Российская академия наук

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ МАТЕМАТИКИ ИМ. С.Л. СОБОЛЕВА СИБИРСКОГО ОТДЕЛЕНИЯ РАН
(ИМ СО РАН)

УДК 519.17, 519.72

№ госрегистрации 01201172121

Инв. №

УТВЕРЖДАЮ
Директор
член-корреспондент РАН
_____________ Гончаров С.С.
«___»______________ 2012 г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

В рамках федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы

по государственному контракту № 14.740.11.0868
шифр заявки 2010-1.5-502-001-007
по теме:

ФУНДАМЕНТАЛЬНЫЕ ТЕОРЕТИКО-ГРАФОВЫЕ МОДЕЛИ В ПРОБЛЕМАХ РАСПРЕДЕЛЕНИЯ РАДИОЧАСТОТ В СЕТЯХ СОТОВОЙ СВЯЗИ, ТЕОРИИ КОДИРОВАНИЯ И КРИПТОГРАФИИ, АНАЛИЗЕ СЕТЕЙ, ОБРАБОТКЕ И ПЕРЕДАЧИ ДАННЫХ

Наименование этапа № 4: «Анализ полученных результатов»
(итоговый)

Руководитель НИР, д.ф.-м.н. _______________ А.В. Косточка

Новосибирск 2012

СПИСОК ИСПОЛНИТЕЛЕЙ

рук. темы, в.н.с. ИМ СО РАН, д.ф.-м.н	___________________	Косточка А.В. (Введение, Заключение, Приложения А–Г, разделы 1.1, 2, 3, 4)
отв. исполнитель темы, зав. лаб. ИМ СО РАН, д.ф-м.н.	___________________	Бородин О.В. (Реферат, Приложения А–Г, разделы 1.7, 2, 4)
гл.н.с. ИМ СО РАН, д.ф.-м.н.	___________________	Кельманов А.В. (разделы 1.6, 2)
в.н.с. ИМ СО РАН, д.ф.-м.н.	___________________	Пяткин А.В. (разделы 1.1, 1.6)
в.н.с. ИМ СО РАН, д.ф.-м.н.	___________________	Кротов Д.С. (разделы 1.3, 1.4)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Глебов А.Н. (разделы 1.1, 1.2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Добрынин А.А. (разделы 1.2, 2,4)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Мельников Л.С. (раздел 1.2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Потапов В. Н. (разделы 1.3, 1.4)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Августинович С.В. (раздел 1.3)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Токарева Н.Н. (разделы 1.5, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Фрид А.Э. (раздел 1.4)
с.н.с. ИМ СО РАН, к.ф.-м.н.	___________________	Могильных И.Ю. (разделы 1.4, 2)
аспирант ИМ СО РАН	___________________	Замбалаева Д.Ж. (раздел 1.2)
аспирант ИМ СО РАН	___________________	Воробьев К.В. (раздел 1.3)
аспирант НГУ	___________________	Коломеец Н.А. (раздел 1.4)

аспирант ИМ СО РАН	___________________	Макаров М.А. (раздел. 1.4)
аспирант НГУ	___________________	Валюженич А.А. (раздел 1.3)
Студент НГУ	___________________	Паршина О.Г. (раздел 1.3)
Нормоконтролер	___________________	Кравченко С.В.

Реферат

Отчет 64 с., 70 источников, 4 прил.

Тема: ФУНДАМЕНТАЛЬНЫЕ ТЕОРЕТИКО-ГРАФОВЫЕ МОДЕЛИ В ПРОБЛЕМАХ РАСПРЕДЕЛЕНИЯ РАДИОЧАСТОТ В СЕТЯХ СОТОВОЙ СВЯЗИ, ТЕОРИИ КОДИРОВАНИЯ И КРИПТОГРАФИИ, АНАЛИЗЕ СЕТЕЙ, ОБРАБОТКЕ И ПЕРЕДАЧИ ДАННЫХ

Ключевые слова: *теория графов; раскраска графов; декомпозиция графов; инварианты графов; совершенные раскраски; булевы функции; теория кодирования; бент-функции; криптография; дистанционно регулярные коды; кластерный анализ.*

Основным объектом исследования являются актуальные проблемы в области применения теоретико-графовых моделей и методов дискретной математики к проблемам анализа коммуникационных сетей, надежности и эффективности передачи информации, защиты информации и анализа данных.

Выполнение НИР в целом направлено на проведение поисковых фундаментальных исследований в области современной математики (теория графов и ее приложения, методы эффективного кодирования и передачи информации, защита информации, анализ данных и распознавание образов) с целью получения научных результатов мирового уровня, на подготовку и закрепление в сфере науки и образования научных и научно-педагогических кадров, а также формирование эффективных и жизнеспособных научных коллективов.

В результате выполнения НИР исполнителями получен ряд результатов мирового уровня. Получены новые фундаментальные результаты, найдены новые подходы, разработаны новые алгоритмы, опубликованы новые статьи, защищены диссертации, осуществляется внедрение результатов в учебный процесс НГУ.

В ходе выполнения этапа 4 проведён анализ полученных в рамках НИР результатов. К основным результатам отнесены следующие:

- Показано, что каждый плоский субкубический плоский граф, т.е. граф со степенями не более 3, обхвата не менее 12 допускает 2-дистанционную 5-раскраску.
- Доказана предписанная ациклическая 4-раскрашиваемость плоских графов, не содержащих ни 3-циклов, смежных с циклами длины не более 6, ни 4-циклов, смежных с циклами длины не более 7.
- Доказано, что любой планарный граф, в котором 3-циклы находятся на расстоянии не менее 4 друг от друга и не имеют общих ребер с 5-циклами, является 3-раскрашиваемым.
- Получено исчерпывающее описание строения плоских графов в терминах звезд при младших вершинах. Опровергнута гипотеза Йендроля и Харанта.

- Доказана справедливость гипотезы Вудала–Сеймура о наличии миноров полного двудольного графа $K_{s,t}$ в (s + t)-хроматических графах для широкого диапазона параметра t для каждого фиксированного значения s.
- Асимптотически (и в некоторых случаях точно) найдено хроматическое число для графов, тесно связанных с раскрасками евклидовых пространств.
- Рассмотрена задача о двух коммивояжерах в различных постановках. Для задачи на максимум построен приближенный алгоритм с оценкой точности 7/9 и кубической временной сложностью.
- Показана NP-полнота задачи о наименее плотном разрезе и предложены полиномиальные алгоритмы её решения для некоторых классов графов, в частности, для графов пересечений единичных интервалов и графов с ограниченной древесной шириной.
- Установлен критерий, который по параметрам совершенной 2-раскраски двоичного куба определяет, является ли она кратным совершенным кодом заданного радиуса некоторой кратности. Показано, что существуют кратные совершенные коды любого нечетного радиуса сколь угодно большой длины.
- В терминах совершенных структур охарактеризованы коды с параметрами трижды укороченных 1-совершенных двоичных кодов. Доказано, что соответствующие расширенные коды всегда порождают совершенную раскраску вершин гиперкуба в шесть цветов.
- Доказано, что существует экспоненциальное число неэквивалентных пропелинейных расширенных совершенных кодов. Показано, что все такие коды имеют малый ранг, который на единицу больше ранга расширенного линейного кода Хэмминга.
- Получено описание всех бент-функций от $2k$ переменных, находящихся на минимальном расстоянии от квадратичной бент-функции.
- Показано, что каждое изометричное отображение множества булевых функций от n переменных в себя, оставляющее класс бент-функций на месте, является комбинацией аффинного преобразования координат и сдвига на аффинную функцию.
- Доказана NP-полнота актуальных задач разбиения конечного множества векторов, а также выбора подмножеств векторов в евклидовом пространства по критерию минимума суммы квадратов расстояний.

В результате исследований получены новые фундаментальные результаты мирового уровня, которые вошли в кандидатские и докторские диссертации, дипломные работы исполнителей, доложены на различных научных форумах, опубликованы в статьях и внедряются в учебный процесс Новосибирского государственного университета.

Обозначения и сокращения

ИМ СО РАН – Институт математики им. С.Л. Соболева Сибирского отделения Российской академии наук.

НГУ – Новосибирский государственный университет

ММФ – Механико-математический факультет

Содержание

Введение

Выполнение поисковых научно-исследовательских работ по проекту направлено на проведение фундаментальных исследований в области анализа теоретико-графовых моделей в проблемах анализа структурных объектов, теории кодирования, передачи информации и криптографии, обработке данных. Основной целью НИР проекта является получение научных результатов мирового уровня, позволяющих укрепить позиции российской школы в области теоретических направлений в дискретной математике и информатике (методы эффективного кодирования и передачи информации, защита информации, анализ данных и распознавание образов, анализ структур методами теории графов). Одной из целей проведения работ является привлечение научных сотрудников, студентов и аспирантов к современным передовым методам и подходам в научно-исследовательской работе в указанных областях, что будет способствовать повышению эффективности и устойчивости российских научных коллективов.

Запланированная работа по этапу 4 включала анализ и обобщение полученных результатов в области анализа структуры граф-моделей передачи информации и обработки данных, в теории кодирования информации, в теории и приложений бент-функций в криптографии и в смежных областях.

В состав разрабатываемой научной продукции входят математические модели задач, алгоритмы и методы решения поставленных задач, публикации результатов исследований в отечественных и зарубежных изданиях, учебные курсы, диссертации, отчет о НИР, содержащий обоснование развиваемых направлений исследований, изложение методик проведения исследований, а также описание полученных результатов.

На этапе 4 разработана программа внедрения результатов выполненных поисковых научно-исследовательских работ в образовательный процесс. Результаты НИР включены в состав читаемых в НГУ общих и специальных математических курсов «Теория графов», «Совершенные структуры», «Теория графов и алгоритмы», «Теория кодирования», «Криптография и криптоанализ», «Коды и схемы», «Экстремальные задачи анализа данных и распознавания образов», используются при проведении специальных семинаров по современным разделам математики в Институте математики им. С.Л. Соболева СО РАН.

Результаты работ подтверждены публикациями в реферируемых журналах по математике и ее приложениям, а также выступлениями на российских и международных научных форумах по тематике НИР. Полученные результаты носят фундаментальный характер и, прежде всего, являются вкладом в общую математическую теорию.

1. Анализ и обобщение полученных результатов

В процессе выполнения госконтракта, согласно календарному плану, проводились исследования по следующим направлениям: анализ граф-моделей передачи информации и смежные вопросы теории кодирования, анализ данных и распознавании образов, теория кодирования и передачи информации, булевы функции и защита информации.

В итоговом отчете проведен анализ и обсуждаются возможные обобщения и применение полученных результатов, в том числе полученные на последнем этапе.

1.1. Раскраска графов и смежные вопросы

Структура многих информационных и вычислительных систем естественно моделируются графами и их обобщениями (гиперграфами). Современное развитие информационно-телекоммуникационных технологий приводит к появлению новых постановок задач в области теории и методов раскраски графов.

1. В теоретических исследованиях проблемы распределения радиочастот в сетях связи используется следующая теоретико-графовая модель. Вершины плоского графа (источники) должны быть раскрашены (получить частоты) так, чтобы цвета (целые числа) любых двух вершин, находящихся друг от друга на расстоянии 1, отличались не менее чем на p, а вершин на расстоянии 2 – не менее чем на q. Таким образом, нахождение (p,q)-дистанционного хроматического числа позволяет минимизировать количество занятых частот [1-4]. При $p = 1$ и $q = 2$ возникает задача 2-дистанционной раскраски плоских графов. Под обхватом графа понимается длина наименьшего цикла. Получен новый результат по 2-дистанционным раскраскам. Показано, что каждый плоский субкубический плоский граф (т.е. граф со степенями не более 3) обхвата не менее 12 допускает 2-дистанционную 5-раскраску.

Тем самым улучшены результаты Распо, Монтасьера, у которых обхват графов был не менее 14 [5] и результаты Аве с обхватом графов не менее 13 [6]. Эти результаты находятся на мировом уровне и опубликованы в ведущем зарубежном журнале по дискретной математике.

2. Бородин и др. (2002) высказали гипотезу, что каждый плоский граф предписанно ациклически 5-раскрашиваем и доказали, что 7 цветов достаточно. В пяти зарубежных работах она подтверждена для следующих классов плоских графов: без 3- и 4-циклов, без 4- и 5-циклов, без 4- и 6-циклов, без 4-циклов и хордальных 6-циклов, без 4-циклов и 3-циклов на расстоянии менее 3 друг от друга, а также без 4-циклов и пересекающихся 3-циклов. Также доказано, что плоские графы без 4-циклов предписанно ациклически 6-раскрашиваемы. До-

казано, что каждый плоский граф без 4-циклов предписанно ациклически 5-раскрашиваем, что является совместным усилением шести зарубежных работ в этом направлении.

Этот результат является выдающимся, далеко опережающим мировой уровень в области ациклической раскраски плоских графов. В 2011 г. он был включен в число важнейших результатов ИМ СО РАН.

3. Граф G является (j,k)-раскрашиваемым, если можно так разбить его вершины на два множества V_1 и V_2, что в подграфе $G[V_1]$ степень каждой вершины не превышает j, а в $G[V_2]$ степень каждой вершины не превышает k. Доказано, что при $k \geq 2j+2$ каждый граф с наибольшей средней степенью не более $2(2-(k+2)/(j+2)(k+1))$ является (j,k)-раскрашиваемым. С другой стороны, построены графы с наибольшей средней степенью сколько угодно близкой к $2(2-(k+2)/(j+2)(k+1))$, которые не являются (j,k)-раскрашиваемыми.

На самом деле доказан еще более точный результат: найдено наилучшее достаточное условие для (j,k)-раскрашиваемости графа G в терминах минимума, $\varphi_{j,k}(G)$, величины $\varphi_{j,k}(W,G) = (2-(k+2)/(j+2)(k+1))|W| - |E(G[W])|$ по всем подмножествам W множества $V(G)$. Конкретно, доказано, что каждый граф G с $\varphi_{j,k}(G) > -1/(k+1)$ является (j,k)-раскрашиваемым. С другой стороны, построено бесконечно много не (j,k)-раскрашиваемых графов G с $\varphi_{j,k}(G) = -1/(k+1)$.

4. В развитие предыдущего результата, доказано, что каждый граф с наибольшей средней степенью не более 14/5 является (1,1)-раскрашиваемым. С другой стороны, построены графы с наибольшей средней степенью сколько угодно близкой к 14/5, которые не являются (1,1)-раскрашиваемыми. Это, в частности, улучшает результат Хавета и Серени. Отметим, что результат отличается от того, который получился бы подстановкой $j=k=1$ в предыдущий результат.

5. Гипотеза Хадвигера утверждает, что любой граф с хроматическим числом k содержит минор полного k-вершинного графа K_k. Эта гипотеза доказана только для $k \leq 6$. Неизвестно даже, существует ли (хотя бы маленькое) число $c > 0$ такое, что любой граф с хроматическим числом k содержит минор полного ck-вершинного графа K_{ck}. Близкая к ней гипотеза утверждает, что любой n-вершинный граф с числом независимости α содержит минор полного (n/α)-вершинного графа $K_{n/\alpha}$. Фокс доказал, что любой n-вершинный граф с числом независимости α содержит минор полного $(n/(2-c)\alpha)$-вершинного графа $K_{(n/(2-c)\alpha)}$, где $c > 1/57$. Нами доказан более сильный результат с $c > 1/19.2$.

Это дает возможность улучшить понимание гипотезы Хадвигера, развитые методы будут использованы для получения более точных оценок. Рассматриваемая задача тесно связана с задачей о существовании других миноров в графах с данным числом независимости и данным хроматическим числом.

6. Гиперграф называется d-вырожденным, если каждый его непустой подграф имеет вершину степени (в этом подграфе) не более d. Каждый d-вырожденный гиперграф легко покрасить в d+1 цвет. Гиперграф G является почти d-вырожденным, если сам G не является d-вырожденным, но каждый его собственный подграф является d-вырожденным. В частности, если G является почти d-вырожденным, то после удаления любого ребра получившийся гиперграф является (d+1)-раскрашиваемым. Изучены и охарактеризованы почти d-вырожденные гиперграфы, которые нельзя раскрасить в d+1 цвет. По определению каждый такой гиперграф является (d+1)-критическим по раскраске.

Эта задача является NP-полной, т.е. не существует хорошего описания всех k-критических графов. Результаты дают описание интересного подкласса таких графов: графов, после удаления любого ребра которых есть очевидный способ раскраски в $k-1$ цвет. Работа является шагом к пониманию структуры k-критических графов и решает задачи, поставленные Бородиным в 1974 г. (проблема 1.4. в книге [7]).

7. Пусть G – гиперграф с раскрашенными ребрами. Тогда радужным подграфом в G называется подграф, все ребра которого раскрашены разными цветами. Цветовой степенью вершины v в графе с раскрашенными ребрами называется число разных цветов, используемых на ребрах, инцидентных с v. Ванг и Ли выдвинули гипотезу, что при $k \geq 4$ каждый граф с раскрашенными ребрами и минимальной цветовой степенью k содержит радужное паросочетание с как минимум $\lceil k/2 \rceil$ ребрами. Правильно раскрашенный K_4 не имеет такого паросочетания, в связи с чем возникло ограничение $k \geq 4$ в гипотезе. Ли и Ксу доказали, что гипотеза справедлива для некоторых других правильно раскрашенных полных графов. Позже Ле Солнер, Стокер, Венгер и Вест доказали гипотезу для четных k. В настоящем проекте гипотеза доказана полностью.

Разноцветные паросочетания графах тесно связаны с паросочетаниями в 3-униформных 3-дольных гиперграфах. Известно, что нахождение наибольшего паросочетания в таких гиперграфах является NP-трудной задачей. Таким образом, оценки на размеры паросочетаний, особенно когда доказательство дает полиномиальный алгоритм построения «больших» паросочетаний, интересны для теории и методов оптимизации. Доказательства представленных результатов обладают этим свойством.

8. Получена точная верхняя оценка 2D – 1 для реберного 2-дистанционного хроматического числа плоских графов с достаточно большим обхватом, где D – максимальная степень графа.

Результат не улучшаем, и является одним из немногих точных результатов по так называемой сильной реберной раскраске, исследуемой уже более 20 лет.

9. Доказана предписанная ациклическая 4-раскрашиваемость плоских графов, не содержащих ни 3-циклов, смежных с циклами длины не более 6, ни 4-циклов, смежных с циклами длины не более 7 (все известные ранее достаточные условия ациклической 4-раскрашиваемости полностью запрещали 4-циклы).

Этот результат усиливает целый ряд зарубежных результатов и является первым по предписанной ациклической 4-раскраске, когда 4-циклы допускаются, хотя на них и налагаются некоторые необходимые ограничения.

