Российская академия наук
УЧРЕЖДЕНИЕ РОССИЙСКОЙ АКАДЕМИИ НАУК ИНСТИТУТ МАТЕМАТИКИ
ИМ. С.Л. СОБОЛЕВА СИБИРСКОГО ОТДЕЛЕНИЯ РАН
(ИМ СО РАН)

УДК 519.17, 519.72
№ госрегистрации 01201172121
Инв. №

УТВЕРЖДАЮ
И.о. директора
член-корреспондент РАН
______________ Гончаров С.С.
«___»______________ 2011 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: «Проведение фундаментальных исследований»
(промежуточный, этап № 2)

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

Новосибирск 2011

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

студент НГУ	___________________	Валюженич А.А. (раздел 1.2)
Студент НГУ	___________________	Лаев А.Ю. (раздел 1.7)
Нормоконтролер	___________________	Кравченко С.В.

Реферат

Отчет 43 с., 1 ч., 62 источника, 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; ТЕОРИЯ КОДИРОВАНИЯ; ДИСТАНЦИОННО РЕГУЛЯРНЫЕ КОДЫ; СОВЕРШЕННЫЕ РАСКРАСКИ; БУЛЕВЫ ФУНКЦИИ; БЕНТ-ФУНКЦИИ; КЛАСТЕРНЫЙ АНАЛИЗ.

Основным объектом исследования являются актуальные проблемы дискретной математики и ее приложений.

Основной целью проекта является получение научных результатов мирового уровня, позволяющих укрепить позиции российской школы в области теоретических направлений в дискретной математике и информатике (теория графов и ее приложения, методы эффективного кодирования и передачи информации, защита информации, анализ данных и распознавание образов). Важной целью 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.

В процессе работ использовались классические и современные методы теории графов, методы оптимизации и дискретного анализа, методы теории кодирования, а также новые подходы участников проекта.

В результате фундаментальных исследований 2 этапа получены новые результаты мирового уровня.

1. Доказано, что каждый плоский граф без 4-циклов предписанно ациклически 5-раскрашиваем, что является усилением шести зарубежных работ в этом направлении.
2. Доказана гипотеза Ванга и Ли о существовании больших радужных паросочетаний в графах с раскрашенными ребрами и большой минимальной цветовой степенью.
3. Описаны почти d-вырожденные гиперграфы с хроматическим числом d+1.
4. Получены новые нижние оценки на размер полного минора в n-вершинных графах с данным числом независимости.
5. Нйдены точные оценки на максимальную среднюю степень графа, которые гарантируют, что вершины графа можно раскрасить в два цвета таким образом, что макси-

мальная степень подграфа, порожденного вершинами первого цвета, не превосходит j, а вершинами второго цвета – не превосходит k.

6. Доказано, что любой n-вершинный граф с числом независимости α содержит минор полного $(n/(2–c)\alpha)$-вершинного графа $K_{(n/(2-c)\alpha)}$, где $c > 1/19.2$.
7. Получены новые бесконечные серии совершенных раскрасок графов Джонсона $J(n,4)$ и $J(n,5)$ из систем троек и четверок Штейнера порядка n. Показано, что всякая раскраска вершин половинного графа дистанционно-бирегулярного графа, индуцированного совершенной сбалансированной 2-раскраской второго половинного графа, является совершенной.
8. Получена новая бесконечная серия совершенных прополинейных кодов, нижняя оценка числа совершенных прополинейных кодов, найден транзитивный непрополинейный код.
9. 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.
10. Получен список параметров совершенных 2-раскрасок для ряда бесконечных серий транзитивных кубических графов, в том числе для всех графов с числом вершин, не превосходящем 18.
11. Описаны все дистанционно регулярные раскраски бесконечной квадратной решетки.
12. Разработан метод получения совершенных раскрасок из уже имеющихся путем индуцирования. С помощью этого метода найдены новые конструкции совершенных 2-раскрасок графов Джонсона.
13. Установлены регулярные свойства укороченных 1-совершенных коды кодов, что дало возможность классифицировать такие коды длины 12 Вычислена группа автоморфизмов Z2Z4-линейных 1-совершенных двоичных кодов.
14. Получено описание всех бент-функций на минимальном расстоянии от квадратичной бент-функции. Подсчитано количество таких бент-функций. Предложена нижняя оценка количества бент-функций на минимальном расстоянии от бент-функций из класса Мэйорана–Мак-Фарланда.
15. Получена новая итеративная нижняя оценка числа бент-функций.
16. Для задачи о двух коммивояжерах на минимум с различными весовыми функциями ребер, принимающими значения 1 и 2, построены следующие приближенные алгоритмы: а) алгоритм с оценкой точности 7/5 (без учета аддитивной константы) и куби-

ческой временной сложностью. б) алгоритм с оценкой точности 4/3 (без учета аддитивной константы) и временной сложностью O(n^5).

17. Для задачи о двух коммивояжерах на максимум 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 $(7q + 3)/(9q + 1)$.
18. 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.

Степень внедрения – результаты исследований используются в образовательном процессе Новосибирского государственного университета при чтении общих и специальных курсов «Теория графов», «Дискретная математика», «Совершенные структуры», «Теория графов и алгоритмы», «Теория кодирования», «Анализ данных и распознавание образов».

Полученные результаты носят фундаментальный характер и, прежде всего, являются вкладом в общую математическую теорию.

Эффективность и значимость работ, помимо чисто научных результатов, заключается в подготовке молодых ученых, непосредственно участвовавших в работах наряду с признанными специалистами, и способствуют закреплению в сфере науки и образования научных и научно-педагогических кадров.

