САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

Кожевников Арист Александрович

СЛОЖНОСТЬ ПРОПОЗИЦИОНАЛЬНЫХ СИСТЕМ ДОКАЗАТЕЛЬСТВ, ОПЕРИРУЮЩИХ НЕРАВЕНСТВАМИ

01.01.06 — математическая логика, алгебра и теория чисел

А В Т О Р Е Ф Е Р А Т

диссертации на соискание учёной степени

кандидата физико-математических наук

Санкт-Петербург — 2007

Работа выполнена в Санкт–Петербургском отделении Математического института им. В. А. Стеклова Российской академии наук

Научный руководитель	—	кандидат физико-математических наук, доцент Гирш Эдуард Алексеевич
Официальные оппоненты	—	доктор физико-математических наук, Пономаренко Илья Николаевич
	—	кандидат физико-математических наук, доцент Тишков Артём Валерьевич
Ведущая организация	—	Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук

Защита диссертации состоится “ ” 2007 года в часов на заседании Диссертационного совета Д 212.232.29 по защите диссертаций на соискание учёной степени доктора наук при Санкт–Петербургском государственном университете по адресу: 198504, Санкт–Петербург, Старый Петергоф, Университетский пр., 28, математико-механический факультет Санкт–Петербургского государственного университета.

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

Защита будет проходить в Санкт–Петербургском отделении Математического института им. В. А. Стеклова РАН по адресу: Санкт–Петербург, наб. реки Фонтанки, д. 27, ауд. 311.

Автореферат разослан “ ” 2007 года.

Учёный секретарь диссертационного совета,
доктор физико-математических наук,
профессор Нежинский В. М.

Общая характеристика работы

Актуальность темы. Необходимость математического изучения понятия доказательства была сформулирована и обоснована Д. Гильбертом совместно с П. Бернайсом в "Основаниях математики". Д. Гильберта интересовала непротиворечивость всей математики и, в частности, непротиворечивость доказательств основных теорем. Для того, чтобы проверить корректность доказательства за разумное время, необходимо, чтобы само доказательство было разумного размера. Отсюда возникает важный вопрос о сложности систем доказательств, изучение которого было инициировано работой С. А. Кука и Р. А. Рекхоу 1979 г.: в естественном предположении, что каждый шаг доказательства проверяется за полиномиальное время, требуется оценить количество шагов доказательства.

Формальное определение системы доказательств следующие: *системой доказательств* для языка L называется полиномиально вычислимая функция, отображающая слова из некоторого конечного алфавита (кандидаты на роль доказательств) на L, чьи элементы можно рассматривать как теоремы.

Исторически сложилась более естественная, похожая на обычное математическое доказательство, терминология для описания систем доказательств. В ней, в качестве L используется один из естественных языков математических объектов, например, язык пропозициональных тавтологий в нормальной форме. *Доказательством* в такой системе называется конечная последовательность *строк*, заканчивающейся строкой, которую мы хотим доказать. Каждая строка в доказательстве получается из предыдущих строк по *правилу вывода*. Если правило не имеет посылки, оно называется *аксиомой*.

Пропозициональной системой доказательств называется система доказательств для языка **TAUT** пропозициональных тавтологий в дизъюнктивной нормальной форме (ДНФ). Поскольку такой язык содержится в co-**NP**, то любую систему доказательств для co-**NP**-трудного языка L можно считать пропозициональной системой доказательств, для этого необходимо лишь зафиксировать конкретное сведение.

Многие системы доказательств не имеют коротких выводов простых фактов, например, известная резолюционная система доказательств, введённая Дж. Робинсоном в 1965 г., не имеет короткого доказательства принципа Дирихле. С другой стороны, можно естественным образом переписать данную формулу в виде системы линейных неравенств, например, записав каждую дизъюнкцию следующем образом:

$$\bigvee x_i \vee \bigvee \neg y_i \quad \to \quad \sum x_i + \sum (1 - y_i) \geq 1.$$

Далее, при помощи *полуалгебраических систем доказательств* можно выводить из неравенств новые полиномиальные неравенства, являющиеся полуалгебраическими следствиями искомых. В частности, для принципа Дирихле в используемых полуалгебраических системах это приводит к короткому доказательству. На эффективность данной техники для других тавтологий мог бы позволить надеяться предложенный в 1979 Л. Г. Хачияном полиномиальный алгоритм решения задачи линейного программирования, а также различные алгоритмы, основанные на методе внутренней точки.

