На правах рукописи

Опарин Всеволод Владиславович

Оценки сложности вывода в системах доказательств, основанных на методе резолюций

01.01.06 — математическая логика, алгебра и теория чисел

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Санкт-Петербург — 2016

Работа выполнена на кафедре математических и информационных технологий
Санкт-Петербургского национального исследовательского
Академического университета Российской академии наук

Научный руководитель:
Ицыксон Дмитрий Михайлович
кандидат физико-математических наук, ученый секретарь ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российскоий академии наук

Официальные оппоненты:
Шур Арсений Михайлович
доктор физико-математических наук
профессор ФГАОУВО «Уральского федерального университета имени первого Президента России Б. Н. Ельцина», профессор кафедры алгебры и дискретной математики
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: Национальный исследовательский университет «Высшая школа экономики»

Защита состоится «30» ноября 2016 г. в 16:00 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 «____» _____ 2016 г.

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

Общая характеристика работы

Актуальность темы. Теория сложности доказательств — одна из активно развиваемых областей математической логики. В рамках теории изучаются формальные системы доказательств.

Согласно теореме Кука–Рекхоу классы **NP** и **co-NP** равны тогда и только тогда, когда существует система доказательств, которая для каждой тавтологии ϕ имеет доказательство полиномиального от длины ϕ размера. Программа Кука состоит в том, чтобы рассматривать все более и более сильные системы доказательств и получать нижние суперполиномиальные оценки на размеры доказательств. В идеале это могло бы привести к разделению классов **P** и **NP**.

Резолюционная система доказательств (Res) — одна из наиболее изученных систем. Впервые система была введена Блэком в 1938 г. и позднее популяризована в работах Дэвиса и Путнама в 1960 г. и Робинсона в 1965 г.

Помимо программы Кука, резолюционная система доказательств интересна в рамках автоматизированного поиска доказательств и алгоритмов для задачи выполнимости пропозициональной формулы. В главной роли здесь выступают DPLL алгоритмы и их более современные версии, CDCL алгоритмы.

Известно, что оптимальный протокол работы DPLL алгоритма совпадает с минимальным древовидным резолюционным доказательством. При анализе CDCL алгоритмов, протокол работы сравнивают с резолюционными системами доказательств в общем виде. Трудные формулы для резолюционных систем оказываются также трудны для DPLL и CDCL алгоритмов.

В 1968 г. Цейтин получил первые суперполиномиальные нижние оценки для резолюционных систем доказательств регулярного вида. Трудные формулы кодировали утверждение, что сумма степеней вершин графа нечетна; такие формулы называют цейтинскими. В 1987 г. Уркухарт показал для цей-

тинских формул экспоненциальные нижние оценки на резолюционные доказательства в общем виде.

Первые экспоненциальные нижние оценки для резолюций в общем виде получил Хакен в 1985 г. В качестве трудных формул использовался принцип Дирихле. Формула $\mathtt{PHP}_n^m$ кодирует утверждение, что можно посадить m кроликов в n клеток так, чтобы в каждой клетке сидело не более одного кролика. При $m > n$ формула невыполнима. Хакен показал, что формула $\mathtt{PHP}_{n-1}^n$ имеет резолюционное доказательство размера $2^{\Omega(n)}$. В 1988 г. Басс и Туран показали нижнюю оценку $2^{\Omega(n^2/m)}$ для формулы $\mathtt{PHP}_n^m$. В 1999 г. Басс и Питасси показали, что формула $\mathtt{PHP}_n^m$ имеет доказательство размера $2^{\Omega(n)}$ при $m = 2^{\sqrt{n \log n}}$. Также Басс и Питасси показали, что для любых $m > n$ формула $\mathtt{PHP}_n^m$ имеет резолюционное доказательство размера $2^{O(n)}$, что показало точность уже полученных нижних оценок.

В 2004 г. Разборов рассмотрел формулу для принципа совершенного паросочетания $\mathtt{PMP}_G$. Формула $\mathtt{PMP}_G$ выполнима тогда и только тогда, когда в графе G есть совершенное паросочетание.

