МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

На правах рукописи

Сергеев Игорь Сергеевич

НЕКОТОРЫЕ ВОПРОСЫ СИНТЕЗА ПАРАЛЛЕЛЬНЫХ СХЕМ

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
доктора физико-математических наук

МОСКВА — 2021

Работа выполнена в Федеральном государственном унитарном предприятии «Научно-исследовательский институт «Квант».

Научный консультант: **Гашков Сергей Борисович**,
доктор физико-математических наук,
профессор, Московский государственный
университет им. М. В. Ломоносова,
проф. кафедры дискретной математики.

Официальные оппоненты: **Аблаев Фарид Мансурович**,
доктор физико-математических наук,
профессор, Казанский (Приволжский)
федеральный университет,
зав. кафедрой теоретической кибернетики.

Ложкин Сергей Андреевич,
доктор физико-математических наук,
профессор, Московский государственный
университет им. М. В. Ломоносова,
зав. кафедрой математической кибернетики.

Посыпкин Михаил Анатольевич,
доктор физико-математических наук,
доцент, ФГУ «Федеральный
исследовательский центр
«Информатика и управление» РАН»,
заместитель директора по научной работе.

Защита диссертации состоится 24 сентября 2021 г. в 16 ч. 45 мин. на заседании диссертационного совета МГУ.01.17 при Московском государственном университете имени М.В. Ломоносова по адресу: 119234, Российская Федерация, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М.В. Ломоносова, Механико-математический факультет, ауд. 1408.

E-mail: VGChdissovet@yandex.ru

С диссертацией, а также со сведениями о регистрации участия в удаленном интерактивном режиме защиты можно ознакомиться на сайте ИАС «Истина»: https://istina.msu.ru/dissertations/378944357/

Автореферат разослан 24 июля 2021 г.

Заместитель председателя
диссертационного совета МГУ.01.17
доктор физико-математических наук,
профессор А. О. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы и степень ее разработанности

Задачи синтеза схем, удовлетворяющих критериям эффективности, учитывающим глубину, в теории булевых функций стали рассматриваться ненамного позже, чем задачи оптимизации числа элементов схем (сложности). Еще в 1956 г. О. Б. Лупанов[1] поставил и решил задачу оптимального синтеза вентильных схем глубины 2 — за несколько лет до получения своих основных результатов об асимптотически оптимальном синтезе в различных моделях вычислений.

К 1960-м годам вопросы синтеза быстрых схем для арифметики стали активно изучаться, исходя из потребностей электроники. Сама теория быстрых вычислений, как принято считать, ведет отсчет с опубликованной по инициативе А. Н. Колмогорова работы[2] о быстром умножении чисел, в которой, наряду с рекордным по сложности методом А. А. Карацубы, представлен метод параллельного умножения Ю. П. Офмана.

Ряд фундаментальных асимптотических проблем теории синтеза параллельных схем был решен О. Б. Лупановым. В частности, им определена асимптотика функции Шеннона глубины схем над произвольным булевым базисом, и при этом решена задача об одновременной минимизации глубины и сложности[3], получена асимптотика функции Шеннона сложности формул ограниченной глубины (альтернирования)[4, 5] и решена аналогичная задача для схем[6]. Вопросы сложности вентильных схем ограниченной глубины всесторонне изучены Э. И. Нечипоруком[7]. Исследование асимптотических вопросов было продолжено в Московском университете учениками О. Б. Лупанова. Так, С. Б. Гашков установил величину функции Шеннона глубины булевых функций в стандартном

[1] Лупанов О. Б. О вентильных и контактно-вентильных схемах. Доклады АН СССР. 1956. **111**(6), 1171–1174.

[2] Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. Доклады АН СССР. 1962. **145**(2), 293–294.

[3] Лупанов О. Б. О схемах из функциональных элементов с задержками. Проблемы кибернетики. Вып. 23. М.: Наука, 1970, 43–81.

[4] Лупанов О. Б. О реализации функций алгебры логики формулами из конечных классов (формулами ограниченной глубины) в базисе $\&, \vee, \bar{}$. Проблемы кибернетики. Вып. 6. М.: Физматлит, 1961, 5–14.

[5] Лупанов О. Б. О сложности универсальной параллельно-последовательной сети глубины 3. Труды МИ АН СССР. 1973. Т. 143. М.: Наука, 1973, 127–131.

[6] Лупанов О. Б. О реализации функций алгебры логики схемами из функциональных элементов «ограниченной глубины» в базисе $\&, \vee, \bar{}$. Сб. работ по математической кибернетике. Т. 2. М.: Изд-во ВЦ АН СССР, 1977, 3–8.

[7] Нечипорук Э. И. О топологических принципах самокорректирования. Проблемы кибернетики. Вып. 21. М.: Наука, 1969, 5–102.

базисе с точностью до аддитивной постоянной[8] и аналогичный результат получил для многочленов (включая важный случай функций k-значной логики)[9]. С. А. Ложкиным получена асимптотика функции Шеннона глубины для базисов с нулевыми весами элементов[10] и серия асимптотических оценок высокой точности в различных моделях параллельных вычислений[11, 12, 13, 14, 15, 16], в частности, наиболее точные оценки функции Шеннона глубины схем для ряда базисов, включая стандартный и монотонный. А. Е. Андреев (ученик В. Б. Кудрявцева), расширяя результат Нечипорука, установил асимптотику сложности реализации вентильными схемами глубины 2 для классов недоопределенных матриц[17]. А. Б. Угольников получил описание порядков функции Шеннона глубины для всех конечных систем булевых функций[18]. О. М. Касим-Заде определил значение функции Шеннона глубины произвольного бесконечного булева базиса с точностью до аддитивной постоянной[19]. Его ученик А. В. Кочергин получил асимптотику функции Шеннона глубины

[8]Гашков С. Б. О глубине булевых функций. Проблемы кибернетики. Вып. 34. М.: Наука, 1978, 265–268.

[9]Гашков С. Б. О параллельном вычислении некоторых классов многочленов с растущим числом переменных. Вестник Московского университета. Серия 1. Математика. Механика. 1990. №2, 88–92.

[10]Ложкин С. А. Асимптотическое поведение функций Шеннона для задержек схем из функциональных элементов. Математические заметки. 1976. **19**(6), 939–951.

[11]Ложкин С. А. О связи между глубиной и сложностью эквивалентных формул и о глубине монотонных функций алгебры логики. Проблемы кибернетики. Вып. 38. М.: Наука, 1981, 269–271.

[12]Ложкин С. А. О глубине функций алгебры логики в некоторых базисах. Annales Univ. Budapest. Sec. Computatorica. 1983. IV, 113–125.

[13]Ложкин С. А. О глубине функций алгебры логики в произвольном полном базисе. Вестник Московского университета. Серия 1. Математика. Механика. 1996. №2, 80–82.

[14]Ложкин С. А. О синтезе формул, сложность и глубина которых не превосходят асимптотически наилучших оценок высокой степени точности. Вестник Московского университета. Серия 1. Математика. Механика. 2007. №3, 19–25.

[15]Ложкин С. А., Коноводов В. А. О синтезе и сложности формул с ограниченной глубиной альтернирования. Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2012. №2, 28–36.

[16]Ложкин С. А., Данилов Б. Р. О задержке схем в модели, учитывающей значения на входах функциональных элементов. Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2013. №4, 25–33.

[17]Андреев А. Е. О сложности реализации вентильными схемами недоопределенных матриц. Математические заметки. 1987. **41**(1), 77–86.

[18]Угольников А. Б. О глубине формул в неполных базисах. Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988, 242–245.

[19]Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным бесконечным базисом. Вестник Московского университета. Серия 1. Математика. Механика. 2012. №6, 55–57.

для любого полного базиса k-значной логики[20].

С 1980-х гг. активно развивается направление получения нижних оценок сложности индивидуальных функций при ограничении на глубину вычисления. Число работ в этой области измеряется сотнями. Дело в том, что ограничение на глубину позволяет доказывать в традиционных моделях вычислений (схемы, формулы над полными базисами) сверхполиномиальные и даже экспоненциальные нижние оценки. Первый результат такого рода был получен еще одним учеником Лупанова Г. А. Ткачевым[21]. Далее, в работах М. Фёрста, Дж. Сакса, М. Сипсера[22], Э. Яо[23] и Й. Хостада[24] были заложены основы теории. Фундаментальный вклад в теорию нижних оценок сложности схем ограниченной глубины внесли работы А. А. Разборова, также представителя школы Московского университета (схемы в базисе $\{\vee, \wedge, \oplus\}$[25], схемы из пороговых элементов[26], арифметические схемы[27]).

Развитие методов синтеза параллельных схем для конкретных функций или классов функций, а также исследование пределов возможностей этих методов стимулируется приложениями, прежде всего, в области микроэлектроники. Широко известные результаты в области синтеза параллельных схем принадлежат еще одному математику из школы Лупанова В. М. Храпченко: конструкция асимптотически минимального по глубине сумматора[28], эффективные параллельные схемы для оператора умножения и симметрических функций[29], метод параллельного пе-

[20]Кочергин А. В. О глубине функций многозначной логики. Дисс. на соискание ученой степени кандидата физ.-мат. наук. М.: МГУ, 2013.

[21]Ткачев Г. А. О сложности реализации одной последовательности булевых функций схемами из функциональных элементов и π-схемами при дополнительных ограничениях на структуру схем. Комбинаторно-алгебраические методы в прикладной математике. Горький: изд-во Горьк. ун-та, 1980, 161–207.

[22]Furst M., Saxe J., Sipser M. Parity, circuits, and the polynomial time hierarchy. Math. Syst. Theory. 1984. **17**, 13–27.

[23]Yao A. C. Separating the polynomial time hierarchy by oracles. Proc. 26th Symp. on Found. of Comput. Sci. (Portland, 1985). Washington: IEEE, 1985, 1–10.

[24]Håstad J. Computational limitations of small-depth circuits. MIT Press, 1986.

[25]Разборов А. А. Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения. Математические заметки. 1987. **41**(4), 598–607.

[26]Razborov A., Wigderson A. $n^{\Omega(\log n)}$ lower bounds on the size of depth-3 threshold circuits with AND gates at the bottom. Inform. Proc. Letters. 1993. **45**, 303–307.

[27]Grigoriev D., Razborov A. Exponential lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. Appl. Algebra Eng. Comm. Comput. 2000. **10**(6), 465–487.

[28]Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора. Проблемы кибернетики. Вып. 19. М.: Наука, 1967, 107–120.

[29]Храпченко В. М. Некоторые оценки для времени умножения. Проблемы кибер-

рестроения булевых формул[30, 31]. К числу важнейших результатов в указанной области следует отнести метод синтеза параллельных префиксных схем Р. Ладнера и М. Фишера[32], параллельные схемы сортировки М. Айтаи, Я. Комлоша и Э. Семереди[33], параллельные схемы для деления, возведения в степень и других целочисленных операций П. Бима, С. Кука и Дж. Гувера[34]. Для построения быстрых методов умножения в различных алгебраических структурах широко применяются идеально распараллеливаемые алгоритмы быстрого преобразования Фурье, идея которого восходит к работам И. Гуда[35], Дж. Кули и Дж. Тьюки[36].

За прошедшие полвека существенно изменился понятийный аппарат теории. Современные исследования глубины функций часто выполняются в терминах коммуникационной сложности подходящим образом определенных протоколов. Понятие коммуникационной сложности было введено Э. Яо[37]. На ее связь с глубиной схем было указано в работе М. Карчмера и А. Вигдерсона[38]. Наличие такой связи привело к появлению специальных методов нижних оценок глубины конкретных функций. Прежде такие оценки, как правило, извлекались лишь в качестве следствий из известных нижних оценок сложности формул или схем. Наиболее яркие результаты получены А. Вигдерсоном с М. Карчмером (нижняя оценка монотонной глубины функции проводимости) и Р. Разом[39] (нижние оценки монотонной глубины пермамента и кликовых

нетики. Вып. 33. М.: Наука, 1978, 221–227.

[30]Яблонский С. В., Козырев В. П. Математические вопросы кибернетики. «Информационные материалы» Научного совета по комплексной проблеме «Кибернетика» АН СССР. Вып. 19а. М., 1968, 3–15.

[31]Храпченко В. М. О соотношении между сложностью и глубиной формул. Методы дискретного анализа в синтезе управляющих систем. Вып. 32. Новосибирск: ИМ СО АН СССР, 1978, 76–94.

[32]Ladner R. E., Fischer M. J. Parallel prefix computation. J. ACM. 1980. **27**(4), 831–838.

[33]Ajtai M., Komlós J., Szemerédi E. Sorting in $c \log n$ parallel steps. Combinatorica. 1983. **3**(1), 1–19.

