

УДК 519.1, 519.7

КАФЕДРА ДИСКРЕТНОЙ МАТЕМАТИКИ

В. В. Кочергин¹, Н. П. Редькин², С. Б. Гашков³, А. В. Чашкин⁴, Р. М. Колпаков⁵, М. Д. Ковалёв⁶,
Ю. В. Таранников⁷, О. С. Дудакова⁸, Ю. А. Комбаров⁹, М. В. Старостин¹⁰, С. А. Корнеев¹¹

В статье о кафедре дискретной математики механико-математического факультета МГУ имени М. В. Ломоносова рассказывается об истории кафедры, затронуты вопросы трактовки самого термина «дискретная математика», становления и быстрого развития дискретной математики в современном понимании. Кроме того, представлен обзор основных полученных в последнее время на кафедре дискретной математики результатов в области теории схемной сложности и сложности вычислений, теории дискретных функций и функциональных систем, комбинаторике, теории графов, дискретной геометрии и в других разделах дискретной математики.

Ключевые слова: дискретная математика, математическая кибернетика, теория гра-

¹ Кочергин Вадим Васильевич — доктор физ.-мат. наук, зав. каф. дискретной математики мех.-мат. ф-та МГУ; e-mail: vvkoch@yandex.ru.

Kochergin Vadim Vasil'evich — Doctor of Physical and Mathematical Sciences, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Head of Chair of Discrete Mathematics.

² Редькин Николай Петрович — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: npredkin@mail.ru.

Red'kin Nikolay Petrovich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

³ Гашков Сергей Борисович — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: sbgashkov@gmail.com.

Gashkov Sergey Borisovich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁴ Чашкин Александр Викторович — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: chashkin@inbox.ru.

Chashkin Alexandr Viktorovich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁵ Колпаков Роман Максимович — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: foroman@mail.ru.

Kolpakov Roman Maximovich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁶ Ковалёв Михаил Дмитриевич — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: mkov@rambler.ru.

Kovalyov Mikhail Dmitrievich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁷ Таранников Юрий Валерьевич — доктор физ.-мат. наук, доц. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: yutarann@gmail.com.

Tarannikov Yuriy Valer'evich — Doctor of Physical and Mathematical Sciences, Associate Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁸ Дудакова Ольга Сергеевна — кандидат физ.-мат. наук, доц. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: olga.dudakova@gmail.com.

Dudakova Olga Sergeevna — Candidate of Physical and Mathematical Sciences, Associate Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

⁹ Комбаров Юрий Анатольевич — кандидат физ.-мат. наук, доц. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: yuri.kombarov@gmail.com.

Kombarov Yuriy Anatol'evich — Candidate of Physical and Mathematical Sciences, Associate Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

¹⁰ Старостин Михаил Васильевич — кандидат физ.-мат. наук, асс. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: murmol@bk.ru.

Starostin Mikhail Vasil'evich — Candidate of Physical and Mathematical Sciences, Assistant, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

¹¹ Корнеев Сергей Александрович — кандидат физ.-мат. наук, асс. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: korneev.sa.42@gmail.com.

Korneev Sergey Alexandrovich — Candidate of Physical and Mathematical Sciences, Assistant, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

фов, комбинаторика, схемная сложность, функциональная система, дискретная геометрия.

The article about the Department of Discrete Mathematics of the Faculty of Mechanics and Mathematics of Lomonosov Moscow State University discusses the questions of interpretation of the term "discrete mathematics the formation and rapid development of discrete mathematics in the modern sense, and also provides information about the history of the department. In addition, a brief overview of the main recent results obtained at the Department of Discrete Mathematics in the field of the theory of circuit complexity and computational complexity, the theory of discrete functions and functional systems, combinatorics, graph theory, discrete geometry and other areas of discrete mathematics is presented.

Key words: discrete mathematics, mathematical cybernetics, graph theory, combinatorics, circuit complexity, functional system, discrete geometry.

Дискретная математика — это та часть математики, которая изучает математические объекты, системы и процессы дискретного характера. Такими объектами являются, например, натуральные числа, двоичные слова (битовые строки), конечные множества элементов любой природы и многое другое. В дискретной математике много красивых математических задач, формулируемых чрезвычайно просто, но зачастую весьма трудных для решения. Возникновение дискретной математики относится к глубокой древности. Уже тогда приходилось решать трудные комбинаторно-логические задачи, разрабатывать эффективные алгоритмы выполнения арифметических действий, решать уравнения в целых числах, зашифровывать и расшифровывать секретные сообщения.

К дискретной математике (в широком смысле) можно относить не только такие направления как комбинаторный анализ, теория графов, математическая логика, дискретная геометрия, но и многие разделы алгебры, теории чисел, теории вероятностей и других областей математики.

Становление дискретной математики в современном виде и ее бурное развитие началось в середине XX века и связано с созданием различных дискретных устройств, развитием вычислительной, телекоммуникационной и электронно-цифровой техники, ее необыкновенно быстрым внедрением практически во все области нашей жизни. Современные компьютеры представляют собой устройства дискретного действия, основанные на цифровых формах представления информации, и для их применения наиболее естественно использование дискретных математических моделей. Возникло огромное число важнейших задач, связанных с описанием и оптимизацией работы электронных цифровых машин, коммуникационных сетей и относящихся к ним алгоритмов и программ. Проектирование современных вычислительных устройств и их применение давно уже немыслимы без использования аппарата дискретной математики и тесно примыкающей к ней научной дисциплины — математической кибернетики, изучающей процессы управления, управляющие системы и связанные с ними математические модели передачи и обработки информации в живой природе и технике.

Под влиянием потребностей практики в дискретной математике возникли новые области: теория дискретных функций, теория автоматов, теория кодирования, теория сложности вычислений, надежность, контроль и диагностика управляющих систем, теория функциональных систем, теория дискретных экстремальных задач и многие другие. Модели и методы дискретной математики имеют фундаментальное значение для информатики и компьютерных наук, широко используются в области информационных технологий. Дискретная математика имеет важнейшие приложения в естественных, технических и социальных науках, в частности, в статистической и квантовой физике, генетике и биоинформатике, экологии, экономике и социологии.