10. Харант и Йендроль дали описание строения плоских графов в терминах звезд при младших вершинах, поглощающее ряд известных результатов в этой области. Там же была сформулирована гипотеза об идеальном описании такого рода. Ранее Бородиным и Ивановой были построены два класса контрпримеров к данной гипотезе. Сейчас получено описание конструкции, в котором все параметры являются неулучшаемыми

Данный результат усиливает известный зарубежный результат, доводя его до неулучшаемого и поглощая при этом ряд более ранних результатов. Попутно даются два класса контрпримеров к известной гипотезе Харанта-Йендроля.

11. В работах [8-11] дано приближенное описание строения плоских графов в терминах цепей из двух ребер. Получено точное описание такого рода, т.е. в котором все параметры являются неулучшаемыми.

Полученный результат закрывает некое направление в структурной теории плоских графов. Перечисленные приближенные результаты входят в недавний обзор С.Йендроля, готовящийся к публикации в журнале Discrete Mathematics. Полученный результат превосходит мировой уровень.

12. Получены новые условия на среднюю степень графа, дающие возможность провести декомпозицию графа на компоненты с максимальной степенью не более 1.

Дальнейшие направления исследований: полученные результаты и развитая техника позволяют надеяться на полное решение проблемы о дефективных 2-раскрасках графов с данной максимальной средней степенью. Другими словами, развитие наших методов может позволить для каждых j и k найти точное значение функции $f((j,k)$ – наибольшего m такого, что любой граф с максимальной средней степенью менее m имеет (j,k)-раскраску: разбиение множества вершин графа G на два подмножества V_1 и V_2 таких, что максимальная степень в порожденном подграфе $G[V_1]$ не превосходит j, а максимальная степень в порожденном подграфе $G[V_2]$ не превосходит k.

13. Доказано обобщение известной теоремы Гретцша о 3-раскрашиваемости плоских графов: если к плоскому графу без циклов длины 3 добавить вершину степени не больше 4, то полученный граф по-прежнему 3-раскрашиваем. Результат является неулучшаемым, т.к.

если к 5-циклу добавить вершину степени 5, то 3-раскрашиваемости нет. Попутно усилен результат работы [12], в которой допускается добавление вершины степени не больше 3.

Проблема 3-раскрашиваемости плоских графов привлекает большое внимание специалистов по теории графов во всем мире. Каждый новый, тем более точный, результат в этом направлении является ценным.

14. Подготовлена большая обзорная статья о раскраске плоских графов [13], принятая в печать в международный журнал Discrete Mathematics.

Данный факт свидетельствует о том, что новосибирская школа по раскраске и строению плоских графов считается мировым лидером в этой области, в которой работают сотни специалистов и написаны тысячи статей. Обзор этой области дан впервые и является несколько неожиданным событием: до сих пор она считалась не поддающейся описанию в виде статьи. Попутно в обзоре даны доказательства нескольких новых результатов. В нем же сформулирован целый ряд актуальных проблем, часть из которых поставлена впервые.

15. Исследована задача подсчёта правильных рёберных 3-раскрасок, тотальных 4-раскрасок, а также $L(2,1)$-нумераций спана 5 для кубических графов. Получены экспоненциальные верхние и нижние оценки для числа таких раскрасок в n-вершинном кубическом графе. Также предложены алгоритмы динамического программирования для подсчёта числа указанных раскрасок в графах с ограниченной древесной шириной.

16. Доказана 4-раскрашиваемость графов без индуцированных подграфов K_3 и $2P_3$. Ранее было известно лишь о 5-раскрашиваемости таких графов.

Поскольку задачи о хроматическом числе графов с запрещенными подграфами довольно сложны и представляют большой теоретический интерес, этот результат имеет мировой уровень.

17. Доказано, что любой планарный граф, в котором 3-циклы находятся на расстоянии не менее 4 друг от друга и не имеют общих ребер с 5-циклами, является 3-раскрашиваемым.

Одним из самых известных результатов о раскрасках плоских графов является теорема Грётцша о 3-раскрашиваемости плоских графов без 3-циклов. В поисках усилений данного результата Хавел (1970) задал вопрос о том, существует ли такая константа H, что любой плоский граф с минимальным расстоянием между 3-циклами не меньше H, является 3-раскрашиваемым. Из результатов Аксенова и Мельникова следует, что H > 3. Недавно гипотеза Хавела была доказана Дворжаком, Кралем и Томасом для очень больших значений H. В то же время, остаётся открытым вопрос о справедливости гипотезы Хавела для минимального возможного значения H = 4. Полученный результат является важным продвижением на пути к решению гипотезы Хавела в указанной сильной постановке, отличаясь от неё лишь требованием отсутствия общих ребер у 5-циклов с 3-циклами. Этот результат усиливает теорему Грёцша и находится на переднем краю мировых исследований в области раскрасок планарных графов.

18. Гармонической раскраской графа G называется такая правильная раскраска вершин G, в которой каждая пара цветов появляется не более чем на одной паре смежных вершин. Гармоническое хроматическое число графа G, обозначаемое $h(G)$, равно наименьшему числу цветов, достаточному для гармонической раскраски графа G. Вычисление гармонического хроматического числа является NP-трудной задачей даже для деревьев. Доказано, что если T является лесом с n вершинами и максимальной степенью $\Delta(T) \geq (n+2)/3$, то выполняется следующее равенство:

$$h(T) = \begin{cases} \Delta + 1, \textit{ если } T \textit{ содержит несмежные вершины степени } \Delta(T) \\ \Delta + 2, \textit{иначе.} \end{cases}$$

Из доказательства извлекается алгоритм полиномиальной сложности для оптимальной гармонической раскраски таких лесов и деревьев.

Дальнейшие направления исследований: построение оптимальных гармонических раскрасок для более широких классов деревьев и лесов, анализ гармонических раскрасок ребер графов. Гармонические раскраски графов k цветов – это гомоморфизмы этих графов в полный k-дольный граф. Проблема исследования структуры гомоморфизмов является одной из важнейших в математике.

19. Пусть $K^*_{s,t}$ обозначает граф, полученный из полного двудольного графа $K_{s,t}$ путем добавления всех возможных ребер между s вершинами степени t. Мы развиваем подход из нашей ранней работы [14] для доказательства того, что если выполняется соотношение $t / \log_2 t \geq 1000s$, то каждый граф G со средней степенью вершин $t + 8s \log_2 s$ или более, имеет $K^*_{s,t}$-минор. Это улучшает соответствующий результат, доказанный ранее Кюном и Остасом.

Полученный результат – это новый шаг к решению проблемы о существовании данных миноров графах с заданными характеристиками. Нахождение миноров является одной из целей структурной теории графов, развиваемой Сеймуром, Робертсоном и Томасом.

20. Пытаясь решить гипотезу Хадвигера, Вудал и Сеймур сформулировали более слабую гипотезу, состоящую в том, что для любых $s \leq t$ любой граф с хроматическим числом $s + t$ содержит минор полного двудольного графа $K_{s,t}$. Ранее Косточкой было доказано, что для любых фиксированных s и $t > \max\{4^{15s2 + s},(240s \log_2 s)^{8s \log2 s + 1}\}$, каждый граф с хроматическим числом $s + t$ имеет $K^*_{s,t}$-минор. Это подтвердило гипотезу Вудала – Сеймура в случае, когда величина t сильно превышает значение s. Мы доказываем, что гипотеза верна и для меньших значений t, а именно, для $t > C(s \log_2 s)^3$.

Дальнейшее направление исследований состоит в решении гипотезы для более широкого круга значений параметров s и t. Решение проблемы для всех значений параметров означало бы приближенное решение гипотезы Хадвигера.

21. В теории раскраски представляет интерес получение оценок на хроматическое число евклидова пространства $\chi(R^n)$, которое по определению есть наименьшее число цветов необходимое для раскраски всех точек в R^n так, что любые две точки на расстоянии 1 получают разные цвета. Ларман и Роджерс ввели и изучали последовательность графов G_n в R^n такую, что $\chi(R^n) \geq \chi(G_n) \geq (1+o(1))n^2/6$. На протяжении многих лет эта оценка была наилучшей для некоторых пространств низкой размерности. Было выдвинуто предположение, что хроматическое число графов G_n больше, чем эта оценка. Мы доказали, что $\chi(G_n) \sim n^2/6$, а также получили точную оценку в случаях $n = 2^k$ и $n = 2^k - 1$.

Задачи раскраски евклидовых пространств изучаются около 50-ти лет. Удалось асимптотически (и в некоторых случаях точно) найти хроматическое число для графов, тесно связанных с раскрасками евклидовых пространств. Эта задача связывает теорию графов с геометрией евклидовых пространств.

22. Круговым графом называется граф пересечений конечного множества хорд в круге. Наилучшая известная верхняя оценка хроматического числа кругового графа с размером наибольшей клики k равна $50{\cdot}2^k$. Мы получили лучшую оценку $2k$–1 для более простого подкласса круговых графов, так называемых чистых графов. Используя этот результат, доказано, что хроматическое число любого кругового графа с размером наибольшей клики 3, не превосходит 38.

Задача раскраски круговых NP-трудна. Поэтому интересны полиномиальные процедуры раскраски таких графов в гарантированное число цветов. Оба результата носят такой характер. Дальнейшие исследования: обобщение разработанных методов для получения лучших общих оценок на хроматическое число круговых графов с данным размером наибольшей клики. В настоящее время известны только экспоненциальные оценки. Задача является важным частным случаем общей проблемы оптимальной раскраски графов.

23. Доказано, что любой n-вершинный гиперграф без r-регулярных подграфов имеет не более $2^{n-1} + r - 2$ ребер. Мы предполагаем, что если $n > r$, то любой n-вершинный гиперграф без r-регулярных подграфов, имеющий наибольшее число ребер, содержит полную звезду, т.е. 2^{n-1} различных ребер, содержащих какую-то вершину. Эта гипотеза доказана для $n \geq 425$. При этом условие $n > r$ ослабить нельзя.

В 1980-х годах В.А. Ташкинов получил важные результаты о r-регулярных подграфах в d-регулярных графах [15, 16]. Ситуация с регулярными подграфами гиперграфов является гораздо более трудной. В работе изучена структура наиболее плотных «плохих» примеров гиперграфов без r-регулярных подгиперграфов. Дальнейшие исследования: изучение «плохих» униформных гиперграфов без r-регулярных подгиперграфов. Если униформный гиперграф имеет много ребер, то более вероятно, что он содержит r-регулярных подграф.

24. Радужный подграф графа с раскрашенными ребрами это подграф, все ребра которого имеют разные цвета. Цветная степень вершины v есть число разных цветов, использованных на ребрах, инцидентных v. Доказано, что если n велико (а именно, $n \geq 4.25k^2$), то каждый n-вершинный граф G с минимальной цветной степенью k содержит радужное паросочетание с не менее чем k ребрами.

25. Числом независимости, $\alpha(H)$, гиперграфа H называется наибольший размер подмножества вершин, не содержащего ни одного ребра H. Доказано, что если H_n есть n-вершинный $(r + 1)$-униформный гиперграф, в котором каждое r-элементное подмножество вершин содержится в не более чем d ребрах и $0< d< n / (\log n)^{3r2}$, то выполняется неравенство

$$\alpha(H_n) \geq c_r \left(\frac{n}{d} \log \frac{n}{d} \right)^{1/r}$$

где $c_r > 0$ удовлетворяет $c_r \sim r/e$, когда $r \to \infty$. Значения c_r улучшают и обобщают некоторые ранее известные результаты, которые используют известную теорему Атья, Комлоса, Принса, Спенсера и Семереди. Наше более короткое доказательство использует метод Ширера и Алона. Полученная нами оценка близка к наилучшей в том смысле, что для каждого $r \geq 2$ и всех значений $d \in N$, существует бесконечно много гиперграфов H_n таких, что

$$\alpha(H_n) \leq b_r \left(\frac{n}{d} \log \frac{n}{d} \right)^{1/r}$$

где $b_r > 0$ зависит только от r. Кроме того, для многих значений d показано, что $b_r \sim c_r$, когда $r \to \infty$. Поэтому результат почти точен для r. Также указано приложение результатов к числам Рамсея для гиперграфов, связанных с независимыми окрестностями.

Проблема нахождения наибольшего независимого множества в графах и гиперграфах является одной из классических. Новое, более простое, доказательство дает лучшее понимание структуры униформных гиперграфов с ограниченным числом независимости. Дальнейшие исследования: обобщение результатов двух направлениях –для гиперграфов без других разреженных циклов и для гиперграфов без данных полных подграфов. Интересны и проблемы типа задачи Турана: сколь много ребер может иметь r-униформный гиперграф, не содержащий разреженного цикла длины 1? Задачи о существовании больших независимых множеств связаны не только с комбинаторными проблемами, но и с известными проблемами в других частях математики: теории чисел, геометрии, теории вероятностей.

26. Известный результат в теории Рамсея говорит, что порядок роста чисел Рамсея $R(3,t)$ для графов есть $t^2/\log t$. Рассмотрен аналог этой проблемы для униформных гиперграфов. Треугольником называется гиперграф, состоящий из ребер e, f и g таких, что $|e \cap f| = |f \cap g| = |g \cap e| = 1$ и $e \cap f \cap g = \varnothing$. Для $r \geq 2$, пусть $R(3,K^r_t)$ обозначает наименьшее натуральное число n такое, что при любой раскраске ребер полного r-униформного гиперграфа K^r_n в два цвета, или существует треугольник первого цвета, или есть K^r_t второго цвета. Мы находим с точностью до логарифмического множителя порядок роста величины $\mathrm{R}(3,K^r_t)$ для всех $r \geq 3$: $c_1(t/\log t)^{3/2} \leq R(3, K^r{}_t) \leq c_2 t^{3/2}$ для некоторых c_1, $c_2 > 0$. Когда $r = 3$, мы улучшаем нижнюю оценку до $c_1 t^{3/2}(\log t)^{-3/4}$. Оказалось, что при переходе от $r = 2$ к $r = 3$ происходит скачок, а потом ситуация не меняется. Получены также оценки на некоторые другие числа Рамсея для гиперграфов.

Оценка числа независимости для графов без «разреженных» 3-циклов это результат в том же направлении, что и предыдущий. Он может также рассматриваться как оценка числа Рамсея для разреженного треугольника против полного подграфа.

27. Пусть плоский граф $G = G(S)$ образован суперпозицией множества S простых замкнутых кривых на плоскости в общем положении, т.е. кривые не имеют самопересечений, не касаются друг друга, и никакие три кривые не имеют общей точки. Вершины графа G соответствуют точкам пересечения кривых из S, а ребра — дугам кривых, соединяющим соседние точки пересечения. Построенные таким образом 4–регулярные плоские графы называются графами Грёцша–Закса. Вероятно, Г. Грёцш в 50-х годах прошлого столетия был первым, кто исследовал задачу раскраски графов, образованных пересечениями кривых на плоскости [17-21]. Если все кривые являются окружностями, то соответствующие графы называются графами Кёстера. Ранее в работах участников проекта были опровергнуты некоторые гипотезы о хроматическом числе таких графов, построены новые 4-хроматические и 4-критические графы Грёцша-Закса [22-25]. Трудной проблемой в этой области является построение 4-хроматических и 4-критических графов Кёстера. Построен новый 4-хроматический граф Кёстера на 32 вершинах, образованный пересечением 7 кривых на плоскости. Этот граф является вершинно 4-критическим (т.е. удаление любой вершины уменьшает хроматическое число графа), но не реберно 4-критическим (четыре ребра являются не критическими). Дальнейшее направление исследований состоит в построении 4-критических графов Кестера и новых графо Гретцша-Закса.

28. Коради и Хайнал доказали в 1962 г. гипотезу Эрдеша о том, что любой граф с минимальной степенью не менее $2k$ и $n \leq 3k$ вершинами содержит k вершинно непересекающихся циклов. Эта оценка точна, т.к. для каждого k есть бесконечное множество экстремальных примеров. Важным случаем является $n = 3k$, т.к. все неперекающиеся k циклов должны быть 3-циклами. Доказано, что при $k \leq 3$ граф G с минимальной степенью не менее $2k - 1$ и $n \leq 3k$ вершинами не содержит k вершинно неперекающихся циклов тогда и только тогда,

когда либо G содержит независимое множество размера $n - 2k + 1$, либо k нечетно, $n = 3k$ и G является дополнением графа, который есть объединение полного графа K_k с полным двудольным графом $K_{k,k}$.

Это является усилением классической теоремы, доказанной около 50-ти лет назад. Получено понимание структуры графов с большой минимальной степенью, не содержащих k вершинно непересекающихся циклов. Дальнейшее направление исследований состоит в получении аналога результата Оре, для которого ограничена снизу не минимальная степень вершин, а сумма степеней несмежных вершин. Эта задача тесно связана, с одной стороны, с задачами вложения графов в графы с заданными параметрами, а с другой стороны, с уравновешенной раскраской.

29. Одна из центральных задач раскраски графов – выяснение структуры критических по раскраске графов. В 1957 г. Дирак поставил проблему: сколь мало ребер может иметь k-критический граф? Важные результаты по этой проблеме были получены Галлаи (1963), Оре (1967), Кривелевичем (1999), Косточкой и Штибицем (2000-2004). Оре сформулировал гипотезу о том, какой должен быть ответ. Но все результаты были далеки от этой гипотезы даже для наиболее простого случая $k = 4$. Проблема не раз была включена в списки важных проблем по раскраске графов. В рамках проекта Косточка с соавторами получили асимптотическое решение этой проблемы. Проблема полностью решена для $k = 4$ и любого n, а также для каждого k и $n \equiv 1 \pmod{k-1}$. Для этих значений k и n подтверждена справедливость гипотезы Оре. Интересные приложения этих результатов к раскраске графов получены Бородиным и другими. В частности, получено простое доказательство теоремы Гретцша о 3-раскрашиваемости плоского графа без треугольников. Дальнейшее направление исследований состоит в полном доказательстве гипотезы Оре и описании экстремальных графов, решении аналогичных проблем для гиперграфов и для предписанной раскраски.

1.2. Оптимизационные задачи на графах и сетях

Рассматривается несимметричная задача о двух коммивояжерах на максимум, заключающаяся в нахождении двух реберно непересекающихся ориентированных гамильтоновых циклов максимального веса в полном ориентированном графе. Данная задача является обобщением классической задачи коммивояжера на максимум, а также модификацией симметричного случая задачи о двух коммивояжерах на максимум, который активно исследуется в последнее время. Известно, что задача коммивояжера и все содержательные варианты задачи о двух коммивояжерах NP-полны. Поэтому представляет интерес вопрос о выделении полиномиально разрешимых подклассов этих задач и о построении эффективных приближенных алгоритмов их решения с гарантированными оценками точности [26-38].

