На правах рукописи

Куликов Александр Сергеевич

Схемная сложность явно заданных булевых функций

01.01.06 — математическая логика, алгебра и теория чисел

Автореферат
диссертации на соискание учёной степени
доктора физико-математических наук

Санкт-Петербург — 2016

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

Официальные оппоненты: АБЛАЕВ Фарид Мансурович,
доктор физико-математических наук, профессор,
чл.-корр. АН РТ,
Казанский федеральный университет,
заведующий кафедрой

ВЕРЕЩАГИН Николай Константинович,
доктор физико-математических наук, профессор,
Московский государственный университет
им. М. В. Ломоносова, профессор

РАЗБОРОВ Александр Александрович,
доктор физико-математических наук,
чл.-корр. РАН,
Федеральное государственное бюджетное учреждение науки
Математический институт им. В. А. Стеклова
Российской академии наук, главный научный сотрудник

Ведущая организация: Федеральное государственное бюджетное учреждение науки
Институт проблем передачи информации
им. А. А. Харкевича РАН

Защита состоится 26 апреля в 16:00 на заседании диссертационного совета Д002.202.02 в ФГБУН Санкт-Петербургское отделение 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-Петербургское отделение Математического института им. В. А. Стеклова Российской академии наук, http://www.pdmi.ras.ru/

Автореферат разослан «____» _____ 2016 г.

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

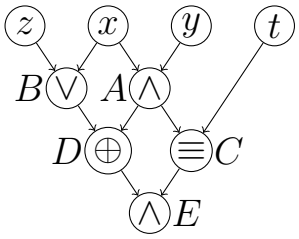
Общая характеристика работы

Актуальность темы

Вычислительная модель. Обозначим через $B_{n,m}$ множество всех булевых функций $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ с n входами и m выходами, где $\mathbb{F}_2 = \{0,1\}$ — поле из двух элементов. Через B_n будем обозначать $B_{n,1}$. Через n всегда будем обозначать число входных битов рассматриваемой функции. Под булевой функцией мы, как правило, будем понимать бесконечную последовательность функций $f_1, f_2, \ldots$, где $f_i \in B_i$ для всех i. Функция называется симметрической, если её значение зависит только от суммы входных битов.

Центральным вопросом теории сложности вычислений является вопрос о минимальном количестве бинарных операций (как функции от n), необходимом для вычисления заданной функции. Естественной вычислительной моделью является модель булевых схем. Булевой схемой называется ациклический ориентированный граф, в котором каждая внутренняя вершина имеет ровно два входящих ребра и помечена бинарной булевой операцией, входные биты подаются в n вершин входящей степени ноль и некоторые m вершин помечены как выходные. Внутренние вершины также называются функциональными элементами. Схема естественным образом вычисляет булеву функцию из $B_{n,m}$, где n — это число входных вершин, а m — число выходных. Нетрудно видеть, что схема соответствует естественной и очень просто устроенной программе для вычисления булевой функции из $B_{n,m}$: каждая инструкция в такой программе вычисляет и сохраняет в новой переменной результат бинарной булевой операции, применённой к двум переменным, каждая из которых является либо входным битом, либо результатом одной из предыдущих операций. Размером схемы будем называть количество внутренних вершин схемы (то есть вершин, входящая степень которых больше нуля). Это соот-

ветствует числу инструкций в программе. Ниже показана схема размера пять, вычисляющая булеву функцию от четырёх переменных, и соответствующая ей программа.



$$B = (z \vee x)$$
$$A = (x \wedge y)$$
$$D = (B \oplus A)$$
$$C = (A \equiv t)$$
$$E = (D \wedge C)$$

Схемной сложностью $C(f)$ булевой функции f называется размер минимальной схемы, вычисляющей данную функцию (поскольку под функцией мы понимаем бесконечную последовательность функций, по одной для каждой длины входа, то $C(f)$ — это функция от n). В данной работе мы будем интересоваться верхними и нижними оценками на схемную сложность явно заданных булевых функций. Под "явно заданными" функциями понимаются функции класса NP.