В развитии результатов третьего этапа в последующих работах этого направления следует ожидать формирование эффективного инструментария для исследования проблем дискретной математики, использующего новые подходы и постановки задач.

В результате исследований по ряду направлений получены новые фундаментальные результаты мирового уровня, часть из которых доложена на научных форумах и подготовлена к печати.

Обозначения и сокращения

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

НГУ – Новосибирский государственный университет.

Содержание

Введение

Выполнение НИР направлено на проведение фундаментальных исследований в области анализа теоретико-графовых моделей в проблемах анализа сетей, теории кодирования и криптографии, обработке и передачи 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 (теория графов и ее приложения, методы эффективного кодирования и передачи информации, защита информации, анализ данных и распознавание образов). Одной их 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.

В запланированных исследованиях по этапу 2 делается анализ поставленных задач, и проводятся поисковые исследования в области анализа теоретико-графовых моделей, исследования алгоритмической сложности экстремальных дискретных задач, построения кодов различных типов и бент-функций. По результатам исследований подготовлены научно-методические материалы для публикаций.

1. Анализ поставленных задач. Поисковые исследования в области анализа теоретико-графовых моделей, исследования алгоритмической сложности экстремальных дискретных задач, построения кодов различных типов и бент-фунций

В рамках работ второго этапа НИР основной акцент сделан на исследование конкретных проблем в теории графов и смежных вопросах теории кодирования, в области обработки, передаче и защите информации, в анализе данных и распознавании образов

В отчете приведено описание работ по пунктам календарного плана в соответствии с техническим заданием.

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. В теоретических исследованиях проблемы распределения радиочастот в мобильных 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. На практике $p \geq q$, поскольку с увеличением расстояния интерференция волн ослабевает. При $p = 1$ и $q = 2$ возникает задача 2-дистанционной раскраски плоских графов. Это направление теоретических исследований в теории графов в настоящее время интенсивно развивается и имеет перспективные приложения для построения и анализа структур телекоммуникационных сетей. Интересным типом раскраски, возникающей в приложениях (кодирование) является инъективная раскраска. Она похожа на 2-дистанционную, только соседние вершины можно красить в одинаковый цвет. В области теории раскраски графов и ее приложений коллектив исполнителей ведет активную работу много лет (см., например, публикации [1-15]), а в теории плоских графов является одним из ведущих в мире.

В этом направлении работ по 2 этапу получены следующие результаты:

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

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

3. 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).

4. 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 $\varphi_{j,k}(G) = –1/(k+1)$.

5. 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.

6. 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 $c > 1/19.2$.

7. 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.

8. 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.

1.2 Экстремальные структуры и построение кодов.

Множество A с заданной на нём n-арной операцией $q(x_1,..., x_n)$: $A^n \to A$ 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). Продолжены исследования по асимптотической оценке числа n-арных квазигрупп порядков больших 4.

В этом направлении получены следующие результаты:

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.

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 4×4×... ×4×k, где k = 1,2,3 достраивается до латинского гиперкуба.

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.

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.

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:

5. 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.

6. 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.

1.3 Совершенные раскраски и коды

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 A 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 [16-30].

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 результаты:

1. Показана связь совершенных раскрасок половинных графов дистанционно-бирегулярных графов и существование новых совершенных 2-раскрасок графов Джонсона J(n,w).

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.

Среди транзитивных кодов можно особо выделить пррополинейные коды, как коды, наиболее близкие к групповым, так как они позволяют определить групповую операцию на кодовых словах. Код называется прополинейным, 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 прополинейной структурой на коде C. Отметим, что для одного кода может существовать большое количество как различных, так и неизоморфных прополинейных структур на нем. Это говорит о потенциальной возможности использования прополинейных кодов на практике в криптографии - в аналогах таких криптосистем, как криптосистемы Мак-Элиса и Ниддерайтера. Отдельно среди прополинейных структур на коде можно выделить нормализованно-прополинейные, для которых $p_x=p_y$ тогда и только тогда когда x+y принадлежат ядру кода C. Коды с такими прополинейными структурами называются нормализованно-прополинейными. Поиск прополинейных структур является предпочтительным 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.

Получен следующий результат:

3. 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 пропролинейным.

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 $S(x,r) = \{y \in H_n: d(x,y) \le r\}$. 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 [17-19]. 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.

4. 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.

5. 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.

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.

Получены следующие результаты.

6. 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.

1.4 Булевы функции с экстремальными свойствами (бент-функции)

Бент-функции – это булевы функции от четного числа переменных, максимально удаленные от класса аффинных функций. Впервые бент-функции были рассмотрены О. Ротхаусом в 1960-х годах. Бент-функции имеют большое число приложений: в криптографии, теории кодирования, теории информации [38, 39]. Тем не менее, для них до сих пор существует много нерешенных проблем. Наиболее важная проблема – описание всех бент-функций. Или, в более упрощенном виде, нахождение конструкций бент-функций. 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. Описываются все бент-функции на минимальном расстоянии от квадратичной бент-функции, а также показывается, что число таких бент-функций от 2k переменных равно $2^k \cdot (2^1 + 1) \cdot \ldots \cdot (2^k + 1)$.

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.

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 С++. 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).

1.5 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 [39–47].

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.

В отчетном этапе проекта анализировались и исследовались следующие задачи разбиения конечного множества векторов, а также выбора подмножеств векторов в конечном множестве векторов евклидова пространства.