За несколько десятилетий доля дискретной математики в общем потоке мировых математических исследований выросла многократно.

Дискретная математика в Московском университете имеет длительную историю и давние традиции, восходящие к XIX в. В 1930-х гг. в МГУ В. И. Шестаков одним из первых в мире (по-видимому, раньше и американского инженера и ученого К. Э. Шеннона, и группы японских инженеров) применил аппарат алгебры логики к описанию работы дискретных электромеханических устройств — релейно-контактных схем, являвшихся основой вычислительной техники тех лет. Начиная с 1950-х гг. Московский университет становится одним из крупнейших мировых центров дискретной математики и математической кибернетики. С этого времени в МГУ не только ведутся регулярные целенаправленные исследования в этой области, но и начинается систематическая подготовка специалистов по дискретной математике.

Кафедра дискретной математики образована на механико-математическом факультете МГУ в 1981

году. Основателем кафедры и ее первым заведующим был академик Олег Борисович Лупанов (1932–2006), выдающийся математик, один из создателей современной дискретной математики и математической кибернетики, автор основополагающих научных результатов в этой области, руководитель большой научной школы. В 2006–2020 гг. кафедрой заведовал Октай Мурадович Касим-Заде (1953–2020). С 2021 г. кафедру дискретной математики возглавляет Вадим Васильевич Кочергин.

В штатном составе кафедры 6 профессоров, 7 докторов наук. На кафедре ведётся активная научная работа по основным направлениям современной дискретной математики и математической кибернетики. К числу приоритетных направлений относятся:

- теория графов;
- комбинаторный анализ;
- теория сложности;
- синтез управляющих систем;
- теория надёжности и контроля управляющих систем;
- теория кодирования;
- математические вопросы криптологии;
- дискретная геометрия;
- анализ алгоритмов;
- теория булевых функций;
- дискретная оптимизация;
- многозначные логики;
- вычисления и автоматы;
- некоторые другие.

Сотрудники кафедры ведут на механико-математическом факультете обязательные занятия по теории дискретных функций и дискретной математике, читают большое число специальных курсов лекций по основным направлениям дискретной математики и математической кибернетики, руководят научной работой студентов и аспирантов, на кафедре работают научно-исследовательские и учебные специальные семинары.

За последние 4 года штатными и внештатными сотрудниками кафедры защищено 4 докторские диссертации.

В разное время сотрудники кафедры принимали участие в прикладных исследованиях и разработках по темам: логический синтез интегральных электронных схем, быстрые вычисления в конечных полях, словарная комбинаторика и алгоритмы на словах, автоматический анализ и обработка естественно-языковых текстов, структура и геометрические свойства плоских шарнирно-рычажных механизмов, распространение электромагнитных волн в плоских диэлектрических волноводах, математические методы анализа социологической информации и другим.

Дополнительную информацию о кафедре дискретной математики можно найти в сети Интернет по адресу <http://new.math.msu.su/departament/dm/>.

Тематика направлений научных исследований, проводимых на кафедре, в немалой степени определяется принадлежностью большинства сотрудников к научной школе О. Б. Лупанова. Несмотря на то, что практически все основополагающие результаты Олега Борисовича относятся к одному из направлений дискретной математики и математической кибернетики — синтезу и сложности схем, многоплановость как исходных решаемых проблем, так и возникающих при их решении вспомогательных задач, разнообразие применяемых методов, а также необычайно широкий спектр задач, ставившихся перед учениками, способствовали значительным продвижениям в большинстве разделов дискретной математики.

Еще в конце 50-х гг. прошлого века два фундаментальных результата О. Б. Лупанова — построение для почти всех функций алгебры логики асимптотически наилучших булевых схем (схем из функциональных элементов) в произвольном полном конечном базисе и решение «проблемы Шеннона», заключавшейся

в устранении четырехкратного разрыва между верхней и нижней оценками минимального числа контактов, достаточного для реализации контактной схемой произвольной булевой функции от заданного числа переменных, — заложили основу тесно связанного с практическими потребностями исследования математических моделей вычислительной, телекоммуникационной, а позднее и всей цифровой техники нового научного направления — асимптотической теории синтеза и сложности управляющих систем.

К этому направлению относятся разработанные О. Б. Лупановым асимптотически оптимальные методы синтеза вентильных схем глубины 2, контактно-вентильных схем, схем из функциональных элементов без ветвления выходов элементов (формул) и с ограниченным ветвлением выходов элементов (формул с частичной памятью), формул ограниченной глубины, параллельно-последовательных контактных схем, релейно-контактных схем и др. Олегом Борисовичем был развит общий метод получения «мощностных» нижних оценок и установлено, что во многих случаях расширение запаса используемых средств не приводит к существенному уменьшению сложности схем достаточно общего вида. О. Б. Лупановым было обнаружено явление, названное им эффектом Шеннона, заключающееся в том, что почти все функции имеют почти одинаковую сложность, асимптотически равную сложности самой сложной функции. Оказалось, что этот эффект имеет место для большинства исследуемых модельных классов управляющих систем.

Важнейшее значение имеет предложенный и обоснованный Олегом Борисовичем весьма общий подход к синтезу управляющих систем — принцип локального кодирования, ставший крупным вкладом в дискретную математику и математическую кибернетику, существенно углубивший понимание закономерностей синтеза и изменившим некоторые представления о сути понятия сложности. В нем тесно переплелись теоретическая математика, практические приложения и некоторые аспекты философского характера. С использованием принципа локального кодирования самим О. Б. Лупановым, его учениками и последователями установлено большое количество асимптотически точных оценок для различных классов и разных управляющих систем.