Верхние оценки на схемную сложность. Нетрудно видеть, что любую функцию $f \in B_n$ можно вычислить схемой размера $O(n2^n)$, представив функцию в виде дизъюнктивной нормальной формы. В 1956 г. Д. Мюллером было показано, что $C(f) = O(2^n/n)$, а в 1958 г. О. Б. Лупанов установил, что

$$C(f) \leq \left(1 + O\left(\frac{\log n}{n}\right)\right) \frac{2^n}{n}.$$

Симметрические функции могут быть посчитаны схемами гораздо меньшего размера: хорошо известно, что схемная сложность любой симметрической функции не превосходит $5n + o(n)$. В 2010 г. данная оценка была улучшена до $4.5n + o(n)$ Е. А. Деменковым и др. [1].

Нижние оценки на схемную сложность. Уже в 1949 г. К. Шэннон показал, что почти все булевы функции множества B_n требуют схем размера $\Omega(2^n/n)$. Это следует из простых мощностных соображений: число 2^{2^n} различных функций от n переменных растёт быстрее, чем число схем малого размера. Данное доказательство, однако, неконструктивно — оно не даёт примера явно заданной булевой функции высокой схемной сложности. Под явно заданной, как правило, понимается функция $f = \{f_1, f_2, \dots\}$, для которой $\bigcup_{i=1}^{\infty} f_i^{-1}(1) \in \mathrm{NP}$.

Доказательство суперполиномиальных нижних оценок на схемную сложность явно заданных булевых функций оказалось очень трудной задачей (отметим, что такая оценка повлекла бы за собой неравенство классов P и NP). К настоящему моменту удалось доказать лишь небольшие линейные нижние оценки. В 1965 г. Б. М. Клосс и В. А. Малышев доказали нижнюю оценку $2n-O(1)$ для функции $\oplus_{1\le i<j\le n} x_i x_j$. В 1974 г. К. П. Шнорр доказал нижнюю оценку $2n-O(1)$ для широкого класса функций со следующим естественным свойством: для любых двух входных переменных среди четырёх подфункций, получаемых подстановкой констант данным двум переменным, будет хотя бы три разные. В 1977 г. Л. Стокмайер привёл доказательство нижней оценки $2.5n - O(1)$ для многих симметрических функций (в частности, для функции $\mathrm{MOD}_n^{m,r}$, выдающей 1 тогда и только тогда, когда сумма n входных битов сравнима с r по модулю $m \ge 3$). В том же году В. Пол доказал нижнюю оценку $2n - o(n)$ для функции индексации, а также нижнюю оценку $2.5n - o(n)$ для специально построенной функции, комбинирующей несколько функций индексации. Наконец, в 1984 г. Н. Блюм расширил идеи В. Пола и получил доказательство нижней оценки $3n - o(n)$.

Другие модели. Сложность вычислительной задачи зависит от рассматриваемой модели вычислений. К распространённым моделям относятся ма-

шины Тьюринга, равнодоступные адресные машины (RAM-машины), булевы схемы. Схемы в полном бинарном базисе — гибкая модель вычислений. Использование k-арного базиса вместо бинарного изменяет сложность лишь в константу раз. Использование фиксированного множества элементов неограниченной арности (например, конъюнкций, дизъюнкций и отрицаний) сохраняет сложность, измеряемую как число проводов в схеме. Нахождение функции, которую трудно вычислить схемами, может рассматриваться как комбинаторная задача (в отличие от нижних оценок для равномерных моделей). Поэтому доказательство суперлинейной нижней оценки на схемную сложность — важный рубеж на пути получения сильных нижних оценок.