[34]Beame P. W., Cook S. A., Hoover H. J. Log depth circuits for division and related problems. SIAM J. Comput. 1986. **15**(4), 994–1003.

[35]Good I. J. The interaction algorithm and practical Fourier analysis. J. R. Statist. Soc. B. 1958. **20**(2), 361–372; 1960. **22**(2), 372–375.

[36]Cooley J. W., Tukey J. W. An algorithm for the machine calculation of complex Fourier series. Math. Comp. 1965. **19**, 297–301.

[37]Yao A. C. Some complexity questions related to distributed computing. Proc. 11th Symp. on Theory of Computing (Atlanta, 1979). NY: ACM, 1979, 209–213.

[38]Karchmer M., Wigderson A. Monotone circuits for connectivity require superlogarithmic depth. SIAM J. Discrete Math. 1990. **3**(2), 255–265.

[39]Raz R., Wigderson A. Monotone circuits for matching require linear depth. J. ACM. 1992. **39**(3), 736–744.

функций).

Взаимоотношения между понятиями глубины и сложности варьируются в зависимости от вычислительной модели. Сложность функции в модели деревьев решений (решающих диаграмм) определяется глубиной реализующего ее дерева. В терминах построения деревьев решений формулируются многие задачи теории алгоритмов, например, задачи сортировки или поиска за минимальное число сравнений.

В настоящее время, спустя 60 лет после своего зарождения, теория параллельного синтеза продолжает развиваться и расширяться, оказываясь вовлеченной в широкий спектр практических задач от проектирования электронных компонентов до суперкомпьютерных и распределенных вычислений.

Цель работы

Цель настоящей работы — развитие математического аппарата теории синтеза параллельных схем, направленное на решение проблем оптимального синтеза с ограниченной глубиной, минимизации глубины вычислений, построения быстрых параллельных алгоритмов. Среди решаемых задач: получение соотношений между глубиной и сложностью булевых формул, верхние и нижние оценки сложности формул для симметрических булевых функций, асимптотически оптимальный синтез вентильных схем ограниченной глубины, изучение отношений различных линейных мер сложности булевых матриц, синтез минимальных параллельных префиксных схем, асимптотически оптимальный синтез схем и формул ограниченной глубины из многовходовых элементов, построение сбалансированных по глубине деревьев решений для сортировки.

Область и методы исследования

Тема диссертационной работы относится к направлению «теория алгоритмов и вычислимых функций», разделу «алгоритмическая теория информации и теория сложности» из паспорта специальности 01.01.06.

В работе используются методы теории сложности вычислений и дискретной математики, в том числе, теории асимптотически оптимального синтеза и комбинаторики, а также элементарные методы алгебры и теории чисел.

Научная новизна

Результаты работы являются новыми и получены автором самостоятельно.

Теоретическая и практическая ценность

Работа носит теоретический характер. Ее результаты могут найти применение прежде всего в теоретических исследованиях закономерностей синтеза параллельных схем. Часть результатов имеет прикладной потенциал в схемотехнике или практике быстрых вычислений. Это относится, в первую очередь, к конструкциям параллельных умножителей, параллельных префиксных схем и отчасти к методу быстрой сортировки.

Апробация результатов

Результаты диссертации неоднократно докладывались на научных семинарах «Синтез и сложность управляющих систем» и «Математические вопросы кибернетики» в МГУ (2009–2012, 2021 гг.), на международных семинарах серии «Дискретная математика и ее приложения» (МГУ, 2010, 2019 гг.), на молодежных научных школах по дискретной математике и ее приложениям в ИПМ им. Келдыша (2013, 2015 гг.), на международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород 2011 г.), на международной конференции «Современные проблемы анализа и преподавания математики» в МГУ в 2010 г., на семинаре «Теоретическая кибернетика» в ИПМ им. Келдыша в 2019 г. и на семинаре «Дискретная математика и математическая кибернетика» в МГУ в 2020 г.

Публикации

Перечень публикаций, в которых представлены основные результаты, приведен в конце автореферата: в рецензируемых изданиях опубликовано 16 работ.

Структура и объем работы

Диссертация состоит из шести глав, разбитых на разделы и параграфы (первая глава является вводной), и заключения. Текст диссертации изложен на 287 страницах. Список литературы включает 243 пункта.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во вводной **главе 1** описывается направление исследований, объясняется его актуальность, формулируются цели и постановка задач, дается краткая историческая справка о предшествующих работах в данной области, перечисляются основные результаты диссертации, приводятся сведения о публикациях автора по теме диссертации и об апробации результатов. Подробнее состояние вопроса по каждой из тем изложено в соответствующих главах.

В **главе 2** представлены результаты о соотношении между глубиной и сложностью булевых формул, о построении эффективных по глубине или сложности формул для симметрических булевых функций и о нижних оценках сложности формул в базисе k-местных функций.

Множество *формул над базисом* B, *сложность* формулы, *глубина* формулы и функция, реализуемая формулой, определяются индуктивно следующим образом: 0) символы переменных являются формулами сложности 1, глубины 0 и реализуют соответствующие тождественные функции; 1) выражение $G(F_1, ..., F_k)$, где G — символ, обозначающий k-местную функцию $g \in B$, а F_i — формула сложности L_i и глубины D_i, реализующая функцию f_i, является формулой сложности $L_1 + \ldots + L_k$, глубины $\max\{D_1, ..., D_k\} + 1$ и реализует функцию $g(f_1, \ldots, f_k)$.

Сложность $L_B(f)$ (глубина $D_B(f)$) реализации булевой функции f формулами над базисом B определяется как минимум сложности (глубины) формул, реализующих f. Сложность $L_B(K)$ (глубина $D_B(K)$) класса функций K определяется как $\max_{f \in K} L_B(f)$ (соответственно $\max_{f \in K} D_B(f)$). Формула, реализующая булев оператор, определяется как совокупность формул, реализующих отдельные функции — компоненты оператора. Сложность булевого оператора определяется как сумма сложностей его компонент, а глубина — как максимум глубины компонент.

Далее при сравнении порядков роста неотрицательных функций используются обозначения: $f = \omega(g)$ равносильно $g = o(f)$; $f = \Omega(g)$ равносильно $g = O(f)$ и может быть записано как $g \preceq f$ или $f \succeq g$; $f \asymp g$ означает $f = \Theta(g)$. Обозначения $f \sim g$, $f \gtrsim g$, $f \lesssim g$ используются соответственно для асимптотического равенства и неравенств.

Тривиальным образом в любом базисе, состоящем из не более чем k-местных функций, выполняется $D_B(f) \geq \log_k L_B(f)$. Базисы, для которых также выполнено $D_B(f) \preceq \log L_B(f)$, называются равномерными. Равномерность базиса B можно охарактеризовать величиной (равной константе или ∞)

$$c_B = \overline{\lim_{N \to \infty}} \max_{L_B(f) = N} \frac{D_B(f)}{\log_2 N}.$$

Определение означает, что для любой выражаемой в базисе B функции f выполнено $D_B(f) \leq (c_B + o(1)) \log_2 L_B(f)$, а также существует бесконечная последовательность функций f_k, для которой $D_B(f_k) \geq (c_B - o(1)) \log_2 L_B(f_k)$.

Еще в 1960-х гг. В. М. Храпченко[40] доказал, что функционально пол-

[40] Яблонский С. В., Козырев В. П. Математические вопросы кибернетики. «Информационные материалы» Научного совета по комплексной проблеме «Кибернетика»

ные конечные булевы базисы являются равномерными, что значит: глубина и логарифм сложности формул для любой функции над такими базисами совпадают по порядку. Впоследствии А. Б. Угольников[41] и М. Рагаз[42] установили аналогичный факт для произвольных конечных булевых систем.

Начиная с 1970-х гг. было получено множество оценок констант равномерности для различных базисов. Основной интерес представляют арифметические базисы из операций сложения и умножения, а также деления, и булев аналог — монотонный базис из операций конъюнкции и дизъюнкции — в связи с практической задачей о параллельном перестроении арифметических выражений. Для общих арифметических базисов $B_A = \{+, *\}$, $B_{AD} = \{+, *, /\}$ и булева монотонного базиса $B_M = \{\vee, \wedge\}$ рекордные верхние оценки были получены Д. Маллером, Ф. Препаратой[43] ($c_{B_{AD}} < 2.89$), В. М. Храпченко[44] ($c_{B_M} < 1.73$) и С. Р. Косараю[45] ($c_{B_A} \leq 2$). Нетривиальные нижние оценки констант равномерности были известны только для монотонных арифметических базисов из работ Э. Шамира, М. Шнира[46] ($c_{B_A} > 1.16$), Д. Копперсмита и Б. Шибера[47] ($c_{B_A} \geq 1.5$), а в булевом случае — для некоторых неарифметических базисов невысокой выразительной силы, например, для базиса из единственной функции «штрих Шеффера»[48].

Задача получения нетривиальной нижней оценки для булева монотонного базиса B_M оставалась нерешенной на протяжении 50 лет. Решение представлено автором в разделе 2.2 диссертационной работы.

Для этого строится специальная последовательность бесповторных булевых функций. Стратегия рассуждения состоит в рассмотрении двух главных подформул минимальной по глубине формулы для данной

АН СССР. Вып. 19а. М., 1968, 3–15.

[41]Угольников А. Б. О глубине и полиномиальной эквивалентности формул для замкнутых классов двузначной логики. Матем. заметки. 1987. **42**(4), 603–612.

[42]Ragaz M. Parallelizable algebras. Arch. math. Logic. 1986/87. **26**, 77–99.

[43]Muller D. E., Preparata F. P. Restructuring of arithmetic expressions for parallel evaluation. J. ACM. 1976. **23**(3), 534–543.

[44]Храпченко В. М. О соотношении между сложностью и глубиной формул. Методы дискретного анализа в синтезе управляющих систем. Вып. 32. Новосибирск: ИМ СО АН СССР, 1978, 76–94.

[45]Kosaraju S. R. Parallel evaluation of division-free arithmetic equations. Proc. 18th Symp. on Theory of Comput. (Berkeley, 1986). NY: ACM, 1986, 231–239.

[46]Shamir E., Snir M. On the depth complexity of formulas. Math. Syst. Theory. 1979/80.**13**(4), 301–322.

[47]Coppersmith D., Schieber B. Lower bounds on the depth of monotone arithmetic computations. J. Complexity. 1999. **15**(1), 17–29.

[48]Храпченко В. М. Об асимптотической оценке времени сложения параллельного сумматора. Проблемы кибернетики. Вып. 19. М.: Наука, 1967, 107–120.

функции. Доказывается, что либо одна из подформул содержит бесповторную функцию, «похожую» на исходную (т.е. при переходе на меньшую глубину функция не сильно упрощается), либо суммарное число существенных переменных, от которых зависят две подфункции, реализуемые главными подформулами, заметно возрастает. Далее сложность формул оценивается при различных ограничениях на глубину и используется тот факт, что сложность формулы глубины d не может быть больше, чем 2^d. Результатом применения метода к рассматриваемой последовательности функций является

Теорема 2.2 *Справедливо соотношение:* $c_{B_M} > 1.06$.

Метод работает и в арифметическом базисе B_A, позволяя получать потенциально более высокие нижние оценки, чем в булевом случае, однако уступающие уже известным оценкам для этого базиса.

Разделы 2.3, 2.4 посвящены эффективной реализации симметрических функций. *Симметрические функции* — это функции, значения которых не изменяются при перестановке аргументов. В булевом случае значение симметрической функции определяется арифметической суммой переменных. Класс всех симметрических булевых функций n переменных обозначается через S_n.

Вопросы эффективной реализации симметрических функций в различных вычислительных моделях всегда находились в фокусе внимания теории сложности. Для приложений, практических и теоретических, представляют интерес методы синтеза как конкретных симметрических функций, так и подклассов (пороговые, периодические функции), реже симметрических функций вообще. Одно из главных приложений — параллельные схемы умножения чисел, основанные на эффективном вычислении арифметической суммы битов. Известные конструкции параллельных схем для деления и некоторых других арифметических операций с числами или элементами конечных полей[49, 50, 51] также опираются на быстрые схемы для симметрических функций.

Первые результаты о сложности, а затем и о глубине формул для симметрических булевых функций были получены В. М. Храпченко в

[49] Beame P. W., Cook S. A., Hoover H. J. Log depth circuits for division and related problems. SIAM J. Comput. 1986. **15**(4), 994–1003.

[50] Сергеев И. С. О схемах логарифмической глубины для инвертирования в конечных полях характеристики два. Математические вопросы кибернетики. Вып. 15. М.: Физматлит, 2006, 35–64.

[51] Гашков С. Б., Сергеев И. С. О построении схем логарифмической глубины для инвертирования в конечных полях. Дискретная математика. 2008. **20**(4), 8–28.