Первая полуалгебраическая система доказательств, *"секущие плоскости"* (CP), оперирующая только линейными неравенствами, была введена в работах Р. Е. Гомори 1963 г. и В. Хватала 1973 г. Доказательство нижней экспоненциальной оценки для системы "секущие плоскости" долгое время оставалось важным открытым вопросом. В работе А. Гёрдта 1991 г. была доказана нижняя экспоненциальная оценка для CP с ограниченной степенью ложности, в работах М. Боне и др. 1995 г. и Я. Крайчека 1997 г. для CP с унарными коэффициентами, в работах Р. Импалияццо и др. 1995 г. и Я. Крайчека 1998 г. для древовидных "секущих плоскостей". Для системы без ограничений нижняя экспоненциальная оценка была доказана П. Пудлаком в 1997 г. Нижняя экспоненциальная оценка для другой изучаемой в диссертации системы *"поднять и спроецировать"* была доказана аналогичной техникой С. Дашем в 2002 г.

Для *системы Ловаса-Схрайвера*, оперирующей квадратичными неравенствами, нижние экспоненциальные оценки были известны только для древовидных доказательств систем неравенств, не обладающих короткой записью в виде булевой формулы (один из результатов работы Д. Ю. Григорьева и др. 2002 г.). Также было известно несколько условных нижних оценок: для системы, объединённой с CP, П. Пудлака 1997 г., и для древовидной версии системы, П. Бима и др. 2005 г.

Цели работы. **1.** Доказать нижние экспоненциальные оценки на размер вывода в полуалгебраических системах доказательств, для которых они были не известны. Предложить новые методы доказательства таких оценок.

2. Показать верхние полиномиальные оценки на размер вывода формул, не имеющих полиномиальной верхней оценки в других системах доказательств, доказав, таким образом, экспоненциальное отделение одной системы от другой.

3. Промоделировать правила одной полуалгебраической системы доказательств в другой за полиномиальное или субэкспоненциальное количество шагов, показав таким образом, что первая система доказательств не слишком сильнее последней.

Общая методика работы. В работе используются методы, традиционные для теории сложности доказательств. В диссертации доказан ряд конкретных верхних и нижних оценок для полуалгебраических систем доказательств, основанных на методе моделирования одной системы в другой, методе интерполяции доказательства булевой схемой и методе уменьшения доказательства подстановками. В работе предложен новый метод выбора подстановок, сохраняющих свойства графа-расширителя, по которому была построена формула.

Основные результаты работы. **1.** Получены нижние экспоненциальные оценки на размер статических и древовидных доказательств в системе Ловаса-Схрайвера для цейтинских тавтологий. Доказана моделируемость системы доказательств "поднять и спроецировать" с унарными коэффициентами в системе "секущие плоскости".

2. Доказана верхняя полиномиальная оценка на размер доказательства цейтинских тавтологий в крайчековском расширении генценовского типа системы "поднять и спроецировать". Улучшены нижние экспоненциальные оценки на размер древовидного доказательства в рассматриваемой системе доказательств, устранена зависимость от максимального размера коэффициентов.

3. Изучена сложность систем Ловаса-Схрайвера старших степеней с ограничением на свободный член: рассматриваемые системы экспоненциально отделены от системы "секущие плоскости" и обобщения резолюционной системы доказательств, оперирующего формулами в k-ДНФ. Получена нижняя экспоненциальная оценка на размер доказательств цейтинских тавтологий.

Научная новизна. Все основные результаты диссертации являются новыми.