Более сильные, чем $3n$, нижние оценки известны для различных ограниченных базисов. Один из наиболее популярных таких базисов U_2 состоит из всех бинарных функций, кроме функции чётности и её дополнения. В 1976 г. К. П. Шнорр доказал, что сложность функции чётности в таком базисе равна $3n-3$. У. Цвик в 1991 г. привёл доказательство нижней оценки $4n-O(1)$ для многих симметрических функций. В 2001 г. О. Лахич и Р. Раз доказали нижнюю оценку $4.5n-o(n)$ на сложность $(n-o(n))$-смешанной функции (функции, все подфункции которой относительно любых $n-o(n)$ переменных различны). К. Ивама и Х. Морицуми в 2002 г. улучшили оценку до $5n-o(n)$. Интересно отметить, что для улучшения нижней оценки $5n-o(n)$ в базисе U_2 нужны новые идеи: в 2011 г. К. Амано и Й. Таруй привели пример $(n-o(n))$-смешанной функции, схемная сложность которой над U_2 не превосходит $5n+o(n)$.

Несмотря на то, что неизвестно нелинейных нижних оценок для схем в базисе константной арности, более сильные оценки известны для ограниченных классов схем. Например,

- для монотонных схем (А. А. Разборов, 1985 г.),

- для схем константной глубины (Э. Яо, 1985 г.; Й. Хостад, 1986 г.)
- для формул (Б. А. Субботовская, 1961 г.; Э. И. Нечипорук, 1961 г.; Й. Хостад, 1998 г.)

Данные нижние оценки, однако, не транслируются в нелинейные нижние оценки для неограниченных моделей схем в базисе константной арности.

Связь с алгоритмами для задачи выполнимости схемы. Недавние результаты Р. Вильямса устанавливают интересную связь между доказательством нижних оценок на сложность схем из некоторого класса и доказательством верхних оценок на время работы алгоритмов, проверяющих выполнимость схем из этого класса. А именно, существование алгоритма, решающего задачу выполнимости существенно быстрее, чем за 2^n, влечёт за собой экспоненциальную нижнюю оценку на схемную сложность функций из большого сложностного класса (такого, например, как NEXP). С использованием данной связи Р. Вильямсом в 2014 г. были доказаны безусловные нижние оценки для ACC_0 схем (схем константной глубины с элементами неограниченной арности, вычисляющими конъюнкцию, дизъюнкцию, отрицание и произвольные MOD-функции). Э. Бен-Сассон и Э. Виола в 2014 г. показали, что для доказательства конкретной линейной нижней оценки на схемную сложность функции из E^{NP} достаточно уменьшить константу в основании экспоненты времени работы алгоритма для задачи 3-выполнимости до соответствующего значения (стоит, однако, отметить, что известные на данный момент константы не дают новых нижних оценок).

Техники, использующиеся в доказательстве нижних оценок на схемную сложность, применяются также при разработке эффективных алгоритмов для задачи выполнимости схем и формул.

Цели работы

Основной целью данной работы является как усиление известных нижних и верхних оценок на схемную сложность явно заданных булевых функций, так и разработка новых методов получения таких оценок.

Методы исследований

Для доказательства нижних оценок на схемную сложность используется стандартный метод элиминации функциональных элементов. Однако во всех доказательствах данной работы, основанных на этом методе, используются и новые идеи, ранее не использованные в литературе. Для доказательства нижней оценки $7n/3 - O(1)$ используется нестандартная мера сложности, присваивающая различные веса элементам разных типов. Для доказательства оценки $3n - o(n)$ используются линейные подстановки. Для доказательства оценки $(3+\frac{1}{86})n-o(n)$ используется обобщённая модель схем с циклами, нестандартная мера сложности, а также отложенные линейные подстановки. Для доказательства оценки $3.11n$ используется так называемый взвешенный метод элиминации элементов, индукция в котором ведётся по размеру текущего множества задания функции, а не по числу входных переменных, как во всех предыдущих доказательствах.

Для доказательства верхних оценок на схемную сложность впервые использованы решатели задачи пропозициональной выполнимости (так называемые SAT-солверы) для поиска оптимальных схем малого размера.

Теоретическая и практическая ценность

Диссертация имеет теоретический характер. Полученные новые нижние оценки на размер схем могут быть использованы для дальнейшего изучения

сложности булевых функций. В то же время полученные верхние оценки могут быть применены при практической реализации микросхем. Некоторые из полученных в диссертации результатов уже включены в содержание специальных курсов и учебников по теории сложности вычислений.