1. Для задачи о двух коммивояжерах на минимум различными весовыми функциями ребер, принимающими значения 1 и 2 (задача 2-PSP(1,2)-min-2w) построены следующие приближенные алгоритмы: а) алгоритм с оценкой точности 7/5 (без учета аддитивной константы) и кубической временной сложностью. б) алгоритм с оценкой точности 4/3 (без учета аддитивной константы) и временной сложностью $O(n^5)$.

В последнее время наряду с классической задачей коммивояжёра некоторыми авторами рассматривается такое естественное её обобщение, как задача об m коммивояжёрах (m-PSP), состоящая в поиске m рёберно непересекающихся гамильтоновых циклов минимального или максимального суммарного веса в полном взвешенном графе. Из результатов Де Корта следует, что задача m-PSP NP-трудна [29, 30]. Наибольший интерес у исследователей вызывает задача о двух коммивояжёрах (2-PSP). Нами построены два полиномиальных алгоритма с гарантированными оценками точности для специального случая задачи 2-PSP на минимум, когда веса рёбер графа принимают значения 1 и 2, причём весовые функции различны для двух гамильтоновых циклов. Оба алгоритма значительно улучшают ранее полученную для данной задачи оценку точности 11/7. В основе алгоритмов лежит специальная теоретико-графская техника последовательного «улучшения» двух рёберно непересекающихся частичных туров в полном графе и метод перераспределения весовых вкладов между вершинами графа, типичный для исследования плоских графов, и ранее использованный Берманом и Карпински при построении приближённого алгоритма для задачи одного коммивояжера на минимум с весами рёбер 1 и 2.

2. Для задачи о двух коммивояжерах на максимум (задача 2-PSP-max) построен приближенный алгоритм с оценкой точности 7/9 и кубической временной сложностью. Для случая, когда весовая функция принимает значения в промежутке [1,q], получена модификация указанного алгоритма, имеющая оценку точности (7q + 3)/(9q + 1).

Полученный результат обеспечивает наилучшую на сегодняшний день оценку точности 7/9 эффективного алгоритма для наиболее общего варианта задачи о двух коммивояжёрах на максимум с произвольными неотрицательными весами рёбер. Указанная оценка точности превосходит как ранее полученную для этой же задачи Агеевым, Бабуриным и Гимади оценку 3/4, так и наилучшую на данный момент оценку 25/33 для «более простой» задачи одного коммивояжёра на максимум [37], что говорит о высоком качестве полученного результата и его соответствии передовому уровню мировых исследований в области задач маршрутизации. При разработке алгоритма использована оригинальная техника раскрасок рёбер графа, позволяющая построить пару гамильтоновых циклов нужного веса.

3. Для несимметричной задачи о двух коммивояжерах на максимум построен алгоритм, имеющий асимптотическую оценку точности 2/3 и кубическую оценку временной сложности.

Применительно к несимметричной задаче о двух коммивояжёрах на максимум, повторена (с точностью до асимптотики) оценка точности 2/3 эффективного приближенного алгоритма, ранее полученная в работе Каплана и др. для несимметричной задачи одного коммивояжёра. Как и в случае с разработанным нами алгоритмом с оценкой 7/9 для симметричной задачи 2-PSP-max, данный алгоритм основан на построении специальной раскраски ребер вспомогательного орграфа и последующем выделении пары рёберно непересекающихся частичных туров достаточно большого веса.

4. Доказано, что любой планарный граф с обхватом не менее 6 является (5,5)-разбиваемым. Иными словами, множество вершин такого графа можно разбить на два подмножества так, что в подграфе, порожденном каждым подмножеством, число вершин любой цепи не превосходит 5.

Михоком в середине 80-х годов прошлого века было введено понятие путевой (a,b)-разбиваемости графов, которое с тех пор активно исследуется. Им же было показано, что для любых фиксированных значений параметров a, b существуют плоские графы, не являющиеся (a,b)-разбиваемыми. При этом во всех известных примерах таких графов содержится большое число циклов длины 3. Поэтому вызывает интерес вопрос о том, для какого наименьшего значения $g > 3$ существуют такие константы a, b, что любой плоский граф с обхватом не менее g является (a,b)-разбиваемым. Из полученного нами результата следует, что искомое значение g не превосходит 6.

5. Показана NP-полнота задачи о наименее плотном разрезе и предложены полиномиальные алгоритмы её решения для некоторых классов графов, в частности, для графов пересечений единичных интервалов и для графов с ограниченной древесной шириной.

Плотностью разреза в графе называется отношение числа имеющихся рёбер разреза к их максимально возможному количеству (которое равно произведению мощностей долей разреза). Этот параметр является важной характеристикой уязвимости сетей с точки зрения разрушения линий связи (ребер графа). Задача о наименее плотном разрезе заключается в поиске в данном графе разреза с минимальной плотностью, что соответствует «узкому месту» сети, т.е. набору линий связи, разрушение которых приведет к наибольшему ухудшению работы сети.

6. Показано, что задача определения жёсткости графов без индуцированного подграфа $2K_2$ является NP-полной.

Жесткостью графа называется минимальное отношение мощности разрезающего множества графа к числу компонент связности, получающихся после его удаления. Этот параметр является важной характеристикой уязвимости сетей с точки зрения разрушения узлов связи (вершин графа). Также показано, что жёсткость 25 в таких графах влечёт их гамильтоновость, т. е. для них выполняется гипотеза Хватала. Поскольку гипотеза Хватала в общем случае остается недоказанной (и неопровергнутой) уже более 35 лет, то результат имеет мировой уровень.

7. Пусть связная коммуникационная сеть имеет гексагональную структуру, вложимую в правильную гексагональную решетку на плоскости. Функционирование сети оценивается суммой расстояний между всеми узлами сети в естественной метрике (индекс Винера W или дистанция графа [39-45]). Пусть происходит разрушение сети так, что оставшаяся сеть все еще сохраняет гексагональную структуру. После последовательности разрушающих воздействий образуются изолированные друг от друга гексагональные подсети одинакового размера, не связанные друг с другом. В этом случае оценочная характеристика сети будет определяться как сумма индексов Винера этих подсетей. Описана структура подсетей (в классе гексагональных цепей), для которых сумма их индексов Винера зависит только от их количества и размера. Именно, доказано, что $W(\Theta) = \sum_{G\in\Theta} W(G) = |\Theta|\, \phi(h),$ где Θ есть множество подсетей, суммирование ведется по всем подсетям G, а $\phi(h)$ есть полином третьей степени от числа колец h в подсетях (размер подсетей). Разработанный подход может быть использован для характеризации свойств гексагональных сетей.

1.3. Совершенные раскраски и коды

1. Под совершенной раскраской в m цветов (совершенной m-раскраской) графа G с матрицей A понимается раскраска множества вершин графа G в множество цветов 1,..,m такая, что число вершин цвета j, смежных с фиксированной вершиной цвета i, не зависит от выбора последней вершины и равно a_{ij}. Матрица А называется матрицей параметров совершенной раскраски. Основной задачей является поиск новых совершенных раскрасок различных графов, особый интерес представляют совершенные 2-раскраски графов Джонсона. Отметим, что полностью регулярные, в том числе совершенные коды могут быть определены как совершенные раскраски. Полностью регулярные коды обладают хорошими алгебро-комбинаторными свойствами и включают в себя многие известные коды, такие как, совершенные, расширенные совершенные, Препараты, некоторые БЧХ и другие [46-57].

Дистанционно-бирегулярным графом G называется двудольный граф, каждая вершина которого является полностью регулярными кодом; массивы пересечений двух вершин совпадают, если эти вершины принадлежат одной доле. Соединив вершины, находящиеся на расстоянии 2 в *G*, получим два графа, именуемых половинными графами дистанционно-бирегулярного графа *G*. Известно, что половинные графы дистанционно-бирегулярного графа являются дистанционно-регулярными. Примером дистанционно-бирегулярного графа является граф, индуцированный совокупностью вершин графа Хэмминга $H(n,2)$, имеющих вес d и $d+1$. Половинными графами такого графа являются графы Джонсона $J(n,d)$ и $J(n,d+1)$. Совершенную 2-раскраску половинного графа G' дистанционно-бирегулярного графа G назовем сбалансированной, если вершины второго половинного графа G' имеют ровно 2 различных цветовых состава окрестностей в графе G.

Полученные в этом направлении результаты:

1.1. Показана связь совершенных раскрасок половинных графов дистанционно-бирегу-лярных графов и существование новых совершенных 2-раскрасок графов Джонсона $J(n,w)$.

1.2. Доказано, что раскраска вершин графа G', при которой вершины одного цветового состава красятся в один цвет, является совершенной раскраской в 2 цвета, найдены параметры раскраски. На основе вышеописанных результатов получена новая серия совершенных 2-раскрасок графов Джонсона J(n,4) и J(n,5) из систем троек и четверок Штейнера.

2. Среди транзитивных кодов можно особо выделить пропролинейные коды, как коды, наиболее близкие к групповым, так как они позволяют определить групповую операцию на кодовых словах. Код называется пропролинейным, если существует набор подстановок p_x, где x из C, что (i) Для любого x выполняется: $p_x+p_x(C)=C$ (ii) Для любых кодовых слов x и y выполняется: $p_{x+px(y)}=p_x\, p_y$. Нетрудно видеть, что свойство (i) эквивалентно транзитивности кода C. Используя теоретико-групповую терминологию, свойство (ii) можно переформулировать следующим образом: группа автоморфизмов кода C содержит регулярную подгруппу, действующую транзитивно на всех его кодовых словах. Последнее свойство позволяет определить бинарную операцию на кодовых словах кода C: $x*y=x+p_x(y)$, относительно которой код C образует группу. Очевидно, что группа, задаваемая операцией *, зависит от выбора подстановок p_x. Такую группу называют пропролинейной структурой на коде C. Отметим, что для одного кода может существовать большое количество как различных, так и неизоморфных пропролинейных структур на нем. Это говорит о потенциальной возможности использования пропролинейных кодов на практике в криптографии - в аналогах таких криптосистем, как криптосистемы Мак-Элиса и Ниддерайтера. Отдельно среди пропролинейных структур на коде можно выделить нормализованно-пропролинейные, для которых $p_x=p_y$ тогда и только тогда когда x+y принадлежат ядру кода C. Коды с такими пропролинейными структурами называются нормализованно-пропролинейными. Поиск пропролинейных структур является предпоч-

тительным с вычислительной точки зрения и, возможно, с практической, для применения в асимметричных криптосистемах. Среди основных проблем и задач, связанных с прополинейными кодами можно выделить нахождение новых прополинейных кодов и получение прополинейного нетранзитивного кода.

В это направлении получены следующий результат:

Найдены новые бесконечные серии нормализованно-прополинейных совершенных кодов из транзитивных кодов классификации Малюгина кодов, получаемых из кода Хэмминга одношаговыми свитчингами. Также доказано, что код Беста с параметрами (10,40,4) является транзитивным кодом, который не является прополинейным.

3. Пусть H_n – это гиперкуб размерности n. Вершины куба – двоичные наборы длины n; вершины смежны, если соответствующие им наборы отличаются ровно в одной координате. Весом $wt(y)$ вершины $y \in H_n$ называется количество единиц в этом наборе. Расстояние Хэмминга $d(x,y)$ между вершинами $x,y \in H_n$ – это количество позиций, в которых x и y различны. Будем называть сферой радиуса r с центром в точке x множество $S(x,r) = \{y \in H_n : d(x,y) = r\}$, а шаром радиуса r с центром в точке x множество $S(x,r) = \{y \in H_n : d(x,y) \leq r\}$. Полиномом Кравчука степени r называется полином $P_r(x,n) = \sum_{i=0}^{i=r} (-1)^i \binom{x}{i}\binom{n-x}{r-i}$. Отображение $T: H_n \to \{1,2,\dots,k\}$ является совершенной раскраской вершин куба в k цветов с матрицей параметров $s_{ij}, i,j \in \{1,2,\dots,k\}$ если оно сюрьективно и для каждых i, j у любой вершины цвета i число соседей цвета j равно s_{ij}. Соответственно раскраска вершин куба в 2 цвета называется совершенной с матрицей параметров $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, если каждая вершина первого цвета имеет a соседей первого цвета и b соседей второго цвета, а каждая вершина второго цвета имеет c соседей первого цвета и d соседей второго. Подмножество вершин графа называется k-кратным совершенным кодом радиуса r, если для каждой вершины шар радиуса r с центром в этой вершине содержит в точности k кодовых вершин. В случае $k = 1$ мы получаем классическое определение совершенного кода. Задача перечисления всех параметров n, r, k при которых такие коды существуют, была решена независимо Зиновьевым, Леонтьевым и Тиетвайненом. При произвольном k эта проблема еще далека от решения. В соответствии с введенными определениями ставится задача: найти все n, b, c такие, что соответствующая совершенная раскраска будет совершенным k-кодом. Полученные результаты по совершенным раскраскам:

3.1. Установлен критерий, который по параметрам совершенной 2-раскраски двоичного n-куба определяет, является ли она кратным совершенным кодом заданного радиуса $r > 1$

некоторой кратности. Показано, что существуют кратные совершенные коды любого нечетного радиуса сколь угодно большой длины.

3.2. В терминах совершенных структур охарактеризованы коды с параметрами трижды укороченных 1-совершенных двоичных кодов. Доказано, что соответствующие расширенные коды (с расстоянием 4) всегда порождают совершенную раскраску (регулярное разбиение) вершин гиперкуба в шесть цветов.

3.3. Совершенная раскраска с параметрами $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ является кратным совершенным кодом радиуса r тогда и только тогда, когда $\mathrm{P_r}(\frac{b+c}{2} - 1, \mathrm{n} - 1) = 0$, при этом кратность кода $\mathrm{k} = \frac{c}{b+c}\sum_{i=0}^{r}\binom{n}{i}$.

При $r = 1$ критерий выглядит так: $c = a + 1$, т. е. параметрами совершенных раскрасок, являющихся совершенными кратными кодами, будут $\begin{pmatrix} c-1 & b \\ c & d-1 \end{pmatrix}$ с кратностью $k = c$. Известно, что такие совершенные раскраски существуют для любых допустимых b, c, причем они будут кратными совершенными кодами любого нечётного радиуса, так как по определению $P_r(\frac{n-1}{2}, n-1) = 0$ при нечётных r. Таким образом, $\forall m, l, r \in N : r \equiv 1 \pmod 2$ существуют кратные совершенные коды радиуса 1 при $n = 2^m l{+}1$ кратности $k = i \cdot l$ для всех $\mathrm{i} \in \{1, \ldots, 2^m\}$, $i \equiv 1 \pmod 2$. Эти же коды будут кратными совершенными кодами любого нечётного радиуса. Рассмотрены критерии также для случаев $r = 2$ и $r = 3$. Приведены все совершенные раскраски, являющиеся кратными совершенными кодами радиуса 2 в 10-мерном кубе и соответствующие им кратности.

На сегодняшний день существуют конструкции, позволяющие строить большое число различных совершенных раскрасок с различными параметрами. Приведённые выше результаты позволяют искать среди них неизвестные ранее кратные совершенные коды. Описанные в статье определения и задачи легко переносятся и на другие классы графов такие, как кубические транзитивные, циркулярные и графы Джонсона.

4. Коды с параметрами несколько раз укороченных двоичных 1-совершенных кодов имеют параметры, близкие к параметрам совершенных кодов. В частности, трижды (и меньшее число раз) укороченные 1-совершенные коды являются оптимальными. До настоящего времени о множестве всех кодов с такими параметрами больше ничего известно не было. Нами получены следующие результаты.

Установлены регулярные свойства всех таких кодов (варианты дистанционной инвариантности, полной регулярности, корреляционная иммунность характеристической функции). Это дало возможность классифицировать эти кодов длины 12 при помощи ЭВМ, число классов эквивалентности равно 237610. Аналогичный результат получен для дважды укороченных 1-совершенных кодов. Вычислена группа автоморфизмов Z2Z4-линейных 1-совершенных двоичных кодов.

5. Пусть $G = (V, E)$ – регулярный граф. Для всякого кода (т.е. подмножества вершин) C определим дистанционное разбиение множества вершин этого графа относительно C: $V = \cup_{i=0,\dots,p} C_i$, где $p = \max\{d(x, C)\colon x \in C\}$ является радиусом покрытия кода C. Код C в G называется полностью регулярным, если любая вершина из слоя C_j имеет γ_j, α_j, β_j соседей соответственно из слоев C_{j-1}, C_j и C_{j+1}. Набор чисел $\{\gamma_j, \alpha_j, \beta_j : j = 0, \dots, p\}$ называется массивом пересечения кода C. Вершинами графа Джонсона $J(n, w)$ являются все w-элементные подмножества n-элементного множества; две вершины смежны, если их пересечение имеет мощность $w - 1$. Совокупность w-элементных подмножеств n-элементного множества (блоков), называется $t - (n, w, \lambda)$-схемой, если любое t- элементное подмножество содержится в точности в λ блоках. Рассматриваются лишь схемы, у которых все блоки различны. Блоки такой схемы можно рассматривать как вершины графа Джонсона. Силой схемы называется максимальное t, для которого она является $t - (n, w, \lambda)$-схемой.

Известно, что полностью регулярные коды в графах Джонсона можно рассматривать как подкласс t-схем со специальными комбинаторными свойствами. Ранее разными авторами было получено конструктивное описание всех полностью регулярных кодов силы 0 в графах Джонсона, а также показано, что всякая блок-схема силы $w - 1$ с размером блока w является полностью регулярным кодом в графе $J(n, w)$. Эти схемы включают в себя широко известные системы троек и четверок Штейнера. Здесь рассматриваются классические конструкции Оллтопа расширения блок-схем из существующих и показывается, что их применение к полностью регулярным кодам дает новые полностью регулярные коды. В качестве исходных блок-схем для этих конструкций берутся блок-схемы с размером блока, равным половине от числа точек. Пусть D является $t - (n, w, \lambda)$-схемой. Введем следующие обозначения: $D^1 = \{\Delta \cup (n + 1) : \Delta \in D\}$, $D^2 = \{\{1, \dots, n\} \setminus \Delta : \Delta \in D\}$. Рассмотрим случай, когда $n = 2w$. Опишем две конструкции Оллтопа. Ниже $\bar{D}$ обозначает подмножество вершин графа $J(2w + 1, w)$, дополнительное к D. Получены следующие результаты:

Теорема 1. *Пусть D является* $t - (2w + 1, w, \lambda)$-*схемой,* t *четно. Тогда* $D^1 \cup D^2$ *является* $(t + 1) - (2w + 2, w + 1, \lambda)$-*схемой.*

Теорема 2. *Пусть D является* $t - (2w + 1, w, \lambda)$-*схемой,* t *нечетно и* $|D| = \binom{2w+1}{w}/2$. *Тогда* $D^1 \cup \bar{D}^2$ *является* $(t + 1) - (2w, w, \lambda)$-*схемой.*

Вариант этих утверждений для полностью регулярных кодов имеет вид:

Теорема 3. *Пусть C является полностью регулярным кодом с* $p = 1$ *в* $J(2w + 1, w)$. *Тогда код* $C^1 \cup C^2$ *является полностью регулярным в* $J(2w + 2, w + 1)$.