Практическая и теоретическая ценность. Работа носит теоретический характер. Результаты работы могут быть использованы для дальнейшего изучения сложности как полуалгебраических, так и других пропозициональных систем доказательств. В частности, техника работы с графами-расширителями открывает широкие перспективы для доказательства нижних экспоненциальных оценок. Работа также может представлять интерес для практического использования полуалгебраических систем доказательств и алгоритмов в системах автоматического доказательства и автоматической верификации.

Апробация работы. Результаты диссертации докладывались на семинаре по дискретной математике ПОМИ РАН, а также на международных конференциях “Вторые дни логики и вычислимости в Санкт-Петербурге”, посвящённой столетию А. А. Маркова (август 2003, Санкт-Петербург, Россия), “Международном коллоквиуме по автоматам, языкам и программированию”, ICALP (июль 2006, Венеция, Италия) и “Международной конференции по теории и практическому применению задачи выполнимости”, SAT (август 2006, Сиэтл, США).

Публикации. Основные результаты диссертации изложены в шести научных статьях, перечисленных в конце автореферата, в том числе в одной статье, опубликованной в журнале, рекомендованном Высшей аттестационной комиссией.

Структура и объем диссертации. Диссертация состоит из введения и четырёх глав. Нумерация разделов, формул, примеров, лемм и теорем ведётся отдельно для каждой главы. Текст диссертации изложен на 96 страницах (исключая список литературы). Список литературы содержит 57 наименований.

Содержание работы

Во **введении** приводится обоснование актуальности темы диссертации, формулируются цели и задачи работы, а также кратко описывается структура диссертации.

Основным объектом исследования является *сложность полуалгебраических пропозициональных систем доказательств*, т.е. оценка размеров выводов тавтологий в ДНФ (дизъюнктивной нормальной форме), использующих конечное число проверяемых за полиномиальное время аксиом и правил вывода, оперирующих полиномиальными неравенствами.

Основные понятия теории сложности доказательств определяются в **первой главе**. Система доказательств A *полиномиально моделируется* в системе доказательств B, если для любого доказательства ρ в A существует доказательство полиномиальной от $|\rho|$ длины того же факта в B. Доказательство *нижних экспоненциальных оценок* для системы Π обычно заключается в предоставлении такой последовательности $x_n \in L, n \in \mathbb{N}$, в которой длина каждого x_n полиномиально зависит от n и любое Π-доказательство x_n имеет экспоненциальный от n размер.

Полуалгебраические системы доказательств преобразовывают каждый дизъюнкт отрицания исходной тавтологии F, содержащий переменные $v_1, \ldots, v_t$, в неравенство

$$l_1 + \ldots + l_t \geq 1, \tag{1}$$

где $l_i = v_i$, если переменная v_i входит положительно в исходный дизъюнкт, и $l_i = 1 - v_i$, если v_i входит отрицательно. Далее из полученной системы выводится противоречие $0 \geq 1$ при помощи естественных правил работы с неравенствами и правил, использующих факт булевости переменных. Следовательно, если таким образом может быть выведено противоречие, формула F действительно является тавтологией.

В работе изучается сложность нескольких полуалгебраических систем доказательств. Первые две из них, системы *"секущие плоскости"* (CP, Cutting Planes) и *"поднять и спроецировать"* (L&P, Lift and Project) оперируют только линейными неравенствами. Обе системы используют аксиомы

$$x \geq 0, \qquad 1 - x \geq 0, \tag{2}$$

для каждой переменной x. Система CP использует правила:

$$\frac{f_1 \geq 0 \quad f_2 \geq 0}{\lambda_1 f_1 + \lambda_2 f_2 \geq 0} \quad (\text{где } \lambda_i \in \mathbb{N}), \tag{3}$$

$$\frac{a \cdot \sum_i a_i x_i \geq c}{\sum_i a_i x_i \geq \lceil \frac{c}{a} \rceil} \quad (\text{где } a \in \mathbb{N}, c, a_i \in \mathbb{Z}, \text{ а } x_i \text{ — переменные}). \tag{4}$$

В системе L&P последнее правило заменяется на

$$\frac{f \geq 0 \quad g \geq 0}{fx + g(1-x) + c(x^2 - x) \geq 0}, \tag{5}$$

где константа c выбирается таким образом, чтобы заключение правила было линейным.