Разборов показал, что формула $\mathtt{PMP}_G$ имеет минимальное резолюционное доказательство размера $2^{\Omega(\delta(G)/\log^2 n)}$, где n — число вершин в графе, а $\delta(G)$ — минимальная степень графа. Данчев и Риис в 2001 г. и Алекнович в 2004 г. рассмотрели задачу замощения домино шахматной доски с двумя выколотыми угловыми клетками. Для доски размера $2n \times 2n$ соответствующие формулы содержат $\Theta(n^2)$ переменных и эквивалентны $\mathtt{PMP}_G$. Авторы показали нижнюю оценку $2^{\Omega(n)}$ на размер резолюционного доказательства.

В 2015 г. Ицыксон, Слободкин и Соколов показали, что если взять специальный двудольный граф с n и $m = O(n)$ вершинами в долях при $m > n$, и степень каждой вершины будет ограничена константой, то любое резолюционное доказательство формулы $\mathtt{PMP}_G$ будет иметь размер хотя бы $2^{\Omega(n)}$.

Как следствие, авторы получили нижнюю оценку $2^{\Omega(n)}$ для двудольной клики $K_{n,m}$ при $m = O(n)$ и клики K_{2n+1}.

Для произвольного графа G на n вершинах известна тривиальная верхняя оценка $2^{O(n \log n)}$ для формул $\mathtt{PMP}_G$.

Вопрос 1. Является ли нижняя оценка $2^{\Omega(n)}$ для формулы $\mathtt{PMP}_G$ точной или ее можно улучшить?

В 2014 г. Ицыксон и Соколов рассмотрели расширение DPLL алгоритма — алгоритм линейных расщеплений. Алгоритм линейных расщеплений ищет выполняющий набор для пропозициональной формулы ϕ. Алгоритм поддерживает систему линейных уравнений Ψ над полем $\mathbb{F}_2$, изначально пустую. Выполняющий набор ищется среди решений системы Ψ. Алгоритм работает рекурсивно; на каждом шаге выбирается линейная комбинация $\bigoplus_{i \in I} x_i$ для некоторого множества индексов I и в одном рекурсивном запуске в систему добавляется уравнение $\bigoplus_{i \in I} x_i = 0$, в другом — $\bigoplus_{i \in I} x_i = 1$. Если система оказывается несовместна или какой–либо дизъюнкт не имеет выполняющего набора среди решений Ψ, алгоритм откатывается на шаг назад.

В соответствие алгоритму Ицыксон и Соколов сопоставили систему доказательств Res-Lin. Вместо обычных дизъюнктов система оперирует дизъюнкциями линейных уравнений по модулю два. Соответствующее правило резолюции выглядит следующим образом:

$$\frac{\bigoplus_{i \in I} x_i = 0 \vee C_1 \quad \bigoplus_{i \in I} x_i = 1 \vee C_2}{C_1 \vee C_2}.$$

Сами линейные уравнения появляются в результате правила ослабления:

$$\frac{C}{D},$$

где дизъюнкция линейных уравнений D семантически следует из C.

В своей работе авторы показали, что древовидное доказательство в системе Res-Lin эквивалентно протоколу работы алгоритма линейных расщеп-

лений. Размер минимального доказательств совпадает с оптимальным временем работы алгоритма линейных расщеплений с точностью до константы.

Примеры, основанные на системах линейных уравнений, оказываются простыми для Res-Lin. В 2014 г. Ицыксон и Соколов доказали экспоненциальную нижнюю оценку $2^{\Omega(n)}$ на размер древовидного доказательства Res-Lin для формулы $\mathtt{PHP}_n^{n+1}$. В 1999 г. Ивама и Миязаки показали, что минимальное древовидное доказательство в системе Res для $\mathtt{PHP}_n^{n+1}$ имеет размер $2^{\Theta(n \log n)}$.