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

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

Задача SVS-NF.

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

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

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

Задача SVS-FN.

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

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

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

Задача SVS-NN.

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

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

Задача MSSC-NN.

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 $\mathbb{R}^q$, натуральное число J и положительное число A. *Вопрос*: существует ли разбиение множества $\mathcal{Y}$

на непустые кластеры $\mathsf{C}_1,\mathsf{C}_2,\ldots,\mathsf{C}_J$, $\mathsf{B}_1,\mathsf{B}_2,\ldots,\mathsf{B}_K$ и $\mathsf{B} = \mathsf{Y} \setminus ((\cup_j \mathsf{C}_j) \cup (\cup_k \mathsf{B}_k))$ такое, что имеет место неравенство

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

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

Задача MSSC-FN.

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

Задача MSSC-NF.

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

Задача MSSC-FF.

Дано: множество $\mathsf{Y} = \{\mathbf{y}_1,\mathbf{y}_2,\ldots,\mathbf{y}_N\}$ и алфавит $\{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K\}$ векторов из 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 Y на непустые кластеры $\mathsf{C}_1,\mathsf{C}_2,\ldots,\mathsf{C}_J$, $\mathsf{B}_1,\mathsf{B}_2,\ldots,\mathsf{B}_K$ и $\mathsf{B} = \mathsf{Y} \setminus ((\cup_j \mathsf{C}_j) \cup (\cup_k \mathsf{B}_k))$ такое, что справедливо неравенство (1), при ограничениях $|\mathsf{C}_j| = M_j$, $j = 1,2,\ldots,J$, и $|\mathsf{B}_k| = N_k$, $k = 1,2,\ldots,K$, на мощности кластеров?

Основным результатом настоящей работы является установление статуса NP-полноты сформулированных выше задач.

Для приведенных ниже задач построены полиномиальные 2-приближенные алгоритмы.

Задача VS (Vector Subset).

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 $\mathsf{C} \subseteq \mathsf{Y}$ мощности M такое, что целевая функция

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

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

Задача VS-2 (Vector Subset 2).

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

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

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

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

Задача MSSC-Case.

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

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

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

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

Задача VS-3 (Vector Subset 3).

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

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

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

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

По результатам проведенных исследований на этапе 2 получены следующие результаты.

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

2. Предложен 2-приближённый алгоритм для труднорешаемой задачи, к которой сводится одна из проблем разбиения множества векторов евклидова пространства на два подмножества (кластера) по критерию минимума суммы квадратов расстояний.

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

1.6 Метрические инварианты графов

Инвариантом f графа называется функция на графах, принимающая одинаковые значения на изоморфных графах, т.е. если для графов G и H выполняется $G \cong H$, то $f(G)=f(H)$. Метрические инварианты графов, определяемые как функции от расстояний между вершинами графа, находят многочисленные приложения в областях, для которых изучаемые объекты или отношения между ними моделируются графами. В качестве моделей структуры коммуникационных сетей традиционно используются неориентированные или ориентированные графы и гиперграфы. Для приближенной характеризации «структурной сложности» часто используются интегральные метрические инварианты, которые характеризуют структуру описываемого объекта (разветвленность, компактность) и являются эффективно вычислимыми. Активно применяемым инвариантом является индекс Винера, $W(G)$, определяемый как сумма расстояний между всеми парами вершин в графе, где под расстоянием понимается длина кратчайшей цепи, соединяющей пару вершин в G. В силу универсальности этого инварианта он используется во многих приложениях – от характеризации молекулярных графов до оценки компактности сетей.

Известно, что по заданному графу можно строить новый граф, более значимо отражающий те или иные особенности исходного графа. Одним из таких графов является реберный граф, порождаемый смежностью ребер в исходном графе. Реберный граф $L(G)$ для графа G определяется следующим образом: множество вершин $L(G)$ соответствует множеству ребер графа G, и две различные вершины в $L(G)$ являются смежными тогда и только тогда, когда соответствующие им ребра смежны в G. Известно использование инвариантов реберных графов для характеризации структурной сложности исходных графов. Итерированный реберный граф определяется как $L^n(G) = L(L^{n-1}(G))$, где $L^1(G)=L(G)$. В значительной степени теория индекса Винера реберных графов была продвинута в работах участников проекта (см., например, [48–52].

В ходе выполнения работ по этапу 2 сделан обзор по свойствам индекса Винера для (итерированных) реберных графов. В обзоре затронуты следующие вопросы: оценки значений индекса Винера $W(L(G))$ в зависимости параметров графа G, значение инварианта для классов графов. Особое внимание уделяется проблеме сохранения индекса Винера, т.е. выполнению равенства $W(G) = W(L^n(\mathrm{G}))$. Рассмотрены классы графов, для которых впервые выполняется это свойство при $n = 1$ (би- и трициклические графы). Свойства этих семейств графов порождают два направления исследований – изучение инварианта при увеличении цикломатического числа графа (количества циклов) и при увеличении обхвата графа (размера цикла наименьшей длины). Систематизированы результаты по квадратичным реберным графам (n = 2), в основном, для класса ациклических структур, сформулированы открытые вопросы в теории индекса Винера для (итерированных) реберных графов. Обзор принят к печати (раздел в книге).

