigeonhole Principle // Combinatorica. — 1994. — Т. 14, № 4. — С. 417—433.

19. *Alekhnovich M.*, *Razborov A. A.* Satisfiability, Branch-Width and Tseitin tautologies // Computational Complexity. — 2011. — Т. 20, № 4. — С. 649—678.

20. *Atserias A.*, *Kolaitis P. G.*, *Vardi M. Y.* Constraint Propagation as a Proof System // Principles and Practice of Constraint Programming - CP 2004, 10th International Conference, CP 2004, Toronto, Canada, September 27 - October 1, 2004, Proceedings. Т. 3258 / под ред. M. Wallace. — Springer, 2004. — С. 77—91. — (Lecture Notes in Computer Science).

21. *Beame P.*, *Kautz H. A.*, *Sabharwal A.* Towards Understanding and Harnessing the Potential of Clause Learning // J. Artif. Intell. Res. (JAIR). — 2004. — Т. 22. — С. 319—351.

22. *Ben-Sasson E.* Hard examples for the bounded depth Frege proof system // Computational Complexity. — 2002. — Т. 11, № 3/4. — С. 109—136.

23. *Buss S.*, *Kołodziejczyk L.*, *Zdanowski K.* Collapsing modular counting in bounded arithmetic and constant depth propositional proofs // Transactions of the American Mathematical Society. — 2015. — Нояб. — Т. 367.

24. *Chuzhoy J.*, *Tan Z.* Towards Tight(er) Bounds for the Excluded Grid Theorem // Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019. — 2019. — С. 1445—1464.

25. *Clegg M.*, *Edmonds J.*, *Impagliazzo R.* Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability // Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996 / под ред. G. L. Miller. — ACM, 1996. — С. 174—183.

26. *Cook S. A.*, *Reckhow R. A.* The relative efficiency of propositional proof systems // The Journal of Symbolic Logic. — 1979. — Март. — Т. 44, № 1. — С. 36—50.

27. *Dantchev S. S.*, *Riis S.* Tree Resolution Proofs of the Weak Pigeon-Hole Principle // Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001. — 2001. — С. 69—75.

28. *Davis M.*, *Logemann G.*, *Loveland D.* A machine program for theorem-proving // Communications of the ACM. — 1962. — Т. 5. — С. 394—397.

29. *Davis M.*, *Putnam H.* A computing procedure for quantification theory // Journal of the ACM. — 1960. — Т. 7. — С. 201—215.

30. *Filmus Y.*, *Hrubes P.*, *Lauria M.* Semantic Versus Syntactic Cutting Planes // 33rd Symposium on Theoretical Aspects of Computer Science, STACS 2016, February 17-20, 2016, Orléans, France. Т. 47 /

под ред. N. Ollinger, H. Vollmer. — Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016. — 35:1—35:13. — (LIPIcs).

31. *Fleming N.*, *Pankratov D.*, *Pitassi T.*, *Robere R.* Random Θ(log n)-CNFs Are Hard for Cutting Planes // 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017 / под ред. C. Umans. — IEEE Computer Society, 2017. — С. 109—120.

32. *Furst M.*, *Saxe J. B.*, *Sipser M.* Parity, circuits, and the polynomial-time hierarchy // 22nd Annual Symposium on Foundations of Computer Science (sfcs 1981). — 1981. — С. 260—270.

33. *Galesi N.*, *Talebanfard N.*, *Torán J.* Cops-Robber Games and the Resolution of Tseitin Formulas // ACM Trans. Comput. Theory. — 2020. — Т. 12, № 2. — 9:1—9:22.

34. *Garg A.*, *Göös M.*, *Kamath P.*, *Sokolov D.* Monotone circuit lower bounds from resolution // Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018 / под ред. I. Diakonikolas, D. Kempe, M. Henzinger. — ACM, 2018. — С. 902—911.

35. *Håstad J.* On Small-Depth Frege Proofs for Tseitin for Grids // 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017. — 2017. — С. 97—108.

36. *Hrubes P.*, *Pudlák P.* A note on monotone real circuits // Inf. Process. Lett. — 2018. — Т. 131. — С. 15—19.

37. *Itsykson D.*, *Sokolov D.* Lower Bounds for Splittings by Linear Combinations // Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II. Т. 8635 / под ред. E. Csuhaj-Varjú, M. Dietzfelbinger, Z. Ésik. — Springer, 2014. — С. 372—383. — (Lecture Notes in Computer Science).

38. *Krajıcek J.* An exponential lower bound for a constraint propagation proof system based on ordered binary decision diagrams // J. Symb. Log. — 2008. — Т. 73, № 1. — С. 227—237.

39. *Krajıček J.* Interpolation Theorems, Lower Bounds for Proof Systems, and Independence Results for Bounded Arithmetic // J. Symb. Log. — 1997. — Т. 62, № 2. — С. 457—486.

40. *Krajıček J., Pudlák P.* Propositional proof systems, the consistency of first order theories and the complexity of computations // The Journal of Symbolic Logic. — 1989. — Сент. — Т. 54, № 3. — С. 1063—1079.

41. *Meinel C., Slobodova A.* On the complexity of constructing optimal ordered binary decision diagrams // Proceedings of Mathematical Foundations of Computer Science. — 1994. — Т. 841. — С. 515—524.

42. *Messner J.* On Optimal Algorithms and Optimal Proof Systems // Proceedings of the 16th Symposium on Theoretical Aspects of Computer Science. Т. 1563. — 1999. — С. 361—372. — (Lecture Notes in Computer Science).

43. *Pan G., Vardi M. Y.* Symbolic Techniques in Satisfiability Solving // Journal of Automated Reasoning. — 2005. — Т. 35, № 1—3. — С. 25—50.

44. *Pudlák P.* Lower Bounds for Resolution and Cutting Plane Proofs and Monotone Computations // J. Symb. Log. — 1997. — Т. 62, № 3. — С. 981—998.

45. *Pudlák P.* On reducibility and symmetry of disjoint NP pairs // Theoretical Computer Science. — 2003. — Т. 295, № 1—3. — С. 323—339.

46. *Razborov A. A.* On provably disjoint NP-pairs // Electron. Colloquium Comput. Complex. — 1994. — Т. 1, № 6.

47. *Smolensky R.* Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity // Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA. — 1987. — С. 77—82.

48. *Urquhart A.* Hard Examples for Resolution // Journal of the ACM. — 1987. — Т. 34, № 1. — С. 209—219.