Основные результаты

1. Доказана нижняя оценка $7n/3 - O(1)$ на схемную сложность широкого класса функций, представляемых многочленами степени n.

2. Доказана нижняя оценка $3n - o(n)$ на схемную сложность аффинных дисперсеров сублинейной размерности.

3. Доказана нижняя оценка $(3 + \frac{1}{86})n - o(n)$ на схемную сложность аффинных дисперсеров сублинейной размерности.

4. Доказана нижняя оценка $3.11n$ на схемную сложность квадратичных дисперсеров.

5. Доказана нижняя оценка $5n - o(n)$ на схемную сложность над базисом U_2 линейной функции с $o(n)$ выходами.

6. Доказана нижняя оценка $3.24n$ на схемную сложность в среднем случае над базисом U_2 для дисперсера сублинейной размерности относительно проекций.

7. Построен алгоритм, решающий задачу выполнимости схем в базисе U_2 за время $(2-\varepsilon)^n$ для схем размера не более $3.24n$ (где $\varepsilon > 0$ — константа).

8. Показано, что для получения нелинейных нижних оценок на схемную

сложность будет недостаточно привести явные конструкции дисперсеров относительно более сильных подстановок.

9. Доказана верхняя оценка $3n$ на схемную сложность функции MOD_n^3.

10. Доказано, что функции $\mathrm{MOD}_n^{m,r}$ одновременно для всех $m = 1, \ldots, n$ можно вычислить схемой размера $O(n)$.

Научная новизна

Все полученные оценки на размер схем являются новыми и ранее не известными. Нижняя оценка $3n - o(n)$ на схемную сложность является первой известной оценкой на схемную сложность аффинных дисперсеров сублинейной размерности. Такая же оценка $3n-o(n)$, но для другой функции и гораздо более сложным способом была доказана Н. Блюмом в 1984 г. Нижняя оценка $(3 + \frac{1}{86})n - o(n)$ является самой сильной из известных для схем над полным бинарным базисом. Нижняя оценка $5n - o(n)$ является рекордной для схем над базисом U_2 для функций с $o(n)$ выходами. Нижняя оценка $3.24n$ на схемную сложность в среднем является самой сильной из известных. Верхняя оценка $3n$ является самой сильной известной оценкой на схемную сложность функции MOD_n^3. Построенный алгоритм для задачи выполнимости булевых схем является самым быстрым из известных.

Апробация работы

Основные результаты обсуждались на следующих конференциях и семинарах:

1. Международная студенческая школа Fall School of Logic and Complexity in Prague (Чехия, 2009).

2. Международный семинар Estonian Theory Days (Эстония, 2009).

3. Российский семинар “Логика и теоретическая информатика” (Россия, 2009).

4. Международный семинар Franco-Russian workshop on Algorithms, complexity and applications (Россия, 2010).

5. Международная конференция Computability in Europe (Португалия, 2010).

6. Международный семинар Exact Complexity of NP-hard Problems (Германия, 2010).

7. Семинар Университета Киото (Япония, 2010).

8. Международный семинар Estonian Theory Days (Эстония, 2011).

9. Международная конференция International Symposium on Mathematical Foundations of Computer Science (Польша, 2011).

10. Международная конференция Computability in Europe (Англия, 2012).

11. Международная конференция International Computer Science Symposium in Russia (Россия, 2012).

12. Международный семинар SAT Interactions (Германия, 2012).

13. Семинар Математического института Чешской академии наук (Прага, 2013).

14. Международный семинар Optimal algorithms and proofs (Германия, 2014).

15. Семинар Университета Калифорнии в Сан-Диего (США, 2015).

16. Семинар Курантовского института математических наук (США, 2015).

17. Международный семинар Connections Between Algorithm Design and Complexity Theory (США, 2015).

18. Семинар Уральского федерального университета (Россия, 2015).

19. Международный семинар Problems in Theoretical Computer Science (Россия, 2015).

20. Международная конференция Annual Innovations in Theoretical Computer Science (США, 2016).