начале 1970-х гг.: как верхние оценки[52, 53], так и нижние[54] (все — для стандартного базиса). Позже к ним были добавлены аналогичные результаты для полного бинарного базиса; метод доказательства нижних оценок разработан М. Фишером, А. Майером и М. Патерсоном[55]. Серия уточнений верхних оценок продолжалась до начала 1990-х гг., когда усилиями М. Патерсона, Н. Пиппенджера, У. Цвика[56] были определены принципы оптимального конструирования формул из заданных подформул-компрессоров, и тем самым обобщены ранее известные методы.

Предположительно, известные верхние оценки сложности и глубины формул гораздо дальше отстоят от истинных значений, чем нижние, и требуют существенного уточнения. Спустя 20 лет после упомянутых выше работ, автору настоящей работы удалось сделать шаг в указанном направлении, предложив новые методы синтеза формул для симметрических функций с использованием популярных (в теории быстрых алгоритмов) идей использования нескольких взаимно простых модулей и приближенных вычислений. Эти методы позволили на 10–20% улучшить верхние оценки глубины и логарифма сложности формул (к сожалению, рекордные полученные оценки неконструктивны).

Большая часть известных верхних оценок сложности и глубины реализации симметрических функций как формулами, так и схемами из функциональных элементов над полными базисами, связаны с эффективной реализацией булевого (n, m)-оператора $C_n(x_1, \ldots, x_n) = (C_{n,m-1}, ..., C_{n,0})$ подсчета числа единиц в булевом наборе $(x_1, \ldots, x_n)$, где $m = \lceil \log_2(n+1) \rceil$. Сведение к вычислению C_n используется при минимизации глубины и сложности формул для умножения двоичных чисел.

Предлагаемый новый метод синтеза основан на простом применении модулярной арифметики. Вместо прямого вычисления арифметической суммы σ булевых переменных $x_1, \ldots, x_n$ вычисляются числа $(\sigma \bmod 2^k)$ и $(\sigma \bmod 3^l)$, где $2^k \cdot 3^l > n$, причем для вычисления $(\sigma \bmod 3^l)$ используется троичная система счисления. Искомое число σ может быть затем опреде-

[52] Храпченко В. М. О сложности реализации симметрических функций формулами. Математические заметки. 1972. **11**(1), 109–120.

[53] Храпченко В. М. Некоторые оценки для времени умножения. Проблемы кибернетики. Вып. 33. М.: Наука, 1978, 221–227.

[54] Храпченко В. М. Об одном методе получения нижних оценок сложности π-схем. Математические заметки. 1971. **10**(1), 83–92.

[55] Fischer M. J., Meyer A. R., Paterson M. S. $\Omega(n \log n)$ lower bounds on length of Boolean formulas. SIAM J. Comput. 1982. **11**(3), 416–427.

[56] Paterson M. S., Pippenger N., Zwick U. Optimal carry save networks. LMS Lecture Notes Series. Boolean function complexity. Vol. 169. Cambridge University Press, 1992, 174–201.

лено при помощи Китайской теоремы об остатках. Эффективность способа обусловлена тем, что самые сложные для метода компрессоров разряды суммы σ — старшие — вычисляются практически «бесплатно» из младших средствами модулярной арифметики.

Еще один прием, упрощающий формулы, состоит в дополнительном приближенном вычислении суммы σ. Отрезок $[0,\, n]$ накрывается интервалами длины T. Тогда значение σ определяется по номеру интервала и остаткам $\sigma \bmod 2^k$, $\sigma \bmod 3^l$ при условии $2^k \cdot 3^l \geq T$. Размер формул сокращается благодаря тому, что процесс вычисления суммы компрессорами останавливается раньше (когда найденных разрядов достаточно для восстановления числа по модулю T).

Для иллюстрации возможностей предлагаемых методов синтеза выбираются базис B_2 всех двуместных булевых функций и стандартный базис $B_0 = \{\wedge, \vee, \bar{}\}$. Как известно, множество полных бинарных базисов распадается на два класса эквивалентности относительно сложности формул. Базисы B_0 и B_2 являются представителями этих классов.

Через $C_n^{(3)}(x_1, \ldots, x_n) = \left(C_{n,m-1}^{(3)}, ..., C_{n,0}^{(3)}\right)$, $m = \lceil \log_3(n+1) \rceil$, обозначим булев $(n, 2m)$-оператор вычисления арифметической суммы булевых переменных $x_1, \ldots, x_n$ в троичной системе счисления. Компонента $C_{n,i}^{(3)}$ является 2-битным кодом соответствующей цифры из троичной записи числа.

Пусть $n = (2^r - 1)(2t - 1) - 1$. Разобьем отрезок $[0, n]$ на $2^r - 1$ интервалов длины $2t - 1$. Обозначим через $J_n^t(x_1, \ldots, x_n) = \left(J_{n,r-1}^t, \ldots, J_{n,0}^t\right)$, $r = \left\lceil \log_2 \left(\frac{n+1}{2t-1} + 1\right) \right\rceil$, (n, r)-оператор вычисления номера интервала, в котором находится арифметическая сумма σ переменных.

Лемма 2.10 *Пусть $2^k \cdot 3^l \geq 6t - 3$. Тогда для любого полного конечного базиса B справедливы оценки*

$$L_B(C_n) \leq 2^{O\left(\log^2 \log n\right)} \cdot L_B\left(J_n^t, C_{n,k-1}, \ldots, C_{n,0}, C_{n,l-1}^{(3)}, \ldots, C_{n,0}^{(3)}\right),$$

$$D_B(C_n) \leq D_B\left(J_n^t, C_{n,k-1}, \ldots, C_{n,0}, C_{n,l-1}^{(3)}, \ldots, C_{n,0}^{(3)}\right) + O\left(\log^2 \log n\right).$$

Произвольная симметрическая функция представима в виде функции разрядов числа $\sigma_2 = \sigma \bmod 2^k$ и кода числа $\sigma_3 = \sigma \bmod 3^l$. Для эффективной реализации требуется предварительно выполнить специальную перекодировку числа σ_3. Для этого число разбивается на достаточно длинные блоки, которые перекодируются в двоичное представление.

Пусть $l = \lambda b$, где $\lambda, b \in \mathbb{N}$, и $b = \Theta(\log n / \log \log n)$. Число $\sigma_3 = \sigma \bmod 3^l$ переписывается в системе счисления с основанием 3^b, где цифры представляются двоичными числами. Обозначим компоненты опе-

ратора, вычисляющего σ_3 в указанной системе счисления, через $C_{n,i}^{(3^b)}$, $i = 0, \ldots, \lambda\nu - 1$, где $\nu = \lceil b \log_2 3 \rceil$.

Кроме того, обозначим через $R_n(x_1, ..., x_n) = (R_{n,n-1}, \ldots, R_{n,0})$ оператор упорядочения набора из n чисел: $R_{n,n-1} \geq \ldots \geq R_{n,0}$. Методом каскадов доказывается

Лемма 2.11 *Пусть* $2^k \cdot 3^{\lambda b} \geq 6t - 3$, $\nu = \lceil b \log_2 3 \rceil$, $r = \left\lceil \log_2 \left(\frac{n+1}{2t-1} + 1 \right) \right\rceil$, $s = k + \nu\lambda + r$. *Пусть* $B \in \{B_0, B_2\}$. *Положим*

$$
\begin{aligned}
(L_{s-1}, \ldots, L_0) = R_s \Big(& L_B(J_{n,r-1}^t), \ldots, L_B(J_{n,0}^t), \\
& L_B(C_{n,k-1}), \ldots, L_B(C_{n,0}), L_B\left(C_{n,\nu\lambda-1}^{(3^b)}\right), \ldots, L_B\left(C_{n,0}^{(3^b)}\right) \Big), \\
(D_{s-1}, \ldots, D_0) = R_s \Big(& D_B(J_{n,r-1}^t), \ldots, D_B(J_{n,0}^t), \\
& D_B(C_{n,k-1}), \ldots, D_B(C_{n,0}), D_B\left(C_{n,\nu\lambda-1}^{(3^b)}\right), \ldots, D_B\left(C_{n,0}^{(3^b)}\right) \Big).
\end{aligned}
$$

Тогда

$$
\begin{aligned}
L_B(S_n) &\leq 2^{O\left(\log^2 \log n\right)} \left(\sum_{i=0}^{s-1} 2^{s-i} L_i \right), \\
D_B(S_n) &\leq \max_{0 \leq i < s} \{D_i + s - i\} + O\left(\sqrt{\log n}\right).
\end{aligned}
$$

Операторы C_n и $C_n^{(3)}$ реализуются развитой в предшествующих работах[57] техникой при помощи компрессоров. *Двоичный* (k, l)*-компрессор* ширины 1 — это формула (или схема), реализующая булев оператор $(x_1, \ldots, x_k) \to (y_1, \ldots, y_l)$, определяемый условием $\sum 2^{a_i} x_i = \sum 2^{b_j} y_j$, где $k > l$, $a_i, b_j \in \mathbb{Z}$. (k, l)-компрессор произвольной ширины строится из параллельных копий компрессоров ширины 1 и позволяет сводить сложение k чисел к сложению l чисел. Аналогично определяется q-ичный компрессор.

Леммы 2.10 и 2.11 в сочетании с методом компрессоров (подходящие компрессоры построены автором диссертации) без использования приближенного вычисления номера интервала приводят к следующим конструктивным оценкам.

[57] Paterson M. S., Pippenger N., Zwick U. Faster circuits and shorter formulae for multiple addition, multiplication and symmetric Boolean functions. Proc. 31st Symp. on Found. of Comput. Sci. (St. Louis, 1990). Washington: IEEE, 1990, 642–650.

Теорема 2.3 *Справедливы соотношения:*

$$L_{B_0}(C_n) \preceq n^{4.47}, \quad L_{B_0}(S_n) \preceq n^{4.48}, \quad L_{B_2}(C_n) \preceq n^{3.03}, \quad L_{B_2}(S_n) \preceq n^{3.04},$$
$$D_{B_0}(C_n) \lesssim 4.87 \log_2 n, \qquad D_{B_0}(S_n) \lesssim 4.88 \log_2 n,$$
$$D_{B_2}(C_n) \lesssim 3.34 \log_2 n, \qquad D_{B_2}(S_n) \lesssim 3.34 \log_2 n.$$

Для вычисления номера интервала можно адаптировать вероятностную процедуру, предложенную Л. Вэльянтом[58]. Тогда аппарат лемм 2.10 и 2.11 задействуется в полном объеме, при этом неконструктивно получается усиление теоремы 2.3.

Теорема 2.4 *Имеют место оценки:*

$$L_{B_0}(C_n) \preceq n^{3.91}, \quad L_{B_0}(S_n) \preceq n^{4.01}, \quad L_{B_2}(C_n) \preceq n^{2.84}, \quad L_{B_2}(S_n) \preceq n^{2.95},$$
$$D_{B_0}(C_n) \lesssim 4.14 \log_2 n, \qquad D_{B_2}(C_n) \lesssim 3.02 \log_2 n,$$
$$D_{B_0}(S_n) \lesssim 4.24 \log_2 n, \qquad D_{B_2}(S_n) \lesssim 3.1 \log_2 n.$$

Для сравнения, ранее известные оценки[59, 60] для оператора C_n имели вид: $L_{B_0}(C_n) \preceq n^{4.57}$, $L_{B_2}(C_n) \preceq n^{3.13}$, $D_{B_0}(C_n) \lesssim 4.94 \log_2 n$, $D_{B_2}(C_n) \lesssim 3.44 \log_2 n$.

В разделе 2.5 отдельно рассмотрен вопрос о реализации периодических симметрических функций (MOD-функций). Через MOD_n^m обозначается булев (n, m)-оператор сложения n одноразрядных чисел по модулю m. Компоненты оператора — MOD-*функции* — определяются как

$$\mathrm{MOD}_n^{m,r}(x) = \left(\sum_{i=1}^{n} x_i \equiv r \bmod m \right),$$

$r \in \mathbb{Z}_m$, где $x = (x_1, \ldots, x_n)$. Основной интерес представляют функции с малыми простыми числами m в качестве периодов, в том числе, в связи с новым модулярным методом синтеза симметрических функций, использующим недвоичные системы счисления.

Универсальный способ вычисления MOD-функции, как и произвольной симметрической булевой функции, состоит в сведении к реализации оператора C_n. Но конкретные MOD-функции с малыми периодами можно вычислять быстрее. Нетривиальные верхние оценки получены Д. ван

[58] Valiant L. G. Short monotone formulae for the majority function. J. Algorithms. 1984. **5**, 363–366.