Система Ловаса-Схрайвера (LS, Lovász-Schrijver) оперирует квадратичными неравенствами, использует правило сложения (3) и правило умножения на литерал:

$$\frac{f \geq 0}{fx \geq 0}, \qquad \frac{f \geq 0}{f(1-x) \geq 0} \qquad (\text{где } \deg f = 1). \tag{6}$$

Для того чтобы переменные принимали лишь значения 0 и 1, множество аксиом (2) следует расширить следующими аксиомами для каждой из переменных:

$$x^2 - x \geq 0. \tag{7}$$

Систему можно расширить до LS_+ следующем множеством аксиом:

$$f^2 \geq 0 \qquad (\text{где } \deg f = 1). \tag{8}$$

Описанные выше системы можно усилить, позволив им оперировать неравенствами старших степеней. В частности, в LS^k в правиле (6) неравенство f может быть любой степени, меньшей k. Различные системы доказательств можно комбинировать между собой, разрешая одной системе использовать правила вывода из другой. Таким образом определяется система LS^k+CP^k, оперирующая правилами LS^k и CP^k.

Полуалгебраическая система генценовского типа $\mathrm{R}(\mathfrak{S})$ представляет собой естественное усиление $\mathfrak{S}$ — любой из определённых выше систем, позволяющее работать с предположениями: в частности, можно предположить, что линейная сумма с целочисленными коэффициентами f больше чем целое c или, наоборот, f не больше чем c и вывести в каждом предположении противоречие. Запишем правила вывода $\mathrm{R}(\mathfrak{S})$ (мы будем обозначать через Γ произвольную дизъюнкцию неравенств):

$$\frac{f_1 \geq 0 \bigvee \Gamma, f_2 \geq 0 \bigvee \Gamma}{h \geq 0 \bigvee \Gamma}, \quad \text{если} \quad \frac{f_1 \geq 0, f_2 \geq 0}{h \geq 0} \text{ — правило вывода } \mathfrak{S},$$

$$\frac{\Gamma}{\Gamma \bigvee f \geq 0}, \qquad \frac{f \geq 0 \bigvee f \geq 0 \bigvee \Gamma}{f \geq 0 \bigvee \Gamma},$$

и множеством аксиом

$$f \geq 1 \bigvee f \leq 0 \qquad \text{где } f \text{ — линейная сумма с коэффициентами из } \mathbb{Z}.$$

Отметим, что мы можем удалять из дизъюнкций противоречие $0 \geq 1$, поскольку из него можно легко вывести любое неравенство.

Поскольку длина доказательства измеряется количеством битов, используемых в доказательстве, на ней сказывается способ записи коэффициентов. В CP и L&P для записи коэффициентов используется двоичная система счисления. В диссертации рассматриваются их ослабления CP_1 и $\mathrm{L\&P}_1$, отличающиеся от исходных тем, что оперируют целочисленными коэффициентами в унарной записи.

Другим естественным ослаблением систем доказательств являются *древовидные системы доказательств*, в которых мы не имеем возможности использовать уже доказанные факты многократно и обязаны выводить их каждый раз заново. Для систем LS^n и LS^n_+ древовидное доказательство можно записать одной большой формулой, получив таким образом, *статическое доказательство*, задаваемое коэффициентами $\omega_{i,s}$ и мультимножествами $U^+_{i,s}$, $U^-_{i,s}$, определяющими полиномы

$$u_{i,s} = \omega_{i,s} \cdot \prod_{k \in U^+_{i,s}} x_k \cdot \prod_{k \in U^-_{i,s}} (1 - x_k),$$

такие, что

$$\sum_{i=1}^{t} s_i \sum_{s} u_{i,s} = -1, \tag{9}$$

где s_i — исходные неравенства (включая аксиомы).