1.7. Оптимизационные задачи на графах и сетях

Одним из естественных обобщений классической задачи коммивояжера (Traveling Salesman Problem – TSP) является задача об m коммивояжерах m-Peripatetic Salesman Problem – m-PSP, состоящая в поиске в полном взвешенном неориентированном графе m реберно непересекающихся гамильтоновых циклов с минимальным или максимальным суммарным весом ребер. Эти задачи исследуются как для произвольной, так и метрической весовой функции. С тех пор как задача 2-PSP была впервые упомянута в [58], появилось много работ, посвященных ее исследованию. Было доказано, что задача о существовании двух реберно непересекающихся гамильтоновых циклов в неориентированном графе NP-полна, что влечет NP-трудность задачи 2-PSP как на минимум, так и на максимум даже в случае, если веса ребер принимают лишь значения 1 и 2. В [59] рассматривались некоторые полиномиально разрешимые случаи задачи на минимум 2-PSP. В работах [60,61] были предложены и проанализированы некоторые способы нахождения нижних и верхних оценок для применения в методе ветвей и границ. В [62] представлен полиэдральный подход к решению задачи m-PSP. Ввиду NP-трудности известных модификаций задач TSP и m-PSP большинство работ, посвященных их исследованию, связано с анализом полиномиально разрешимых случаев а также с построением приближенных эвристических алгоритмов и полиномиальных алгоритмов (как детерминированных, так и рандомизированных) с гарантированными оценками точности для полученного решения.

В ходе выполнения работ по проекту были получены следующие результаты для задачи коммивояжера:

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).

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 слу-

чая, когда весовая функция принимает значения в промежутке [1,q], получена модификация указанного алгоритма, имеющая оценку точности (7q + 3)/(9q + 1).

Важными характеристиками коммуникационных сетей с точки зрения их живучести являются их уязвимость и надежность. Эти параметры определяют как сеть продолжает функционировать при разрушении ее узлов и связей. В теоретико-графовой модели сети указанным характеристикам живучести соответствуют понятия связности и реберной связности графа. 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. Задача о наименее плотном разрезе заключается в поиске в данном графе разреза с минимальной плотностью. В этом направлении на этапе 2 получены следующие результаты:

1. 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.

2. Звёздный индекс графа – это минимальное число звёздных (или пороговых) подграфов, которыми можно покрыть все рёбра графа, делённое на число вершин. Найдены некоторые оценки для звёздного индекса. Доказано, что задача определения его точного значения является NP-полной.

1.8. Полученные результаты

Здесь приводится список всех результатов, выполненных в ходе фундаментальных поисковых исследований на этапе 2 проекта (из этого списка в заключении указаны только результаты мирового уровня).

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

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

3. 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).

4. 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. Построены графы с наибольшей сред-

ней степенью сколько угодно близкой к $2(2-(k+2)/(j+2)(k+1))$, которые не являются (j,k)-раскрашиваемыми.

5. Доказано, что любой n-вершинный граф с числом независимости α содержит минор полного $(n/(2-c)\alpha)$-вершинного графа $K_{(n/(2-c)\alpha)}$, где $c > 1/19.2$.

6. 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.

7. Полностью доказана гипотеза Ванг и Ли: 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.

8. 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.

9. 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 $4\times 4\times \ldots \times 4\times k$, где $k = 1,2,3$ достраивается до латинского гиперкуба.

10. Для числа n-арных квазигрупп порядка k, $Q(n,k)$, 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 $k > 6$.

11. 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.

12. 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 $n = 2k$.

13. 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.

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

15. 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.

16. 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.

17. Получен 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.

18. 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.

19. Установлены регулярные свойства укороченных 1-совершенных коды 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.

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

21. Для работы с булевыми функциями разработана программная система *Boolean Functions*. Основное предназначение библиотеки – работа с булевыми функциями специального вида (бент-функциями).

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

23. Предложен 2-приближённый алгоритм для труднорешаемой задачи, к которой сводится одна из проблем разбиения множества векторов евклидова пространства на два подмножества (кластера) по критерию минимума суммы квадратов расстояний.

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

25. Для задачи о двух коммивояжерах на минимум различными весовыми функциями ребер, принимающими значения 1 и 2 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 $O(n^5)$.

26. Для задачи о двух коммивояжерах на максимум 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 $(7q + 3)/(9q + 1)$.

27. 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.

28. Получены оценки звёздного индекса графов. Доказано, что задача определения его точного значения является NP-полной.

2. Подготовка научно-методических материалов для публикаций.

По результатам исследований по второму этапу опубликовано 27 статей, приняты к публикации 14 статей и отправлено в журналы 13 статей исполнителей проекта. Сделаны 11 докладов на международных и 11 докладов на отечественных научных конференциях. Статьи опубликованы и приняты к публикации в ведущих зарубежных и российских изданиях. Среди них такие журналы как «Сибирский математический журнал», «Дискретный анализ и исследование операций», «Математические заметки», «Журнал вычислительной математики и математической физики», «Проблемы передачи информации», «Автоматика и телемеханика», «Discrete Mathematics», «Discrete Applied Mathematics», «Journal of Graph Theory», «Discussione Mathematicae. Graph Theory», «Adv. Math. Communications», «Designs, Codes and Cryptography». Из других изданий отметим «Математические труды ИМ СО РАН», «Сибирские электронные математические известия» (htpp://semr.math.ncs.ru), труды конференций. В печати находится учебное пособие по криптографии для студентов НГУ.

3. Показатели

3.1. Количество подготовленных и опубликованных статей:

Вышло из печати 27 статей, приняты к печати 14 статей, отправлено в журналы 13 статей (см. Приложение А).

3.2. Количество сделанных докладов:

Сделаны 11 докладов на международных и 11 докладов на отечественных научных конференциях (см. Приложение Б).