Вопрос 2. Является ли нижняя оценка $2^{\Omega(n)}$ на размер древовидного доказательства формулы $\mathtt{PHP}_n^m$ в системе Res-Lin точной или ее можно улучшить?

Резолюционные системы доказательств не ограничиваются пропозициональными формулами. В 2002 г. Митчелл рассмотрел резолюционную систему доказательств NG-Res для задачи выполнения ограничений (CSP). CSP состоит из множества переменных X и набора ограничений S, которые зависят от этих переменных. Переменные X принимают значения из некоторого фиксированного алфавита D. Размер D может быть больше двух. Задача состоит в поиске подстановки $\rho : X \to D$, которая бы выполнила все ограничения.

Ограничения, имеющие вид $\neg(x_1 = \sigma_1 \wedge x_2 = \sigma_2 \wedge \cdots \wedge x_t = \sigma_t)$, где $\sigma_i \in D$ для $i \in [t]$, будем называть запрещающими наборами. Запрещающий набор N соответствует ограничению $f \in S$, если (1) множества переменных, от которых зависят f и N, совпадают; (2) любая подстановка выполняющая f, выполняет N.

Доказательство в системе NG-Res — это последовательность запрещающих наборов, каждый из которых соответствует ограничению из S, выводится по правилу резолюции (принимает $k = |D|$ посылок в отличии от Res):

$$\frac{\neg(x = a_1 \wedge \alpha_1) \quad \cdots \quad \neg(x = a_k \wedge \alpha_k)}{\neg(\alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_k)}$$

или по правилу ослабления:

$$\frac{\neg(\alpha)}{\neg(\alpha \wedge x = a)}.$$

Последний запрещающий набор — тождественно ложный.

Максимальное число переменных среди всех запрещающих наборов доказательства называется шириной доказательства. Минимум по ширинам всех доказательств CSP ϕ называется минимальной шириной доказательства ϕ и обозначается $W(\phi \vdash 0)$. Максимальное число переменных, от которых зависят ограничения самой CSP ϕ, обозначим $W(\phi)$.

В 2001 г. Бен–Сассон и Вигдерсон предложили наиболее мощную технику получения нижних оценок, через минимальную ширину доказательства. Митчелл обобщил технику до CSP и получил следующую теорему.

Теорема 1 (Митчелл, 2002)**.** Для CSP ϕ, зависящей от n переменных, выполняются следующие неравенства:

$$\begin{aligned} S_T(\phi) &\geq 2^{W(\phi\vdash 0)-W(\phi)}, && (1)\\ S(\phi) &\geq \exp\left(\Omega\left(\frac{(W(\phi\vdash 0)-W(\phi))^2}{n}\right)\right), && (2) \end{aligned}$$

где S и S_T — размеры минимальных доказательств в NG-Res общего вида и древовидного соответственно.

Для получения нижней оценки на минимальную ширину доказательства используют расширительную способность CSP. Пусть F — множество ограничений; обозначим ∂F множество переменных, от каждой из которых зависит ровно одно ограничение в F. Расширительная способность CSP ϕ

$$e_t(\phi) = \min_{F \subseteq S} |\partial F|,$$

где минимум берется по всем множествам F таким, что $\frac{1}{t+1}|S| \leq |F| \leq \frac{t}{t+1}|S|$.

Прямой перенос техники Бен–Сассона и Вигдерсона на CSP дает нижнюю оценку $W(\phi \vdash 0) \geq e_k(\phi)$, где k — размер алфавита. Можно заметить,

что чем больше k, тем больше вариантов для подмножества F. Соответственно, с увеличением размера алфавита, значение $e_k(\phi)$ уменьшается.

Вопрос 3. Можно ли улучшить нижнюю оценку на ширину так, чтобы она не зависела от размера алфавита?

Для CSP ϕ, чувствительной к подстановкам, можно получить нижнюю оценку $W(\phi \vdash 0) \geq e_2(\phi) - 1$.