Теорема 4. *Пусть* C *является полностью регулярным кодом с* $p = 1$ *в* $J(2w + 1, w)$, $|C| = \binom{2w+1}{w}/2$. *Тогда код* $C^1 \cup \bar{C}^2$ *является полностью регулярным в* $J(2w + 2, w + 1)$.

С использованием двух утверждений и классификации полностью регулярных кодов в $J(9, 4)$ с радиусом покрытия 1, построены полностью регулярные коды в графе $J(10, 5)$ с массивами пересечений $\{\alpha_0 = 13, \beta_0 = 12, \gamma_1 = 16, \alpha_1 = 9\}$ и $\{\alpha_0 = 5, \beta_0 = 20, \gamma_1 = 8, \alpha_1 = 17\}$. Отметим, что конструкции расширения полностью регулярных кодов применимы к кодам произвольной силы t (в отличие от варианта конструкций для блок-схем).

6. В теории пропелинейных расширенных совершенных кодов получены результаты:

6.1. Доказано, что существует экспоненциальное число неэквивалентных пропелинейных расширенных совершенных кодов с ростом длины кодов. Показано, что все такие коды имеют малый ранг, который на единицу больше ранга расширенного линейного кода Хэмминга.

6.2. Исследованы структурные свойства пропелинейных кодов, в частности, пропелинейных совершенных двоичных кодов. Исследуется связь транзитивных кодов с пропелинейными, в частности, показано, что существует двоичный код - известный код Беста длины 10, мощности 40, с кодовым расстоянием 4, который транзитивен, но не является пропелинейным. Предложено несколько конструкций пропелинейных кодов, и новый богатый класс пропелинейных совершенных двоичных кодов, названных нормализованными. Приведена нижняя оценка числа неэквивалентных пропелинейных совершенных двоичных кодов, имеющих разные ранги.

7. Изучены свойства двоичных кодов, близких по параметрам к 1-совершенным. Произвольный двоичный ($n = 2^{m-3}$, 2^{n-m-1}, 4) -код, то есть код с параметрами трижды укороченного расширенного кода Хэмминга, является элементом регулярного разбиения (цветом совершенной раскраски) вершин n-куба на шесть частей (цветов). Произвольный двоичный (n= $n = 2^{m-4}$, 2^{n-m}, 3) -код, то есть код с параметрами трижды укороченного кода Хэмминга является элементом регулярного семейства (не обязательно разбиения) из шести подмножеств вершин n-куба. Как следствие, коды C и D являются полностью полурегулярными, то есть весовое распределение такого кода зависит только от минимального и максимального веса кодовых слов и параметров кода. Более того, если код D самокомплиментарный (антиподальный), то он полностью регулярен.

7.1. Установлено, что код с параметрами дважды или трижды укороченного кода Хэмминга порождает совершенную структуру с определёнными параметрами над булевым гиперкубом. Доказан критерий регулярности разбиения вершин графов для достаточно общего класса графов.

7.2. В качестве вспомогательного результата доказывается, в терминах распределения расстояния, достаточно общий критерий регулярности разбиения вершин графов (для достаточно общего класса графов, включая дистанционно регулярные графы).

1.4. Экстремальные структуры и построение кодов

1. Множество A с заданной на нём n-арной операцией $q(x_1,..., x_n)$: $A^n \rightarrow A$ называется *n-арной квазигруппой порядка* |A|, если в уравнении $x_0 = q(x_1, ..., x_n)$ любые n элементов из x_0, x_1, ..., x_n однозначно задают оставшийся элемент. В этом случае, согласно принятым в литературе обозначениям, n-*арной квазигруппой порядка* |A| называют также операцию q. Как следует из определения, n-арная квазигруппа обратима по каждому из n аргументов (в случае конечного множества A это свойство можно взять за определение), причём обратные функции также являются n-арными квазигруппами. n-Арная квазигруппа называется *разделимой*, если она представляется в виде бесповторной суперпозиции квазигрупп меньшей арности, где порядок переменных в суперпозиции не обязан совпадать с исходным порядком аргументов квазигруппы. Подфункция n-арной квазигруппы, полученная фиксацией одной или нескольких переменных, является квазигруппой меньшей арности (размерности) и называется *ретрактом* исходной n-арной квазигруппы.

Таблица значений n-арной квазигруппы называется *латинским* n-*кубом*. Известно, что любой латинский прямоугольник дополняется до латинского квадрата (теорема Кёнига - Холла). В работах Кочела, Маккея и Ванлесса построены примеры латинских параллелепипедов любого порядка большего чем 4, не дополняемых до латинских гиперкубов.

Пусть Q(n,k) - число n-арных квазигрупп порядка k. Известно, что любая неразделимая n-арная квазигруппа порядка 4 является полулинейной. Число полулинейных квазигрупп также было вычислено ранее. При помощи теоремы о классификации получена рекуррентная формула для чисел Q(n,4). В этом направлении получены следующие результаты:

1.1. Доказано, что если все (n–2)- и (n–1)-мерные ретракты n-арной квазигруппы порядка p разделимы, то и сама квазигруппа является разделимой. Если число p является простым, то для разделимости n-арной достаточно разделимости всех её (n–1)-мерных ретрактов.

1.2. Доказано, что любой набор попарно совместимых (нигде не совпадающих) n-арных квазигрупп порядка 4 дополняется до (n+1)-арной квазигруппы. Другими словами, любой латинский параллелепипед размера $4\times4\times... \times4\times k$, где k = 1,2,3 достраивается до латинского гиперкуба.

1.3. Доказано, что при любых n> 2 и k>4 справедливы неравенства $((k–3)\,(k–1)/2)^{n/2} < \log_2 Q(n,k) < c_k(k–2)^n$, где c_k не зависит от n. Таким образом, верхняя асимптотическая граница для чисел Q(n,k) улучшена при любых k > 4, нижняя – при нечётных k > 6.

1.4. Доказано, что бесконечномерная квазигруппа порядка 4 является разделимой (представимой в виде суперпозиции) или полулинейной на каждом смежном классе по множеству аргументов с конечным носителем. Предложена конструкция неизмеримых по Лебегу множеств, основывающаяся на бесконечномерных квазигруппах.

Далее будут продолжены исследования по асимптотической оценке числа n-арных квазигрупп порядков больших 4.

2. Совершенным кликосочетанием в k-значном n-мерном кубе называется разбиение вершин куба на непересекающееся одномерные грани. В булевом n-мерном кубе понятие совершенного кликосочетания совпадает с понятием совершенного паросочетания. Совершенное кликосочетание называется точным, если в каждой двумерной грани содержится ровно один элемент кликосочетания.

Булевозначная функция называется корреляционно-иммунной порядка m, если её единицы равномерно распределены по граням размерности n–m. Булевозначная функция называется совершенной раскраской, если её единицы регулярно распределены по шарам радиуса 1, а именно количество единиц в шаре зависит только от значения функции в центре шара. Бент-функциями называются булевы функции максимально удалённые от множества линейных функций. Компонентой функции будем называть множество вершин, на котором функция отличается от другой функции с теми же параметрами.

Получены следующие результаты:

2.1. Доказано, что число совершенных кликосочетаний в k-значном n-мерном кубе выражается как k-мерный перманент массива смежности некоторого гиперграфа. Вычислен порядок логарифма числа совершенных кликосочетаний в k-значном n-мерном кубе равный $k^n \ln(n)$ при любом натуральном k и $n\to\infty$. Построены точные кликосочетания при k равном степени двойки и n=2k.

2.2. Показано, что для любого из перечисленных комбинаторных объектов мощность компоненты в промежутке между 2^k и 2^{k+1} может принимать только значения вида 2^{k+1}- 2^p, где p принимает значения между 0 и k, а 2^p - минимальная мощность компоненты для комбинаторного объекта с теми же параметрами. Для бент-функций доказано существование компонент любой мощности из данного спектра. Для совершенных раскрасок с некоторыми параметрами и корреляционно-иммунных функций найдены компоненты некоторых из указанных выше мощностей.

3. Спектром гамильтонова цикла (кода Грея) в булевом n-мерном кубе называется набор $a = (a_1, a_2, \ldots, a_n)$, где a_i – число рёбер i-го направления в цикле. Известны необходимые условия существования кода Грея со спектром a: числа a_i чётные и для любого $k = 1, \ldots, n$ сумма k произвольных компонент набора a не меньше чем $2k$. Задача состояла в том, чтобы выяснить, являются ли эти необходимые условия на спектр гамильтонова цикла достаточными для существования кода Грея с таким спектром. Нами предложено асимптотическое решение этой задачи, а именно, доказано, что любой допустимый набор является спектром гамильтонова цикла в любом булевом n-кубе, если это верно для булева N-куба при некотором достаточно большом N. В доказательстве применяется конструкция гамильтонова цикла, использующая представление булева n-куба как декартова произведения кубов размерности k и $n - k$.. Отметим, что известно несколько способов построения кодов Грея с различными свойствами, в частности, построены гамильтоновы циклы с максимально равномерным (для фиксированной размерности) спектром, найден порядок логарифма числа различных кодов Грея в булевом n-кубе, определена асимптотика логарифма этого числа (при $n \to \infty$).

3.1. Булевым n-кубом называется множество Q_n двоичных слов длины n, а также граф GQ_n, вершинами которого являются элементы Q_n, и пара вершин смежна, если и только если соответствующие слова различаются ровно в одной позиции. Рассмотрим гамильтонов цикл в GQ_k, состоящий из рёбер непересекающихся совершенных паросочетаний P_1 и P_2, и вложим паросочетание P_1 в GQ_n. Так как каждой вершине из GQ_k в декартовом произведении $GQ_k \times GQ_{n-k}$ соответствует булев $(n - k)$-куб, каждому ребру из P_1 можно поставить в соответствие пару параллельных $(n - k)$-кубов, т. е. один $(n - k + 1)$-куб. Заменим каждое ребро $v \in P_1$ гамильтоновым циклом H_v в $(n - k + 1)$-кубе, проходящим через это ребро. Удалив P_1 из объединения P_2 и циклов H_v, $v \in P_1$, получим новый гамильтонов цикл в $GQ_k \times GQ_{n-k} = GQ_n$. Если паросочетание со спектром $(b'_1, \ldots, b'_k)$ и хотя бы один из циклов в GQ_{n-k+1} имеют полный ранг, то в результате конструкции можно получить гамильтонов цикл полного ранга. Основным результатом является следующая

Теорема. *Существует такое число N, что если любой допустимый целочисленный набор длины N является спектром некоторого гамильтонова цикла (полного ранга в случае, когда $\sum_{i=1}^{k} a_i > 2^k$ при любом $k < N$), то для любого целого $n > 2$ любой допустимый целочисленный набор длины n является спектром некоторого гамильтонова цикла в GQ_n.*

3.2. Под q-ичной параллельно-последовательной контактной схемой (π-схемой) понимается обычная (двоичная) π-схема, контактам которой приписаны символы x_i^{δ}, $i = 1, \ldots, n$; $\delta = 0, 1, \ldots, q-1$. При этом символом x_i^{δ} является не булева переменная или её отрицание, а функция от x_i, определённая на $B_q = \{0, 1, \ldots, q - 1\}$ и принимающая значения из $\{0, 1\}$.

Значение функции x_i^{δ} равно 1, если $x_i = \delta$, и равно 0, если $x_i \neq \delta$. Для определённых таким образом переменных естественно ввести операции дизъюнкции и конъюнкции. Поэтому любой обобщённой π-схеме будет соответствовать формула, сложность которой определяется числом вхождений в неё переменных. Функция $f : B_q^{\,n} \to \{0, 1\}$ проводимости q-ичной π-схемы определяется по аналогии с двоичным случаем: по определению q-ичная π-схема реализует функцию $f(x_1, \ldots, x_n) = \bigvee_C Kc$, где дизъюнкция берётся по всем простым (без самопересечений) цепям, соединяющим полюсы схемы, а K_C – это конъюнкция всех функций $x_{i1}^{\delta 1}, \ldots, x_{ik}^{\delta k}$, приписанных контактам цепи C. Как и в двоичном случае, мы говорим, что контакт, помеченный x_i^{δ}, замкнут на наборе $(\alpha_1, \ldots, \alpha_n) \in B_q^{\,n}$, если $\alpha_i = \delta$, и разомкнут в противном случае. Сложностью $L(S)$ q-ичной π-схемы S называется число контактов в S. Сложностью $L_\pi(f)$ функции $f : B_q^{\,n} \to \{0, 1\}$ в классе π-схем называется $\min_S L(S)$, где минимум берётся по всем q-ичным π-схемам, реализующим f. На множестве $B_q^{\,n}$ определим следующую функцию (линейную функцию, существенно зависящую от всех своих переменных):

$$\varphi_q(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если } x_1 + \ldots + x_n = 0 \ (mod\ q), \\ 0 & \text{в противном случае.} \end{cases}$$

Установлено, что сложность реализации в классе обобщённых (троичных) π-схем троичного счётчика кратности 3, зависящего от трёх переменных, равна 18, т.е. $L_\pi(\varphi_3(x_1, x_2, x_3)) = 18$. Доказательство неравенства $L_\pi(\varphi_3(x_1, x_2, x_3)) \geq 18$ опирается на подход Храпченко В. М. к получению нижних оценок сложности π-схем.

3.3. Бесконечное вправо слово над алфавитом $\sum$ – это слово вида $\omega = \omega_1\omega_2\omega_3\ldots$, где все $\omega_i \in \sum$. Для слова ω определим число $R_\omega(i) = 0.\omega_i\,\omega_{i+1}\ldots$. Отображение $h : \sum^* \to \sum^*$ называется *морфизмом*, если $h(xy) = h(x)h(y)$ для любых слов $x, y \in \sum^*$, ω – *неподвижная точка* морфизма φ, если $\varphi(\omega) = \omega$. Всякий морфизм однозначно определяется образами символов алфавита $\sum$, которые мы назовем *блоками*. Морфизм называется *равноблочным*, если его блоки имеют одинаковую длину. Морфизм $\varphi : \sum^* \to \sum^*$ называется *маркированным*, если его блоки имеют вид $\varphi(a_i) = b_i x c_i$, где x – произвольное слово, а b_i и c_i – символы алфавита $\sum$, причем все b_i и все c_i различны. В дальнейшем рассматриваются только маркированные равноблочные морфизмы с длиной блоков l. Отметим, что для всех неподвижных точек $\varphi(\omega) = \omega$ таких морфизмов существует число L_ω такое, что любое подслово слова ω длины не менее L_ω однозначно разбивается на блоки. Определим функцию $\gamma : \mathrm{R}^2 \setminus \{(a, a) \mid a \in \mathrm{R}\} \to \{<, >\}$, которая двум различным действительным числам ставит в соответствие их отношение. Равноблочный морфизм $\varphi : \{0, 1\}^* \to \{0, 1\}^*$ будем называть *сравнимым*, если его неподвижная точка $\omega = \varphi(\omega)$ удовлетворяет следующему условию: пусть $\omega_i = \omega_j$, где $i \equiv i'\,(mod\ l)$, $j \equiv$

$j' \,(mod\; l)$ и $0 \le i',\; j' \le l-1$, причем i' и j' фиксированы. Если $i' \ne j'$ или если ω_i и ω_j лежат в блоках разного типа в правильном разбиении ω, то отношение $\gamma(R_\omega(i), R_\omega(j))$ определено однозначно. Следующие три утверждения содержат условие, по которому можно определить, является ли маркированный морфизм сравнимым.

Утверждение 1. *Пусть ω − неподвижная точка маркированного равноблочного морфизма φ, причем $\varphi(0) = A$, $\varphi(1) = B$. Тогда*

1) *если $0u1$ является подсловом A или B, причем $A = 0u0x$, где x − некоторое слово, то φ не является сравнимым морфизмом*;

2) *если $1u0$ является подсловом A или B, причем $B = 1u1x$, где x − некоторое слово, то φ не является сравнимым морфизмом*.

Утверждение 2. *Пусть ω − неподвижная точка маркированного равноблочного морфизма φ*, причем $\varphi(0) = A$, $\varphi(1) = B$. *Тогда*

1) *если $0u$ является суффиксом A или B, причем $A = 0u0x$, где x − некоторое слово, то φ не является сравнимым морфизмом*;

2) *если $1u$ является суффиксом A или B, причем $B = 1u1x$, где x − некоторое слово, то φ не является сравнимым морфизмом*.

Утверждение 3. *Пусть ω − неподвижная точка маркированного равноблочного морфизма φ, для которого не выполнены условия утверждений* 1 *и* 2. *Тогда φ − сравнимый морфизм*.

3.4. Пусть ω − бесконечное вправо непериодическое слово над алфавитом $\sum$. Тогда определим *бесконечную перестановку*, порождаемую словом ω, как упорядоченную тройку $\delta = \langle \mathrm{N}, <_\delta, < \rangle$, где $<_\delta$ и $<$ − линейные порядки на N. При этом $<_\delta$ определяется следующим образом: $i <_\delta j$ тогда и только тогда, когда $R_\omega(i) < R_\omega(j)$. Определим *комбинаторную сложность* $\lambda(n) = |\mathrm{Perm}(n)|$ перестановки δ_ω, порождаемой некоторым словом ω, как число различных её подперестановок.

Понятие перестановки, порожденной бесконечным непериодическим словом, было введено Макаровым, который вычислил комбинаторную сложность перестановок, порожденных хорошо известным семейством слов Штурма.

Найдена комбинаторная сложность перестановок, порожденных неподвижными точками сравнимых морфизмов. Определим функцию $\delta(n, z)$: если $n = l^s|z| + 1$ для некоторого натурального s, то $\delta(n, z) = 1$, иначе $\delta(n, z) = 0$.

Теорема. *Пусть ω − неподвижная точка сравнимого морфизма φ. Тогда комбинаторная сложность перестановки, порожденной ω, вычисляется следующим образом*: $\lambda(n) =$

$\sum_{a_1\in A_1}[C_{a_1}^{nar}(n)(m_{a_1}+n_{a_1}) + (C_{a_1}^{bad}(n)+C_{a_1}^{wide}(n))(m_{a_1}+2n_{a_1})] + \sum_{a_2\in A_2}C_{a_2}(n)m_{a_2} - \sum_{z\in Z}[S_z(n-1)(k_z+t_z+r_z)(1-\delta(n,z))+(k_z+r_z)\,\delta(n,z)]$ *для* $n \geq L_\omega$.