3.3. Защиты диссертаций

Исполнителями НИР представлена 1 кандидатская и защищена 1 докторская диссертации (см. Приложение В).

3.4. Список студентов, аспирантов, докторантов и молодых исследователей, закрепленных в сфере науки и образования.

Студент НГУ Н.А. Коломеец зачислен в аспирантуру ИМ СО РАН с 01.10.2011 г.

3.5. Проведено 12 научных докладов по теме исследований (см. Приложение Г).

4. Заключение

В процессе выполнения работ по этапу 2 НИР получены следующие результаты мирового уровня.

1. Доказано, что каждый плоский граф без 4-циклов предписанно ациклически 5-раскрашиваем, что является усилением шести зарубежных работ в этом направлении.
2. Доказана гипотеза Ванга и Ли о существовании больших радужных паросочетаний в графах с раскрашенными ребрами и большой минимальной цветовой степенью.
3. Описаны почти d-вырожденные гиперграфы с хроматическим числом d+1.
4. Получены новые нижние оценки на размер полного минора в n-вершинных графах с данным числом независимости.
5. Для многих значений j и k найдены точные оценки на максимальную среднюю степень графа, которые гарантируют, что вершины графа можно раскрасить в два цвета таким образом, что максимальная степень подграфа, порожденного вершинами первого цвета, не превосходит j, а вершинами второго цвета – не превосходит k.
6. Доказано, что любой n-вершинный граф с числом независимости α содержит минор полного (n/(2–c)α)-вершинного графа $K_{(n/(2-c)\alpha)}$, где c > 1/19.2.
7. Получены новые бесконечные серии совершенных раскрасок графов Джонсона J(n,4) и J(n,5) из систем троек и четверок Штейнера порядка n. Показано, что всякая раскраска вершин половинного графа дистанционно-бирегулярного графа, индуцированного совершенной сбалансированной 2-раскраской второго половинного графа, является совершенной.
8. Получена новая бесконечная серия совершенных прополинейных кодов, нижняя оценка числа совершенных прополинейных кодов, найден транзитивный непрополинейный код.
9. 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.
10. Получен список параметров совершенных 2-раскрасок для ряда бесконечных серий транзитивных кубических графов. В частности – для всех графов с числом вершин, не превосходящем 18.
11. Описаны все дистанционно регулярные раскраски бесконечной квадратной решетки.

12. Разработан метод получения совершенных раскрасок из уже имеющихся путем индуцирования. С помощью этого метода найдены новые конструкции совершенных 2-раскрасок графов Джонсона.
13. Установлены регулярные свойства укороченных 1-совершенных коды кодов, что дало возможность классифицировать такие коды длины 12 Вычислена группа автоморфизмов Z2Z4-линейных 1-совершенных двоичных кодов.
14. Получено описание всех бент-функций на минимальном расстоянии от квадратичной бент-функции. Подсчитано количество таких бент-функций. Предложена нижняя оценка количества бент-функций на минимальном расстоянии от бент-функций из класса Мэйорана—Мак-Фарланда.
15. Получена новая итеративная нижняя оценка числа бент-функций.
16. Для задачи о двух коммивояжерах на минимум с различными весовыми функциями ребер, принимающими значения 1 и 2, 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).
17. Для задачи о двух коммивояжерах на максимум 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).
18. Показана NP-полнота задачи о наименее плотном разрезе графа и предложены полиномиальные алгоритмы её решения для некоторых классов графов, в частности, для графов пересечений единичных интервалов и для графов с ограниченной древесной шириной.

Полученные результаты доложены на различных научных форумах и будут опубликованы в высокорейтинговых журналах.

Предполагается использование полученных результатов в обязательных и специальных учебных курсах. По тематике исследований проведено 12 научных семинаров.

По результатам 2 этапа НИР представляется целесообразным продолжение работ.

5. Список использованных источников

1. Бородин О.В., Иванова А.О., Неустроева Т.К. Достаточные условия минимальной дистанционной раскрашиваемости плоских графов с обхватом 6 // Сибирские Электронные Матем. Известия - 2006 - Т. 3 - С. 441-450.
2. Бородин О.В., Иванова А.О., Неустроева Т.К. (p,q)-раскраска разреженных плоских графов // Мат. Заметки ЯГУ. 2006. Т. 13. Вып. 2. С. 3-9.
3. Бородин О.В., Иванова А.О., Неустроева Т.К. Предписанная (p,q)-раскраска разреженных плоских графов // Сибирские Электронные Матем. Известия. 2006. Т. 3. С. 355-361.
4. Бородин О.В., Дмитриев И.Г., Иванова А.О. Реберная 2-дистанционная раскраска плоских субкубических графов // Мат. заметки ЯГУ, 2008, Т. 15, вып. 1. С. 20-26.
5. Бородин О.В., Иванова А.О. Предписанная 2-дистанционная (D+2)-раскраска плоских графов с обхватом 6 и D≥24 // Сиб. мат. журнал – Т. 50, n. 6, 2009, С. 1216-1224.
6. 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.
7. Borodin O.V., Ivanova A.O. List 2-distance (D+2)-coloring of planar graphs with girth six // Europ. J. Combin. V. 30, 2009, P. 1257-1262.
8. Kostochka A.V., Kierstead H.A. Equitable versus nearly equitable coloring and the Chen-Lih-Wu conjecture // Combinatorica,V. 30, 2010, P. 201-216.
9. Kierstead H.A., Kostochka A.V., Mydlarz M., Szemeredi E. A fast algorithm for equitable coloring // Combinatorica, V. 30, 2010, P. 217-224.
10. Kostochka A.V., Rodl V. Constructions of sparse uniform hypergraphs with high chromatic number // Random Structures and Algorithms, V. 36, 2010, P. 46-56.
11. Kostochka A.V., Kumbhat M. Coloring simple uniform hypergraphs with few edges // Random Structures and Algorithms, V. 35, 2009, P. 348-368.
12. Kierstead H.A., Kostochka A.V. Ore-type versions of Brooks' theorem // J. Combin. Theory, Series B, V. 99, 2009, P. 298-305.
13. Borodin O.V., Hartke S.G., Ivanova A.O., Kostochka A.V., West D.B. Circular (5,2)-Coloring of Sparse Graphs // Siberian Electronic Math. Reports, V. 5, 2008, P. 417-426.
14. Bohme T., Kostochka A.V., Thomason A. Hadwiger numbers and over-dominating colourings // Discrete Math. V. 310, 2010, P. 2662-2665.
15. Kostochka A.V. On K{s,t} minors in (s+t)-chromatic graphs // J. Graph Theory, V. 311, 2011, V. 996-1005.
16. Hamming R.W. Error detecting and errorcorrecting codes / /Bell Syst. J. 1950.V.29. P.147-160.