Расширительная способность цейтинской формулы $\texttt{Ts}(G)$, построенной на графе G, совпадает с расширительной способностью графа G. Теорема Митчелла для расширенной версии формул дает нижнюю оценку $2^{e_2(G)-d-1}$ на размер древовидного доказательства в системе NG-Res, где d — максимальная степень графа. Кажется естественным, чтобы в основании степени стояло значение размер алфавита k, а не 2. Возможно, детальный анализ конкретной формулы может дать такую оценку.

Вопрос 4. Верно ли, что для невыполнимой цейтинской формулы $\texttt{Ts}(G)$ можно показать нижнюю оценку $k^{e_2(G)-d}$ на размер древовидных доказательств в системе NG-Res?

Техники Бен–Сассона и Вигдерсона, а затем Митчелла активно используют расширительную способность формулы для получения нижних оценок.

Вопрос 5. Является ли расширительная способность формулы необходимым свойством, хотя бы на примере древовидных доказательств NG-Res?

Резолюционные системы доказательств находят свое применение в комбинаторике слов.

Пусть P множество частичных строк над бинарным алфавитом (на некоторых позициях в строках стоят пустые символы: $\square$). В задаче избегаемости частичных строк спрашивается, существует ли бесконечная в обе стороны строка, которая не содержит в качестве подстроки ни одной строки из P.

Задачу избегаемости можно переформулировать в терминах выполнимости пропозициональной формулы на бесконечном числе переменных

$\cdots x_{-1}x_0x_1\cdots$. Сопоставим каждой строке $s \in P$ счетное число дизъюнктов, каждый из которых запрещает подстроку s на конкретной позиции в бесконечной строке. Такие формулы будем называть подвижными, поскольку дизъюнкт как бы двигается вдоль строки.

Известно, что если запрещенные строки не содержат пропусков, то задача избегаемости решается за полиномиальное время методом Ахо–Корасика. В 2002 г. Лотар предложил систему вывода над строками: если бесконечная строка избегает строки $xy0$ и $y1$ (или $xy1$ и $y0$), где x и y — некоторые конечные строки, то она же избегает строку xy. Бесконечной строки не существует тогда и только тогда, когда можно вывести пустую строку.

В 2009 г. Бланше с соавторами показали, что задача избегаемости с пропусками **NP**–труда, Блэкели показал принадлежность **PSPACE**. В работе [1] мои соавторы Ицыксон и Охотин показали **PSPACE**–полноту задачи избегаемости и то, что отсутствие строки можно доказать в резолюционной системе доказательств с выводом размера $2^{O(n^2)}$, где n — размер задачи.

Структура подвижной формулы позволяет расширить систему доказательств дополнительным правилом сдвига. Если есть вывод дизъюнкта $x_{i_1}^{\sigma_1} \vee \cdots \vee x_{i_t}^{\sigma_t}$, то можно вывести сдвиг на j позиций $x_{i_1+j}^{\sigma_1} \vee \cdots \vee x_{i_t+j}^{\sigma_t}$ для любого $j \in \mathbb{Z}$.

Вопрос 6. Может ли правило сдвига существенно сократить размер доказательства подвижной формулы?

Аналогичное правило сдвига можно добавить в систему секущих плоскостей, полиномиального исчисления и другие

Вопрос 7. Существуют ли трудные формулы с экспоненциальными нижними оценками на размеры доказательств в системах доказательств с правилом сдвига (резолюционных, секущих плоскостях, полиномиальном исчислении)?

Цели работы.

1. Получить верхнюю оценку на принцип паросочетания в произвольном графе в системе Res, которая совпадает с нижней с точностью до константы в экспоненте.

2. Получить верхнюю оценку на принцип Дирихле для древовидных доказательств в системе Res-Lin, которая совпадает с нижней с точностью до константы в экспоненте.

3. Доказать нижнюю оценку на минимальную ширину доказательства в NG-Res, не зависящую от размера алфавита.