4. Связный регулярный граф $G = (V, E)$ степени k называется сильно регулярным с параметрами (v, k, λ, μ), если $|V| = v$, любая смежная пара вершин имеет λ общих соседей, и любая пара несмежных вершин имеет μ общих соседей. Пусть V – конечное множество, T – подмножество множества трехэлементных подмножеств V. T называется сильно регулярной системой троек с параметрами $\Lambda = (\lambda_0, \lambda_1, \lambda_2, \lambda_3)$ и $M = (\mu_0, \mu_1, \mu_2, \mu_3)$, если для любых трех различных вершин u, v, w верно следующее:

1. Если $\{u, v, w\} \in T$, то

(a) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\}, \{u; v; x\} \notin T\}| = \lambda_0$,

(b) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\} \notin T, \{u; v; x\} \in T\}| = \lambda_1$,

(c) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\} \notin T, \{u, x, w\}, \{u; v; x\} \in T\}| = \lambda_2$,

(d) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\}, \{u; v; x\} \in T\}| = \lambda_3$.

2. Если $\{u, v, w\} \notin T$, то

(a) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\}, \{u; v; x\} \notin T\}| = \mu_0$,

(b) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\} \notin T, \{u; v; x\} \in T\}| = \mu_1$,

(c) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\} \notin T, \{u, x, w\}, \{u; v; x\} \in T\}| = \mu_2$,

(d) $|\{x \in V \setminus \{u, v, w\} \mid \{x, v, w\}, \{u, x, w\}, \{u; v; x\} \in T\}| = \mu_3$.

Для системы троек T и любой ее вершины u определим граф G на $V \setminus \{u\}$, ребрами которого являются пары $\{v, w\}$, где $\{u; v; w\} \in T$. Говорят, что граф G *индуцирован* системой T и вершиной u. Несложно доказать, что индуцированные графы сильно регулярной системы троек являются сильно регулярными, при этом относительно любой вершины системы троек индуцируется сильно регулярный граф с одинаковым набором параметров (v, k, λ, μ). Сильно регулярная система троек T называется *сильно регулярным расширением* графа G, если в результате этой операции относительно любой вершины системы троек получается граф, изоморфный G. Исследуется существование сильно регулярных расширений сильно регулярных графов на небольшом количестве вершин. Основным результатом является

Теорема. *Существуют сильно регулярные расширения графа Петерсена с параметрами* $\Lambda = (2, 2, 0, 0)$ *и* $M = (2, 1, 1, 0)$ *и графа решетки* 3×3 *с параметрами* $\Lambda = (0, 2, 0, 1)$ *и* $M = (1, 0, 2, 0)$. *Не существует сильно регулярных расширений графов Шрикхандэ, Пэли порядка* 13 *и* $\overline{L(K6)}$.

5. Пусть $E^n = \{0, 1\}^n$ – булев куб с расстоянием Хэмминга, заданным на его вершинах: $d(x, y) = |\{i \mid x_i \neq y_i\}|$. *Двоичным кодом* длины n называется любое его подмножество. Минимальное расстояние между различными вершинами кода определяет его *кодовое рас-*

стояние. Два кода *эквивалентны*, если существует изометрия булева куба, отображающая один код в другой. Различные результаты по восстановлению кодов были получены при изучении совершенных двоичных кодов. Для них найдено подмножество кодовых слов, зная которое, можно однозначно восстановить весь код: произвольный совершенный двоичный код длины n с кодовым расстоянием 3 единственным образом определяется расположением своих кодовых слов веса $(n-1)/2$.

Пусть C – приведенный двоичный код мощности k длины n. Упорядочим векторы из $\{0\} \times E^{k-1}$ некоторым образом и обозначим через $\alpha_0, \dots, \alpha_{2^{k-1}-1}$ количество столбцов соответствующего вида в проверочной матрице кода C с нулевой верхней строкой. Зная размерности подкодов четной мощности кода C, можно составить $C_k^2 + C_k^4 + \dots = 2^{k-1} - 1$ уравнений, связывающих величины $\alpha_1, \dots, \alpha_{2^{k-1}-1}$. В дополнение имеем равенство для числа нулевых столбцов $\alpha_0 = n - \mathrm{Dim}(C)$. В результате получаем квадратную систему линейных уравнений для α_i. Известно, что эта система имеет единственное решение и тем самым невырожденна. Вопрос о минимальности набора размерностей подкодов четной мощности в терминах построенной системы формулируется следующим образом. Будет ли система при удалении одного уравнения всякий раз иметь два или более целочисленных решения? Ответом на этот вопрос служит следующий полученный результат:

Теорема. *Размерности подкодов четной мощности двоичного кода образуют минимальный набор размерностей, определяющий код с точностью до эквивалентности.*

6. Изучено избегание рамочного шаблона в перестановках. Показано, что гипотеза Стенли-Вилфа, а также теорема Эрдеша и Секереша не выполняются в общем случае для таких шаблонов.

Введено понятие рамочного шаблона и изучено избегание таких шаблонов в перестановках. Доказано, что знаменитая гипотеза Стенли-Вилфа не верна для всех рамочных шаблонов, кроме одиннадцати, из которых семь удовлетворяют гипотезе, а для четырех (все они имеют длину 4) вопрос остается открытым. Кроме того, доказано, что хорошо известная теорема Эрдеша и Секереша не выполняется для рамочных шаблонов длины больше двух. В дальнейшем развитии исследований планируется получить результаты в проблеме перечисления перестановок, одновременно избегающих двух или большего числа рамочных шаблонов длины три.

1.5. Булевы функции с экстремальными свойствами (бент-функции)

1. Бент-функции имеют большое число приложений: в криптографии, теории кодирования и теории информации. Бент-функции представляют собой булевы функции от четного

числа переменных, максимально удаленные от класса аффинных функций. Впервые бент-функции были исследованы О. Ротхаусом в 1960-х годах. Тем не менее, многие проблемы для них до сих пор остаются нерешенными. Наиболее важной проблемой представляется описание всех бент-функций или, в более упрощенном виде, нахождение конструкций бент-функций [58-60].

Известно, что любая квадратичная бент-функция аффинно эквивалентна бент-функции из класса Мэйорана–Мак-Фарланда. Поэтому интересна более общая задача нахождения нижней оценки количества бент-функций на минимальном расстоянии от произвольной бент-функции из класса Мэйорана–Мак-Фарланда. Проблема определения числа всех бент-функций – булевых функций от четного числа переменных, максимально удаленных от множества аффинных функций, – является одной из фундаментальных в этой области. Известно, что разрыв между существующими нижней и верхней оценками этого числа очень большой.

В ходе выполнения проекта получены следующие результаты:

1.1. Описываются все бент-функции на минимальном расстоянии от квадратичной бент-функции, а также показывается, что число таких бент-функций от 2k переменных равно $2^k \cdot (2^1 + 1) \cdot \ldots \cdot (2^k + 1)$.

1.2. Сформулирована гипотеза об оценке количества бент-функций на расстоянии 2^k (минимальное возможное расстояние между двумя различными бент-функциями от 2k переменных) от произвольной бент-функции.

2. Показано, что каждое изометричное отображение множества булевых функций от n переменных в себя, оставляющее класс бент-функций на месте, является комбинацией аффинного преобразования координат и сдвига на аффинную функцию. Доказано, что аффинные функции – это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние. Поставлены новые вопросы о метрической регулярности множеств в булевом кубе.

3. Для работы с булевыми функциями разработана система *Boolean Functions*. Эта система ориентирована на пользователей-программистов и представляет собой библиотеку классов и функций на языке C++. Она может быть полезна для проведения компьютерных экспериментов и тестов, связанных с булевыми функциями. Основное предназначение библиотеки – работа с булевыми функциями специального вида (бент-функциями). Дальнейшее развитие этой системы предполагает создание программных средств для работы с более широкими классами булевых функций.

1.6. Сложностные вопросы анализа данных и распознавания образов

Качественные и количественные показатели информационно-телекоммуникационных систем напрямую связаны с эффективностью и точностью методов решения проблем дискретной оптимизации. Прикладные задачи, на решение которых ориентированы эти системы, порождают многообразие редуцированных экстремальных задач, обусловленных обеспечением оптимальности состава, структуры и функционирования самих систем, обработки зашумленных потоков телекоммуникационных данных. Многие из этих задач являются типичными представителями класса так называемых труднорешаемых задач. Эта тематика тесно связана с задачами теории графов, с экстремальными задачами размещения, покрытия, маршрутизации, упаковки, разбиения, с задачами теории расписаний, математической теории анализа данных и распознавания образов [61].

Конструктивная модель какой-либо содержательной проблемы анализа данных и распознавания образов формулируется в форме задачи оптимизации подходящего критерия или функционала (максимума правдоподобия, минимума суммы квадратов уклонений и т.п.), адекватно отражающего исходную проблему. Оптимизация этого критерия в комбинации с многообразием объективно существующих структур (моделей) анализируемых данных и распознаваемых объектов порождает разнообразие редуцированных экстремальных задач, к которым сводится поиск оптимального решения. При этом сходные в содержательном плане проблемы сводятся к отличающимся экстремальным задачам. Зачастую простейшие и давно известные содержательные проблемы анализа структурированных данных и распознавания образов, типичные для актуальных приложений, сводятся к решению экстремальных задач, статус сложности которых неизвестен. Знание сложности решаемой задачи имеет решающее значение для возможности построения эффективных алгоритмов обработки структур и данных. Одной из важных проблем в этой области является определение сложности задач, связанных с поиском подмножеств векторов [62-70].

1. Доказана NP-полнота следующих актуальных задач разбиения конечного множества векторов, а также выбора подмножеств векторов в конечном множестве векторов евклидова пространства по критерию минимума суммы квадратов расстояний:

Задача SVS-FF.

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из $\mathbb{R}^q$, вектор $\mathbf{v} \in \mathbb{R}^q$, натуральные числа $M_1,\ M_2$ и положительное число A. *Вопрос*: существуют ли такие непустые непересекающиеся подмножества $\mathcal{Y}_1 \subset \mathcal{Y}$ и $\mathcal{Y}_2 \subset \mathcal{Y}$, мощности которых равны M_1 и M_2 соответственно, что имеет место неравенство

$$\frac{1}{M_1}\|\sum_{\mathbf{u}\in \mathrm{Y}_1}\mathbf{u}\|^2+2\sum_{\mathbf{y}\in \mathrm{Y}_2}(\mathbf{y},\mathbf{v})\geq A?$$

Задача SVS-NF.

Дано: множество $\mathrm{Y}=\{\mathbf{y}_1,\mathbf{y}_2,\dots,\mathbf{y}_N\}$ векторов из R^q, вектор $\mathbf{v}\in\mathrm{R}^q$, натуральное число M и положительное число A. *Вопрос*: существуют ли такие непустые непересекающиеся подмножества $\mathrm{Y}_1\subset\mathrm{Y}$ и $\mathrm{Y}_2\subset\mathrm{Y}$, что имеет место неравенство

$$\frac{1}{|\mathrm{Y}_1|}\|\sum_{\mathbf{u}\in \mathrm{Y}_1}\mathbf{u}\|^2+2\sum_{\mathbf{y}\in \mathrm{Y}_2}(\mathbf{y},\mathbf{v})\geq A,$$

при ограничении $|\mathrm{Y}_2|=M$ на мощность подмножества Y_2?

Задача SVS-FN.

Дано: множество $\mathrm{Y}=\{\mathbf{y}_1,\mathbf{y}_2,\dots,\mathbf{y}_N\}$ векторов из R^q, вектор $\mathbf{v}\in\mathrm{R}^q$, натуральное число M и положительное число A. *Вопрос*: существуют ли такие непустые непересекающиеся подмножества $\mathrm{Y}_1\subset\mathrm{Y}$ и $\mathrm{Y}_2\subset\mathrm{Y}$, что имеет место неравенство

$$\frac{1}{M}\|\sum_{\mathbf{u}\in \mathrm{Y}_1}\mathbf{u}\|^2+\sum_{\mathbf{y}\in \mathrm{Y}_2}\{2(\mathbf{y},\mathbf{v})-\|\mathbf{v}\|^2\}\geq A,$$

при ограничении $|\mathrm{Y}_1|=M$ на мощность подмножества Y_1?

Задача SVS-NN.

Дано: множество $\mathrm{Y}=\{\mathbf{y}_1,\mathbf{y}_2,\dots,\mathbf{y}_N\}$ векторов из R^q, вектор $\mathbf{v}\in\mathrm{R}^q$ и положительное число A. *Вопрос*: существуют ли такие непустые непересекающиеся подмножества $\mathrm{Y}_1\subset\mathrm{Y}$ и $\mathrm{Y}_2\subset\mathrm{Y}$, что имеет место неравенство

$$\frac{1}{|\mathrm{Y}_1|}\|\sum_{\mathbf{u}\in \mathrm{Y}_1}\mathbf{u}\|^2+\sum_{\mathbf{y}\in \mathrm{Y}_2}\{2(\mathbf{y},\mathbf{v})-\|\mathbf{v}\|^2\}\geq A?$$

Задача MSSC-NN.

Дано: множество $\mathrm{Y}=\{\mathbf{y}_1,\mathbf{y}_2,\dots,\mathbf{y}_N\}$ и алфавит $\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_K\}$ векторов из R^q, натуральное число J и положительное число A. *Вопрос*: существует ли разбиение множества Y на непустые кластеры $\mathrm{C}_1,\mathrm{C}_2,\dots,\mathrm{C}_J$, $\mathrm{B}_1,\mathrm{B}_2,\dots,\mathrm{B}_K$ и $\mathrm{B}=\mathrm{Y}\setminus((\cup_j \mathrm{C}_j)\cup(\cup_k \mathrm{B}_k))$ такое, что имеет место неравенство

$$\sum_{j=1}^{J}\sum_{\mathbf{y}\in \mathrm{C}_j}\|\mathbf{y}-\overline{\mathbf{y}}(\mathrm{C}_j)\|^2+\sum_{k=1}^{K}\sum_{\mathbf{y}\in \mathrm{B}_k}\|\mathbf{y}-\mathbf{v}_k\|^2+\sum_{\mathbf{y}\in \mathrm{B}}\|\mathbf{y}\|^2\leq A? \tag{1}$$

где $\overline{\mathbf{y}}(\mathrm{C}_j)=\frac{1}{|\mathrm{C}_j|}\sum_{\mathbf{y}\in \mathrm{C}_j}\mathbf{y}$, $j=1,2,\dots,J$, – центр j-го кластера?

Задача MSSC-FN.

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ и алфавит $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K\}$ векторов из $\mathbb{R}^q$, натуральные числа $M_1, M_2, \ldots, M_J$ и число $A>0$. *Вопрос*: существует ли разбиение множества $\mathcal{Y}$ на непустые кластеры $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_J$, $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_K$ и $\mathcal{B} = \mathcal{Y} \setminus ((\cup_j \mathcal{C}_j) \cup (\cup_k \mathcal{B}_k))$ такое, что справедливо неравенство (1), при ограничениях $|\mathcal{C}_j| = M_j$, $j = 1,2,\ldots,J$.

Задача MSSC-NF.

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ и алфавит $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K\}$ векторов из $\mathbb{R}^q$, натуральные числа $N_1, N_2, \ldots, N_K$ и число $A>0$. *Вопрос*: существует ли разбиение множества $\mathcal{Y}$ на непустые кластеры $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_J$, $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_K$ и $\mathcal{B} = \mathcal{Y} \setminus ((\cup_j \mathcal{C}_j) \cup (\cup_k \mathcal{B}_k))$ такое, что имеет место неравенство (1), при ограничениях $|\mathcal{B}_k| = N_k$, $k = 1,2,\ldots,K$.

Задача MSSC-FF.

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ и алфавит $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K\}$ векторов из $\mathbb{R}^q$, натуральные числа $M_1, M_2, \ldots, M_J$, $N_1, N_2, \ldots, N_K$ и положительное число A. *Вопрос*: существует ли разбиение множества $\mathcal{Y}$ на непустые кластеры $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_J$, $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_K$ и $\mathcal{B} = \mathcal{Y} \setminus ((\cup_j \mathcal{C}_j) \cup (\cup_k \mathcal{B}_k))$ такое, что справедливо неравенство (1), при ограничениях $|\mathcal{C}_j| = M_j$, $j = 1,2,\ldots,J$, и $|\mathcal{B}_k| = N_k$, $k = 1,2,\ldots,K$, на мощности кластеров?

2. Предложены 2-приближённые алгоритмы для следующих NP-трудных задач поиска подмножества векторов евклидова пространства по критерию минимума суммы квадратов расстояний:

Задача VS (Vector Subset).

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из $\mathbb{R}^q$ и натуральное число $M > 1$.

Найти: подмножество $\mathcal{C} \subseteq \mathcal{Y}$ мощности M такое, что целевая функция

$$S(C) = \sum_{\mathbf{y} \in C} \| \mathbf{y} - \overline{\mathbf{y}}(\mathcal{C}) \|^2 + \sum_{\mathbf{y} \in \mathcal{Y} \setminus C} \| \mathbf{y} \|^2,$$

где $\overline{\mathbf{y}}(\mathcal{C}) = \dfrac{1}{|\mathcal{C}|} \sum_{\mathbf{y} \in C} \mathbf{y}$, минимальна.

Задача VS-2 (Vector Subset 2).

Дано: множество $\mathcal{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из $\mathbb{R}^q$ и натуральное число $M > 1$.

Найти: подмножество $\mathcal{C} \subseteq \mathcal{Y}$ векторов такое, что целевая функция

$$F(\mathsf{C}) = \sum_{\mathbf{y}\in\mathsf{C}} \| \mathbf{y} - \bar{\mathbf{y}}(\mathsf{C}) \|^2 ,$$

где $\bar{\mathbf{y}}(\mathsf{C}) = \frac{1}{|\mathsf{C}|}\sum_{y\in\mathsf{C}} \mathbf{y}$, минимальна, при ограничении $|\mathsf{C}| = M$ на мощность искомого подмножества.

Задача MSSC-Case.

Дано: множество $\mathsf{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из R^q и натуральное число $M > 1$.

Найти: такое разбиение множества Y на $N - M + 1$ непустых кластеров $\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_{N-M+1}$, что мощность одного из этих кластеров равна M и

$$R(\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_{N-M+1}) = \sum_{j=1}^{N-M+1} \sum_{\mathbf{y}\in\mathsf{C}_j} \| \mathbf{y} - \bar{\mathbf{y}}_j(\mathsf{C}_j) \|^2 \to \min ,$$

где $\bar{\mathbf{y}}_j(\mathsf{C}_j) = \frac{1}{|\mathsf{C}_j|}\sum_{y\in\mathsf{C}_j} \mathbf{y}$, $j = 1, \ldots, N - M + 1$, - центр J -го кластера.