17. Зиновьев В. А., Леонтьев В.К. О совершенных кодах // Препринт/ИППИ АН СССР, 1972. Вып. 1. С. 26-35.
18. Зиновьев В. А., Леонтьев В.К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Вып. 2. С. 123-132.
19. Tietavainen A. On the nonexistence of perfect codes over the finite fields // SIAM J.Appl. Math. 1973. V. 24. P. 88-96.
20. Delsarte P. An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. V. 10. P.1-97.
21. Семаков Н.В., Зиновьев В.А., Зайцев Г.В. Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. N. 1. С. 38-50.
22. Van Tilborg H. C. A. Uniformly packed codes // Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 1975.
23. Delsarte P. An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. V. 10. P.1-97.
24. Gordon M.D. Perfect Single Error-Correcting Codes in the Johnson Scheme // IEEE Trans. Inform. Theory. 2006. V. 52. N. 10. P. 4670-4672.
25. Martin W. J. Completely Regular Designs // J. Combin. Designs. 1998. V. 6. P. 261-273.
26. Dehon M. On the existence of 2-designs Sl(2,3,v) without repeated blocks // Discrete Math. 1983. V. 43. P. 155-171.
27. Hanani H. On quadruple systems // Canad. J. Math. 1960. V. 15. P. 145-157.
28. Hartman A., Phelps K. Tetrahedral quadruple systems//Utilitas Math. 1990. V.37. P.181-189.
29. 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.
30. Августинович С.В., Бородин О.В., Фрид А.Э. Дистрибутивные раскраски плоских триангуляций минимальной степени 5 // Дискрет. анализ и исслед. операций. Сер. 1. - 2001. Т. 8, N 3. - С. 3-16.
31. Августинович С.В., Могильных И.Ю. Совершенные раскраски графов Джонсона J(8,3) и J(8,4) в два цвета // Дискрет. анализ и исслед. операций. - 2010. - Т. 17, N 2. - С. 3-19.
32. Кротов Д. С. О совершенных раскрасках половинного 24-куба // Дискрет. анализ и исслед. операций. - 2008. - Т. 15, N 5. - С. 35-46.
33. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки М.:Связь, 1979.
34. Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии, М.: Изд-во МЦНМО, 2004.
35. Friedman J. On the bit extraction problem, Proc.33rd IEEE Symposium on Foundations of Computer Science (1992), P. 314-319.

36. Bierbrauer J. Bounds on orthogonal arrays and resilient functions // J. Combinatorial Designs, 3, 1995, P. 179-183.
37. Хорошилова Д.Б. О циркулярных совершенных раскрасках в два цвета // Дискрет. анализ и исслед. операций. 2009. Т. 16, N 1. - С. 80-92.
38. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения // Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011, 180 с.
39. Anil K. Jain K. Data Clustering: 50 Years Beyond k-Means // Pattern Recognition Letters. 2010. Vol. 31. P. 651-666.
40. Aloise D., Hansen P. On the Complexity of Minimum Sum-of-Squares Clustering // Les Cahiers du GERAD, G-2007-50. 2007. 12 p.
41. 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.
42. Долгушев А.В., Кельманов А.В. К вопросу об алгоритмической сложности одной задачи кластерного анализа // Дискретн. анализ и исслед. операций. 2010. Т. 17, №2. С. 39-.
43. MacQueen J.B. Some Methods for Classification and Analysis of Multivariate Observations // Proc. 5-th Berkeley Symp. Of Mathematical Statistics and Probability. 1967. Vol.1. P.281-297.
44. 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.
45. 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.
46. 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.
47. 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.
48. Добрынин А. А., Гутман И., Йовашевич В. Бициклические графы и их реберные графы с совпадающим индексом Винера // Дискрет. анализ и исслед. операций. 1997.Т. 4(2) С.3-9.
49. Dobrynin A.A., Mel'nikov L.S. Some results on the Wiener index of iterated line graphs // Electronic Notes in Discrete Mathematics, Vol. 22, 2005, 469-475.
50. Добрынин А.А., Мельников Л.С. Индекс Винера графов и их реберных графов // Дискрет. анализ и исслед. операций. Сер. 2. - 2004. - Т. 11, n. 2 . - С. 25-44.
51. Dobrynin A.A., Mel'nikov L.S. Wiener index of generalized stars and their quadratic line graphs // Discuss. Math. Graph Theory. - 2006. - Vol. 26, n.1 - P. 161-175.
52. Dobrynin A.A., Mel'nikov L.S. Wiener index for graphs and their line graphs with arbitrary large cyclomatic numbers // Appl. Math. Lett. - 2005. - Vol. 18, n. 3. - P. 307-312.