[59] Paterson M., Zwick U. Shallow circuits and concise formulae for multiple addition and multiplication. Comput. Complexity. 1993. **3**, 262–291.

[60] Grove E. Proofs with potential. Ph.D. thesis. Univ. of California, Berkeley, 1993.

Лейенхорстом[61] (для сложности формул в базисе B_2 при $m = 3, 5, 7$) и Э. Чином[62] (для глубины в базисе B_0 при $m = 3, 5, 11$) около 1990 г. Через 25 лет автором настоящей работы получены новые оценки — часть из них при помощи предложенного общего приема сведения к задаче об оптимальном покрытии матриц прямоугольниками.

Предлагаемый метод позволяет строить эффективные формулы в стандартном базисе, опираясь на подходящие покрытия связанных с функциями булевых матриц. Для $S \subset \mathbb{Z}_m$ вводятся функции

$$\mathrm{MOD}_n^{m,S}(x) = \left(\sum_{i=1}^{n} x_i \bmod m \in S \right).$$

Набор всех функций $\mathrm{MOD}_n^{m,S}$, $0 < |S| < m$, задает значение суммы переменных по модулю m, используя максимальную однозначную кодировку элементов множества $\mathbb{Z}_m$. Задача состоит в поиске формул вида

$$\mathrm{MOD}_n^{m,S}(x) = \bigvee_k \mathrm{MOD}_{n_1}^{m,A_k}(x^1) \cdot \mathrm{MOD}_{n_2}^{m,B_k}(x^2),$$

где $x = (x^1, x^2)$. Их можно интерпретировать в терминах покрытий множеств или матриц. Каждому множеству S сопоставим (m, m)-матрицу I_m^S, строки и столбцы которой занумерованы числами из $\mathbb{Z}_m$, а элементы определяются как $I_m^S[i, j] = (i+j \in S)$. Тогда формула отвечает покрытию матрицы I_m^S сплошь единичными подматрицами (прямоугольниками) на пересечении строк A_k и столбцов B_k.

Далее в работе путем подбора покрытий малого ранга для небольших циркулянтных матриц строятся формулы над базисом B_0, доставляющие новые верхние оценки сложности и глубины MOD-функций с периодами 5 и 7. Кроме того, другим способом доказываются новые верхние оценки глубины оператора MOD_n^3 в базисе B_0 и оператора MOD_n^7 в базисе B_2.

Теорема 2.5 *Справедливы соотношения:*

$$L_{B_0}(\mathrm{MOD}_n^5) \preceq n^{3.22}, \qquad L_{B_0}(\mathrm{MOD}_n^7) \preceq n^{3.63},$$
$$D_{B_0}(\mathrm{MOD}_n^3) \lesssim 2.8 \log_2 n, \qquad D_{B_0}(\mathrm{MOD}_n^5) \lesssim 3.35 \log_2 n,$$
$$D_{B_0}(\mathrm{MOD}_n^7) \lesssim 3.87 \log_2 n, \qquad D_{B_2}(\mathrm{MOD}_n^7) \lesssim 2.93 \log_2 n.$$

[61] van Leijenhorst D. C. A note on the formula size of the "mod k" functions. Inf. Proc. Letters. 1987. **24**, 223–224.

[62] Chin A. On the depth complexity of the counting functions. Inf. Proc. Letters. 1990. **35**, 325–328.

Раздел 2.6 посвящен проблеме получения нижних оценок сложности при реализации формулами в базисе U_k из k-местных булевых функций, монотонно невозрастающих или монотонно неубывающих по каждой переменной. Базис U_k служит обобщением стандартного базиса B_0 (точнее, эквивалентного ему базиса $U_2 = B_2 \setminus \{\oplus, \sim\}$) и эквивалентен базису из всех монотонных k-местных функций и отрицания. Это максимальный k-арный базис, в котором сложность линейной функции $l_n(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$ нелинейна.

Самым сильным инструментом нижней оценки сложности (глубины) формул симметрических функций в базисе U_2 пока остается метод Храпченко[63]. Он позволяет получать квадратичные нижние оценки сложности для функций, принимающих разные значения в средних слоях булева куба. Оценка Храпченко связана с понятием *чувствительности* булевой функции f, которая определяется как

$$s(f) = \max_{N \subset f^{-1}(0),\, P \subset f^{-1}(1)} \frac{|R(N,P)|^2}{|N| \cdot |P|},$$

где $R(N,P)$ — множество пар соседних наборов из N и P, т. е. отличающихся в одной координате. Храпченко установил соотношение $L_{U_2}(f) \geq s(f)$. Максимальную чувствительность $s(f) = n^2$ среди функций n переменных имеет линейная функция $f = l_n$. Другие популярные примеры — функция голосования $m_n(x_1, \ldots, x_n) = (\sum x_i \geq n/2)$, для которой $s(m_n) \sim n^2/4$, монотонные пороговые функции вообще, определитель матрицы над $GF(2)$.

В ряде работ изучалась сложность вычисления линейной функции и функции голосования в полных k-арных базисах. В основном нижние оценки получались методом сжатия формул при случайных подстановках, восходящем к работе Б. А. Субботовской[64]. Получаемые оценки имеют вид $L_B(l_n) = \Omega\left(n^{\Gamma_B}\right)$, где Γ_B — экспонента сжатия базиса B.

Сама Субботовская (Мучник)[65] получила оценки $\Gamma_B \geq 1 + \frac{1}{3k-4}$ для некоторых k-арных базисов $B \subset U_k$. Н. А. Перязев[66] доказал, что

[63] Храпченко В. М. Об одном методе получения нижних оценок сложности π-схем. Математические заметки. 1971. **10**(1), 83–92.

[64] Субботовская Б. А. О реализации линейных функций формулами в базисе $\vee, \&, {}^-$. Доклады АН СССР. 1961. **136**(3), 553–555.

[65] Мучник Б. А. Оценка сложности реализации линейной функции формулами в некоторых базисах. Кибернетика. 1970. **4**, 29–38.

[66] Перязев Н. А. Сложность представлений булевых функций формулами в немонолинейных базисах. «Дискретная математика и информатика». Вып. 2. Иркутск: Изд-во Иркут. ун-та, 1995.

$\Gamma_{U_k} \geq 1+\frac{1}{3k-4}$. Для базиса U_3 Х. Чоклер и У. Цвик[67] доказали более сильную оценку $\Gamma_{U_3} \geq 4/3$. Последний результат приводит к наилучшей известной ранее оценке сложности линейной функции в тернарном базисе $L_{U_3}(l_n) = \Omega\left(n^{4/3}\right)$. Там же доказана верхняя оценка $L_{U_3}(l_n) \preceq n^{1.74}$. Для функции голосования К. Уено[68] получил верхнюю оценку $L_{U_3}(m_n) \preceq n^{3.8}$. Отметим, что эта оценка может быть существенно понижена применением методов разделов 2.3 и 2.4.

Для сравнения, в базисе M_k, состоящем из всех k-местных монотонных функций, известные оценки имеют вид $n^{\log_2 3} \preceq L_{M_3}(m_n) \preceq n^{4.3}$ и $L_{M_k}(m_n) \preceq n^{3+c/\ln k}$ (нижняя получена М. М. Рохлиной[69], а верхние — А. Гуптой и С. Махаджаном[70].

Предлагаемый автором метод в определенном смысле расширяет метод Храпченко на k-арные базисы. Для булева базиса B *экспонента Храпченко* χ_B определяется как максимальное число χ, такое, что для любой функции f, выразимой в базисе B, выполнено $L_B(f) \geq s^\chi(f)$. Из определения немедленно следуют оценки $L_B(l_n) = \Omega\left(n^{2\chi_B}\right)$, $L_B(m_n) = \Omega\left(n^{2\chi_B}\right)$. Для произвольного базиса B выполнено $\chi_B \geq 1/2$, а для любого полного k-арного базиса $B \not\subset U_k$, справедливо $\chi_B = 1/2$.

Оказывается удобным от рассмотрения чувствительности булевых функций перейти к изучению подходящих характеристик двудольных графов. Для произвольного двудольного графа $G = (A, B, E)$ на множествах вершин A, B и с множеством ребер E величина $s(G)$ определяется как

$$s(G) = \max_{X \subset A,\, Y \subset B} \frac{|E \cap (X \times Y)|^2}{|X| \cdot |Y|}.$$

Множество двудольных графов $G_i = (A_i, B_i, E_i)$ называется *покрытием* двудольного графа $G = (A, B, E)$, если для всех i выполняется $A_i \subset A$, $B_i \subset B$, при этом $E \subset \bigcup E_i$. Покрытие называется *монотонным*, если для любого множества индексов I одно из двух множеств $A \setminus \bigcup_{i \in I} A_i$ и $B \setminus \bigcup_{i \notin I} B_i$ пусто.

При любом $k \geq 2$ определим *экспоненту сложности* двудольных графов χ_k (соответственно *экспоненту монотонной сложности* χ_k^*) как

[67] Chockler H., Zwick U. Which bases admit non-trivial shrinkage of formulae? Comput. Complexity. 2001. **10**, 28–40.

[68] Ueno K. Formula complexity of ternary majorities. Proc. Int. Computing and Combinatorics Conf. (Sydney, Australia, 2012). Lecture Notes in Comput. Sci. 2012. **7434**, 433–444.

[69] Рохлина М. М. О схемах, повышающих надежность. Проблемы кибернетики. Вып. 23. М.: Наука, 1970, 295–301.

[70] Gupta A., Mahajan S. Using amplification to compute majority with small majority gates. Comput. Complexity. 1996. **6**, 46–63.

максимальное число χ, такое, что для любого двудольного графа G и для любого его покрытия (соответственно монотонного покрытия) $G_1, \ldots, G_k$ выполнено условие субаддитивности

$$s^\chi(G_1) + \ldots + s^\chi(G_k) \geq s^\chi(G).$$

Связь между экспонентой Храпченко и экспонентами сложности графов устанавливает

Утверждение 2.5 *При любом $k \geq 2$ справедливо $\chi_k \leq \chi_k^* \leq \chi_{U_k}$.*

Результат Храпченко на языке графов имеет вид $\chi_2^* = 1$, однако при этом $\chi_2 < 1$. В общем случае автором получены следующие оценки:

Теорема 2.6 *При любом $k \geq 2$ выполнено $\chi_{U_k} \leq \log_{\lceil k/2 \rceil (\lfloor k/2 \rfloor + 1)} k$.*

Теорема 2.7 *При любом $k \geq 2$ справедливо $\chi_k \geq 1/2 + 1/(10 \ln k)$.*

Объединение этих результатов дает

$$\frac{1}{2} + \frac{1}{10 \ln k} \leq \chi_k \leq \chi_k^* \leq \chi_{U_k} \leq \frac{1}{2} + \frac{1}{2 \log_2 (k/2)}$$

(при $k = 2$ последнее неравенство выполнено в смысле $1 < \infty$).

Отдельно для тернарного базиса получена более точная оценка:

Теорема 2.8 *Справедливо $\chi_3^* \geq 0.769$.*

Таким образом, $0.769 \leq \chi_{U_3} \leq \log_4 3 \approx 0.792$. Как следствие, при любом $k \geq 2$ имеет место

$$L_{U_k}(l_n), L_{U_k}(m_n) \in \Omega\left(n^{1+1/(5 \ln k)}\right),$$

(указанная оценка сильнее ранее известных при $k \geq 4$), а при $k = 3$ справедливо

$$L_{U_3}(l_n), L_{U_3}(m_n) \in \Omega\left(n^{1.538}\right).$$

Простые верхние оценки показывают, что на самом деле $L_{U_k}(l_n) \asymp n^{1+\Theta_k(1/\ln k)}$, т.е. результат о сложности линейной функции в определенном смысле окончательный:

Теорема 2.9 (*i*) *При всех $k \geq 2$ справедливо*

$$L_{U_{2k}}(l_n) \leq 2n^{1+1/\log_2 k}, \qquad D_{U_{2k}}(l_n) \leq \lceil \log_k n \rceil.$$

(*ii*) *При любом $k \geq 3$ выполнено*

$$L_{U_{2k}}(m_n) = O\left(n^{1+c_1 \ln \ln k / \ln k} \cdot (\ln n)^{c_2 \ln \ln k}\right),$$

где c_1, c_2 — некоторые константы.

Глава 3 посвящена линейным схемам и объединяет результаты из нескольких направлений. *Линейная схема* над коммутативной полугруппой $(S, +)$ определяется как ориентированный ациклический граф с n вершинами-входами $x_1, \ldots, x_n$, не имеющими входящих ребер, и m вершинами-выходами $y_1, \ldots, y_m$, не имеющими исходящих ребер. В каждой вершине, кроме входов, вычисляется сумма над $(S, +)$ по всем входящим ребрам. *Сложность* схемы — общее число ребер в ней, а *глубина* — число ребер в самом длинном ориентированном пути. Линейная схема реализует некоторое линейное преобразование, но принято говорить, что схема реализует саму матрицу данного преобразования.