Кафедра дискретной математики бережно хранит и развивает традиции научной школы О. Б. Лупанова. Многие сотрудники кафедры являются учениками Олега Борисовича (С. Б. Гашков, А. В. Чашкин, В. В. Кочергин, Ю. В. Таранников и Н. П. Редькин) или учениками его учеников (Р. М. Колпаков и О. С. Дудакова — ученики А. Б. Угольников, Ю. А. Комбаров — ученик Н. П. Редькина, М. В. Старостин — ученик О. М. Касим-Заде, С. А. Корнеев — ученик В. В. Кочергина).

Большой организационный и научно-педагогический вклад в становление и развитие кафедры дискретной математики внесли ученики О. Б. Лупанова О. М. Касим-Заде и А. Б. Угольников (1951–2013). В частности, О. М. Касим-Заде разработан общий подход к получению оценок сложности схем над бесконечными базисами, позволивший оценивать функцию Шеннона с точностью до полиномиальной эквивалентности; полностью решен вопрос об асимптотике функции Шеннона глубины схем над бесконечными базисами; разработана асимптотическая теория сложности неявных и параметрических представлений булевых функций и на ее основе решен ряд известных открытых проблем; исследованы основные энергетические меры сложности схем из функциональных элементов — мощность и активность схем, полностью описана качественная картина их асимптотического поведения; решена проблема А. В. Кузнецова о неявной выразимости в двузначной логике; получен критерий неявной полноты во всех конечнозначных логиках, найдено точное решение комбинаторной задачи покрытия n -мерного булева куба центрированными антицепями, получены серьезные продвижения в исследовании проблемы Заранкевича — одной из важнейших экстремальных задач комбинаторного анализа и теории графов. А. Б. Угольников установил для произвольного полного базиса асимптотику роста схемной сложности класса монотонных булевых функций, а также других нетривиальных замкнутых классов, получил значительные продвижения в задаче о схемной и формульной сложности замкнутых классов в неполных и вырожденных базисах, доказал рекордную нижнюю оценку формульной сложности конкретных последовательностей функций многозначной логики, установил равномерность по сложности и глубине всех конечных базисов булевых функций и существование неравномерных базисов функций многозначной логики, заложил фундамент для получения его многочисленными учениками интересных результатов в области теории функциональных систем.

Также стоит отметить основополагающие работы С. С. Рышкова (1930–2006) в области теории точечных решеток (геометрии положительных квадратичных форм) и теории параллелоэдров — выпуклых многогранников, параллельными копиями которых можно без наложений замостить евклидово пространство заданной размерности. С. С. Рышкова пригласил на кафедру дискретной математики вскоре после ее образования лично О. Б. Лупанов, считавший, что на кафедре обязательно должна присутствовать и геометрическая составляющая. В настоящее время это направление — «дискретная геометрия» — на кафедре представляет М. Д. Ковалев, ученик С. С. Рышкова.

Далее прилагаются краткие описания основных полученных на кафедре дискретной математики в

последнее время результатов, подготовленные на основе материалов самих авторов.

Зав. кафедрой В. В. Кочергин. Исследования различных обобщений классической задачи о сложности возведения в степень, т. е. задачи нахождения величины $l(x^n)$ — минимального числа операций умножения, достаточного для вычисления по переменной x величины x^n (результаты промежуточных вычислений могут использоваться многократно), в аддитивной постановке называемой задачей об аддитивных цепочках — одно из основных направлений научной работы В. В. Кочергина.

Для двух известных обобщений задачи об эффективном возведении в степень — задачи Р. Беллмана о сложности вычисления одночлена от m переменных, т. е. нахождения величины $l(x_1^{n_1} x_2^{n_2} \dots x_m^{n_m})$, и задачи Д. Кнута о сложности вычисления набора из m степеней одной переменной, т. е. нахождения величины $l(x^{n_1}, x^{n_2}, \dots, x^{n_m})$, им получены асимптотически точные решения.

Получен ряд асимптотически точных оценок сложности для трех следующих вычислительных задач; 1) задача Пиппендэжера о сложности вычисления системы одночленов от нескольких переменных; 2) задача об аддитивной сложности системы линейных форм (для этой задачи получено окончательное асимптотически точное решение); 3) некоммутативный аналог задачи Беллмана — задача о сложности сборки слов схемами конкатенации; 4) задача вычисления систем элементов свободных абелевых групп; 5) задача Лупанова о сложности вычисления элементов конечных абелевых групп (подробнее об этих и других обобщениях задачи об эффективном возведении в степень см., например, сборник «Математические вопросы кибернетики», вып. 20).

В. В. Кочергиным также рассматривалась задача о нахождении наименьшего числа дуг в ориентированном графе без ориентированных циклов с двумя группами выделенных вершин — входами и выходами, в котором число путей от каждого входа к каждому выходу задано целочисленной матрицей с неотрицательными элементами. Для этой задачи найдено асимптотически точное решение в случае, когда либо число входов, либо число выходов не превышает трех.

В области исследования сложности классических логических схем стоит выделить цикл совместных с А. В. Михайлович работ, посвященных немонотонной сложности булевых функций и функций многозначной логики. В этих работах, во-первых, обобщен известный результат А. А. Маркова об инверсионной сложности (минимального для реализации числа отрицаний) булевых функций — для произвольного базиса, состоящего из всех монотонных булевых функций и конечного множества немонотонных функций и для любой булевой функции найдена немонотонная сложность, т. е. минимальное число немонотонных элементов, достаточное для реализации этой функции схемой в заданном базисе; во-вторых, установлены точные значения инверсионной сложности произвольной системы функций многозначной логики над двумя естественными базисами B_P и B_L , состоящими из всех монотонных относительно порядка $0 < 1 < \dots < k-1$ функций k -значной логики и отрицания Поста или Лукасевича соответственно; в-третьих, для произвольной функции k -значной логики доказаны отличающиеся не более чем на 3 верхние и нижние оценки обычной сложности, понимаемой как общее число элементов в схеме, при реализации над базисами B_P и B_L ; в-четвертых, для произвольной функции многозначной логики и произвольного базиса описанного вида установлено значение немонотонной сложности с точностью до небольшой константы, не зависящей от базиса.