4. Показать, что для невыполнимой цейтинской формулы $\mathtt{Ts}(G)$, построенной на графе G с максимальной степенью d, древовидное доказательство в системе NG-Res имеет нижнюю оценку $k^{e_2(G)-d}$.

5. Построить верхнюю оценку на древовидные доказательства в системе NG-Res через расширительную способность CSP.

6. Построить пример подвижных формул, на которых классические системы доказательств отделяются от систем доказательств со сдвигом.

7. Получить нижнюю оценку на системы доказательств со сдвигом: резолюционные, секущих плоскостей и полиномиального исчисления.

Научная новизна. Все результаты диссертации являются новыми.

Теоретическая и практическая ценность. Работа носит теоретический характер. Ее результаты могут быть использованы для дальнейших исследований в структурной теории сложности и теории сложности доказательств.

Методы исследований. В работе используются методы теории сложности вычислений и доказательств.

Основные результаты.

1. Доказано, что формула $\mathtt{PMP}_G$ для любого графа G на n вершинах без совершенного паросочетания имеет доказательство в системе Res размера $O(n^2 \cdot 2^n)$. Оценка совпадает с ранее известной нижней с точностью до константы в показателе экспоненты.

2. Доказано, что формула $\mathtt{PHP}_n^m$ при $m > n$ имеет древовидное доказательство размера $2^{O(n)}$ в системе Res-Lin. Оценка совпадает с нижней с точностью до константы в показателе экспоненты.

3. Доказано, что минимальная ширина доказательства чувствительных к подстановкам CSP ϕ ограничена снизу $e_2(\phi) - 1$. Нижняя оценка не зависит от размера алфавита.

4. Доказано, что обобщенные цейтинские формулы $\mathtt{Ts}(G, f)$, построенные на основе графа G с максимальной степенью d и расширительной способностью $e_2(G)$ над алфавитом размера k, имеют древовидные доказательства в NG-Res размера как минимум $k^{e_2(G)-d}$.

5. Показана формально необходимость расширительной способности графа для нижних оценок на древовидные доказательства в системе NG-Res. По CSP ϕ над алфавитом размера k можно построить граф зависимостей $G = \langle V, E \rangle$, который описывает сколько общих переменных имеет каждая пара ограничений. Показано, что в графе G существует подграф H такой, что древовидная сложность CSP ϕ в системе NG-Res не больше $k^{e(H) \cdot \log_{3/2} |V|}$.

6. Построен пример невыполнимой подвижной формулы, которая имеет вывод полиномиального размера в резолюционной системе доказательств со сдвигом, однако в любой классической системе доказательств без сдвига вывод имеет экспоненциальный размер.

7. Доказаны нижние экспоненциальные оценки для систем доказательств с правилом сдвига (резолюционных, секущих плоскостей и полиномиального исчисления).

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

1. Международная конференция “First Russian-Finnish Symposium on Discrete Mathematics” (Турку, RuFiDim 2012).

2. Международная конференция “The 8th International Computer Science Symposium in Russia” (Екатеринбург, CSR 2013).

3. Международная конференция “19th International Conference on Theory and Applications of Satisfiability Testing” (Бордо, SAT 2016).

4. Международная конференция “41st International Symposium on Mathematical Foundations of Computer Science” (Краков, MFCS 2016)

5. Научный семинар в LIRMM, Университет Монпелье 2, 2016.

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

В работе [1] **PSPACE**–полнота задачи избегаемости принадлежит соавторам; диссертанту принадлежит доказательство теоремы о разделении систем доказательств с правилом сдвига и без него. При этом разделяющие формулы предложил Д.М. Ицыксон. Нижние оценки на системы доказательств с правилом сдвига получены диссертантом.

Работа [2] написана в соавторстве с научным руководителем. Научному руководителю принадлежит постановка задачи, диссертанту принадлежит техническая часть всех доказательств.