Задача VS-3 (Vector Subset 3).

Дано: множество $\mathsf{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из R^q и натуральное число $M > 1$.

Найти: подмножество $\mathsf{C} \subseteq \mathsf{Y}$ векторов такое, что целевая функция

$$H(\mathsf{C}) = \sum_{\mathbf{z}\in\mathsf{C}} \sum_{\mathbf{y}\in\mathsf{C}} \| \mathbf{y} - \mathbf{z} \|^2$$

минимальна, при ограничении $|\mathsf{C}| = M$ на мощность искомого подмножества.

Задачи VS-1, VS-2 и VS-3 полиномиально эквивалентны. Кроме того, если считать, что в задаче MSSC-Case мощность, например, первого кластера C_1 зафиксирована и равна M, то имеет место равенство, $F_4(\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_J) = F_2(\mathsf{C}_1)$, так как из условий задачи следует, что мощности кластеров из совокупности $\{\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_J\} \setminus \mathsf{C}_1$ равны 1.Поэтому задачи MSSC-Case и VS-2 эквивалентны. Известно, что в форме верификации свойств сформулированные задачи NP-полны в сильном смысле [70].

Одна из возможных содержательных трактовок проблемы анализа данных, которая приводит к решению сформулированных задач, состоит в следующем. Имеется таблица, содержащая результаты измерения набора числовых информационно значимых характеристик для совокупности некоторых материальных объектов. Часть объектов из этой совокупности идентичны и имеют одинаковые характеристики. Число идентичных объектов известно. Оставшиеся объекты различны и имеют отличающиеся характеристики. В каждом результате измерения, представленном в таблице, имеется ошибка, причем соответствие между объектом и набором неизвестно. Характеристики идентичных объектов, в отличие от характеристик остальных объектов, имеют принципиальную информационную ценность. Требуется, используя критерий минимума суммы квадратов расстояний, найти подмножество наборов, соответствующих идентичным объектам и оценить по результатам измерения набор характеристик этих объектов (учитывая, что данные содержат ошибку измерения).

Рассмотренные задачи индуцируются близкой в содержательном плане проблемой. Отличие этой проблемы от сформулированной выше состоит лишь в том, что элементы таблицы упорядочены по времени, причем известно, что временной интервал между двумя последовательными результатами измерения характеристик идентичных объектов ограничен сверху и снизу некоторыми константами. Подобные этой содержательные проблемы с временными ограничениями на результаты измерения каких-либо информационно значимых характеристик весьма актуальны, в частности, при помехоустойчивой off-line обработке числовых и векторных последовательностей, которые в приложениях трактуются как дискретные одномерные или многомерные сигналы.

Нами показана NP-полнота оптимизационных задач, которые индуцируются проблемой поиска в последовательности векторов евклидова пространства, содержащей конечное число членов, такой подпоследовательности, что она имеет фиксированное число элементов и включает векторы близкие между собой по критерию минимума суммы квадратов расстояний. Из полученного результата следует труднорешаемость соответствующей проблемы анализа упорядоченных по времени табличных данных. Остается заметить, что эффективные алгоритмы с гарантированными оценками точности для решения рассмотренных задач в настоящее время неизвестны.

1.7. Разработка программы внедрения результатов ПНИР в образовательный процесс

В ходе выполнения проекта получено много новых результатов в таких областях дискретной математики как теория графов, теория кодирования, теоретические основы криптографии, обработка и анализ данных и другим разделам, которые входят как составная часть в учебные и специальные курсы, читаемые в Новосибирском государственном университете. С момента основания Сибирского отделения и НГУ преподавателями механико-математического факультета являются активно работающие учёные институтов СО РАН, в том числе участники настоящего проекта. Для внедрения результатов ПНИР в образовательный процесс разработана программа на период 2012 – 2013 гг.

1. Программа внедрения результатов работ в 2012 году.

В 2012 г. планируется внедрение результатов, полученных в ходе выполнения первых трех этапов проекта. Эти результаты планируется включить в программы общих и специальных курсов, читаемых участниками проекта на ММФ НГУ курсов. Среди них:

1.1. Специальный учебный курс «Теория графов», читаемый старшим преподавателем к.ф.-м.н. А. Н. Глебовым студентам 1-6 курсов ММФ НГУ дополнить следующими разделами в объёме 8 академических часов:

– Теоремы Грёцша и Грюнбаума о 3-раскраске. Гипотезы Стейнберга и Хавела, их модификации и обобщения. Положительные результаты о 3-раскрашиваемости планарных графов. (4 ч.)

– Предписанные раскраски вершин и ребер графов. Характеризация предписанно 2-раскрашиваемых графов. Теорема Томассена о предписанной 5-раскрашиваемости плоских графов. Теорема Гэлвина о предписанной реберной раскраске двудольных графов. (4 ч.)

1.2. Специальный учебный курс «Криптография и криптоанализ. Современные методы», читаемый доцентом к.ф.-м.н. Н. Н. Токаревой студентам 2–6 курсов ММФ НГУ дополнить следующими разделами в объёме 10 академических часов:

– Криптографические свойства булевых функций (6 ч.).

– Математические методы доказательства криптографической стойкости шифров (4 ч.).

1.3. Специальный учебный курс «Совершенные структуры», читаемый доцентом к.ф.-м.н. С. В. Августиновичем студентам 4–6 курсов ММФ НГУ дополнить следующими разделами в объёме 8 академических часов:

– Интерпретация понятия «Совершенная структура» в терминах групповых алгебр (2 ч.).

– Метод трансфер-матрицы в перечислении раскрасок (2ч.).

– Собственные функции на графах Кели неабелевых групп (2 ч.).

– Совершенные 2-раскраски транзитивных графов (2 ч.).

1.4. Основной учебный курс «Теория графов и алгоритмы», читаемый старшим преподавателем к.ф.-м.н. А. Н. Глебовым студентам 3 курса ММФ НГУ дополнить следующими разделами в объёме 7 академических часов:

– Задача коммивояжера: общая постановка, сложностной статус, разновидности задачи. Алгоритмы точного решения. Эффективные приближенные алгоритмы. Эвристики и алгоритмы с гарантированными оценками точности. Задача об m коммивояжерах. (3 ч.).

– Теоремы Грёцша и Грюнбаума о 3-раскраске. Гипотезы Стейнберга и Хавела и их модификации. Предписанные раскраски планарных графов (4 ч.).

1.5. Специальный учебный курс «Факторные языки», читаемый доцентом к.ф.-м.н. А.Э. Фрид и аспирантом А.А. Валюженичем студентам 1-6 курсов ММФ НГУ дополнить следующими разделами в объёме 4 академических часов:

– Пример тупикового бесквадратного слова наименьшей длины над произвольным алфавитом (2 ч.).

– Теорема Файна-Вильфа, ее следствия, применения и обобщения. (2 ч.).

1.6. Специальный учебный курс «Коды и схемы», читаемый ассистентом к.ф.-м.н. И. Ю. Могильных студентам 3-6 курсов ММФ НГУ дополнить следующими разделами в объёме 8 академических часов:

– Сведение проблемы изоморфизма кодов к задаче изоморфизма графы минимальных расстояний (2 ч.).

– Орбитный метод конструирования совершенных раскрасок (2 ч.).

– Метод локальных фрагментов в задачах существования полностью регулярных кодов и совершенных раскрасок. (4 ч.).

1.7. Специальный учебный курс «Экстремальные задачи анализа данных и распознавания образов», читаемый студентам 4–6 курсов ММФ НГУ дополнить следующими разделами в объёме 8 академических часов:

– NP-полнота некоторых задач выбора подмножеств «похожих» векторов (2 ч.).

– NP-полнота некоторых задач кластерного анализа (2 ч.).

– 2-приближенный алгоритм для задачи поиска подмножества «похожих» векторов (2ч.).

– Псевдополиномиальный алгоритм для задачи поиска подмножества «похожих» векторов (2 ч.).

В печати находится учебное пособие для студентов ММФ НГУ «Симметричная криптография. Краткий курс» (54 стр., 2012), разработанное Н.Н. Токаревой. В нее включены результаты, полученные в ходе исследований свойств бент-функций.

2. Программа внедрения результатов работ в 2013 году.

В 2013 г. планируется внедрение результатов, полученных в ходе выполнения двух последних этапов проекта. Эти результаты планируется включить в программы общих и специальных курсов, читаемых участниками проекта на ММФ НГУ. Среди них:

2.1. Специальный учебный курс «Теория графов», читаемый старшим преподавателем к.ф.-м.н. А. Н. Глебовым студентам 1-6 курсов ММФ НГУ дополнить следующими разделами:

– Дистанционные раскраски плоских графов. Раскраски сетей, полученных пересечением замкнутых кривых на плоскости.

– Дистанционные метрические инварианты графов. Оценки инвариантами компактности и разветвленности структур. Индекс Винера и его свойства.

2.2. Специальный учебный курс «Криптография и криптоанализ. Современные методы», читаемый доцентом к.ф.-м.н. Н. Н. Токаревой студентам 2–6 курсов ММФ НГУ дополнить следующими разделами:

– Криптографические свойства классов бент-функций.

– Оценка криптографической стойкости шифров.

2.3. Специальный учебный курс «Совершенные структуры», читаемый доцентом к.ф.-м.н. С. В. Августиновичем студентам 4–6 курсов ММФ НГУ дополнить следующими разделами:

– Дискретное уравнение свертки.

– Теорема о периодизуемости дискретных центрированных функций.

– Многомерные перманенты в перечислительной комбинаторике

2.4. Основной учебный курс «Теория графов и алгоритмы», читаемый старшим преподавателем к.ф.-м.н. А. Н. Глебовым студентам 3 курса ММФ НГУ дополнить следующими разделами:

– Современные подходы к решению обобщений задачи коммивояжера: задачи о двух коммивояжерах на максимум и минимум с гарантированной оценкой точности.

– Метод перераспределения зарядов при решении задач раскраски плоских графов.

2.5. Специальный учебный курс «Факторные языки», читаемый доцентом к.ф.-м.н. А.Э. Фрид и аспирантом А.А. Валюженичем студентам 1-6 курсов ММФ НГУ дополнить следующими разделами:

– Схемы порождения бесконечных перестановок.

– Перестановочная сложность языков, избегающих произвольного рамочного паттерна.

2.6. Специальный учебный курс «Коды и схемы», читаемый ассистентом к.ф.-м.н. И. Ю. Могильных студентам 3-6 курсов ММФ НГУ дополнить следующими разделами:

– Использование компьютерных вычислений в теории кодирования

– Спектральные методы в исследовании совершенных структур

– Алгоритм Визинга построения минимальных совершенных раскрасок графов.

2.7. Специальный учебный курс «Экстремальные задачи анализа данных и распознавания образов», читаемый студентам 4–6 курсов ММФ НГУ дополнить следующими разделами:

– Методы доказательства NP-полноты задач кластерного анализа.

– Оценки сложности алгоритмов решения задач поиска подмножеств векторов.

1.8. Подготовка итогового отчета по НИР

При подготовке итогового отчёта осуществлён анализ полученных результатов, оценка их новизны и значимости, разработана программа внедрения результатов в учебный процесс Новосибирского государственного университета.

2. Показатели

За время выполнения НИР исполнителями защищена 1 кандидатская и 1 докторская диссертации, представлены к защите 1 докторская и 1 кандидатская диссертации (см. Приложение А).

Принято в штат Института математики им. С.Л. Соболева СО РАН 1 аспирант после защиты кандидатской диссертации. Зачислены в аспирантуру ИМ СО РАН 1 выпускник НГУ, в аспирантуру НГУ – 1 выпускник НГУ.

Количество подготовленных и опубликованных научных трудов: опубликовано 53 статьи и подготовлено 1 учебное пособие (см. Приложение Б). Количество участников проекта, опубликовавших результаты в высокорейтинговых журналах – 18. Статьи опубликованы и приняты к публикации в ведущие зарубежные и российские издания, среди которых такие журналы как «Сибирский математический журнал», «Дискретный анализ и исследование операций», «Дискретная математика», «Graphs and Combinatorics», «Combinatorics, Probability and Computing», «Random Structures and Algorithms», «Discrete Applied Mathematics», «Discrete Mathematics», «J. Automata, Languages and Combinatorics», «J. Graph Theory», «Discussione Mathematicae. Graph Theory», «Designs, Codes and Cryptography», «J. Discrete Algorithms», «J. Combinatorial Theory Ser. B».

Количество сделанных научных докладов: сделано 18 докладов на отечественных 25 докладов на международных научных форумах (см. Приложение В).

Количество проведенных семинаров: сделано 42 доклада по тематике проекта на семинарах ИМ СО РАН (см. Приложение Г).

3. Заключение

В ходе выполнения НИР получены следующие основные результаты:

- Показано, что каждый плоский субкубический плоский граф, т.е. граф со степенями не более 3, обхвата не менее 12 допускает 2-дистанционную 5-раскраску.
- Доказана предписанная ациклическая 4-раскрашиваемость плоских графов, не содержащих ни 3-циклов, смежных с циклами длины не более 6, ни 4-циклов, смежных с циклами длины не более 7.
- Доказано, что любой планарный граф, в котором 3-циклы находятся на расстоянии не менее 4 друг от друга и не имеют общих ребер с 5-циклами, является 3-раскрашиваемым.
- Получены новые условия на среднюю степень графа, дающие возможность провести декомпозицию графа на компоненты с максимальной степенью не более 1.
- Асимптотически (и в некоторых случаях точно) найдено хроматическое число для графов, тесно связанных с раскрасками евклидовых пространств.
- Рассмотрена задача о двух коммивояжерах в различных постановках. Для задачи на максимум построен приближенный алгоритм с оценкой точности 7/9 и кубической временной сложностью.
- Показана NP-полнота задачи о наименее плотном разрезе и предложены полиномиальные алгоритмы её решения для некоторых классов графов, в частности, для графов пересечений единичных интервалов и графов с ограниченной древесной шириной.
- Установлен критерий, который по параметрам совершенной 2-раскраски двоичного куба определяет, является ли она кратным совершенным кодом заданного радиуса некоторой кратности. Показано, что существуют кратные совершенные коды любого нечетного радиуса сколь угодно большой длины.
- В терминах совершенных структур охарактеризованы коды с параметрами трижды укороченных 1-совершенных двоичных кодов. Доказано, что соответствующие расширенные коды с расстоянием 4 всегда порождают совершенную раскраску вершин гиперкуба в шесть цветов.
- Установлено, что код с параметрами дважды или трижды укороченного кода Хэмминга порождает совершенную структуру с определёнными параметрами над булевым гиперкубом. Доказан критерий регулярности разбиения вершин графов для достаточно общего класса графов.
- Доказано, что существует экспоненциальное число неэквивалентных пропелинейных расширенных совершенных кодов с ростом длины кодов. Показано, что все такие ко-

ды имеют малый ранг, который на единицу больше ранга расширенного линейного кода Хэмминга.

- Показано, что каждое изометричное отображение множества булевых функций от n переменных в себя, оставляющее класс бент-функций на месте, является комбинацией аффинного преобразования координат и сдвига на аффинную функцию.
- Доказана NP-полнота актуальных задач разбиения конечного множества векторов, а также выбора подмножеств векторов в евклидовом пространства по критерию минимума суммы квадратов расстояний.

Выполненные в рамках НИР работы соответствуют требованиям технического задания, календарного плана и нормативной документации.

Приведены списки опубликованных работ, выступлений на научных форумах, а также другие показатели успешной работы в рамках данного проекта.

Полученные результаты имеют мировой уровень, а коллектив исполнителей представляет передовой фронт науки в указанных областях.

По результатам НИР можно сделать вывод о полном выполнении календарного плана работ по проекту.

4. Список использованнх источников

1. Бородин О.В., Иванова А.О., Неустроева Т.К. Предписанная (p,q)-раскраска разреженных плоских графов // Сибирские Электронные Математические Известия. 2006. Т. 3. С. 355-361.
2. Borodin O.V., Ivanova A.O., Neustroeva T. K. List 2-distance (D+1)-coloring of planar graphs with given girth // J. Applied Industrial Math., 2008, V. 2, N. 3, P. 317-328.
3. Бородин О.В., Иванова А.О. Предписанная 2-дистанционная (D+2)-раскраска плоских графов с обхватом 6 и D ≥ 24 // Сибирский мат. журнал – Т. 50, n.6,2009, С.1216-1224.
4. Borodin O.V., Ivanova A.O. 2-Distance (D+2)-coloring of planar graphs with girth six and D ≥ 18 // Discrete Math. V. 309, 2009, P. 6496-6502.
5. Montassier M., Raspaud A. A note on 2-facial coloring of plane graphs // Inform. Process. Lett. V. 98(6), 2006, P. 235-241.
6. Havet F. Choosability of square of planar subcubic graphs with large girth // Discrete Math. V.309, 2009, P. 3353-3563.
7. Jensen T.R., Toft B. Graph coloring problems. – Wiley, 1995.
8. Ando K., Iwasaki S., Kaneko A. Every 3-connected planar graph has a connected subgraph with small degree sum // Annual Meeting of Math. Society of Japan, 1993.
9. Borodin O.V. Minimal vertex degree sum of a 3-path in plane maps // Discuss. Math. Graph Theory. Vol.17, no. 2, 1997 P. 279-284.
10. Jendrol' S. Paths with restricted degrees of their vertices in planar graphs // Czechoslovak Math. J. Vol. 49 (124) (1999) P. 481-490.
11. Jendrol' S. A structural property of convex 3-polytopes // Geom. Dedicata Vol. 68 (1997), P. 91–99.
12. Jensen T.R., Thomassen C. The color space of a graph // J. Graph Theory, 34, no. 3 (2000) P. 234–245.
13. Borodin O.V. Colorings of plane graphs: a survey // Discrete Math., accepted 21.10.12.
14. Kostochka A., Prince N. On Ks,t-minors in graphs with given average degree // Discrete Math. 308, 2008, P. 4435–4445.
15. Ташкинов В.А. Однородные части однородных псевдографов // Матем. заметки, Т.36(2), 1984, С. 239–259.
16. Ташкинов В.А. 3-однородные части 4-однородных графов // Матем. заметки, Т.43(2), 1988, С. 263–275.
17. Sachs H. A three-colour-conjecture of Grötzsch./Problemes Combinatoires et Theorie des Graphes. Paris: Editions du Centre National de la Recherche Scientifique, 1978, P. 441.