21. Международный семинар Low-Depth Complexity Workshop (Россия, 2016).

22. Международная конференция International Symposium on Mathematical Foundations of Computer Science (Польша, 2016).

23. Семинар Московского государственного университета (Россия, 2016).

24. Международная конференция Annual IEEE Symposium on Foundations of Computer Science (США, 2016).

Публикации

Результаты исследований отражены в 11 работах, опубликованных в изданиях, индексируемых международными базами данных (MathSciNet, Scopus).

В работе [10] диссертанту принадлежит сведение задачи существования схемы небольшого размера к задаче выполнимости формулы в конъюнктивной нормальной форме. В работе [1] диссертанту принадлежит идея использования блока Стокмайера для улучшения верхней оценки на схемную сложность симметрических функций. В работе [9] диссертанту принадлежит идея

использования меры, присваивающей различные веса элементам схемы разных типов, с помощью которой доказывается основной результат работы. В работе [2] диссертанту принадлежит идея использования аффинного дисперсера и линейных подстановок, с помощью которых доказывается основной результат работы. В работе [4] автору принадлежит постановка задачи и доказательство теоремы о вычислении всех MOD_m^r функций при фиксированном r. В работах [11] и [3] диссертанту принадлежит лемма о неоптимальности схемы, содержащей переменные исходящей степени 1, а также часть разбора случаев в доказательстве нижней оценки $5n - o(n)$. В работе [5] диссертантом доказана лемма о перестройке схемы при аффинной подстановке, основной результат работы получен в неразрывном сотрудничестве. В работе [7] лемма 1, показывающая, что случайно выбранная функция с вероятностью 1 является квадратичным дисперсером, доказана диссертантом; лемма 2 доказана А. Г. Головнёвым, лемма 3 получена в неразрывном сотрудничестве. В работе [8] диссертантом доказаны лемма 8 и следствие 9. В работе [6] диссертантом доказана лемма 1.

Структура и объём диссертации

Диссертация объёмом 143 страницы состоит из введения и двух основных глав, разбитых на разделы и подразделы. Список цитируемой литературы состоит из 72 наименований.

Содержание работы

Работа поделена на две основные главы: в первой главе доказываются нижние оценки на схемную сложность, во второй — верхние. **Глава 1** начинается с описания метода элиминации элементов. В качестве примера ис-

пользуется доказательство К. П. Шнорра нижней оценки $2n - O(1)$ на схемную сложность. Доказательство проводится для широкого класса функций, удовлетворяющих следующему свойству: для любых двух переменных среди четырёх подфункций, получающихся подстановкой констант этим двум переменным, есть хотя бы три различные. В доказательстве показывается, что в любой схеме, вычисляющей такую функцию, найдётся переменная, из которой выходят хотя бы два провода. При подстановке константы в такую переменную удаляются хотя бы два элемента, после чего требуемая оценка получается по индукции.

В **разделе 1.1** нижняя оценка К. П. Шнорра усиливается до $\frac{7n}{3} - O(1)$ наложением дополнительного ограничения на степень функции. Интересно отметить, что само доказательство при этом остаётся почти таким же простым и при этом по-прежнему работает для очень широкого класса функций. Основной идеей доказательства является использование нестандартной меры сложности схем, присваивающей различные веса элементам разного типа. Такие меры использованы впервые.

В **разделе 1.2** приводится очень простое (содержащее всего два случая) доказательство нижней оценки $3n - o(n)$ на схемную сложность аффинных дисперсеров сублинейной размерности. Аффинным дисперсером размерности d называется функция $f \in B_n$, не обращающаяся в константу ни на каком аффинном подпространстве $\mathbb{F}_2^n$ размерности хотя бы d. Такие объекты активно изучаются в последнее время в области извлечения случайности. В частности, сравнительно недавно Э. Бен-Сассоном и С. Коппарти была приведена явная конструкция аффинного дисперсера сублинейной размерности (то есть $d = o(n)$). Для получения нижних оценок на схемную сложность таких функций важно следующее их свойство: они не обращаются в константу после любых $n - d$ ограничений типа $p(x) = 0$, где p — линейный многочлен (такие ограничения как раз и задают аффинное подпространство). Исполь-