В теоретических исследованиях, в основном, представлены следующие разновидности линейных схем: схемы над $(\mathbb{B}, \vee)$ (классические вентильные схемы, OR-схемы), схемы над $(\mathbb{B}, \oplus)$ (вентильные схемы по модулю 2, XOR-схемы), схемы над $(\mathbb{Z}, +)$ (аддитивные схемы, SUM-схемы), $\mathbb{B} = \{0, 1\}$.

В разделе 3.2 приводится решение задачи асимптотически оптимального синтеза линейных схем ограниченной глубины для класса матриц размера $m \times n$ с ограничениями на размер коэффициентов, в частности, для класса $\mathbb{B}^{m\times n}$ булевых матриц. Оценки, относящиеся к небулевым матрицам, подразумевают использование SUM-схем. Обозначим $E_q = \{0, 1, \ldots, q-1\}$. Пусть $\mathsf{L}_d(q, m, n)$ означает функцию Шеннона сложности реализации класса матриц размера $m \times n$ с элементами из E_q с глубиной d; $\mathsf{L}(q, m, n)$ — обозначение для функции Шеннона без ограничения на глубину. Далее полагаем $m \le n$.

В 1956 г. О. Б. Лупанов получил асимптотику сложности класса $\mathbb{B}^{m\times n}$ (булевых матриц размера $m \times n$) при реализации вентильными схемами в случае $\log m = o(\log n)$

$$\mathsf{L}(2, m, n) \sim \mathsf{L}_2(2, m, n) \sim \frac{mn}{\log n},$$

используя схемы глубины 2. Это один из первых результатов теории асимптотически оптимального синтеза. Чуть позже Э. И. Нечипорук[71] при помощи конструкции глубины 3 получил асимптотику сложности при определенных соотношениях между m и n (а именно, при $\log m \sim c_{p,r} \log n$, где $c_{p,r} = \frac{p}{p(r-1)+r}$, $p, r \in \mathbb{N}$), включая важный случай $m = n$:

$$\mathsf{L}(2, m, n) \sim \mathsf{L}_3(2, m, n) \sim \frac{mn}{\log(mn)}.$$

Некоторые результаты в направлении исследования асимптотики слож-

[71] Нечипорук Э. И. О вентильных схемах. Доклады АН СССР. 1963. **148**(1), 50–53.

ности класса узких матриц, при $m \asymp \log n$, получены В. А. Орловым[72] и А. В. Чашкиным[73].

В конце 1970-х гг. Н. Пиппенджер[74], обобщая результаты Лупанова и Нечипорука, решил задачу при любых m и n, исключая случай узких матриц, но использовал схемы растущей глубины. Верхняя оценка Пиппенджера справедлива при условии $H = mn \log q \to \infty$ и имеет вид

$$\mathsf{L}(q, m, n) \leq 3m \log_3(q-1) + (1 + \tau(H)) \frac{H}{\log_2 H} + O(n),$$

где $\tau(H) \asymp \sqrt{\frac{\log\log H}{\log H}}$. При $\log n = o(m \log q)$ она асимптотически точна, как показывает полученная Пиппенджером нижняя оценка

$$\mathsf{L}(q, m, n) \geq 3m \log_3(q-1) + \left(1 - \Theta\left(\frac{\log\log H}{\log H}\right)\right) \frac{H}{\log_2 H}.$$

Вопрос о возможности получения асимптотики сложности в ограниченной глубине долгое время оставался открытым, пока автор диссертации, отталкиваясь от конструкций Нечипорука и Пиппенджера, не показал, что асимптотика сложности на самом деле достигается на схемах глубины 3. В таком виде результат уже неулучшаем. Более того, при некоторых дополнительных предположениях относительно параметров асимптотически точные оценки доказаны с остаточным членом «правильного» порядка $\tau(H) \asymp \frac{\log\log H}{\log H}$.

Отметим, что задаче о сложности реализации матрицы вентильными схемами подобна задача о сложности реализации матрицы (векторными) аддитивными цепочками. Только сложность аддитивной схемы измеряется не числом ребер, а числом бинарных операций сложения. Методы оптимального синтеза вентильных схем, как правило, могут быть перестроены в методы оптимального синтеза аддитивных цепочек, и наоборот. А. Брауэр[75] установил асимптотику сложности аддитивных цепочек для случая $m = n = 1$ еще в 1939 г. Н. Пиппенджер[76] адаптировал к модели векторных аддитивных цепочек асимптотически оптимальный метод

[72] Орлов В. А. Реализация «узких» матриц вентильными схемами. Проблемы кибернетики. Вып. 22. М.: Наука, 1970, 45–52.

[73] Чашкин А. В. О сложности узких систем булевых функций. Дискретная математика. 1999. **11**(3), 149–159.

[74] Pippenger N. The minimum number of edges in graphs with prescribed paths. Math. System Theory. 1979. **12**, 325–346.

[75] Brauer A. On addition chains. Bull. AMS. 1939. **45**, 736–739.

[76] Pippenger N. On the evaluation of powers and monomials. SIAM J. Comput. 1980. **9**(2), 230–250.

синтеза вентильных схем. Затем уточнение верхней оценки было получено С. Б. Гашковым и В. В. Кочергиным[77]. Впоследствии В. В. Кочергин получил ряд обобщений, в частности, для класса матриц с индивидуальными ограничениями на размер каждого коэффициента[78, 79].

Автором диссертации доказываются следующие результаты.

Теорема 3.1 *(i) Пусть* $m \le n$, $m = \Omega\left(\log^{3/2} n\right)$ *и* $q = n^{o(1)}$. *Тогда*

$$L_3(q,m,n) \le (1+\tau(q,n))\frac{mn}{\log_q(mn)}, \qquad \tau(q,n) \asymp \sqrt{\frac{\log(q\log n)}{\log n}}.$$

(ii) Пусть дополнительно выполнено $q = \log^{O(1)} n$, $m = \Omega\left(\log^2 n\right)$ *и* $m \in n^{\mu}\log^{\pm O(1)} n$ *для некоторой постоянной* $\mu \in \mathbb{Q}$. *Тогда*

$$L_3(q,m,n) \le (1+\tau(n))\frac{mn}{\log_q(mn)}, \qquad \tau(n) \asymp \frac{\log\log n}{\log n}.$$

Теорема 3.2 *(i) Пусть* $m \le n$, $m = \Omega\left(\log^{3/2} n\right)$ *и* $q = o\left(n/\log^2 n\right)$. *Тогда*

$$L_4(q,m,n) \le (1+\tau(n))\frac{mn}{\log_q(mn)}, \qquad \tau(n) \asymp \sqrt{\frac{\log\log n}{\log n}}.$$

(ii) Пусть дополнительно $m = \Omega\left(\log^2 n\right)$ *и* $m \in n^{\mu}\log^{\pm O(1)} n$ *для некоторой постоянной* $\mu \in \mathbb{Q}$. *Тогда*

$$L_4(q,m,n) \le (1+\tau(n))\frac{mn}{\log_q(mn)}, \qquad \tau(n) \asymp \frac{\log\log n}{\log n}.$$

Теорема 3.3 *Пусть* $m \le n$, $H = mn\log q \to \infty$.

(i) Пусть $1 \le d \le \lfloor \log_3(q-1) \rfloor$. *Определим* $s_d = \lfloor \log_3(q-1) \rfloor - d$ *при* $d \ge \log_3(q-1)/2$ *и* $s_d = d-1$, *иначе. Тогда*

$$L_{d+3}(q,m,n) \le (1+\tau(H))\frac{H}{\log_2 H} + n + mq^{1/d}(\lfloor \log_3(q-1) \rfloor + s_d),$$

[77] Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней. Методы дискретного анализа в теории графов и сложности. Вып. 52. Новосибирск: ИМ СО РАН, 1992, 22–40.

[78] Кочергин В. В. О сложности вычисления систем одночленов с ограничениями на степени переменных. Дискретная математика. 1998. **10**(3), 27–34.

[79] Кочергин В. В. О сложности аддитивных вычислений. Диссертация на соискание ученой степени доктора физ.-мат. наук. М.: МГУ, 2008.

где $\tau(H) \asymp \sqrt{\frac{\log\log H}{\log H}}$.

(*ii*) *Пусть дополнительно выполнено условие* $n = \log^{O(1)} q$. *Тогда справедливо*

$$L_d(q, m, n) \leq 3m \log_3(q-1) + (1+\tau(H))\frac{H}{\log_2 H},$$

где $d = \lfloor \log_3 q + \sqrt{\log_3 q} \rfloor + 3$ *и* $\tau(H) \asymp \frac{\log\log H}{\log H}$.

Раздел 3.3 посвящен вопросу об экстремальных отношениях сложности булевой матрицы при реализации линейными схемами разных видов. Любой из введенных типов линейных схем позволяет вычислять булевы матрицы. Имеет место эффект Шеннона: почти все булевы матрицы имеют асимптотически одну и ту же сложность, одинаковую в каждой из трех моделей. Это не исключает того, что для некоторых матриц картина может быть иной. Естественно встает вопрос, насколько сильно может отличаться сложность реализации одной и той же матрицы разными видами схем. Сложность реализации матрицы A соответственно OR-, XOR- и SUM-схемами обозначаем через $\mathsf{OR}(A)$, $\mathsf{XOR}(A)$ и $\mathsf{SUM}(A)$, добавляя индекс d, если введено ограничение d на глубину схем.

Первая из задач о сравнительной силе линейных мер сложности была сформулирована и почти решена еще в работе Б. С. Митягина и Б. Н. Садовского[80] 1965 г., а именно, в ней был поставлен вопрос о максимуме отношения OR-сложности и XOR-сложности в классе булевых (n, n)-матриц без прямоугольников (сплошь единичных подматриц) размера 2×2. Однако активные исследования в области начались почти полвека спустя в результате совместных работ автора с С. Б. Гашковым[81] и М. И. Гринчуком[82]. Практически окончательное решение получила проблема Митягина—Садовского, а заодно аналогичные проблемы для класса циркулянтных матриц и всех (n, n)-матриц. Построены как конструктивные, так и неконструктивные примеры. Далее, в течение нескольких

[80]Митягин Б. С., Садовский Б. Н. О линейных булевских операторах. Доклады АН СССР. 1965. **165**(4), 773–776.

[81]Гашков С. Б., Сергеев И. С. О сложности линейных булевых операторов с редкими матрицами. Дискретный анализ и исследование операций. 2010. **17**(3), 3–18.

[82]Гринчук М. И., Сергеев И. С. Редкие циркулянтные матрицы и нижние оценки сложности некоторых булевых операторов. Дискретный анализ и исследование операций. 2011. **18**(5), 38–53.

лет последовала серия работ[83, 84, 85, 86] нескольких коллективов авторов, в которых помимо отношений сложности типа OR/XOR рассмотрены отношение типа SUM/OR, отношение OR-сложности матриц и их дополнений, в том числе, с ограничением на глубину схем. Промежуточные итоги развития теории подведены в соответствующей главе совместной с С. Юкной работы автора[87].

Автору диссертации принадлежит пример последовательности матриц с растущим отношением XOR- и OR-сложности в глубине 2 и примеры матриц с близким к максимальному возможному отношением OR-сложности к сложности дополнительной матрицы, в том числе, в ограниченной глубине. Часть перечисленных результатов доказывается с использованием конструкций экстремальных редких множеств — множеств, свободных от сумм $S + T$ с достаточно большими $|S|$ и $|T|$. Автором доказан результат, расширяющий область применения известных конструкций редких множеств.

Подмножество H полугруппы $(G, +)$ называется (k, l)-*редким*, если оно не содержит подмножеств вида $S + T = \{a + b \mid a \in S,\ b \in T\}$, где $|S| = k$ и $|T| = l$. Для краткости (k, k)-редкое подмножество называется k-редким. К понятию редкого множества близко понятие *редкой матрицы*. Булева матрица называется (k, l)-редкой, если она не содержит сплошь единичных подматриц размера $k \times l$. Для 2-редких матриц также принято название *матриц без прямоугольников*. Э. И. Нечипорук[88] доказал, что OR-сложность (k, l)-редкой (m, n)-матрицы A близка к ее весу $|A|$: $\mathsf{OR}(A) \geq \frac{|A|}{(k-1)(l-1)}$ и $\mathsf{OR}_2(A) \geq \frac{|A|}{\max\{k,l\}-1}$.