В работе [4] диссертанту принадлежит верхняя оценка на формулы, кодирующие принцип совершенного паросочетания, остальные результаты принадлежат соавторам.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения и списка литературы. Общий объем диссертации — 95 страниц. Список литературы включает 45 наименования на 6 страницах.

Содержание работы

Во **введении** описывается состояние области на сегодняшний день, рассматриваются задачи диссертации, ставятся цели, формулируются основные результаты и описывается структура диссертации.

Первая глава посвящена базовым понятиям, используемым в диссертации. Вводятся основные обозначения, упоминаемые классы сложности, определяются понятие системы доказательств, DPLL алгоритма, задачи выполнения ограничений и некоторые понятия теории графов, используемые в работе.

Вторая глава посвящена верхним оценкам в системе доказательств Res и древовидном расширении Res-Lin. В разделе 2.1 определяются два семейства формул, кодирующих принцип Дирихле ($\mathtt{PHP}_n^m$) и принцип совершенного паросочетания ($\mathtt{PMP}_G$).

В разделе 2.2 показывается верхняя оценка в Res для формулы $\mathtt{PMP}_G$.

Теорема 2.2. Пусть граф G содержит n вершин и не имеет совершенного паросочетания. Тогда существует резолюционное доказательство размера $O(n^2 \cdot 2^n)$ для формулы $\mathtt{PMP}_G$.

Раздел 2.3 посвящен верхним оценкам на древовидные доказательства в Res-Lin.

Теорема 2.3. Для любой формулы $\mathtt{PHP}_n^m$ при $m > n$ существует древовидное доказательство в системе Res-Lin размера $2^{O(n)}$.

Теорема 2.5 (следствие из теоремы 2.3)**.** Пусть граф $G = \langle V, E \rangle$ содержит n вершин и не содержит совершенного паросочетания. Тогда для формулы $\mathtt{PMP}_G$ существует древовидное доказательство в системе Res-Lin размера $2^{O(n)}$.

Третья глава посвящена оценкам для системы доказательств NG-Res. В разделе 3.1 показывается нижняя оценка на минимальную ширину доказательства.

Теорема 3.1. Пусть CSP ϕ зависит от множества переменных X, переменные принимают значения из алфавита D, а S — это множество ограничений. Пусть CSP удовлетворяет следующим свойствам.

- CSP ϕ невыполнима.
- Если удалить любое ограничение $f \in S$, CSP станет выполнимой.
- Пусть произвольная подстановка ρ нарушает некоторое ограничение $f \in S$. Для любой переменной x, от которой зависит f, найдется значение $a \in D$ такое, что если заменить значение $\rho(x)$ на a, ограничение f будет выполнено.

Тогда $W(\phi \vdash 0) \geq e_2(\phi) - 1$.

В разделе 3.2 определяется обобщенная цейтинская формула, дается критерий невыполнимости.

В разделе 3.3 показывается нижняя оценка на размер древовидного доказательства в системе NG-Res.

Теорема 3.2. Дюбое древовидное доказательство для цейтинской формулы $\mathtt{Ts}(G)$, построенной над алфавитом $\mathbf{Z}_k$ и графом с расширительной способностью $e_2(G)$ и максимальной степенью d, имеет размер хотя бы $k^{e_2(G)-d}$.

В разделе 3.4 определяется граф зависимостей для произвольной CSP. Показывается верхняя оценка на древовидное доказательство в системе NG-Res.

Теорема 3.3. Пусть ϕ — невыполнимая CSP, определенная над алфавитом размера k, с графом зависимостей $G = \langle V, E \rangle$. Тогда в графе G есть подграф H такой, что

$$S_T(\phi) \leq k^{e(H)\cdot \log_{\frac{3}{2}} |V|},$$

где $S_T(\phi)$ — размер минимального древовидного доказательства ϕ в системе NG-Res.

Четвертая глава посвящена подвижным формулам и системам доказательств с правилом сдвига.

В разделе 4.1 определяются понятия подвижной формулы и системы доказательств с правилом сдвига.