зуя данную конструкцию как чёрный ящик, удаётся очень просто доказать нижнюю оценку $3n - o(n)$. Для этого показывается, что для любой схемы найдётся линейная подстановка, удаляющая из схемы хотя бы три элемента. Таким образом, доказательство в некотором смысле аналогично доказательству К. П. Шнорра, но вместо константных подстановок используются линейные. При этом гораздо более сложным становится вопрос построения функции, устойчивой относительно таких подстановок. Стоит отметить, что полученная нижняя оценка $3n - o(n)$ совпадает с нижней оценкой $3n - o(n)$ Н. Блюма, представленной им в 1984 г. и являющейся рекордной на протяжении последующих тридцати лет. Представленное в работе доказательство значительно проще (содержит всего два случая вместо нескольких десятков), но приводится для более сложной функции.

В **разделе 1.3** нижняя оценка для аффинных дисперсеров сублинейной размерности усиливается до $\left(3 + \frac{1}{86}\right) n - o(n)$. Основными идеями, позволившими достичь данного улучшения, являются следующие три. Во-первых, вместо схем рассматривается более общая модель — схемы с циклами в линейной части. Это позволяет производить линейные подстановки, оставаясь в необходимом классе схем, и пользоваться более сильным предположением индукции. Во-вторых, используются квадратичные подстановки, которые могут рассматриваться как отложенные линейные подстановки: в некоторых проблемных ситуациях производится подстановка $x_i \leftarrow x_j x_k$; впоследствии обязательно также производится подстановка константы вместо x_j или x_k, что делает исходную подстановку линейной. В-третьих, используется аккуратно подобранная мера сложности схем, которая зависит от многих параметров схемы (и даже самого процесса элиминации элементов). Полученная оценка является самой сильной из известных на сегодняшний день (для явно заданных булевых функций).

В **разделе 1.4** приводится гораздо более короткое и технически простое

доказательство нижней оценки $3.11n$ для так называемых квадратичных дисперсеров. Говоря неформально (все формальные определения приведены в соответствующем разделе), такие функции устойчивы относительно достаточно большого количества подстановок типа $x \leftarrow p$, где p — многочлен степени не более двух. В настоящий момент явных конструкций (то есть конструкций из класса NP) таких функций неизвестно, хотя случайно выбранная функция является квадратичным дисперсером с вероятностью $1-o(1)$ и известны конструкции с более слабыми параметрами и конструкции для полей большего размера. Основным ингредиентом доказательства является индукция не по числу переменных, как во всех известных доказательствах, а по количеству точек, удовлетворяющих текущей системе уравнений.

В **разделе 1.5** рассматриваются схемы над ограниченным базисом U_2, содержащим все бинарные функции, кроме функции чётности ($\oplus$) и её дополнения ($\equiv$). Приводится доказательство нижней оценки $5n - o(n)$ для линейной функции с $o(n)$ выходами, матрицей которой является проверочная матрица кода Хэмминга. Такая же оценка, но для функции с одним выходом, получена в 2002 г. К. Ивамой и Х. Морицуми, и является рекордной известной на сегодняшний день для данного базиса. Приведённое в диссертации доказательство значительно короче и проще.

В **разделе 1.6** показывается, что методы, использующиеся при доказательстве нижних оценок на размер схем, могут быть также использованы для построения эффективных алгоритмов проверки выполнимости схемы и доказательства нижних оценок на схемную сложность в среднем. Впервые такая связь была явно продемонстрирована Р. Ченем и В. Кабанцом в 2015 г. В диссертации их идеи развиваются и обобщаются: доказывается общая теорема, которая позволяет по разбору случаев сразу сказать, какой из него получается алгоритм для задачи выполнимости схем и какие получаются нижние оценки на схемную сложность в среднем и наихудшем случаях. Далее

с помощью данного метода доказывается нижняя оценка $3.24n$ на схемную сложность в среднем случае над базисом U_2 для дисперсеров сублинейной размерности относительно проекций (что означает, что схемы размера $3.24n$ не могут даже приближённо считать такие функции), а также верхняя оценка вида $(2-\varepsilon)^n$ для задачи выполнимости схем размера не более $3.24n$. Обе полученные оценки являются самыми сильными из известных на данный момент.