Хорошо известны 2-редкие множества в $\mathbb{Z}_n$ асимптотически экстремальной мощности $\sqrt{n}$, например, множество Зингера[89]. Также описаны некоторые конструкции экстремальных многомерных редких мно-

[83] Katz N. H. On the CNF-complexity of bipartite graphs containing no squares. Lithuanian Math. J. 2012. **52**(4), 385–389.

[84] Pinto T. Biclique covers and partitions. Electr. J. Combinatorics. 2014. **21**(1), 1–19.

[85] Boyar J., Find M. Cancellation-free circuits in unbounded and bounded depth. Theoret. Comput. Sci. 2015. **590**, 17–26.

[86] Find M., Göös M., Järvisalo M., Kaski P., Koivisto M., Korhonen J. H. Separating OR, SUM, and XOR circuits. J. Computer System Sci. 2016. **82**(5), 793–801.

[87] Jukna S., Sergeev I. Complexity of linear boolean operators. Foundations and Trends in Theoretical Computer Science. 2013. **9**(1), 1–123.

[88] Нечипорук Э. И. О самокорректирующихся вентильных схемах. Доклады АН СССР. 1964. **156**(5), 1045–1048.

[89] Singer J. A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 1938. **43**, 377–385.

жеств[90, 91, 92, 93] в группах $(GF(q)^n, +)$ или полугруппе $(N^n, +)$, где $N = \mathbb{N} \cup \{0\}$.

В ряде задач, однако, удобнее иметь дело с числовыми (одномерными) редкими множествами. Рассмотрим отображение $\psi_{q,s,t}$ из E_q^{st} в $E^s_{(2q-1)^t}$, переводящее вектор $(a_0, \ldots, a_{st-1})$ в вектор

$$\left(\sum_{i=0}^{t-1} a_i (2q-1)^i,\ \sum_{i=0}^{t-1} a_{t+i} (2q-1)^i, \ldots, \sum_{i=0}^{t-1} a_{(s-1)t+i} (2q-1)^i \right).$$

Теорема 3.5 *Если подмножество $M \subset E_q^{st}$ полугруппы $(N^{st}, +)$ является (k,l)-редким, то подмножество $\psi_{q,s,t}(M)$ полугруппы $(N^s, +)$ также является (k,l)-редким.*

А. Е. Андреев[94] первым построил пример матрицы экстремальной OR-сложности $n^{2-o(1)}$. Применение теоремы 3.5 к конструкции Я. Коллара, Л. Роньяи и Т. Сабо позволяет явно задать циркулянтную матрицу OR-сложности $n^{2-o(1)}$.

Следствие 3.4 *При любом n можно эффективно указать (k,l)-редкую циркулянтную матрицу порядка n и веса αn^2, где $k = O\left(\sqrt{\frac{\log n}{\log\log n}}\right)$, $l, \alpha^{-1} \in 2^{O(\sqrt{\log n \log\log n})}$.*

Далее приводятся несколько простых результатов об экстремальных отношениях OR-сложности и XOR-сложности булевых матриц: оценки для матриц без прямоугольников, отдельно — в ограниченной глубине, а также конструктивные оценки для класса всех булевых матриц.

Следствие 3.5 *Максимум отношения $\lambda(n) = \mathsf{OR}(A)/\mathsf{XOR}(A)$ по всем булевым (n, n)-матрицам без прямоугольников заключен в пределах:*

$$\sqrt{n}/\log^{1+o(1)} n \preceq \lambda(n) \preceq \sqrt{n},$$

причем нижняя оценка доказывается эффективно.

---

[90] Lindström B. Determination of two vectors from the sum. J. Comb. Theory. 1969. **6**, 402–407.

[91] Brown W. G. On graphs that do not contain a Thomsen graph. Canad. Math. Bull. 1966. **9**, 281–285.

[92] Гашков С. Б. Об одном методе получения нижних оценок сложности монотонных вычислений многочленов. Вестник Московского университета. Серия 1. Математика. Механика. 1987. №5, 7–13.

[93] Kóllar J., Rónyai L., Szabó T. Norm-graphs and bipartite Turán numbers. Combinatorica. 1996. **16**(3), 399–406.

[94] Андреев А. Е. Об одном семействе булевых матриц. Вестник Московского Университета. Серия 1. Математика. Механика. 1986. №2, 97–100.

Следствие 3.7 *Для $n \times n$ матрицы Зингера S_n выполняются соотношения*

$$\mathsf{OR}_4(S_n)/\mathsf{XOR}_4(S_n) \succeq \sqrt{\log n}, \qquad \mathsf{OR}_{2t-1}(S_n)/\mathsf{XOR}_{2t-1}(S_n) \succeq n^{1/2-1/t}$$

при $t \geq 3$.

Следствие 3.8 *Для некоторой явно заданной $n \times n$ матрицы A_n выполнено*

$$\mathsf{OR}(A_n)/\mathsf{XOR}(A_n) \succeq \frac{n}{\Delta}, \qquad \mathsf{OR}(A_n)/\mathsf{XOR}_{2t-1}(A_n) \succeq \frac{n^{1-1/t}}{\Delta}$$

при любом $t \in \mathbb{N}$, где $\Delta = 2^{\Theta(\sqrt{\log n \log\log n})}$.

Вопрос о существовании матриц с растущим отношением XOR- и OR-сложности остается открытым. Автором настоящей работы впервые построен пример последовательности матриц K_n с растущим отношением в глубине 2.

Теорема 3.9

$$\mathsf{OR}_2(K_n) \preceq n \cdot \frac{\log n}{\log\log n}, \qquad \mathsf{XOR}_2(K_n) \succeq n \cdot \frac{\log n \cdot \log\log\log n}{\log\log n}.$$

Кроме того, получены конструктивные оценки для отношений OR-сложности матрицы и ее дополнения.

Теорема 3.11 *Можно эффективно указать $n \times n$ матрицу A, для которой справедливо соотношение*

$$\mathsf{OR}_2(\overline{A})/\mathsf{OR}_2(A) \succeq \sqrt{n}2^{-\Theta(\log^{2/3} n)}.$$

Теорема 3.12 *(i) Для некоторой конкретно заданной булевой $n \times n$ матрицы C выполнено $\mathsf{OR}(\overline{C})/\mathsf{OR}(C) = n \cdot 2^{-O(\sqrt{\ln n \ln\ln n})}$.*

(ii) Для некоторой конкретно заданной булевой $n \times n$ матрицы C выполнено: $\mathsf{OR}(C) = O(n)$, матрица $\overline{C}$ является 2-редкой и $|\overline{C}| = \Omega(n^{4/3})$.

Главу закрывает раздел 3.4, в котором демонстрируется, как аппарат теории линейных схем помогает для сложности $C_{B_M}(T_n^2)$ реализации монотонной симметрической функции с порогом 2 монотонными схемами вывести оценки высокой точности. Тем самым решается проблема, поставленная еще в 1970-х гг Л. Адлеманом и П. Блониарцем[95], о сведении нижней и верхней оценок $\log_2 n - 4 < C_{B_M}(T_n^2) - 2n \leq 2\sqrt{n} + O(\sqrt[4]{n})$.

[95] Bloniarz P. A. The complexity of monotone Boolean functions and an algorithm for finding shortest paths in a graph. Ph.D. thesis. Tech. Report No. 238, Lab. for Computer Science, MIT, 1979.

Теорема 3.13 *Для* $n \in \mathbb{N}$ *выполнено* $C_{B_M}(T_n^2) > 2n + \sqrt{n/8 - 1/4} - 4$.

Таким образом, $C_{B_M}(T_n^2) = 2n + \Theta(\sqrt{n})$. Далее доказывается, что в классе схем глубины 3 (иначе говоря, $\vee\wedge\vee$-схем) известная верхняя оценка не может быть существенно улучшена. Через $C^{(3)}$ обозначен функционал сложности схем глубины 3.

Теорема 3.14 *Для* $n \in \mathbb{N}$ *выполнено* $C^{(3)}_{B_M}(T_n^2) \geq 2n + 2\sqrt{n+27} - 14$.

Как следствие, $C^{(3)}_{B_M}(T_n^2) = 2n + 2\sqrt{n} - O(1) + O(\sqrt[4]{n})$.

В **главе 4** изучается задача минимизации сложности параллельных префиксных схем. Пусть $\circ$ — бинарная ассоциативная операция на некотором множестве $\mathbf{G}$. Множество функций $x_1 \circ \ldots \circ x_i$, $1 \leq i \leq m$, называется системой *префиксов* (или *префиксных сумм*) упорядоченного набора переменных $x_1, \ldots, x_m$, принимающих значения в $\mathbf{G}$. Схемы из функциональных элементов над базисом $\{\circ\}$, реализующие систему префиксных сумм, называют *префиксными схемами*.

Задача оптимизации сложности префиксной схемы становится нетривиальной, если накладывается ограничение на глубину. Параллельные префиксные схемы используются в ряде приложений. В частности, на базе префиксных схем строятся эффективные схемы сумматоров чисел (префиксные сумматоры). Достоинством префиксных сумматоров является возможность балансирования различных характеристик схемы (сложности, глубины, ветвления элементов) за счет подбора конструкции опорной префиксной схемы.

Пусть $L(m)$ означает сложность минимальной универсальной, т.е. подходящей для вычислений в любой полугруппе $(\mathbf{G}, \circ)$, префиксной схемы m входов и глубины $\lceil \log_2 m \rceil$. Через $L(m, k)$ обозначим минимальную сложность префиксной схемы глубины $\lceil \log_2 m \rceil + k$.

Различные конструкции параллельных префиксных схем предлагались с конца 1950-х гг. Наиболее яркий результат получили Р. Ладнер и М. Фишер[96] около 1980 г., впервые получив линейную верхнюю оценку $L(m) \lesssim 4m$. Чуть позже Ф. Фич[97] уточнила эту оценку и доказала нетривиальную нижнюю оценку для случая $m = 2^n$:

$$\left(3\tfrac{1}{3} - o(1)\right) 2^n \leq L(2^n) \leq \left(3\tfrac{421}{792} - o(1)\right) 2^n.$$

Спустя 30 лет автору настоящей работы удалось установить точное значение сложности минимальной префиксной схемы $m = 2^n$ входов и

[96] Ladner R. E., Fischer M. J. Parallel prefix computation. J. ACM. 1980. **27**(4), 831–838.

[97] Fich F. E. New bounds for parallel prefix circuits. Proc. 15th Symp. on Theory of Comput. (Boston, 1983). NY: ACM, 1983, 100–109.

глубины n. Заодно было показано, что сложность схемы может быть понижена при дополнительных предположениях относительно операции $\circ$, в частности, для операции сложения по модулю 2 — эффект, видимо, ранее не замеченный.

Основная часть главы посвящена доказательству точной нижней оценки. Используется классификация элементов схемы: каркасные элементы (они составляют дерево, вычисляющее максимальный префикс), выходы схемы и прочие элементы, названные избыточными. По условию, число каркасных элементов и выходов фиксировано. Технически доказательство заключается в аккуратном подсчете числа избыточных элементов в локальных фрагментах схемы.

Элементу v, на выходе которого реализуется функция $x_i \circ \ldots \circ x_j$, ставится в соответствие метка $\lambda(v) = [i; j]$. Через S обозначается произвольная префиксная схема 2^n входов и глубины n. Необходимую информацию о распределении избыточных элементов предоставляет

Лемма 4.3 *Пусть $k, N, R \in \mathbb{N}$, $N < 2^k$ и $R < 2^{n-2k-1}$, R не является степенью двойки. Тогда в схеме S содержится не менее N избыточных элементов с правыми концами меток из интервала*

$$J_{N,R,k} = [N2^{n-k-1} + R2^k,\ N2^{n-k-1} + (R+1)2^k - 1].$$

Из леммы вытекает

Теорема 4.1 *Справедлива нижняя оценка сложности*

$$L(2^n) \geq 3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5.$$

Более того, лемма 4.3 помогает понять строение минимальных схем.

Теорема 4.2 *Справедлива верхняя оценка сложности*

$$L(2^n) \leq 3.5 \cdot 2^n - (8.5 + 3.5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5.$$

Вместе теоремы 4.1 и 4.2 определяют точное значение $L(2^n)$. Попутно для любых m получаются верхние оценки $L(m) \leq (3.5 - o(1))m$ и $L(m, k) \leq (2 + 2^{-k} - o(1))m$, где $1 \leq k \leq \lceil \log_2 m \rceil - 2$.

Лучшие верхние оценки получены для сложности префиксных XOR-схем, обозначаемой через $L^{\oplus}$. Последовательность σ_n определяется из рекуррентного соотношения $\sigma_n = 2\sigma_{n-3} + \sigma_{n-4} + 1$ с начальными условиями $\sigma_0 = \frac{25}{11}$, $\sigma_1 = \frac{39}{11}$, $\sigma_2 = \frac{56}{11}$, $\sigma_3 = \frac{79}{11}$. При этом $\sigma_n \asymp \chi^n$, где $\chi \approx 1.395$.