Проф. Н. П. Редькин. Н. П. Редькиным предложено обобщение классического понятия схемной сложности булевой функции. Под обобщенной сложностью понимается величина, в отличие от классической сложности не зависящая от базиса и определяемая как верхняя грань сложностей функции, где верхняя грань берется по всем функционально полным базисам, а сложность схем определяется числом функциональных элементов в них. Найдены точные значения обобщенной сложности нескольких важнейших булевых функций. Установлено, что обобщенная сложность конъюнкции $x_1 x_2 \dots x_n$ равна $3(n-1)$ при $n \geq 3$ и четырем при $n = 2$. Также доказано, что обобщенная сложность линейных функций $x_1 \oplus \dots \oplus x_n$ и $x_1 \oplus \dots \oplus x_n \oplus 1$ равна $7(n-1)$ при $n \geq 2$ и трем при $n = 1, 0$ (формально случай $n = 0$ соответствует булевым константам).

Н. П. Редькиным изучалась сложность реализации булевых функций, существенно зависящих от n переменных и обращающихся в единицу на k наборах значений переменных. В важном для практики случае малых относительно n значений параметра k (например, при $k < \ln n$) найдена асимптотика (при растущем n) сложности реализации рассматриваемых функций схемами в некоторых естественных базисах. При этом установлено, что сложность реализации функций зависит не только от параметров k и n , но еще и от некоторых свойств реализуемых функций, и раскрыт характер зависимости.

Для еще одного класса управляющих систем — контактных схем — Н. П. Редькиным установлена сложность реализации характеристических функций сфер и монотонных симметрических пороговых функций.

Значительные продвижения получены при исследовании следующей важнейшей проблемы. При про-

ектировании и построении достаточно сложных схем, содержащих большое количество элементов, приходится учитывать то реальное обстоятельство, что отдельные физические элементы обладают ограниченной надежностью. Возникает некоторая задача построения из не вполне надежных элементов достаточно надежных схем. Один из подходов к решению этой задачи опирается на принцип самокорректирования схем. При использовании этого принципа приходится оценивать сложность проектируемых схем, и особые трудности на этом этапе вызывает получение достаточно точных нижних оценок сложности получающихся самокорректирующихся схем. Для решения этой задачи Н. П. Редькин предложил метод замены базиса. Этот метод позволяет использовать известные нижние оценки сложности самокорректирующихся схем в достаточно простых базисах и на этой основе получать новые достаточно точные (вплоть до асимптотически точных) новые оценки сложности для схем в более сложных базисах.

В области диагностики управляющих систем Н. П. Редькиным получен следующий фундаментальный результат. Установлено, что любую булеву функцию можно реализовать схемой из функциональных элементов в произвольном функционально полном базисе, которая при инверсных неисправностях на выходах элементов допускает единичный проверяющий тест не более чем из трех входных наборов. Этот результат базируется на предложенном методе расширения базисов, который оказался востребованным при получении (разными авторами) новых фундаментальных результатов по диагностике и сложности схем из функциональных элементов.

Проф. С. Б. Гашков. В области изучения сложности вычисления непрерывных функций с помощью алгебраических операций с действительными числами, в случае, когда в качестве базиса берется множество арифметических или алгебраических операций над действительными числами, например, сложение, вычитание, умножение, деление, экспонента и логарифм, синус и арксинус, С. Б. Гашковым, во-первых, исследовалась сложность приближенной реализации (в равномерной чебышевской метрике) как индивидуальных функций, так и функциональных компактов, состоящих из функций заданной гладкости. Для произвольной индивидуальной функции получена верхняя оценка сложности ее ϵ -приближения через ее модули непрерывности k -го порядка. Из этой оценки выведены точные по порядку верхние оценки сложности ϵ -приближения для многих компактов гладких функций в виде колмогоровской ϵ -энтропии компакта, деленной на его логарифм. Для произвольной функции $L(\epsilon)$, удовлетворяющей некоторым естественным условиям, доказано существование в данном компакте функции, у которой сложность ее ϵ -приближения по порядку равна $L(\epsilon)$.

Во-вторых, исследовалась сложность точной реализации индивидуальных функций. Эффективно построен (совместно с И. С. Сергеевым) многочлен n переменных степени меньше d по каждой переменной с коэффициентами 0 и 1, у которого сложность реализации схемами в монотонном континуальном базисе из сложения, умножения и положительных констант равна $d^{n(1-o(1))}$ (очевидная верхняя оценка равна d^n).

Для возникающих в комбинаторике линейных преобразований Паскаля, Стирлинга, Сильвестра, Гаусса и некоторых конечных и континуальных арифметических базисов получены точные по порядку оценки их сложности реализации в этих базисах.

Доказано, что если функция может быть реализована со сложностью L схемой в континуальном базисе, состоящем из арифметических операций и простейших элементарных функций (логарифм, экспонента, прямые и обратные тригонометрические функции), то все ее дифференциалы вплоть до k -го порядка можно вычислить одновременно с ней в том же базисе со сложностью порядка $Lk \log k$.

Для задачи интегрирования рациональных дробей степени n получена верхняя оценка ее сложности в арифметическом базисе с континуумом действительных констант, по порядку равная $n \log^2 n$, при этом основную роль в алгоритме играет один из алгоритмов Остроградского для бесквадратной факторизации действительных многочленов.