18. Jaeger F. Sur les graphes couverts par leurs bicycles et la conjecture des quatre couleurs. // Problemes Combinatoires et Theorie des Graphes. Paris: Editions du Centre National de la Recherche Scientifique, 1978, P. 243–247.
19. Koester G. Coloring problems on a class of 4–regular planar graphs. // Graphs, Hypergraphs and Applications. Proc. Conference on Graph Theory, Eyba, 1984. B.G. Teubner Verlagsgesellschaft, 1985, P. 102–105.
20. Koester G. Bemerkung zu einem Problem von Grötzsch // Wiss. Z. Univ. Halle, 1984, V.33, P.129.
21. Koester G. 4–critical 4–valent planar graphs constructed with crowns. // Math. Scand., 1990, V. 67, P. 15–22.
22. Dobrynin A.A., Mel'nikov L.S. Counterexamples to Grötzsch–Sachs–Koester's conjecture. // Discrete Math., 2006, V. 306, N. 6, P. 591–594.
23. Dobrynin A.A., Mel'nikov L.S Infinite families of 4–chromatic Grötzsch–Sachs graphs. // J. Graph Theory. - 2008. - Vol. 59, n. 4 - P. 279-292.
24. Dobrynin A.A., Mel'nikov L.S. 4–chromatic edge critical Grötzsch–Sachs graphs. // Discrete Math. - 2009 - Vol. 309, n. 8 - P.2564-2566.
25. Dobrynin A.A., Mel'nikov L.S. Two 4–critical Grötzsch–Sachs graphs generated by four curves in the plane //Siberian Electronic Math. Reports, http://semr.math.nsc.ru, 2008,V.5, P. 255–278.
26. Krarup J. The peripatetic salesman and some related unsolved problems // Combinatorial programming: methods and applications (Proc. NATO Advanced Study Inst., Versailles, 1974). - 1975. - P. 173-178.
27. De Kort J.B. Lower bounds for symmetric K-peripatetic salesman problems // Optimization. - 1991. - V. 22, N 1. P. 113-122.
28. De Brey M.J.D., Volgenant A. Well-solved cases of the 2-peripatetic salesman problem // Optimization. - 1997. - V. 39, N 3. P. 275-293.
29. De Kort J.B. Upper bounds for the symmetric 2-peripatetic salesman problem // Optimization. - 1992. - V. 23, N 4. P. 357-367.
30. De Kort J.B. A branch and bound algorithm for symmetric 2-peripatetic salesman problems // European J. Oper. Res. - 1993. - V. 70, N 2. P. 229-243.
31. Duchenne E., Laporte G., Semet F. Branch-and-cut algorithms for the undirected *m*-peripatetic salesman problem // European J. Oper. Res. - 2005. - V.162, N 3- P.700-712.
32. Сердюков А.И. Алгоритм с оценкой для задачи коммивояжера на максимум // Управляемые системы. Сб. науч. тр. Вып. 25. - Новосибирск: Ин-т математики СО АН СССР, 1984. - С. 80-86.

33. Hassin R., Rubinstein S. Better approximations for max TSP // Inform. Process. Lett. - 2000. - V. 75, N 4. - P. 181-186.
34. Chen Z.-Z., Wang L. An improved randomized approximation algorithm for Max TSP // J. Comb. Optim. - 2005. - V. 9, N 4. - P. 401-432.
35. Chen Z.-Z., Okamoto Y., Wang L. Improved deterministic approximation algorithms for Max TSP // Inform. Process. Lett. - 2005. - V. 95, N 2. - P. 333-342.
36. van Zuylen A. Multiplying Pessimistic Estimators: Deterministic Approximation of Max TSP and Maximum Triangle Packing // Lecture Notes Comput. Sci.– 2010 - 619 - P.60-69.
37. Агеев А.А., Бабурин А.Е., Гимади Э.Х. Полиномиальный алгоритм с оценкой 3/4 для нахождения двух реберно непересекающихся гамильтоновых циклов максимального суммарного веса//Дискрет. анализ и исслед. операций.-Сер. 1. 2006. Т. 13, N2. С.11-20.
38. Гимади Э.Х., Глазков Ю.В., Глебов А.Н. Приближенные алгоритмы решения задачи о двух коммивояжерах в полном графе с весами ребер 1 и 2 // Дискрет. анализ и исслед. операций. - Сер. 2. 2007. - Т. 14, N2.- С. 41-61.
39. Entringer R. C., Jackson D. E., Snyder D. A. Distance in graphs // Czechoslovak Math. J. 1976. V. 26, N 2. P. 283-296.
40. Plesnik J. On the sum of all distances in a graph or digraph//J.Graph Theory. 1984.V.8,1-21.
41. Polansky O. E., Bonchev D. The Wiener number of graphs. I. General theory and changes due to some graph operations // Commun. Math. Chem. 1986. V. 21. P. 133-186.
42. Polansky O. E., Bonchev D. Theory of the Wiener number of graphs. II. Transfer graphs and some of their metric properties // Commun. Math. Chem. 1990. V. 25. P. 3-39.
43. Dobrynin A.A., Entringer R., Gutman I. Wiener index for trees: theory and applications // Acta Appl. Math. - 2001. - Vol.66, n. 3 - P. 211-249.
44. Dobrynin A.A. Branchings in trees and the calculation of the Wiener index of a tree // Comm. Math. Chem. (MATCH) - 2000 - Vol. 41 - P. 119-134.
45. Dobrynin A.A., Gutman I., Klavzar S., Zigert P. Wiener index of hexagonal systems // Acta Appl. Math. - 2002. - Vol. 72, n.3 - P. 247-294.
46. Зиновьев В. А., Леонтьев В.К. О совершенных кодах // Препринт/ИППИ АН СССР, 1972. Вып. 1. С. 26-35.
47. Зиновьев В. А., Леонтьев В.К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Вып. 2. С. 123-132.
48. Tietavainen A. On the nonexistence of perfect codes over the finite fields // SIAM J.Appl. Math. 1973. V. 24. P. 88-96.
49. Delsarte P. An Algebraic approach to the association schemes of coding theory // Philips Res. Rep. Suppl. 1973. V. 10. P.1-97.

50. Семаков Н.В., Зиновьев В.А., Зайцев Г.В. Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. N. 1. С. 38-50.
51. Van Tilborg H. C. A. Uniformly packed codes // Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 1975.
52. Gordon M.D. Perfect single error-correcting codes in the Johnson scheme // IEEE Trans. Inform. Theory. 2006. V. 52. N. 10. P. 4670-4672.
53. Martin W. J. Completely regular designs // J. Combin. Designs. 1998. V. 6. P. 261-273.
54. Dehon M. On the existence of 2-designs Sl(2,3,v) without repeated blocks // Discrete Math. 1983. V. 43. P. 155-171.
55. Hanani H. On quadruple systems // Canad. J. Math. 1960. V. 15. P. 145-157.
56. Hartman A., Phelps K. Tetrahedral quadruple systems//Utilitas Math.1990.V.37.P.181-189.
57. Phelps K.T., Stinson D.R., Vanstone S.A. The existence of simple S3(3,4,v) // Discrete Math. 1989. V. 77. P. 255-258.
58. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения // Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011, 180 с.
59. Токарева Н. Н. Группа автоморфизмов множества бент-функций // Дискретная математика. 2010. Т. 22. N 4. С. 34-42.
60. Tokareva N. On the number of bent functions: lower bounds and hypotheses // Cryptology ePrint Archive, Report 2011/083. http://eprint.iacr.org.
61. Anil K. Jain K. Data Clustering: 50 Years beyond k-means // Pattern Recognition Letters. 2010. Vol. 31. P. 651-666.
62. Aloise D., Hansen P. On the complexity of minimum sum-of-squares clustering // Les Cahiers du GERAD, G-2007-50. 2007. 12 p.
63. Aloise D., Deshpande A., Hansen P., Popat P. NP-Hardness of Euclidean sum-of-squares clustering // Les Cahiers du GERAD, G-2008-33. 2008. 4 p.
64. Mahajan M., Nimbhorkar P., Varadarajan K. The planar k-means problem is NP-hard // Lecture Notes in Computer Science. 2009. Vol. 5431. P. 284-285.
65. Долгушев А.В., Кельманов А.В. К вопросу об алгоритмической сложности одной задачи кластерного анализа // Дискр. анализ и исслед. операций.2010. Т.17,№2. С. 39-45.
66. MacQueen J. B. Some methods for classification and analysis of multivariate observations // Proc. 5-th Berkeley Symp. Math. Statistics and Probability. 1967. Vol.1. P.281-297.
67. Кельманов А.В., Пяткин А.В. О сложности одного из вариантов задачи выбора подмножества «похожих» векторов // Доклады РАН. 2008. Т.421, №5. С. 590-592.
68. Кельманов А.В., Пяткин А.В. Об одном варианте задачи выбора подмножества векторов // Дискретн. анализ и исслед. операций. 2008. Т.15, №5. С. 25-40.

69. Кельманов А.В., Пяткин А.В. О сложности некоторых задач поиска подмножеств векторов и кластерного анализа // Журн. вычисл. математики и мат. физики. 2009, Т.49, №11. С. 2059-2067.
70. Кельманов А.В., Пяткин А.В. NP-полнота некоторых задач выбора подмножества векторов // Дискретн. анализ и исслед. операций. 2010. Т.15, №5. С. 31-45.

Приложение А. Список представленных диссертаций

1. Грешнов Александр Валерьевич. «Теоремы существования и аппроксимации в некоммутативном геометрическом анализе». Специальность 01.01.01 – вещественный, комплексный и функциональный анализ. Диссертация на соискание ученой степени доктора физико-математических наук. Ведущая организация: Математический институт им. В.А. Стеклова РАН. Успешная защита состоялась 22 сентября 2011 г. в 16 часов на заседании диссертационного совета Д 003.015.03 при Институте математики им. С.Л. Соболева СО РАН по адресу: ауд. 417, пр. Академика Коптюга 4, г. Новосибирск 630090.

2. Замбалаева Долгор Жамьяновна. «Решение задачи маршрутизации и путевых разбиений графов методами раскрасок и весовых перераспределений». Специальность 01.01.09 – дискретная математика и математическая кибернетика. Диссертация на соискание ученой степени кандидата физико-математических наук. Ведущая организация: Институт математики и механики Уральского отделения РАН. Защита состоялась 30 ноября 2011 г. в 17 часов на заседании диссертационного совета Д 003.015.01 при Институте математики им. С.Л. Соболева СО РАН по адресу: ауд. 417, пр. Академика Коптюга 4, г. Новосибирск 630090.

3. Фрид Анна Эдуардовна. «Комбинаторные сложностные характеристики бесконечных слов, языков и перестановок». Специальность 01.01.09 – «дискретная математика и математическая кибернетика». Ведущая организация: Математический институт им. В.А.Стеклова РАН, г. Санкт-Петербург. Диссертация представлена на соискание ученой степени доктора физико-математических наук. Защита состоится 19 декабря 2012 г. на заседании диссертационного совета Д 003.015.01 при Институте математики им. С.Л. Соболева СО РАН по адресу: ауд. 417, пр. Академика Коптюга 4, г. Новосибирск 630090.

4. Макаров Михаил Александрович. «Комбинаторика на бесконечных перестановках». Специальность 01.01.09 – «дискретная математика и математическая кибернетика». Диссертация представлена на соискание ученой степени кандидата физико-математических наук. Ведущая организация: Уральский федеральный университет им. Б.Н. Ельцина, г. Екатеринбург. Защита состоится 21 ноября 2012 г. на заседании диссертационного совета Д 003.015.01 при Институте математики им. С.Л. Соболева СО РАН по адресу: ауд. 417, пр. Академика Коптюга 4, г. Новосибирск 630090.

Приложение Б. Список публикаций исполнителей.

Опубликованные статьи в журналах и трудах конференций

1. Бородин О.В., Иванова А.О. 2-Дистанционная 4-раскраска плоских субкубических графов // Дискретный анал. и исслед. операций, 18, № 2 (2011) 18-28.
2. Borodin O.V., Ivanova A.O. List injective colorings of planar graphs // Discrete Math., 311, no. 2-3 (2011) 154-165.
3. Бородин О.В., Иванова А.О. Ациклическая предписанная 5-раскрашиваемость плоских графов без 4-циклов // Сиб. матем. журнал, Том 52, № 3 (2011) 522-541.
4. Borodin O.V., Ivanova A.O., Montassier M., Raspaud A. (k,j)-coloring of sparse graphs // Discrete App. Math. V. 159, №17, (2011) 1947-1953.
5. Бородин О.В., Косточка А.В. Вершинные разбиения разреженных графов на независимое множество и подграф максимальной степени не более 1 // Сиб. матем. журнал, Том 52, № 5 (2011) 1004-1010.
6. Balogh J., Kostochka A.V. Large minors in graphs with given independence number // Discrete Math. – 2011 – Vol. 311, P. 2203–2215
7. Бородин О.В., Иванова А.О. Инъективная (D+1)-раскраска плоских графов с обхватом 6 // Сиб.матем. журнал – 2011 – Т. 52, № 1 – С. 30-38
8. Глебов А.Н., Замбалаева Д.Ж. Приближенный алгоритм решения задачи о двух коммивояжерах на минимум с различными весовыми функциями // Дискрет. анализ и исслед. операций. 2011. Т. 18, № 5. С. 11-37.
9. Глебов А.Н., Замбалаева Д.Ж. Полиномиальный алгоритм с оценкой точности 7/9 для задачи о двух коммивояжерах на максимум // Дискрет. анализ и исслед. операций . 2011. Т. 18, № 4. С. 17-48.
10. Глебов А.Н., Гордеева А.В., Замбалаева Д.Ж. Алгоритм с оценкой 7/5 для задачи о двух коммивояжерах на минимум с различными весовыми функциями // Сибирские электронные математические известия (htpp://semr.math.ncs.ru). 2011. Т. 8. С. 296-309.
11. Августинович С.В., Лисицына М.А. Совершенные 2-раскраски транзитивных кубических графов // Дискретн. анализ и исслед. операций. 2011. Т. 18. N 2.С.3-17.
12. Августинович С.В., Васильева А.Ю., Сергеева И.В., Дистанционно регулярные раскраски бесконечной квадратной решетки // Дискретн. анализ и исслед. операций. 2011. Т. 18. № 3. С. 3–10.
13. Avgustinovich, S.V., Mogilnykh, I.Yu. Induced perfect colorings // Siberian Electronic Mathematical Reports, Vol. 8, P. 310–316 (2011).

14. Валюженич А.А. Некоторые свойства основательных последовательностей // Дискретн. анализ и исслед. операций - 2011 - Т.18, № 1 - С. 15-19.
15. Потапов В.Н. Кликосочетания в k-значном n-мерном кубе // Сиб. мат. журн. 2011. Т. 52, N 2. С.384-392.
16. Tokareva N.N. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Communications (AMC). 2011. V. 5, N 4. P. 609-621.
17. Киселев С.А., Токарева Н. Н. О сокращении ключевого пространства шифра A5/1 и обратимости функции следующего состояния в поточном генераторе // Дискретн. анализ и исслед. операций. 2011. Т. 18. N 2. С. 51-63.
18. Krotov D.S., Potapov V.N. On connection between reducibility of an n-ary quasigroup and that of its retracts // Discrete Math. 311:1 (2011), 58-66.
19. Krotov D.S. On weight distributions of perfect colorings and completely regular codes // Designs, Codes and Cryptography, 61:3 (2011), 315-329.
20. Heden O., Krotov D.S. On the structure of non-full-rank perfect q-ary codes // Adv. Math. Communications, 5:2, A special issue ALCOMA'10 (2011), 149-156.
21. Krotov D.S., Ostergard P.R.J., Pottonen O. On optimal binary one-error-correcting codes of lengths 2^{m-4} and 2^{m-3} // IEEE Trans. Information Theory, 57:10 (2011), 6771-6779.
22. Долгушев А.В., Кельманов А.В. Приближённый алгоритм решения одной задачи кластерного анализа // Дискретн. анализ и исслед. операций. 2011. Т.18, № 2. С. 29-40.
23. Кельманов А.В. О сложности некоторых задач кластерного анализа // Ж. вычисл. матем. и матем. физики. 2011. Т.51, №11. С. 2106-2112.
24. Kelmanov A.V., Pyatkin A.V. On the complexity of some clustering problem // J. Math. System Sci. – Vol. 1, n. 1 – 2011 – P. 2-5.
25. Потапов В.Н. О дополняемости частичных n-квазигрупп порядка 4 // Матем. Труды. 2011, Т. 14, № 2, С. 1-26.
26. Krotov D.S. On the automorphism groups of the additive 1-perfect binary codes // Proc. the 3rd International Castle Meeting on Coding Theory and Applications J. Borges and M. Villanueva (eds.) Barcelona, Spain, 2011. 171-176.
27. Borodin O.V., Ivanova A.O. List 2-facial 5-colorability of plane graphs with girth at least 12 // Discrete Math. 312, no. 2, 2012, P. 306–314.
28. Borodin O.V., Ivanova A.O. 2-distance 4-colorability of planar subcubic graphs with girth at least 22 // Discuss. Math. Graph Theory, 32, no. 1, 2012, P. 141–151.
29. Borodin O.V., Ivanova A.O., Montassier M., Raspaud A. (k,1)-coloring of sparse graphs // Discrete Math., 312, no. 6, 2012, P. 1128–1135.

30. Августинович С.В., Васильев Ю.Л., Рычков К.Л. Формульная сложность тернарной линейной функции // Дискретн. анализ и исслед. операций. 2012. Т.19, № 3. С. 3–12.
31. Коломеец Н.А. Построение бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. операций. 2012. Т.19, № 1. С.41–58.
32. Tokareva N.N. Duality between bent functions and affine functions // Discrete Math., V. 312. 2012, P. 666-670.
33. Потапов В.Н. Построение гамильтоновых циклов с заданным спектром направлений рёбер в булевом n-мерном кубе // Дискретн. анализ и исслед. операций. 2012. Т.19, № 2. С. 75–83.
34. Dobrynin A.A., Mel'nikov L.S. Wiener index of line graphs // Distance in Molecular Graphs – Theory (Eds: Gutman I., Furtula B.), Univ. Kraguevac, 2012, P. 85–121.
35. Kostochka A.V., Yancey M. Large rainbow matchings in edge-colored graphs // Combinatorics, Probabiliy and Computing, Vol. 21, 2012, P. 255-263.
36. Avgustinovich S.V., Kitaev S.V., Pyatkin A.V., Valuzhenich A. A. On square-free permutations // J. Automata, Languages and Combinatorics, 2011, V.16, № 1, P.3-10.
37. Bonsma P., Broersma H., Patel V., Pyatkin A.V. The complexity of finding uniform sparsest cuts in various graph classes // J. Discrete Algorithms, 2012, V.14, P.136-149.
38. Kel'manov A.V., Romanchenko S.M. An approximation algorithm for solving a problem of search for a vector subset // J. Applied and Industrial Math. 2012. Vol. 6, No.1, P. 90-96.
39. Кельманов А.В., Романченко С.М. Псевдополиномиальные алгоритмы для некоторых труднорешаемых задач поиска подмножества векторов и кластерного анализа // Автоматика и телемеханика. 2012. № 2, С. 156-162.
40. Потапов В. Н., Кротов Д. С. О числе *n*-арных квазигрупп конечного порядка // Дискрет. Математика – 2012. Т. 24, N 1. – С. 60–69.
41. Воробьев К. В. Кратные совершенные коды в гиперкубе // Дискрет. анализ и исслед. операций – 2012. Т.19, № 4. – С. 60–65.
42. Макаров М. А. Антимонотонные перестановки // Сибирские электронные математические известия – 2012, Т. 9. – С. 346–359.
43. Avgustinovich S., Karhumäki J., Puzynina S. On abelian versions of critical factorization theorem // RAIRO-Theor. Inf. Appl. (ISSN: 0988-3754) – 2012, V 46, N 1. – P. 3–15.
44. Borges Q., Mogilnykh I. Yu., Rifa` J., Solov'eva F. I. Structural properties of binary propelinear codes // Advances in Math. of Communications (ISSN 1930-5346). – 2012, V. 6. N 3. – P. 329–346.
45. Frid A. E. Fine and wilf's theorem for permutations // Siberian Electronic Mathematical Reports – 2012, V. 9. P. 377–381.