Теорема 4.4 *Справедлива верхняя оценка сложности*

$$L^{\oplus}(2^n) \leq 3\tfrac{3}{11} \cdot 2^n - \tau_n,$$

где

$$\tau_n = \frac{\sigma_{n+3} + \sigma_{n+2} + \sigma_{n+1} - \sigma_n - n - 7}{2}.$$

В общем случае доказаны оценки $L^{\oplus}(m) \leq \left(3\frac{3}{11} - o(1)\right) m$ и $L^{\oplus}(m,k) \leq \left(2 + \frac{3}{11} \cdot 4^{1-k} - o(1)\right) m$ при $1 \leq k \leq \lceil (\log_2 m)/2 \rceil - 1$.

В **главе 5** изучаются асимптотические вопросы синтеза схем и формул, использующих многовходовые функциональные элементы конъюнкции и дизъюнкции и либо элементы отрицания, либо отрицания переменных в качестве входов (в последнем случае вычислительные модели аналогичны схемам или формулам де Моргана; для них предложено название AC-схем и AC-формул). Указанные модели исследуются, в первую очередь, в направлении получения нижних оценок сложности индивидуальных функций при ограничении на глубину. Модель AC-схем используется при определении классов сложности AC^k. Значительное число результатов получено для расширений рассматриваемого базиса линейными, симметрическими, пороговыми или периодическими функциями и при ограничениях на глубину схем.

Сложность схемы определяется как число функциональных элементов в ней, *глубина* — как максимальное число элементов в ориентированном пути от входа к выходу схемы. Через $C_d(n)$ и $C(n)$ обозначим сложность реализации класса булевых функций n переменных (т.е. функцию Шеннона) AC-схемами глубины d и, соответственно, неограниченной глубины.

Дополнительно рассматриваются схемы над бесконечным базисом $U = \{x_1 \vee \ldots \vee x_k,\ x_1 \cdot \ldots \cdot x_k \mid k \in \mathbb{N}\} \cup \{^-\}$ (входами схем являются, как обычно, только булевы переменные). Для функций Шеннона сложности таких схем вводятся обозначения $C_d^U(n)$ и $C^U(n)$ в зависимости от вида ограничения на глубину. Принято соглашение, что при подсчете глубины пропускаются элементы отрицания.

Для функций Шеннона сложности схем над базисом U, в которых не учитываются элементы отрицания, вводятся обозначения $C_d^*(n)$ и $C^*(n)$. Такие схемы можно эквивалентным образом определить как схемы над бесконечным базисом $U^\infty = \{(x_1^{\alpha_1} \cdot \ldots \cdot x_k^{\alpha_k})^\beta \mid k \in \mathbb{N}; \alpha_i, \beta \in \{0, 1\}\}$ из обобщенных конъюнкций. (Через x^α обозначается булева степень: $x^1 = x$, $x^0 = \overline{x}$.)

Две последних модели введены для прояснения роли элементов отрицания в оптимальных методах синтеза. Из определений следуют соотношения $C^*(n) \leq C^U(n)$, $C^*(n) \leq C(n)$, $C^U(n) \leq C(n) + n$ (такие же соотношения имеют место при ограничении на глубину).

Под *формулами* понимаются схемы, в которых выходы функциональных элементов не имеют ветвлений. Для функций Шеннона слож-

ности AC-формул введем обозначения $L_d(n)$ и $L(n)$. Обозначим через $L_d^U(n)$ и $L^U(n)$ функции Шеннона сложности формул над базисом U. Понятие формулы с «бесплатными» отрицаниями по существу совпадает с понятием AC-формулы. Вследствие определения, $L(n) \leq L^U(n)$ и $L_d(n) \leq L_d^U(n)$. Принципиальным преимуществом AC-формул является отсутствие ограничений на ветвление отрицаний переменных.

Задача синтеза с глубиной 2 сводится к построению ДНФ или КНФ. Поэтому вопрос о поведении функций Шеннона становится содержательным в глубине 3 и выше.

Поведение функции Шеннона сложности в рассматриваемых моделях практически не изучалось. Лишь работа В. Данцика[98] специально посвящена получению оценок для функции Шеннона сложности схем с отрицаниями. Результаты имеют вид

$$1.914 \cdot 2^{n/2} \lesssim C^U(n) \lesssim C_3(n) \lesssim 2.122 \cdot 2^{n/2}, \qquad C_3(2m) \lesssim 2 \cdot 2^m.$$

Кроме того, оценки $C^*(n) \lesssim \sqrt{2} \cdot 2^{n/2}$ и $L(n) \lesssim 2^n/n$ (для сложности схем с «бесплатными» отрицаниями и AC-формул) вытекают из результатов Э. И. Нечипорука[99] о синтезе схем и формул в базисах с нулевыми весами элементов. Отметим, что для существенно более выразительной модели схем из пороговых элементов очень нетривиальный асимптотически точный результат[100] был доказан О. Б. Лупановым в 1970-е гг. Наконец, известна полученная О. М. Касим-Заде[101] универсальная верхняя оценка $O(2^{n/2})$ функции Шеннона сложности схем над произвольным бесконечным базисом.

Также отметим, что для родственной модели схем из многовходовых элементов конъюнкции и суммы по модулю 2 несколько результатов получены С. Н. Селезневой, в частности, установлен порядок функции Шеннона сложности $\oplus\wedge\oplus$-схем[102].

---

[98] Dančík V. Complexity of Boolean functions with unbounded fan-in gates. Inf. Proc. Letters. 1996. **57**, 31–34.

[99] Нечипорук Э. И. О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами. Проблемы кибернетики. Вып. 8. М.: Физматлит, 1962, 123–160.

[100] Лупанов О. Б. О синтезе схем из пороговых элементов. Проблемы кибернетики. Вып. 26. М.: Наука, 1973, 109–140.

[101] Касим-Заде О. М. Общая верхняя оценка сложности схем в произвольном бесконечном полном базисе. Вестник Московского университета. Серия 1. Математика. Механика. 1997. №4, 59–61.

[102] Селезнева С. Н. Порядок длины функций алгебры логики в классе псевдополиномиальных форм. Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2016. №3, 27–31.

Систематическое исследование поведения функций Шеннона сложности схем и формул с многовходовыми элементами дизъюнкции и конъюнкции было выполнено автором диссертации. В результате установлена асимптотика функции Шеннона сложности AC-схем, причем она достигается на схемах глубины 3. Кроме того, асимптотически точные результаты получены для других видов схем глубины 3 и формул глубины 4 с отрицаниями. Центральным местом в доказательстве верхних оценок является построение покрытий булева куба множествами специального вида, названными псевдосферическими.

В начале приводится вывод нижних оценок, выполняемый (за исключением леммы 5.4) стандартными мощностыми рассуждениями.

Лемма 5.1 *Справедливы оценки:*

$$L^U(n) \gtrsim 2^n/n, \quad L(n) \gtrsim \log_3 2 \cdot 2^n/n > 0.63 \cdot 2^n/n.$$

Лемма 5.2 *Имеет место соотношение:* $C(n) \gtrsim 2 \cdot 2^{n/2}$.

Лемма 5.3 *При любом постоянном* $d \geq 2$ *справедливо*

$$C^*_{d+1}(n) \gtrsim \sqrt{2d/(d-1)} \cdot 2^{n/2}.$$

Лемма 5.4 *Имеет место соотношение:* $C^U(n) \gtrsim 1.944 \cdot 2^{n/2}$.

Далее рассматриваются простые методы синтеза, эксплуатирующие известные идеи.

Теорема 5.1 *Справедлива верхняя оценка:* $L_4(n) \lesssim 2^n/n$.

Теорема 5.2 *Справедлива верхняя оценка:* $L^U_4(n) \lesssim 2^n/n$.

Теорема 5.3 *Справедлива верхняя оценка:* $C_4(n) \lesssim 2 \cdot 2^{n/2}$.

Эффективные методы синтеза схем и формул глубины 3 опираются на специальные разбиения (или покрытия) булева куба, обобщающие покрытие единичными сферами.

Рассмотрим множество A, в котором выбрано некоторое непустое подмножество B; элементы подмножества B называем *отметками*. Для вектора $b = (b_1, \ldots, b_n) \in (B \cup \{*\})^n$ определим множество векторов

$$A\langle^b_B = \{(a_1, \ldots, a_n) \in A^n \mid a_i = b_i, \text{ если } b_i \in B; a_i \notin B, \text{ если } b_i = *\} \subset A^n.$$

Другими словами, на позициях отметок вектора b векторы из $A\langle^b_B$ имеют такие же отметки, а на позициях звездочек — произвольные элементы из $A \setminus B$. Множество $S \subset A^n$ назовем (A,B)-*псевдосферическим*, если каждый вектор из S отличается от остальных значением отметки (т.е. элементом из B) в некоторой позиции.

Пусть $A\wr_B^{n,[h_1,\,h_2]}$ означает множество всех векторов из A^n, имеющих от h_1 до h_2 координат из подмножества B (отметок). Обозначим

$$E(h,q,t,s)=\sum_{k=\max\{0,\,h-q\}}^{t}\binom{t}{k}\binom{q-1}{h-1-k}s^k(s-1)^{h-1-k},$$

$$E([h_1,\,h_2],q,t,s)=\sum_{h=h_1}^{h_2}E(h,q,t,s).$$

Величины $E(h,q,t,s)$ определены при $s\geq 2$ и $h\leq q+t$, а также при $s=1$ и $h\leq t+1$.

Лемма 5.5 *Пусть $B\subset A$, $r\geq 0$, $1\leq h_1\leq h_2$ и либо $|B|=1$ и $h_2\leq t+1$, либо $|B|\geq 2$ и $h_2\leq q+t$. Пусть $\left|A\wr_B^{q+t,[h_1,\,h_2]}\times A^r\right|=M$. Тогда существует разбиение множества $A\wr_B^{q+t,[h_1,\,h_2]}\times A^r$ на*

$$M/q+E([h_1,\,h_2],q,t,|B|)\cdot\binom{q+t}{q}\cdot|B|^q$$

(A,B)-псевдосферических подмножеств мощности не более q.

Лемма позволяет строить разнообразные покрытия асимптотически оптимальной мощности. *Псевдосферой* называется множество двоичных наборов одинаковой длины, таких, что каждый набор имеет координату, значение которой отличает его от всех других наборов множества. Следующий результат усиливает известную оценку А. Е. Липатовой[103] в остаточном члене.

Следствие 5.1 *Куб $\mathbb{B}^n$ может быть покрыт $(1+O(\log n/n))\cdot 2^n/n$ псевдосферами.*

По аналогии, назовем *положительной* (*отрицательной*) *псевдополусферой* такую псевдосферу, в которой каждый набор имеет координату со значением 1 (соответственно, 0), отличающую его от остальных наборов псевдосферы.

Следствие 5.2 *Пусть $B=\{0\}$ или $B=\{1\}$. Тогда куб (с выколотой вершиной) $\mathbb{B}^n\setminus B^n$ может быть покрыт $(1+o(1))2^{n+1}/n$ псевдополусферами.*

В задаче синтеза AC-схем глубины 3 полезно иметь возможность разбиения булева куба или основной его части на $(1+o(1))2^n/q$ множеств

[103] Липатова А. Е. Об одном покрытии множества двоичных наборов и реализации конъюнкций контактными схемами. Математические вопросы кибернетики. Вып. 2. М.: Наука, 1989, 161–173.

мощности не более q, таких, что любой набор σ произвольного множества из разбиения обладает уникальным в рамках своего множества поднабором σ', при этом в каждом случае такой выделяющий поднабор может быть выбран из некоторого общего для всех множеств разбиения множества мощности $(1 + o(1))q$.

Следствие 5.3 *Пусть $B \subset A = \mathbb{B}^p$, $|B| = 1$, $q = p^2(2^{p-2} - 1)$, $t = p^2$. Тогда множество из $(1 - o(1/q))2^{p(q+t)}$ элементов куба A^{q+t} может быть покрыто $(1 + o(1))2^{p(q+t)}/q$ (A, B)-псевдосферическими подмножествами.*

Разбиения, предоставляемые указанными следствиями, позволяют вывести основные результаты о синтезе схем и формул глубины 3.