В области изучения сложности и глубины реализации булевых функций в булевом базисе С. Б. Гашковым доказано (совместно с И. С. Сергеевым), что сложность реализации схемами в базисе из одной функции $x \oplus y$ линейного преобразования над полем из двух элементов с матрицей порядка n , содержащей $O(n^{3/2})$ единиц и не имеющей подматриц 2×2 из 4-х единиц, может быть равна $O(n \log n)$. В частности, это верно для матриц Зингера и Нечипорука, для которых сложность вычисления соответствующей им системы дизъюнкций в базисе из одной операции $x \vee y$ по порядку равна $n^{3/2}$. Эффективно указана $n \times n$ -матрица, у которой сложность реализации в базисе $\{\vee, \&\}$ равна $n^{2-o(1)}$, а сложность реализации в базисе $\{\oplus\}$ равна $O(n^{1+o(1)})$ (очевидные верхняя и нижняя оценки равны $O(n^2)$ и n).

Построены (совместно с И. С. Сергеевым) схемы для инвертирования в гауссовых нормальных базисах в полях $GF(p^n)$ сложности $O(\epsilon^{-c} n^{1+\epsilon})$ и глубины $O(\epsilon^{-1} \log n)$, где $c > 0$ — некоторая константа, а также схемы для инвертирования в некотором семействе полей $GF(2^n)$, имеющие сложность, по порядку равную

сложности умножения $M(n) = O(n \log n \log \log n)$.

Доказано, что в некотором семействе полей $GF(p^n)$ сложность решения уравнений степени не выше четырех равна $O(M(n) \log n)$, где $M(n)$ — сложность умножения в некотором базисе данного поля.

Проф. А. В. Чашкин. Основные результаты А. В. Чашкина относятся к области асимптотических методов реализации булевых функций. Им получено окончательное решение задачи о сложности $L_B(f)$ реализации произвольной частичной булевой функции f данного веса схемами в произвольном полном конечном базисе B . Пусть $F(n, D, N)$ — множество всех n -местных частичных булевых функций, определенных на областях размера D и принимающих единичные значения на N наборах. Установлено, что при $n \rightarrow \infty$ для любой функции $f \in F(n, D, N)$ и любого полного конечного базиса B справедлива асимптотическая оценка $L_B(f) \lesssim \varrho \cdot \frac{\log_2 \binom{D}{N}}{\log_2 \log_2 \binom{D}{N}} + O(n)$, где ϱ — это минимум приведенных весов базиса B и $D \geq n$.

Эта оценка является асимптотически минимальной при всех значениях параметров D и N , при которых первое слагаемое в её правой части растёт быстрее чем n , и точной по порядку в остальных случаях. Аналогичный результат получен при реализации функций из $F(n, D, N)$ неветвящимися программами с условной остановкой. Эти программы допускают при выполнении определенных условий досрочное прекращение вычислений, и средняя сложность такой программы равна среднему, взятому по всем наборам x из области определения реализуемой функции f , числу элементарных операций, выполненных программой при вычислении $f(x)$. Для средней сложности $T(f)$ самой сложной «в среднем» функции f веса N , где $n \log_2 n \ll N \leq 2^{n-1}$ установлено, что $T(f) = \Theta\left(\frac{N}{\log_2 N}\right)$, т. е. средняя сложность функции веса N практически не зависит от размера ее области определения. Развита при получении этого результата техника позволила установить порядок средней сложности самой сложной в среднем недоопределенной функции f , определенной на произвольном множестве D и принимающей значения в множестве непустых подмножеств другого множества M .

Также А. В. Чашкиным изучалась сложность реализации булевых функций вычислительными моделями без памяти. Для сложности $L_1(f)$ реализации функций f из $F(n, D, N)$ схемами без ветвлений (формулами) в базисе из всех не более чем двухместных функций при $n \rightarrow \infty$ и $\log_2 D \sim n$ установлено, что $L_1(f) \lesssim \frac{\log_2 \binom{D}{N}}{\log_2 n} + O(n^{5,62})$. Эта оценка является асимптотически минимальной при $\min(N, 2^n - N) \gg n^{4,62} \log_2 n$. Для средней сложности T_1 реализации самой сложной в среднем n -местной монотонной функции f_M программами без ветвлений установлено равенство $T_1(f_M) = \Theta\left(\frac{2^n}{n \log_2 n}\right)$, правая часть которого в $\sqrt{n}$ раз меньше формульной сложности самой сложной n -местной монотонной функции.

А. В. Чашкин также работает в области изучения сложности графов и индивидуальных булевых функций. В этой области в последнее время им найдено точное значение сложности реализации схемами в базисе $\{\oplus\}$ линейного оператора из 2^n линейных 2^n -местных булевых функций, матрица коэффициентов которого является матрицей Адамара H_n . В настоящее время нижняя оценка этого равенства $L(H_n) = 3(2^n - n - 1)$ является максимальной среди известных нижних оценок линейных операторов.

Проф. Р. М. Колпаков. Первоначальной тематикой научных исследований Р. М. Колпакова являлись дискретные преобразования конечных вероятностных распределений. В качестве дискретных преобразователей вероятностных распределений рассматривались такие классические модели как вероятностные контактные сети и функции конечнозначной логики. Вероятностная контактная сеть рассматривается как преобразователь вероятностей, преобразующий вероятности проводимости ее контактов в вероятность проводимости самой контактной сети. Функция k -значной логики рассматривается как преобразователь k -значных случайных величин: если значения переменных функции являются независимыми в совокупности случайными величинами, то значение функции также является случайной величиной, рассматриваемой как результат применения данной функции к случайным величинам значений ее переменных. Для вероятностных контактных сетей в качестве преобразователей вероятностных распределений установлена конечная порожденность широкого семейства классов бинарных рациональных вероятностных распределений. Для функций конечнозначной логики в качестве преобразователей вероятностных распределений описаны все замкнутые классы конечных рациональных вероятностных распределений, тем самым полностью решена задача выразимости для данных распределений. На основе полученных результатов предложена эффективная полиномиальная процедура проверки выразимости в классе всех функций k -значной логики заданной рациональной конечнозначной случайной величины заданным множеством исходных рациональных конечнозначных случайных величин.