Ещё одно рассматриваемое в данной работе ослабление служит для того, чтобы ограничить количество дизъюнкций, при помощи которых можно записать данное линейное неравенство. Естественным образом это количество связано со следующей *литеральной формой* неравенства $\sum_{i=1}^{s} \alpha_i m_i + \sum_{i=s+1}^{s'} \alpha_i (1 - m_i) \geq c$, где α_i — положительные константы, а m_i — мономы. Для неравенства ι, определим её *степень ложности* как правую часть литеральной формы ι. *Степень ложности доказательства* в LS^k+CP^k определим как максимальную степень ложности всех возникающих в доказательстве неравенств.

Также в **первой главе** диссертации описываются основные семейства формул, используемые в дальнейшем для доказательства нижних и верхних оценок на протяжении всей диссертации. Определяются формулы, кодирующие *принцип Дирихле*, *принцип нераскрашиваемости графа, содержащего клику*, его ослабление и описываются *цейтинские формулы на графах-расширителях.*

Принцип Дирихле с m кроликами и n клетками формализует невозможность предоставить каждому кролику собственную клетку при $m > n$. Данный факт может быть выражен формулой PHP_n^m с $m \cdot n$ булевыми переменными x_{ij}, $1 \le i \le m$, $1 \le j \le n$, равными 1, если i-ый кролик сидит в j-ой клетке.

Пусть дан граф G с n вершинами. Булева формула WQC_n^m, кодирующая два факта, первый о том, что G содержит клику размера m, второй о том, что все вершины G можно раскрасить в $m-1$ цвет таким образом, что соседние вершины имеют разные цвета, является невыполнимой. Зафиксируем некоторый порядок на вершинах графа. Наличие ребра, соединяющего вершины i и j, задаётся булевой переменной p_{ij}. Переменной q_{ki} кодируется факт о том, что i-ая вершина является k-ой вершиной клики. Наконец, переменная $r_{i\ell}$ обозначает то, что i-ая вершина покрашена в ℓ-ый цвет. Таким образом, булева формула будет содержать $n^2 + m \cdot n + (m-1) \cdot n = (n + 2m - 1) \cdot n$ переменных.

Впервые формулы Ts_G, основанные на противоречии, заключающемся в том, что в графе G количество рёбер вокруг всех вершин не может быть нечётным, были использованы в работе Г. С. Цейтина 1968 г. для получения нижней оценки для регулярной резолюции. Позднее эти оценки были расширены для общей резолюции и улучшены до экспоненциальных для графов-расширителей.

Для графа G и подмножества вершин X через $\partial(X)$ мы будем обозначать множество соседей X. Назовём (r, d, c)-*расширителем* граф G с максимальной степенью d, такой, что для любого множества $X \subseteq V$, $|X| \le r$ выполняется $|\partial(X)| \ge c \cdot |X|$.

Вторая глава посвящена сложности статических полуалгебраических систем доказательств. Она содержит короткое статическое LS$_+$-доказательство формулы, кодирующей ослабленный принцип нераскрашиваемости графа, содержащего клику и нижнюю экспоненциальную оценку на размер статического LS$_+$-доказательства цейтинских формул.

Теорема 2.1. *В системе доказательств* LS_+ *существует короткое статическое доказательство четвёртой степени формулы* WQC_n^m.

Короткий вывод опровержения формулы WQC_n^m, кодирующей ослабленный принцип нераскрашиваемости в $(m-1)$ цветов графа с n вершинами, содержащего клику размера m, был найден путём моделирования вывода формулы, кодирующий принцип Дирихле.