53. Добрынин А.А. Индекс Винера для графов произвольного обхвата и их реберных графов // Сиб. журн. индустриальной матем. - 2009 - Т.12 n. 4, С. 44-50.
54. De Kort J.B. Lower bounds for symmetric K-peripatetic salesman problems // Optimization. - 1991. - V. 22, N 1. P. 113-122.
55. 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.
56. De Kort J.B. Upper bounds for the symmetric 2-peripatetic salesman problem // Optimization. - 1992. - V. 23, N 4. P. 357-367.
57. 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.
58. 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.
59. Hassin R., Rubinstein S. Better approximations for max TSP // Inform. Process. Lett. - 2000. - V. 75, N 4. - P. 181-186.
60. Chen Z.-Z., Wang L. An improved randomized approximation algorithm for Max TSP // J. Comb. Optim. - 2005. - V. 9, N 4. - P. 401-432.
61. 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.
62. van Zuylen A. Multiplying Pessimistic Estimators: Deterministic Approximation of Max TSP and Maximum Triangle Packing // Lecture Notes in Computer Science. – 2010 -V. 6196. - P. 60-69.

Приложение А. 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. Инъективная (D+1)-раскраска плоских графов с обхватом 6 // Сиб. матем. журнал, Т. 52, № 1 (2011) 30-38.
4. Бородин О.В., Иванова А.О. Ациклическая предписанная 5-раскрашиваемость плоских графов без 4-циклов // Сиб. матем. журнал, Том 52, № 3 (2011) 522-541.
5. 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.
6. 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.
7. 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.
8. Глебов А.Н., Замбалаева Д.Ж. Полиномиальный алгоритм с оценкой точности 7/9 для задачи о двух коммивояжерах на максимум // Дискрет. анализ ии исслед. операций . 2011. Т. 18, № 4. С. 17-48.
9. 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.
10. 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.
11. Августинович С.В., Васильева А.Ю., Сергеева И.В., Дистанционно регулярные раскраски бесконечной квадратной решетки // Дискретный анализ и исследование операций. 2011. Т. 18. № 3. С. 3–10.
12. Avgustinovich, S.V., Mogilnykh, I.Yu. Induced perfect colorings // Siberian Electronic Mathematical Reports, T. 8, p. 310–316 (2011).
13. Валюженич А.А. Некоторые свойства основательных последовательностей // Дискретн. анализ и исслед. операций, 18:1 (2011), С.15-19

14. Потапов В.Н. Кликосочетания в k-значном n-мерном кубе // Сиб. мат. журн. 2011. Т. 52, N 2. С.384-392.
15. 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.
16. 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.
17. 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.
18. Krotov D.S. On weight distributions of perfect colorings and completely regular codes // Designs, Codes and Cryptography, 61:3 (2011), 315-329.
19. 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.
20. 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.
21. Кельманов А.В., Романченко С.М. Приближённый алгоритм для решения одной задачи поиска подмножества векторов // Дискретн. анализ и исслед. операций. 2011. Т.18, № 1. С. 61-69.
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 Cluster Analysis Problems // Comput. Math. and Math. Physics, 2009, Vol. 51, No. 11, pp. 1983-1988.
25. Kelmanov A.V., Pyatkin A.V. On the Complexity of Some Clustering Problems // Proc. II Int. Conf. «Optimization and applications» (OPTIMA-2011), Petrovac, Montenegro, September 25 – October 2, 2011. – p. 121-124.
26. Потапов В.Н. О дополняемости частичных n-квазигрупп порядка 4 // Матем. Труды. 2011, Т. 14, № 2, С. 1-26.
27. 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.

Статьи и учебные пособия, принятые в печать.

1. Balogh J., Kostochka A.V. Large minors in graphs with a given stability number // Discrete Math.
2. Kostochka A.V., Yancey M. Large rainbow matchings in edge-colored graphs // CPC.
3. Borodin O.V., Ivanova A.O. List 2-facial 5-colorability of plane graphs with girth at least 12 // Discrete Math., DOI 10.1016/j.disc.2011.09.018.
4. Borodin O.V., Ivanova A.O. 2-distance 4-colorability of planar subcubic graphs with girth at least 22 // Discuss. Math. Graph Theory.
5. Borodin O.V., Ivanova A.O. Acyclic 4-choosability of planar graphs with no 4- and 5-cycles // J. Graph Theory.
6. Tokareva N.N. Duality between bent functions and affine functions // Discrete Mathematics, DOI:10.1016/j.disc.2011.06.017
7. Августинович С.В., Васильев Ю.Л., Рычков К.Л. Формульная сложность тернарной линейной функции // Дискретный анализ и исследование операций.
8. Кротов Д.С., Потапов В.Н. О числе n-арных квазигрупп конечного порядка // Дискретн. математика.
9. Потапов В.Н. Бесконечномерные квазигруппы конечного порядка // Матем. заметки.
10. Потапов В.Н. Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Проблемы передачи информации.
11. Кельманов А.В., Романченко С.М. Псевдополиномиальные алгоритмы для некоторых труднорешаемых задач поиска подмножества векторов и кластерного анализа // Автоматика и телемеханика.
12. Воробьёв К.В. Кратные совершенные коды в гиперкубе // Дискретный анализ и исследование операций.
13. Krotov D.S. On the binary codes with parameters of triply-shortened 1-perfect codes // Designs, Codes and Cryptography, DOI 10.1007/s10623-011-9574-1
14. Токарева Н.Н. Криптография. Краткий курс // Учебное пособие, 2011.