В рамках международного научно-исследовательского сотрудничества Р. М. Колпаков активно занимается словарной комбинаторикой и алгоритмикой, в частности, разработкой эффективных алгоритмов поиска регулярных фрагментов в формальных словах фиксированной длины. Классическими примерами

регулярных фрагментов формальных слов являются периодичности и палиндромы, где под периодичностью обычно понимается фрагмент слова, порядок которого не меньше 2 (порядком слова называется отношение его длины к его минимальному периоду). Периодичности и палиндромы в словах имеют фундаментальное значение для комбинаторных свойств слова, его анализа и обработки, в частности, они активно используются для сжатия слов, анализа генетических последовательностей, ускорения алгоритмов поиска образцов в текстах. Получены оптимальные по порядку оценки максимального возможного числа нерасширяемых периодичностей в формальных словах фиксированной длины (под нерасширяемой периодичностью понимается периодичность, которую нельзя расширить ни на одну букву с сохранением ее минимального периода) и предложен оптимальный по времени работы алгоритм поиска таких периодичностей. Аналогичные результаты установлены для случая обобщенных нерасширяемых периодичностей с порядком, меньшим 2, а также для палиндромов с разрывами. Предложена эффективная процедура оценки порядка роста числа слов заданной длины, не содержащих периодичностей заданного порядка.

В последнее время Р. М. Колпаков также занимается вопросами дискретной оптимизации для таких классических задач, как задача о ранце и задача о назначении радиочастотных ресурсов, и активно работает в прикладных научно-исследовательских проектах, связанных с радиокommunikационными сетями.

Проф. М. Д. Ковалёв. Построение и развитие математических моделей теории механизмов — основное направление исследований М. Д. Ковалёва. Создание достаточно общих математических моделей в этой области осложняется разнообразием существующих механизмов. Однако, если сосредоточиться на изучении довольно узких классов механизмов, то математическая формализация возможна и позволяет поднять на более высокий уровень изучение их геометрических свойств. Ключевым является понятие *механизма*. Его можно определить как устройство, конфигурационное пространство (множество положений) которого является связным множеством положительной размерности. Таким образом, механизм можно перевести непрерывно из любого его положения в любое другое его положение. В теории механизмов это обстоятельство чётко не осознано, хотя традиционно механизмами и называют служащие для преобразования движения устройства. Так, в машиноведении бытует термин «различные сборки» механизма. Ими называют неперебиваемые непрерывно друг в друга устройства, составленные из одинаковых звеньев, соединённых в одном и том же порядке. Перейти от одной сборки к другой можно лишь разобрав механизм и пересобрав его. Однако, при этом сборка механизма может оказаться не механизмом, а неизгибаемой конструкцией, то есть на инженерном языке — *фермой*.

Проведённая близко к запросам машиноведения формализация основных понятий теории шарнирно-рычажных механизмов позволяет избежать подобных затруднений. В этой модели рассматриваются плоские устройства, составленные из прямолинейных стержней (рычагов), несущих на концах шарниры. Рычаги могут соединяться между собой и с точками плоскости этими шарнирами, допускающими произвольное проворачивание в плоскости. Структура такого устройства описывается графом G , вершины которого отвечают шарнирам, а рёбра — рычагам. Вершины графа G могут быть двух сортов: кружочки, отвечающие свободным шарнирам, и крестики, отвечающие закреплённым в плоскости шарнирам. На граф G накладывается ряд условий, например, требуется его связность и связность порождённого кружочками его подграфа. В машиноведении традиционно структуру устройства отображают графом Γ , вершины которого отвечают звеньям, а рёбра — кинематическим парам. Но граф Γ в отличие от графа G при наличии совмещённых шарниров не описывает правильно строение плоских шарнирно-рычажных устройств. Была предложена лишённая этого недостатка модификация графа Γ .

Ключевым объектом предпринятой формализации является рычажное отображение F , сопоставляющее положениям свободных шарниров в плоскости квадраты длин рычагов устройства: $d_{ij} = (p_i - p_j)^2$. Формализация привела к доказательству теоремы о чётности числа изостатических ферм, отвечающих правильному значению рычажного отображения. Это вытекает из существования и равенства нулю топологической степени рычажного отображения $F : R^n \rightarrow R^n$. Формализация позволила построить ряд примеров устройств с необычными свойствами, а также породила новые геометрические вопросы. Простейший из них — возможны ли однократные точки внутри образа рычажного отображения? Их существование влекло бы существование геометрически устойчивых ферм, собираемых единственным способом. На основе этой формализации была дана точная формулировка теоремы Кемпе (1876) о возможности черчения по частям любой плоской алгебраической кривой шарниром шарнирного механизма.

Шарнирником называется либо шарнирная ферма, либо определённое положение шарнирного механизма. Была поставлена задача восстановимости шарнирника по его внутренним напряжениям, т. е., — когда не существует других шарнирников p той же структуры, с теми же точками закрепления и с тем же пространством внутренних напряжений, что и у p ? Полностью задача была решена лишь в одномерном случае. Она связана с исследованием так называемой матрицы напряжений. Обнаружен ряд свойств определителя матрицы напряжений. В частности, установлено необходимое и достаточное условие неприводи-

мости этого определителя как многочлена. Приведён пример шарнирника, для которого можно восстановить положения всех свободных шарниров, зная его пространство внутренних напряжений и положения закрепленных шарниров. Однако, это нельзя сделать, зная не всё пространство внутренних напряжений, а лишь какое-либо одно произвольное напряжение.

Были формализованы и проанализированы основные геометрические понятия, связанные с напряжённо-связанными конструкциями, что также привело к постановке ряда новых вопросов в этой области. Первое изложение этой темы в русской учебной литературе дано в учебнике М. Д. Ковалёва «Геометрические вопросы кинематики и статики».