В перечисленных выше разделах показывается, что метод элиминации элементов может быть использован для доказательства более сильных оценок, если у нас в распоряжении имеется функция, устойчивая относительно достаточно сильных подстановок. Например, аффинные дисперсеры позволяют доказать нижнюю оценку $3.01n$, квадратичные — оценку $3.11n$. Естественно задаться вопросом: можно ли доказать нелинейные нижние оценки для функций, устойчивых относительно подстановок типа $x \leftarrow p$, где p — произвольный многочлен степени, скажем, 10 или даже $\log n$? (Отметим в скобках, что на настоящий момент у нас нет явных конструкций даже для функций, где многочлену p разрешается иметь степень всего лишь два.) **Раздел 1.7** посвящён отрицательному ответу на данный вопрос. Показывается, что относительно сколь угодно сильных подстановок есть схемы, из которых удаляется только константное число элементов.

В **главе 2** доказываются новые верхние оценки для симметрических булевых функций. В **разделе 2.1** описывается сведение факта существования схемы необходимого размера к формуле в конъюнктивной нормальной форме (КНФ): по данной таблице истинности функции $f \in B_{n,m}$ и числу r строится формула в КНФ, которая выполнима тогда и только тогда, когда для f существует схема из r элементов. Для проверки выполнимости таких формул можно использовать программы, решающие задачу выполнимости (так называемые SAT-солверы).

Есть несколько причин интересоваться точной схемной сложностью функций от малого числа переменных. Во-первых, для некоторых функций эффективные схемы строятся из блоков константного размера. Уменьшение размера такого блока автоматически даёт более сильную оценку для такой функции в общем случае. Во-вторых, было бы очень полезно иметь энциклопедию оптимальных схем для функций от малого количества переменных. Скажем, знание оптимальных схем для задачи умножения булевых матриц размера $n \times n$ для, например, $n = 2, 3, \ldots, 10$ потенциального могло бы помочь нам понять, как устроен эффективный алгоритм для этой задачи. К сожалению, современные компьютеры и программы не позволяют найти оптимальный размер схем для этой задачи даже при $n = 3$. Д. Кнут недавно реализовал свой вариант сведения и нашёл точную схемную сложность всех функций от четырёх переменных, а также некоторых функций от пяти переменных.

С помощью данного сведения были построены оптимальные схемы для некоторых функций от не более чем пяти переменных. Также был найден блок, с помощью которого функцию MOD_n^3 можно вычислить схемой размера $3n$. Это новая оценка, которая является лучшей из известных. В частности, Д. Кнут выдвинул гипотезу, что сложность функции $\mathrm{MOD}_n^{3,r}$ в точности равна $3n - 5 - [(n + r) \equiv 0 \pmod 3]$. Данная гипотеза верна при малых значениях n.

В **разделе 2.2** изучается вопрос одновременного вычисления нескольких симметрических функций. Известно, что любую симметрическую функцию $f \in B_n$ можно посчитать схемой размера $5n + o(n)$ (это следует из того, что сумму трёх битов можно посчитать схемой размера 5, известной как Full Adder) и даже схемой размера $4.5n + o(n)$, как показано Е. Деменковым и др. [3]. В то же время из мощностных соображений получается, что для почти всех наборов из n симметрических функций из B_n требуются схемы размера $\Omega(n^{2-o(1)})$. Конечно же, в настоящее время мы не знаем ни одного такого на-

бора, требующего даже схем суперлинейного размера. Есть три естественных подкласса симметрических функций:

- $\mathrm{EX}_n^k \in B_n$ равна 1 тогда и только тогда, когда сумма входных n битов равна k;
- $\mathrm{THR}_n^k \in B_n$ равна 1 тогда и только тогда, когда сумма входных n битов хотя бы k;
- $\mathrm{MOD}_n^{m,r} \in B_n$ равна 1 тогда и только тогда, когда сумма входных n битов сравнима с r по модулю m.