В последнем разделе второй главы доказываются нижние экспоненциальные оценки на длину вывода цейтинских формул в статической полуалгебраической системе доказательств Ловаса-Схрайвера. Доказательство основано на идеях из работы Д. Ю. Григорьева и др. 2002 г. и разделено на четыре основные части. В первом подразделе мы показываем, что если граф G является “хорошим” расширителем, то он остаётся “хорошим” расширителем после выкидывания линейного числа рёбер. Для этого мы пользуемся техникой из статьи М. Алехновича и др. 2005 г. Далее, мы вводим систему Туэ преобразования мономов и доказываем некоторые её свойства (в частности, связь со степенями вывода в алгебраической системе доказательств *Positivstellensatz*). В следующем подразделе мы расширяем результат из работы Д. Ю. Григорьева 2001 г., доказывая нижнюю линейную оценку на булеву степень вывода в *Positivstellensatz* биномиальной записи цейтинских формул. Далее мы сводим доказательство в *Positivstellensatz* биномиальной записи цейтинских формул к доказательству в статической LS$_+$ их булевой формы. Наконец, в последнем подразделе мы показываем, как из результатов предыдущих частей, используя идеи Д. Ю. Григорьева и др. 2002 г., получить нижнюю экспоненциальную оценку на размер доказательства в статической LS$_+$ булевой формы цейтинских формул.

Теорема 2.4. *Пусть граф G является $(r = n/2, d, c)$-расширителем, где $d \geq 4$, $c > 1$, а n — количество вершин. Любое статическое доказательство цейтинской формулы* Ts_G *в* LS_+ *имеет размер* $\exp(\Omega(n))$.

В **третьей главе** изучается сложность генценовских расширений полуалгебраических систем доказательств. Через R(LP) мы будем обозначать генценовское расширение системы, оперирующей единственным правилом сложения (3). В разделе 3.1 доказывается полиномиальная эквивалентность систем R(LP) и R(L&P), $\mathrm{R(LP_1)}$ и $\mathrm{R(CP_1)}$, в следующем разделе показывается полиномиальное моделирование L&P с унарными коэффициентами, $\mathrm{LS_1}$, в $\mathrm{CP_1}$.

В разделе 3.3 приводится доказательство верхней полиномиальной оценки на размер R(LP)-доказательств цейтинских тавтологий.

Теорема 3.4. *Для любого целого числа $d \geq 1$ и для любого d-регулярного графа G с нечётным количеством вершин n, существует вывод* Ts_G *в R(LP) полиномиального от n размера.*

В последнем разделе третьей главы мы вводим понятие вещественной коммуникационной сложности и показываем, как переделать доказательство в R(CP)-подобной системе доказательств (что может использовать в качестве правил вывода все допустимые *двухпосылочные* правила вывода) в протокол вещественной игры (в котором два игрока, обмениваясь вещественными числами, должны найти решение поставленной задачи; отметим, что сложность протокола равна количеству переданных чисел). Понятие вещественной коммуникационной игры напрямую связано с понятием вещественной схемы и используемая техника представляет собой частный случай интерполяции схемой. Нижняя экспоненциальная оценка для древовидных R(CP)-подобных систем получается из оценки на размер древовидного протокола вещественной игры, решающей известную теорему Холла (записываемую при помощи формулы $Hall_n$, где $2n$ — размер соответствующего двудольного графа).

Теорема 3.8. *Пусть* π *— древовидное доказательств множества неравенств* $Hall_n$ *в некоторой* $R(CP)$*-подобной системе доказательств. Тогда* $|\pi| \geq exp(\Omega((\frac{n}{W\log(n)+(\log(n))^2})^{1/2}))$, *где* W *— максимальный размер дизъюнкции в* π.

Четвёртая глава посвящена сложности полуалгебраических систем доказательств старших степеней с ограниченной степенью ложности. В первом разделе мы доказываем верхние полиномиальные оценки в LS^2+CP^2 на размер доказательств со степенью ложности, ограниченной корнем от количества переменных, формул, кодирующих принцип Дирихле, и ослабленный принцип нераскрашиваемости графа, содержащего клику. Для этого мы переделываем короткие LS^2+CP^2-доказательства, описанные в работе Д. Ю. Григорьева и др. 2002 г., в доказательства с ограниченной степенью ложности.