Основными результатами серии работ М. Д. Ковалёва по краевой задаче для одномерного уравнения Шредингера и волнового уравнения являются вывод формулы для числа энергетических уровней квантовой частицы в произвольном кусочно-постоянном потенциальном поле, а также вывод формулы для числа собственных оптических мод в плоском волноводе с произвольным числом различных диэлектрических слоёв.

Д.ф.-м.н. Ю. В. Таранников. Приоритетное направление исследований Ю. В. Таранникова — изучение криптографически важных свойств булевых функций. Нелинейностью $nl(f)$ булевой функции f называется расстояние от f до класса аффинных (линейных) функций, т. е. расстояние (число различающих наборов) от f до самой ближайшей к ней аффинной функции. Для нелинейности функции f имеет место оценка $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. Функции, для которых это неравенство превращается в равенство, называются бент-функциями. Бент-функции представляют большой интерес в криптографии, поскольку они хуже всего аппроксимируются аффинными функциями, а это в криптографии является большим достоинством.

Бент-функции были введены Ротхаузом в 1966 году, однако они фактически уже изучались более десятилетия до этого, поскольку эквивалентны нетривиальным разностным множествам в группе $\mathbf{Z}_2^n$. Именно в такой терминологии в 1973 г. Мак-Фарланд предложил семейство бент-функций, получившее название семейства Майораны–Мак-Фарланда, которое долгие годы считалось самым большим из известных семейств бент-функций. В базовом варианте оно содержит $(2^{n/2})! \cdot 2^{2^{n/2}}$ функций от n переменных. Пополнение аффинно эквивалентными функциями увеличивает эту мощность, но ее логарифм все равно остается асимптотически равным $\frac{n}{2} \cdot 2^{n/2}$.

Большой цикл работ Ю. В. Таранникова посвящен изучению корреляционно-иммунных и устойчивых функций, в частности, он построил m -устойчивые функции от n переменных в широком диапазоне параметров (для m от примерно 0,5789 n до $n - 2$), на которых достигается равенство в верхней оценке нелинейности для m -устойчивых функций от n переменных $nl(f) \leq 2^{n-1} - 2^{m+1}$, также полученной Ю. В. Таранниковым. Важно отметить, что все функции, для которых неравенство превращается в равенство, неизбежно должны быть платовидными. Ю. В. Таранников и его ученики впервые нашли точное число платовидных функций для нескольких бесконечных последовательностей носителей спектра. В совместной работе с ученицей И. П. Баксовой была предложена конструкция, использующая разбиение множества двоичных наборов на аффинные подпространства одинаковой размерности. Каждое аффинное подпространство являлось носителем спектра своей подфункции, аффинно эквивалентной некоторой бент-функции от числа переменных, равного размерности подпространства, с добавленными фиктивными переменными. Также было отмечено, что наиболее перспективным в плане получения наибольшей мощности числа бент-функций является набор параметров, при котором разбиение осуществляется на аффинные подпространства размерности два.

В тесном контакте с сотрудниками института математики имени С. Л. Соболева СО РАН Ю. В. Таранникову удалось получить нижнюю оценку числа разбиений пространства двоичных наборов на аффинные подпространства размерности два через оценку числа трансверселей в трехмерном латинском кубе, являющемся трехмерной таблицей Кэли группы $\mathbf{Z}_2^m$, что дало нижнюю оценку асимптотики логарифма числа бент-функций в изучаемом семействе, равную $\frac{3n}{4} \cdot 2^{n/2}$ и в полтора раза превосходящую асимптотику логарифма числа бент-функций в пополненном семействе Майораны–Мак-Фарланда. Тем самым был побит рекорд, продержавшийся полвека.

Доц. О. С. Дудакова. Основные результаты, полученные О. С. Дудаковой, относятся к одному из важнейших направлений дискретной математики, которое развивается на кафедре, — теории функциональных систем. Базовым объектом исследования является семейство функций k -значной логики с различными операторами замыкания, а также их обобщения: функции k -значной логики, определенные не на всех наборах значений переменных (частичные функции, мультифункции и т. п.), которые могут моделировать различные ситуации неопределенности информации. Для получающихся функциональных систем можно рассматривать задачи о полноте, о выразимости, о структуре замкнутых классов и т. д.

Задачами такого типа ранее занимались профессора кафедры О. М. Касим-Заде и А. Б. Угольников, а также их ученики.

О. С. Дудакова занимается исследованием замкнутых относительно суперпозиции классов всюду определенных и частичных монотонных функций в многозначной логике. Частным случаем задачи о выразимости функций в k -значных логиках является задача о конечной порожденности замкнутых классов. Известно, что классы, не имеющие конечных порождающих систем, встречаются уже в таких «широких» семействах, как предполные классы. К настоящему времени полного описания конечно-порожденных предполных классов в P_k не получено. О. С. Дудаковой получен критерий конечной порожденности для некоторого семейства предполных классов монотонных функций k -значной логики, которое можно построить для произвольного значения k ($k > 8$). Кроме того, установлен критерий существования бесконечного семейства классов частичных монотонных функций k -значной логики, содержащих предполный класс всюду определенных монотонных функций. Тем самым получено существенное продвижение в решении так называемой «Проблемы Лау» — задачи описания классов частичных функций, содержащих заданный предполный класс в P_k .

Доц. Ю. А. Комбаров. Исследования Ю. А. Комбарова посвящены реализации булевых функций схемами из функциональных элементов, которые можно рассматривать как представления булевой функции в виде последовательности элементарных операций (например, конъюнкций, дизъюнкций и отрицаний; отдельные операции принято называть элементами). Сейчас схемная сложность (т. е. минимальное число элементов в схеме) известна только для небольшого числа очень простых булевых функций. Для конкретных булевых функций, как правило, представляют интерес как построение компактных схем (другими словами, верхние оценки сложности), так и доказательство того, что любая схема содержит достаточно большое число элементов (т. е. нижние оценки сложности).