Теорема 5.4 *Для функции Шеннона сложности AC-формул глубины 3 справедливо соотношение: $L_3(n) \lesssim 2^n/n$.*

Теорема 5.5 *Функция Шеннона сложности формул глубины 3 над базисом U удовлетворяет соотношению: $L_3^U(n) \lesssim 2 \cdot 2^n/n$.*

Теорема 5.6 *Для функции Шеннона сложности AC-схем глубины 3 имеет место оценка: $C_3(n) \lesssim 2 \cdot 2^{n/2}$.*

В частности, ввиду $C(n) \sim C_3(n) \sim C_3^U(n) \sim C_3^*(n) \sim 2 \cdot 2^{n/2}$, вопрос о сложности AC-схем и схем глубины 3 в асимптотической постановке решен полностью.

В разделе 5.6 изложен авторский вариант доказательства асимптотически точной оценки функции Шеннона сложности схем с бесплатными отрицаниями (первый вариант извлекается в качестве следствия из результата Нечипорука).

Теорема 5.7 *Справедлива верхняя оценка: $C^*(n) \lesssim \sqrt{2} \cdot 2^{n/2}$.*

В **главе 6** рассматривается классическая задача сортировки набора из n элементов линейно упорядоченного множества при помощи попарных сравнений. Алгоритм сортировки можно изобразить в виде бинарного корневого дерева с ориентацией ребер в направлении от корня. Такое дерево обычно называется *деревом сравнений*, а также *деревом решений* или *решающей диаграммой*. Внутренняя вершина дерева соответствует операции сравнения некоторых двух элементов. В зависимости от результата сравнения алгоритм осуществляет переход по одному из ребер к следующей вершине. Концевая вершина (лист) дерева соответствует полученному в результате сравнений упорядочению входного набора. *Сложностью* алгоритма называется глубина дерева — максимальное расстояние в ребрах между корнем и листом.

Пусть $S(n)$ означает минимальную сложность алгоритма сортировки

n-элементного набора. Поскольку глубина дерева с m листьями не меньше $\log_2 m$, имеет место простая нижняя (теоретико-информационная) оценка

$$S(n) \geq \log_2(n!) = n \log_2 n - \log_2 e \cdot n + O(\log n),$$

где $\log_2 e \approx 1.443$. Более того, эта оценка действительна и для сложности сортировки в среднем по всем $n!$ возможным перестановкам входного набора.

Известный метод Форда—Джонсона[104] (метод бинарных вставок), предложенный более 60 лет назад, позволяет получить очень близкую к нижней верхнюю оценку сложности сортировки в виде

$$S(n) \leq \log_2(n!) + cn + O(\log n),$$

где $c < 0.12$. В нескольких разработанных позднее модификациях этого метода константа c в верхней оценке последовательно понижалась и по итогам работы Г. Манахера, Т. Буи, Т. Маи[105] имела величину в районе 0.07. Для средней сложности сортировки по всем перестановкам входного набора известные к 2020 г. верхние оценки[106] имели такой же вид, но с меньшими константами $c < 0.032$.

По существу, алгоритм Форда—Джонсона представляет собой последовательность однотипных процедур вставки элемента в линейно упорядоченное множество. Вставка выполняется бинарным методом: вставляемый элемент сравнивается со срединным элементом целевого множества, затем — со срединным элементом в половине множества, определенной результатом первого сравнения, и т. д. Эффективность алгоритма обеспечивается путем подбора целевых множеств с оптимальными значениями мощности $2^k - 1$.

С другой стороны, известно, что совместная вставка нескольких элементов может быть выполнена быстрее, чем раздельная. Например, если мощность m целевого множества находится в пределах $2^k < m < \frac{17}{14} \cdot 2^k - 1$, то при вставке двух элементов можно сэкономить одно сравнение относительно бинарного метода[107, 108]. Еще выгоднее может быть группировка

[104] Ford L. R., Johnson S. M. A tournament problem. Amer. Math. Monthly. 1959. **66**(5), 387–389.

[105] Manacher G. K., Bui T. D., Mai T. Optimum combinations of sorting and merging. J. ACM. 1989. **36**(2), 290–334.

[106] Iwama K., Teruyama J. Improved average complexity for comparison-based sorting. Theor. Comput. Sci. 2020. **807**, 201–219.

[107] Graham R. L. On sorting by comparisons. Computers in Number Theory. London: Academic Press, 1971, 263–269.

[108] Hwang F. K., Lin S. Optimal merging of 2 elements with n elements. Acta Inf. 1971. **1**, 145–158.

элементов по 4 или 5 с последующей их сортировкой до вставки[109].

В развитие этой идеи, в диссертационной работе предложен алгоритм групповой вставки большого числа элементов, организованный в некотором смысле как система массового обслуживания. Предназначенные для вставки элементы обрабатываются упорядоченными парами по очереди. В какой-то момент после серии сравнений пара может быть разбита, если, например, выясняется, что ее элементы попадают в непересекающиеся подмножества (интервалы) целевого множества; далее элементы пары обрабатываются по отдельности. Одиночный элемент либо вставляется в свой интервал бинарным методом, когда это выгодно, либо помещается во временное хранилище — контейнер. Как только в контейнере оказываются два элемента, из них формируется новая пара и выполняется ее обработка. Алгоритм использует множество контейнеров, относящихся к различным интервалам. В самом конце оставшиеся в контейнерах одиночные элементы вставляются в целевое множество бинарным методом.

На этом пути сложность вставки m элементов в множество мощности $n \gg m$ удается приблизить к теоретико-информационной нижней границе, т. е. $m(\log_2 n + o(1))$. Более точно, пусть $P_m(a)$ обозначает максимальное число n, при котором сложность вставки m упорядоченных пар в упорядоченный набор длины $n-1$ не превосходит $2am$.

Теорема 6.1 *При любом $a \geq 2$ и $2^{a/4} \leq m \leq 2^{a/2}$ выполнено*

$$P_m(a) \geq 2^{a+1/2} - O\left(a^{-\gamma} \cdot 2^a\right),$$

где γ мало, например, $\gamma = \frac{1}{5}$.

Как следствие, метод сортировки при помощи групповых вставок приводит к следующей оценке.

Теорема 6.2 *При любых n выполняется*

$$S(n) = \log_2(n!) + O\left(n \log^{-1/5} n\right).$$

Конечно, оценка справедлива и для средней сложности сортировки.

В **Заключении** перечислены основные результаты диссертации и указаны возможные направления для дальнейших исследований.

Заключение

В диссертации предложены методы решения проблем оптимального синтеза схем и формул при ограничении на глубину, минимизации глубины вычислений, построения быстрых параллельных алгоритмов.

[109] Schulte Mönting J. Merging of 4 or 5 elements with n elements. Theor. Comput. Sci. 1981. **14**, 19–37.

На защиту выносятся обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также основные результаты работы, перечисленные в заключении диссертации:

— нижняя оценка константы равномерности монотонного булева базиса;

— методы синтеза эффективных по глубине или сложности формул для симметрических булевых функций, основанные на применении модулярной арифметики и приближенного суммирования;

— метод синтеза эффективных по глубине или сложности формул для элементарных периодических симметрических функций, основанный на сведении к задаче о покрытии;

— метод доказательства нижних оценок сложности функций при реализации формулами в k-арном базисе, основанный на применении специальных мер сложности двудольных графов;

— решение задачи об асимптотически оптимальном синтезе вентильных схем глубины 3 в общем случае;

— результат о возможности эффективного погружения многомерных редких множеств в пространства меньшей размерности;

— пример последовательности булевых матриц с растущим отношением XOR- и OR-сложности в глубине 2; метод построения примеров последовательности булевых матриц с почти экстремальным отношением OR-сложности к сложности дополнительных матриц;

— точное значение сложности минимальной универсальной префиксной схемы глубины n на 2^n входах; верхние оценки сложности префиксных схем при различных ограничениях на глубину, и отдельно для префиксных XOR-схем;

— метод оптимального синтеза схем и формул глубины 3 из многовходовых элементов (типа конъюнкций, дизъюнкций) и отрицаний, основанный на построении специальных покрытий булева куба;

— решение задачи о сортировке за минимальное число сравнений в асимптотическом смысле с высокой точностью.

Работы автора по теме диссертации, опубликованные в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 01.01.06 — математическая логика, алгебра и теория чисел — и входящих в базы цитирования Scopus, Web of Science и RSCI

1. Гашков С. Б., Сергеев И. С. О сложности линейных булевых операторов с редкими матрицами. Дискретный анализ и исследование операций. 2010. **17**(3), 3–18. Journal of Applied and Industrial Mathematics. 2011. **5**(2), 202–211. [Scopus SJR 2019: 0.2]

2. Гринчук М. И., Сергеев И. С. Редкие циркулянтные матрицы и нижние оценки сложности некоторых булевых операторов. Дискретный анализ и исследование операций. 2011. **18**(5), 38–53. [РИНЦ 2019: 0.245]

3. Сергеев И. С. О минимальных параллельных префиксных схемах. Вестник Московского университета. Серия 1. Математика. Механика. 2011. №5, 48–51. Moscow University Mathematics Bulletin. 2011. **66**(5), 215–218. [Scopus SJR 2019: 0.2]

4. Гашков С. Б., Сергеев И. С. Об одном методе получения нижних оценок сложности монотонных арифметических схем, вычисляющих действительные многочлены. Математический сборник. 2012. **203**(10), 33–70. Sbornik: Mathematics. 2012. **203**(10), 1411–1447. [WoS 2019: 0.8; Scopus SJR 2019: 0.39]

5. Сергеев И. С. Верхние оценки глубины симметрических булевых функций. Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2013. №4, 39–44. Moscow University Computational Mathematics and Cybernetics. 2013. **37**(4), 195–201. [Scopus SJR 2019: 0.15]

6. Сергеев И. С. Верхние оценки сложности формул для симметрических булевых функций. Известия высших учебных заведений. Математика. 2014. №5, 38–52. Russian Mathematics. 2014. **58**(5), 30–42. [Scopus SJR 2019: 0.4]

7. Сергеев И. С. О сложности и глубине формул для симметрических булевых функций. Вестник Московского университета. Серия 1. Математика. Механика. 2016. №3, 53–57. Moscow University Mathematics Bulletin. 2016. **71**(3), 127–130. [Scopus SJR 2019: 0.2]

8. Сергеев И. С. Верхние оценки сложности и глубины формул для MOD-функций. Дискретная математика. 2016. **28**(2), 108–116. Discrete Mathematics and Applications. 2017. **27**(1), 15–22. [Scopus SJR 2019: 0.16]

9. Сергеев И. С. Вентильные схемы ограниченной глубины. Дискретный анализ и исследование операций. 2018. **25**(1), 120–141. Journal of Applied and Industrial Mathematics. 2018. **12**(1), 153–166. [Scopus SJR 2019: 0.2]

10. Сергеев И. С. О сложности схем и формул ограниченной глубины над базисом из многовходовых элементов. Дискретная математика.

2018. **30**(2), 120–137. Discrete Mathematics and Applications. 2019. **29**(4), 241–254. [Scopus SJR 2019: 0.16]

11. Сергеев И. С. О соотношении между глубиной и сложностью монотонных булевых формул. Дискретный анализ и исследование операций. 2019. **26**(4), 108–120. Journal of Applied and Industrial Mathematics. 2019. **13**(4), 746–752. [Scopus SJR 2019: 0.2]

12. Сергеев И. С. О сложности монотонных схем для пороговых симметрических булевых функций. Дискретная математика. 2020. **32**(1), 81–109. [РИНЦ 2019: 0.447]

13. Сергеев И. С. Многоярусное представление и сложность схем из многовходовых элементов. Вестник Московского университета. Серия 1. Математика. Механика. 2020. №3, 42–46. Moscow University Mathematics Bulletin. 2020. **75**(3), 121–125. [Scopus SJR 2019: 0.2]

14. Сергеев И. С. О верхней границе сложности сортировки. Журнал вычислительной математики и математической физики. 2021. **61**(2), 345–362. Computational Mathematics and Mathematical Physics. 2021. **61**(2), 329–346. [WoS 2019: 0.565; Scopus SJR 2019: 0.51]

15. Сергеев И. С. Формульная сложность линейной функции в k-арном базисе. Математические заметки. 2021. **109**(3), 419–435. Mathematical Notes. 2021. **109**(3), 445–458. [WoS 2019: 0.626; Scopus SJR 2019: 0.37]

16. Jukna S., Sergeev I. Complexity of linear boolean operators. Foundations and Trends in Theoretical Computer Science. 2013. **9**(1), 1–123. [Scopus SJR 2019: 1.33]

Работы [1–15] опубликованы в изданиях из базы данных RSCI.

В совместной работе [1] автору принадлежат примеры из §§2–3, отвечающие на основной вопрос, и их анализ. В работе [2] автору принадлежит технический результат §3, а также следствия 3 и 4. В работе [4] автору принадлежат лемма 13, теорема 4 и следствия из них (следствие 1, теорема 5 в общей формулировке). В работе [16] автору принадлежат результат §5.5 и пример в конце §5.6.