В разделе 4.2 показывается, как из трудной формулы для классической системы доказательств (такой, как резолюционная система доказательств, система секущих плоскостей или система полиномиального исчисления) получить трудную формулу для той же системы доказательств с правилом сдвига.

В подразделе 4.2.1 описан сам процесс преобразования. В подразделе 4.2.2 вводится понятие f–устойчивой системы доказательств. Система доказательств является f–устойчивой, если после замены переменных в формуле размер минимального доказательства увеличивается не более чем в f раз. Формулируется теорема, по которой можно получить нижнюю оценку для f–устойчивой системы доказательств с правилом сдвига.

Теорема 4.1. Пусть Π — классическая f–устойчивая система доказательств. Пусть формула ϕ_n имеет кратчайшее доказательство в системе Π размера $S_\Pi(\phi_n)$. Тогда длина кратчайшего доказательства формулы Ψ_n в системе Shift-Π как минимум $\Omega\left(\frac{S_\Pi(\phi_n)}{f^2 \cdot n}\right)$.

В подразделе 4.2.3 показывается, что резолюционная система доказательств, система секущих плоскостей и система полиномиального исчисления $O(n)$–устойчивы. Как следствие, получаются следующие нижние оценки для соответствующих систем доказательств с правилом сдвига.

Следствие 4.1. Существует семейство формул $\{\phi_n\}_{n\geq 1}$, где каждая формула зависит от n переменных и содержит $O(n)$ дизъюнктов, что любое резолюционное доказательство с правилом сдвига соответствующей подвижной формулы Ψ_n имеет размер $2^{\Omega(n)}$.

Следствие 4.2. Существует семейство формул $\{\phi_n\}_{n\geq 1}$, где каждая формула состоит из n дизъюнктов, что любое доказательство в секущих плоскостях с правилом сдвига соответствующей подвижной формулы Ψ_n имеет размер $2^{n^{\Omega(1)}}$.

Следствие 4.3. Существует семейство формул $\{\phi_n\}_{n\geq 1}$, где каждая формула состоит из $O(n^2)$ дизъюнктов, что любое доказательство в полиномиальном исчислении с правилом сдвига соответствующей подвижной формулы Ψ_n имеет размер $2^{n^{\Omega(1)}}$.

В разделе 4.3 показывается экспоненциальное разделение между резолюционной системой доказательств с правилом сдвига и классической системой без него.

Теорема 4.2. Существует семейство подвижных формул $\{\Phi_n\}$ таких, что (1) для любой классической системы доказательств Π, любое доказательство формулы Φ_n имеет размер $\Omega(2^n)$; (2) формула Φ_n имеет резолюционное доказательство с правилом сдвига полиномиального от n размера.

В **заключении** подводятся итоги диссертации, ставятся открытые вопросы.

Публикации автора по теме диссертации в рецензируемых научных изданиях:

1. Itsykson D., Okhotin A., Oparin V. Computational and Proof Complexity of Partial String Avoidability // 41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 - Kraków, Poland. Vol. 58 of *Leibniz International Proceedings in Informatics*. 2016. P. 51:1–51:13.
2. Itsykson D., Oparin V. Graph Expansion, Tseitin Formulas and Resolution Proofs for CSP // Computer Science - Theory and Applications - 8th International Computer Science Symposium in Russia, CSR 2013, Ekaterinburg, Russia, June 25-29, 2013. Proceedings. Vol. 7913 of *Lecture Notes in Computer Science*. 2013. P. 162–173.
3. Oparin V. Tight Upper Bound on Splitting by Linear Combinations for Pigeonhole Principle // Theory and Applications of Satisfiability Testing – SAT 2016: 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings. Cham, 2016. Vol. 9710 of *Lecture Notes in Computer Science*. P. 77–84.
4. Tight Lower Bounds on the Resolution Complexity of Perfect Matching Principles / D. Itsykson, V. Oparin, M. Slabodkin et al. // Fundamenta Informaticae. 2016. Vol. 145, no. 3. P. 229–242.