Ю. А. Комбаровым предложены новые подходы к установлению нижних оценок схемной сложности линейных булевых функций (т. е. функций вида $x_1 \oplus \dots \oplus x_n \oplus c$). С использованием этих подходов найдено точное значение сложности линейных функций в базисе «Штрих Шеффера» (эта задача оставалась нерешенной около 30 лет). Также была описана структура минимальных по сложности схем, реализующих линейные функции в ряде базисов, и получена новая нижняя оценка для базиса, состоящего из многовыходовых дизъюнкторов и конъюнкторов. Доказательство нижних оценок схемной сложности как правило сопряжено с объемным перебором различных вариантов строения схемы. Разработаны инструменты для частичной автоматизации такого перебора.

Получено несколько новых схем небольшой сложности для ряда естественно заданных булевых функций. А именно, улучшена верхняя оценка сложности линейной функции в базисе из многовыходовых конъюнкторов и дизъюнкторов, построена схема глубины два из пороговых элементов с малым ветвлением, реализующая функцию голосования. Ю. А. Комбаровым исследуются методы компьютерной генерации эффективных схем для функций небольшого числа переменных, в частности, они оказались полезны для получения вышеописанных результатов.

К.ф.-м.н. М. В. Старостин. Большинство результатов, полученных М. В. Старостиным, можно отнести к одной из центральных задач теории функциональных систем — задаче выразимости, в которой нужно, обладая некоторым набором объектов и правилом получения новых объектов, описать множество объектов, которые можно получить из заданного. Важнейшую роль играет постановка задачи выразимости, в которой в качестве объектов выступают функции k -значной логики, а новые функции получаются из уже имеющихся посредством операции суперпозиции (композиции). В связи с операцией суперпозиции возникают понятия замкнутых по суперпозиции классов, полных и предполных систем функций.

Большое распространение в теории функциональных систем получили исследования различных операторов, более сильных, чем оператор суперпозиции. Примером такого оператора служит оператор неявной выразимости, введенный А. В. Кузнецовым в 70-х годах.

Говорят, что функция $f(x_1, \dots, x_n) \in P_k$ *неявно выражима* над множеством функций $\Sigma \subseteq P_k$, если найдутся такие $A_i, B_i \in [\Sigma \cup \{x\}]$, что система уравнений $A_1(x_1, \dots, x_n, z) = B_1(x_1, \dots, x_n, z), \dots, A_m(x_1, \dots, x_n, z) = B_m(x_1, \dots, x_n, z)$ эквивалентна уравнению $z = f(x_1, \dots, x_n)$. Множество всех неявно выражимых над Σ функций называется *неявным расширением* Σ и обозначается $I(\Sigma)$.

Изучением оператора неявной выразимости на кафедре начал заниматься О. М. Касим-Заде. Им было получено описание всех неявных расширений в двужначной логике, а также критерий неявной полноты в P_k в терминах систем функций от трех переменных, а его ученица Е. А. Орехова нашла все минимальные неявные полные классы в трехзначной логике.

М. В. Старостин продолжает изучение оператора неявной выразимости в многозначных логиках. В частности, им было получено описание всех 54 неявно предполных классов в трехзначной логике и тем самым установлен критерий неявной полноты в P_3 в терминах неявно предполных классов. Кроме того,

был получен ряд результатов, касающихся семейств неявно полных и неявно предполных классов в P_k при произвольном значении k . Например, доказано, что класс функций, самодвойственных относительно перестановки σ , неявно предполон в P_k тогда и только тогда, когда количество неподвижных точек у σ отлично от единицы.

К.ф.-м.н. С. А. Корнеев. Вычислительная модель схем композиции — основной объект исследования С. А. Корнеева. Изучается сложность вычисления систем мономов схемами, использующими операцию композиции мономов, которая обобщает операцию умножения мономов и определяется следующим образом. Композицией мономов U и V относительно монома R , все степени переменных которого не превосходят соответствующих степеней мономов U и V , называется моном UV/R . В случае пустого монома R операция композиции совпадает с операцией умножения. За счёт индивидуального выбора монома R для каждой операции в схеме композиции можно значительно уменьшить значение сложности вычисления систем мономов по сравнению с классической вычислительной моделью, допускающей только операцию умножения. Для вычислительной модели схем композиции С. А. Корнеевым получены следующие результаты: 1) для задачи о вычислении системы из двух мономов найдено точное значение сложности; 2) для задачи о вычислении системы мономов от двух переменных найдена асимптотика сложности и доказано, что эта сложность может существенно зависеть от каждого монома: приведён такой пример системы мономов от двух переменных, в котором асимптотика сложности меняется при удалении любого монома; 3) для задачи о вычислении системы из трёх мономов от двух переменных найдено значение сложности с точностью до слагаемого, которое может быть равно 0 или 1; 4) найдена асимптотика функции Шеннона при некоторых условиях на соотношение параметров системы мономов; 5) для одной функции шенновского типа найдена асимптотика роста и, что особенно важно, этот результат удалось содержательно перенести на классическую модель вычисления систем мономов.

Представленные миниобзоры, несмотря на насыщенность результатами и разнообразие тем, конечно, далеко не исчерпывают всех направлений исследований, проводимых на кафедре дискретной математики. В частности, остались незатронутыми большие массивы результатов по теории сложности, многозначным логикам, дискретной оптимизации, комбинаторному анализу, теории графов, дискретной геометрии и другим разделам дискретной математики.

*В. В. Кочергин, Н. П. Редькин, С. Б. Гашиков, А. В. Чашкин,
Р. М. Колпаков, М. Д. Ковалёв, Ю. В. Таранников, О. С. Дудакова,
Ю. А. Комбаров, М. В. Старостин, С. А. Корнеев*

Поступила в редакцию
20.06.2024