Известно, что для всех $k = 1, 2, \ldots, n$ все функции из первого и второго классов можно одновременно вычислить схемой размера $O(n)$. Естественно задаться вопросом, верно ли это и для третьего класса. В **разделе 2.2** строятся схемы размера $O(n)$ для вычисления всех MOD-функций одновременно. Таким образом, для нахождения наборов из n симметрических функций схемной сложности $\Omega(n^{1+\varepsilon})$ нужно брать более сложно устроенные симметрические функции.

Публикации автора по теме диссертации.

[1] *Demenkov E., Kojevnikov A., Kulikov A. S., Yaroslavtsev G.* New upper bounds on the Boolean circuit complexity of symmetric functions // Inf. Process. Lett. 2010. Vol. 110, N. 7. P. 264–267.

[2] *Demenkov E., Kulikov A. S.* An Elementary Proof of a $3n - o(n)$ Lower Bound on the Circuit Complexity of Affine Dispersers // Mathematical Foundations of Computer Science 2011 - 36th International Symposium, MFCS 2011, Warsaw, Poland, 2011. Proceedings. Vol. 6907 of *Lecture Notes in Computer Science*. Springer, 2011. P. 256–265.

[3] *Demenkov E., Kulikov A. S., Melanich O., Mihajlin I.* New Lower Bounds on Circuit Size of Multi-output Functions // Theory Comput. Syst. 2015. Vol. 56, N. 4. P. 630–642.

[4] *Demenkov E., Kulikov A. S., Mihajlin I., Morizumi H.* Computing All MOD-Functions Simultaneously // Computer Science - Theory and Applications - 7th International Computer Science Symposium in Russia, CSR 2012, Nizhny Novgorod, Russia, 2012. Proceedings. Vol. 7353 of *Lecture Notes in Computer Science*. Springer, 2012. P. 81–88.

[5] *Find M., Golovnev A., Hirsch E. A., Kulikov A. S.* A Better-than-3n Lower Bound for the Circuit Complexity of an Explicit Function // 57th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2016, New Brunswick, NJ, USA, 2016. Proceedings. 2016. P. 88–97.

[6] *Golovnev A., Hirsch E. A., Knop A., Kulikov A. S.* On the Limits of Gate Elimination // 41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016 - Kraków, Poland. 2016. P. 46:1–46:13.

[7] *Golovnev A., Kulikov A. S.* Weighted Gate Elimination: Boolean Dispersers for Quadratic Varieties Imply Improved Circuit Lower Bounds // Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, 2016. ACM, 2016. P. 405–411.

[8] *Golovnev A., Kulikov A. S., Smal A. V., Tamaki S.* Circuit Size Lower Bounds and #SAT Upper Bounds Through a General Framework // 41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016 - Kraków, Poland. 2016. P. 45:1–45:16.

[9] *Kojevnikov A., Kulikov A. S.* Circuit Complexity and Multiplicative Complexity of Boolean Functions // Programs, Proofs, Processes, 6th Conference

on Computability in Europe, CiE 2010, Ponta Delgada, Azores, Portugal, 2010. Proceedings. Vol. 6158 of *Lecture Notes in Computer Science*. Springer, 2010. P. 239–245.

[10] *Kojevnikov A., Kulikov A. S., Yaroslavtsev G.* Finding Efficient Circuits Using SAT-Solvers // Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, 2009. Proceedings. Vol. 5584 of *Lecture Notes in Computer Science*. Springer, 2009. P. 32–44.

[11] *Kulikov A. S., Melanich O., Mihajlin I.* A $5n - o(n)$ Lower Bound on the Circuit Size over U_2 of a Linear Boolean Function // How the World Computes - Turing Centenary Conference and 8th Conference on Computability in Europe, CiE 2012, Cambridge, UK, 2012. Proceedings. Vol. 7318 of *Lecture Notes in Computer Science*. Springer, 2012. P. 432–439.