В разделе 4.2 мы показываем, как доказательство в LS^k+CP^k можно переделать в доказательство в $\mathrm{Res}(k)$ (обобщение резолюционной системы доказательств, оперирующей формулами в k-ДНФ). Получаемый результат представляет собой обобщение результата Э. А. Гирша и С. И. Николенко 2005 г.

Объединяя результат из предыдущего раздела с нижней экспоненциальной оценкой для $\mathrm{Res}(k)$, доказанной М. Алехновичем в 2005 г., в разделе 4.3 мы доказываем нижнюю экспоненциальную оценку для LS^k+CP^k со степенью ложности, ограниченной линейной от количества переменных функцией, для цейтинских формул, построенных по матрицам-расширителям (обобщениях графов-расширителей).

Для множества строк I матрицы $A \in \{0,1\}^{m \times n}$ мы определим его *границу* ∂I как множество всех столбцов J матрицы A, таких что существует в точности одна строка $i \in I$ для которой $a_{ij} = 1$, для некоторого $j \in J$, в то время как для всех остальных $i' \in I$, $i' \neq i$, выполняется $a_{i',j} = 0$. Мы будем говорить, что A является (r, s, c)-*граничным расширителем*, если: 1. любая строка содержит по крайней мере s единиц; 2. для любого множества строк

I размера по крайней мере r выполняется $|\partial I| \geq c \cdot |I|$. Пусть b обозначает некоторый вектор из $\{0,1\}^n$. Тогда $\Phi(A,b)$ будет обозначать равенство $Ax = b$ по модулю 2, где каждое равенство $\oplus_{t=1}^{s} a_{ij_t} x_{j_t} = b_i$ представляется в виде 2^s эквивалентных дизъюнкций на переменных $x_{j_1}, \ldots, x_{j_s}$.

Теорема 4.3. *Существует такая положительная постоянная δ, что формула $\Phi(A,b)$ для $(\Omega(n/\Delta), 3, c)$-расширителя A, в котором любой столбец содержит по крайней мере Δ единиц, имеет в* LS^k+CP^k *со степенью ложности, ограниченной δn, доказательство только размера* $\exp(\Omega(n))$.

Работы автора по теме диссертации

1. **Кожевников, А. А.** Нижние оценки на длину вывода цейтинских формул в статической системе доказательств Ловаса-Схрайвера / Д. М. Ицыксон, А. А. Кожевников // Записки научных семинаров ПОМИ. — СПб.: 2006.— Т. 340.— С. 10–32.

2. **Kojevnikov, A.** Several notes on the power of Gomory-Chvátal cuts / E. A. Hirsch, A. Kojevnikov // Annals of Pure and Applied Logic. — Elsevier: 2006. — Vol. 411, №3. — P. 429–436.

3. **Kojevnikov, A.** Several notes on the power of Gomory-Chvátal cuts / E. A. Hirsch, A. Kojevnikov. — Electronic Colloquium on Computational Complexity. — 2003, January. — TR012. — 10 p.

4. **Kojevnikov, A.** Improved Lower Bounds for Resolution over Linear Inequalities / A. Kojevnikov. — Electronic Colloquium on Computational Complexity. — 2007, January. — TR010. — 10 p.

5. **Kojevnikov, A.** Exponential Lower Bound on the Size of Static Lovasz-Schrijver Calculus / A. Kojevnikov, D. Itsykson // Proceedings of the 33rd International Colloquium on Automata, Languages and Programming. — Springer: 2006. — LNCS 4052. — P. 323–334.

6. **Kojevnikov, A.** Complexity of Semialgebraic Proofs with Restricted Degree of Falsity / A. Kojevnikov, A. S. Kulikov // Proceedings of the 9th International Conference on Theory and Applications of Satisfiability Testing. — Springer: 2006. — LNCS 4121. — P. 11–21.