46. Krotov D. S. On the binary codes with parameters of triply-shortened 1-perfect codes // Designs, Codes and Cryptography – 2012, V. 64. N 3. – P. 275–283.
47. Borodin O.V., Ivanova A.O. Acyclic 4-choosability of planar graphs without adjacent short cycles // Discrete Math. – 2012 – Vol. 312 – P. 3335-3341.
48. Dobrynin A.A., Mel'nikov L.S. 4-chromatic Grotzsch-Sachs graphs generated by circles in the plain // Discuss. Math. Graph Theory. - 2012 - vol.32, n. 4 - P. 617-627.
49. Добрынин А.А. Декомпозиция индекса Винера для графов гексагональных цепей // Информационные технологии в прикладных исследованиях – 2012 – Изд. НГУЭиУ.-С.70-77.
50. Августинович С.В., Горкунов Е.В. Восстановление кодов по коэффициентам корреляции их подкодов // Дискрет. анализ и исслед. операций – 2012. Т.19, № 6. – С. 3–8.
51. Пяткин А.В., Черных И.Д. Задача Open Shop с маршрутизацией на двухвершинной сети и с разрешением прерываний // Дискрет. анализ и исслед. операций – 2012. – Т.19, № 3. – С. 65–78.
52. Vernitski A., Pyatkin A.V. Astral graphs (threshold graphs), scale-free graphs and related algorithmic questions // J. Discrete Algorithm – Vol. 12 – 2012 – P. 24-28.
53. Borodin O.V., Glebov A.N., Jensen T.R. A step towards the strong version of Havel's three color conjecture // J. Combin. Theory Ser. B. – 2012. – Vol. 102 - P. 1295-1320.

Приложение В. Список сделанных исполнителями докладов

На всероссийских конференциях и семинарах.

1. Бородин О.В., Иванова А.О. Ациклическая раскраска плоских графов и связанные с нею задачи // VI Международная конференция по математическому моделированию, Якутск, Россия, 3-8 июля 2011, Тезисы докладов, Якутск, 2011, С. 90-91 (секционный доклад).
2. Бородин О.В., Иванова А.О. Инъективная и 2-дистанционная раскраски разреженных плоских графов // VI Международная конференция по математическому моделированию, Якутск, Россия, 3-8 июля 2011, Тезисы докладов, Якутск, 2011, С. 92-93 (секционный доклад).
3. Глебов А.Н, Замбалаева Д.Ж., Ивонина Е.В. Эффективные алгоритмы с гарантированными оценками точности для задач одного и двух коммивояжеров на максимум // Байкальская школа-семинар «Методы оптимизации и их приложения» – 2011, пос. Листвянка, о. Байкал, 23–29 июня 2011 (секционный доклад).
4. Кельманов А.В. NP-полнота некоторых задач кластеризации // Математические методы распознавания образов: 15-я Всероссийская конференция, г. Петрозаводск, 11–17 сентября 2011 г.: Сборник докладов. – М.: МАКС Пресс, 2011. – С. 269-272. (пленарный доклад).
5. Потапов В. Н. О мощности компонент корреляционно-иммунных функций, совершенных раскрасок и кодов // Материалы XVI Международной конференции "Проблемы теоретической кибернетики" (Н.Новгород, 20--25 июня 2011 г.) Н.Новгород: Изд-во Нижегородского госуниверситета. 2011. С. 376—379 (секционный доклад).
6. Августинович С.В., Васильева А.Ю. О дистанционно регулярных раскрасках многомерных квадратных решеток. Доклад на международной конференции «Мальцевские чтения», Новосибирск, 11-14 октября 2011. (секционный доклад).
7. Кельманов А.В., Романченко С.М. Алгоритмы с оценками для некоторых задач поиска подмножества векторов и кластерного анализа, «Математические методы распознавания образов: 15-я Всероссийская конференция (ММРО-15)», г. Петрозаводск, 11–17 сент. 2011 г. (секционный доклад).
8. Кельманов А.В., Михайлова Л.В., Хамидуллин С.А. Об одной задаче поиска и идентификация векторных наборов в последовательности, «Математические методы распознавания образов: 15-я Всероссийская конференция (ММРО-15)», г. Петрозаводск, 11– 17 сент. 2011 г. (секционный доклад).

9. Потапов В.Н. О совершенных 2-раскрасках q-значного гиперкуба, 10 Сибирская научная школа-семинар «Компьютерная безопасность и криптография» (SIBECRIPT'11), Томск, 5-10 сентября 2011. (секционный доклад).
10. Токарева Н.Н. Гипотезы о числе бент-функций, 10 Сибирская научная школа-семинар «Компьютерная безопасность и криптография" (SIBECRYPT'11), г. Томск, 5-10 сентября 2011 г. (секционный доклад).
11. Коломеец Н.А. Количество бент-функций на минимальном расстоянии от квадратичной бент-функции, 10 Сибирская научная школа-семинар «Компьютерная безопасность и криптография» (SIBECRYPT'11), г. Томск, 5-10 сентября 2011 г. (секционный доклад).
12. Коломеец Н.А. Boolean Functions – система для работы с булевыми функциями 10 Сибирская научная школа-семинар «Компьютерная безопасность и криптография» (SIBECRYPT'11), г. Томск, 5-10 сентября 2011 г. (секционный доклад).
13. Августинович С.В., Горкунов Е.В. Метрические инварианты для восстановления кодов // Международная (43-я Всероссийская) молодежная школа-конференция «Современные проблемы математики», 29 января - 5 февр. 2012 г., Екатеринбург, Россия. (секционный доклад)
14. Воробьев К.В. О сильно регулярных системах троек // Международная (43-я Всероссийская) молодежная школа-конференция «Современные проблемы математики», 29 января - 5 февраля 2012 г., Екатеринбург, Россия. (секционный доклад)
15. Могильных И. Ю. Полностью регулярные коды в графах Джонсона и блок-схемы троек. Международная (43-я Всероссийская) молодежная школа-конференция «Современные проблемы математики», 29 января - 5 февр. 2012 г., Екатеринбург, Россия. (секционный доклад)
16. Пяткин А.В. Раскраска инциденторов: методы и результаты. V Всероссийская конференция «Проблемы оптимизации и экономические приложения»,Омск, 2-6 июля 2012 г. (секционный доклад)
17. Глебов А.Н, Замбалаева Д.Ж., Ивонина Е.В. Эффективные алгоритмы с гарантированными оценками точности для задач одного и двух коммивояжеров на максимум // Байкальская школа-семинар «Методы оптимизации и их приложения» – 2011, пос. Листвянка, о. Байкал, 23–29 июня 2011 (секционный доклад).
18. Глебов А.Н., Замбалаева Д. Ж. Путевые разбиения плоских графов с заданным обхватом. V Всероссийская конференция «'Проблемы оптимизации и экономические приложения». Омск, 2-4 июля 2012. С. 117. (секционный доклад)

На международных конференциях и семинарах.

1. Kostochka A.V. The Hajnal-Szemerédi theorem: extensions and variations, «Infinite and finite sets», Hungary, Budapest, 13-17 June, 2011 (приглашенный пленарный доклад).
2. Kostochka A.V. CID Conference – Colourings, Independence and Domination, Sklarska Poreba, Poland, September, 2011, (приглашенный пленарный доклад).
3. Kelmanov A.V., Pyatkin A.V. On the Complexity of Some Clustering Problems // Proceedings of II International Conference «Optimization and applications» (OPTIMA-2011), Petrovac, Montenegro, September 25 – October 2, 2011. (секционный доклад).
4. Eremin I.I., Gimadi E.Kh., Kelmanov A.V., Khachay M.Yu. Algorithm for Solving Discrete Optimization and Machine Learning Problems // Proc. II International Conference «Optimization and applications» (OPTIMA-2011), Montenegro, Sept. 25 – Oct. 2, 2011 (секционный доклад).
5. Avgustinovich S.V., Mogilnykh I.Yu. Induced perfect colorings, Международная конференция 3ICMCTA (Third International Castle Meeting on Coding Theory and Applications), Cardona, Spain. (секционный доклад).
6. Potapov V.N. On the multidimensional permanent and q-ary designs, Third Int. Castle Meeting on Coding Theory and Applications (3ICMCTA), Barcelona, Sept. 11-16 2011. (секционный доклад).
7. Kolomeec N.A. Constructions of bent functions on the minimal distance from the quadratic bent function, IEEE International Symposium on Information Theory (ISIT'2011), Saint-Petersburg, Russia, August 1-5. (секционный доклад).
8. Valyuzhenich A. Permutation Complexity of the Fixed Points of Some Uniform Binary Morphisms, Доклад на международной конференции по комбинаторике на словах WORDS2011 в сентябре 2011 года. (секционный доклад).
9. Валюженич А.А. Комбинаторная сложность перестановок, порождаемых неподвижными точками некоторых равноблочных бинарных морфизмов, Международная конференция «Современные проблемы математики, информатики и биоинформатики», посвященная 100-ю А.А.Ляпунова, 11-14 окт. 2011 г. (секционный доклад).
10. Borges J., Mogilnykh I.Yu., Rifa J., Solov'eva F.I. Groups from normalized propelinear codes, Международная конференция Мальцевские чтения-2011. (секционный доклад).
11. Воробьёв К.В. О связи совершенных 2-раскрасок с кратными совершенными кодами в гиперкубе, Международная конференция Мальцевские чтения-2011, Новосибирск, 11-14 октября 2011. (секционный доклад).

12. Потапов В.Н. О бесконечномерных квазигруппах конечных порядков, Международная конференция «Современные проблемы математики, информатики и биоинформатики» посв. 100-летию со дня рождения А.А.Ляпунова, Новосибирск, 11-14 окт. 2011. (секционный доклад).
13. Kostochka A.V. Hypergraph Ramsey numbers: triangles versus cliques. Workshop on the hypergraph Turan problem. Oberwolfach, Germany, April, 2012. (приглашенный пленарный доклад).
14. Kostochka A.V. K_st-minors in dense graphs and in (s+t)-chromatic graphs. Workshop on probabilistic methods in combinatorics, Birmingham Univ., Birmingham, UK, March, 2012. (приглашенный пленарный доклад).
15. Kostochka A.V. Improper 2-colorings of sparse graphs. 1080-th AMS Meeting at George Washington Univ. Washington, DC, March, 2012. (приглашенный пленарный доклад).
16. D. Zambalaeva, A. Glebov. 7/9-approximation algorithm for the maximum 2-PSP. International Symposium on Combinatorial Optimization 2012 (CO 2012). Said Business School, University of Oxford, 17-19 September 2012. P. 95. (секционный доклад)
17. Пяткин А.В., Кельманов А.В. О сложности некоторых задач кластеризации векторных последовательностей. 9-я международная конференция "Интеллектуализация обработки информации". Республика Черногория, г. Будва, 16–22 сентября 2012 г. (секционный доклад).
18. Потапов В. Н., Кротов Д. С. Построение транзитивных МДР-кодов на основе диэдральной группы. XI межд. семинар "Дискретная математика и ее приложения" (Москва, 18-23 июля 2012 г.) (секционный доклад).
19. Avgustinovich S., Vasil’eva A. Distance regular colorings of *n*-dimensional rectangular grid. XIII Int. Workshop on Algebraic and Combinatorial Coding Theory (Pomorie, Bulgaria, June 15-21, 2012) (секционный доклад).
20. Avgustinovich S. V., Gorkunov E. V. Strong isometries of codes. XIII Int. Workshop on Algebraic and Combinatorial Coding Theory (Pomorie, Bulgaria, June 15–21, 2012) (секционный доклад).
21. Borges Q., Mogilnykh I. Yu., Rifa` J., Solov'eva F. I. Lower bound on the number of nonequivalent propelinear extended perfect codes. XIII Int. Workshop on Algebraic and Combinatorial Coding Theory (Pomorie, Bulgaria. June 15–21, 2012). (секционный доклад).
22. Frid A., Puzynina S., Zamboni L. On minimal factorizations of words as products of palindromes. JM2012, Louvain, Belgium, September 11 - 14, 2012 (секционный доклад).

23. Krotov D. S. On calculation of the interweight distribution of an equitable partition. 2012 KIAS Int. Conference on Coding Theory and Applications, Nov. 15-17, 2012, Seoul, Korea (секционный доклад).
24. Valyuzhenich A. Permutation complexity of the fixed points of comparable binary morphisms. RuFiDiM – Second Russian Finnish Symposium on Discrete Mathematics, Turku (Finland), Sept. 25-28, 2012 (секционный доклад).
25. Паршина О. Г. О совершенных 2-раскрасках некоторых циркулянтов. 50-я Международная научная студенческая конференция “Студент и научно-технический прогресс” (13–19 апреля 2012 г.), НГУ, Новосибирск, 2012 (секционный доклад).

Приложение Г. Программа научных семинаров по проекту

1. Вершинные разбиения разреженных графов на независимое множество и подграф с максимальной степенью не более 1.
Докладчики А.В. Косточка, О.В. Бородин
2. Планарные отображения.
Докладчик С.В. Китаев
3. Графы с хроматическим числом близким к максимальной степени.
Докладчик А.В. Косточка
4. Обобщенный алгоритм Визинга построения совершенных раскрасок.
Докладчик С.В. Августинович
5. О системах четверок Штейнера, вложимых в расширенные совершенные коды.
Докладчик Д.И. Ковалевская
6. Свойства индекса Винера для одного класса графов гексагональных цепей.
Докладчик А.А. Добрынин
7. Миноры больших графов в графах с большим хроматическим числом.
Докладчик А.В. Косточка
8. О сложности некоторых задач кластерного анализа и поиска подмножеств векторов в евклидовом пространстве.
Докладчик Кельманов А.В.
9. Алгоритм (n-2)-раскраски Pancake графа.
Докладчик А.А. Терехов
10. О сложности одной задачи поиска подмножества векторов.
Докладчики Пяткин А.В., Кельманов А.В.
11. Задача о двух коммивояжерах на максимум с весами ребер 1 и 2.
Глебов А.Н., Замбалаева Д.Ж.
12. Разноцветные паросочетания в графах.
Докладчик А.В. Косточка
13. Дистанционно регулярные раскраски бесконечной квадратной решетки.
Докладчики С. В. Августинович, А. Ю. Васильева, И. В. Сергеева
14. К задаче о двух коммивояжерах на максимум с оценкой 7/9.
Докладчики А. Н. Глебов, Д. Ж. Замбалаева
15. О слабых изометриях кодов Препараты.
Докладчик И. Ю. Могильных

16. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга.

Докладчики Н. А. Коломеец, А. В.Павлов

17. О связи свитчинговой разделимости графа и его подграфов.

Докладчик Д. С. Кротов

18. Некоторые задачи синтеза схем.

Докладчик С. В. Августинович

19. О несуществовании некоторых совершенных 2-раскрасок графов Джонсона.

Докладчик И. Ю. Могильных

20. Об антиподальных графах.

Докладчик С.В. Августинович

21. О восстановлении q-значных кодов.

Докладчики Е.В. Горкунов, С.В. Августинович

22. Перестановочная сложность неподвижных точек сравнимых морфизмов.

Докладчик А.А. Валюженич

23. Антиподальные дистанционно регулярные графы.

Докладчик И.Ю. Могильных

24. О подвижных множествах в n-мерном кубе.

Докладчик В.Н. Потапов

25. О графах Кестера на 32 вершинах.

Докладчики А.А.Добрынин, Л.С. Мельников

26. О совершенных 2-раскрасках в q-значном гиперкубе.

Докладчик В.Н. Потапов

27. Индуцированные совершенные раскраски в двудольных графах.

Докладчик И.Ю. Могильных

28. О сложности задачи поиска подмножества векторов.

Докладчики А. В. Пяткин, А. В. Кельманов

29. Независимые множества в униформных гиперграфах.

Докладчик А.В. Косточка

А.В. Косточка

30. Уточнение теоремы Хайнала и Корради.

Докладчик А.В. Косточка

31. О наименьшем числе ребер в критических по раскраске графов с n вершинами.

Докладчик А.В. Косточка

32. Числа Рамсея для гиперграфов: треугольники *vs* клики.

Докладчик А.В. Косточка

33. О 4-раскрашиваемости графов без индуцированных подграфов K_3 и $2K_2$.

Докладчик А.В. Пяткин

34. Оценка комбинаторных сложностных характеристик бесконечных языков и перестановок

Докладчик А.Э. Фрид

35. Графы пересечений без треугольников со сколь угодно большим хроматическим числом.

Докладчик Ташкинов В.А.

36. Жесткость и гимильтоновость графов без индуцированных подграфов $2K_2$.

Докладчик А.В. Пяткин (3 заседания)

37. О сложности некоторых задач выбора подпоследовательности векторов.

Докладчики А.В. Кельманов, А.В. Пяткин

38. Совершенные 2-раскраски бесконечных циркулянтных графов со сплошным набором дистанций.

Докладчик О.Г. Паршина

39. Криптографические критерии булевых функций.

Докладчик А.А. Фролова

40. Совершенные коды и замощение абелевых групп.

Докладчик А.Н. Жаров

41. О свойстве антиподальности собственных функций на графах

Докладчики С.В. Августинович, Е.В. Горкунов

42. О современных направлениях в криптографии (по материалам центрально-европейской конференции по криптографии TATRACRYPT’2012)

Докладчики Н.Н. Токарева, А.А. Фролова

Целью докладов являлось ознакомление с новыми результатами и тенденциями по тематике проекта и смежным областям. По результатам семинаров не планировалось издание каких-либо материалов.