Статьи, сданные в журналы.

1. Kostochka A.V. On almost (k–1)-degenerate (k+1)-chromatic graphs and hypergraphs // Discrete Math.
2. Borodin O.V., Glebov A.N., Jensen T.R. A step towards the strong version of Havel's 3 Color Conjecture // J. Graph Theory.

3. Borodin O.V., Ivanova A.O. Acyclic 4-choosability of planar graphs without adjacent short cycles // Discrete Math.
4. Borodin O.V. Colorings of plane graphs: a survey // Discrete Math.
5. Borodin O.V., Kostochka A.V. Defective 2-colorings of sparse graphs // J. Graph Theory.
6. Borodin O.V., Ivanova A.O. Edge 2-distance coloring of planar graph, Discrete Math.
7. Valyuzhenic A. On permutation comlexity of fixed points of uniform binary morphisms, Discrete Math.
8. Borges J., Mogilnykh I.Yu., Rifa J., Solov'eva F.I. Structural properties of binary propelinear codes // Adv. Math. Communications.
9. Коломеец Н.А. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. нализ и исслед. операций.
10. Кельманов А.В., Пяткин А.В. О сложности некоторых задач выбора подпоследовательности векторов // Ж. вычисл. матем. и матем. физики.
11. Кельманов А.В., Романченко С.М., Хамидуллин С.А. Приближённые алгоритмы для некоторых труднорешаемых задач поиска подпоследовательности векторов // Дискретн. анализ и исслед. операций.
12. Dobynin A.A., Mel’nikov L.S. 4-chromatic Koester graphs // Discussione Math. Graph Th.
13. Dobynin A.A., Mel’nikov L.S. Wiener index of line graphs // Distance in Graphs (book).

Приложение Б. Список сделанных исполнителями докладов.

На всероссийских конференциях и семинарах.

Пленарные доклады.

1. 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.

Секционные доклады.

2. Августинович С.В., Васильева А.Ю. О дистанционно регулярных раскрасках многомерных квадратных решеток. Доклад на международной конференции «Мальцевские чтения», Новосибирск, 11-14 октября 2011.
3. 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.
4. 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.
5. Кельманов А.В., Романченко С.М., Хамидуллин С.А. 2-приближенный алгоритм для одной задачи поиска в векторной последовательности совокупности «похожих» элементов, «Математические методы распознавания образов: 15-я Всероссийская конференция (ММРО-15), г. Петрозаводск, 11– 17 сент. 2011 г.
6. Потапов В.Н. Совершенные комбинаторные структуры // XI летняя школа «Современная математика», Дубна, 18-29 июля 2011, (курс из 4-х лекций)
7. 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.
8. Потапов В.Н. Совершенные раскраски и корреляционно-иммунные функции в q-значном гиперкубе // Восьмая молодёжная научная школа по дискретной математике и её приложениям, г. Москва, 24-29 октября 2011 г. (лекция)

9. 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.
10. 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.
11. 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.

На международных конференциях и семинарах.

Пленарные доклады.

1. Kostochka A.V. CID Conference – Colourings, Independence and Domination, Sklarska Poreba, Poland, September, 2011, приглашенный доклад.
2. 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.
3. 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.

Секционные доклады.

4. Avgustinovich S.V., Mogilnykh I.Yu. Induced perfect colorings, Международная конференция 3ICMCTA (Third International Castle Meeting on Coding Theory and Applications), Cardona, Spain.
5. 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.
6. 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.
7. 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.

8. 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.
9. Borges J., Mogilnykh I.Yu., Rifa J., Solov'eva F.I. Groups from normalized propelinear codes, Международная конференция Мальцевские чтения-2011.
10. Воробьёв К.В. О связи совершенных 2-раскрасок с кратными совершенными кодами в гиперкубе, Международная конференция Мальцевские чтения-2011, Новосибирск, 11-14 октября 2011.
11. 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.

Приложение В. 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 состоится 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.

Приложение Г. Программа научных семинаров по 2 этапу проекта.

1. С. В. Августинович, А. Ю. Васильева, И. В. Сергеева

Дистанционно регулярные раскраски бесконечной квадратной решетки.

2. А. Н. Глебов, Д. Ж. Замбалаева

К задаче о двух коммивояжерах.

3. Д. С. Кротов

О связи свитчинговой разделимости графа и его подграфов.

4. И. Ю. Могильных

О слабых изометриях кодов Препараты.

5. А. А. Добрынин

Разложение индекса Винера для подграфов одного класса гексагональной сети.

6. Н. А. Коломеец, А. В.Павлов

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

7. Л. С. Мельников, А. А. Добрынин

О 4-хроматических графах Кёстера.

8. С. В. Августинович

Некоторые задачи синтеза схем.

9. И. Ю. Могильных

О несуществовании некоторых совершенных 2-раскрасок графов Джонсона.

11. А. В. Пяткин, А. В. Кельманов

О сложности задачи поиска подмножества векторов.

12. А. В. Косточка

Разноцветные паросочетания в графах.

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