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
И.о. директора
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: «Проведение фундаментальных исследований»
(промежуточный, этап № 3)

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-В, разделы 1.4, 2, 5)
отв. исполнитель темы, зав. лаб. ИМ СО РАН, д.ф-м.н.	_____	Бородин О.В. (Реферат, Приложения А-В, разделы 1.4, 2)
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. (раздел 1.6)
в.н.с. ИМ СО РАН, д.ф.-м.н.	_____	Кротов Д.С. (разделы 1.1, 1.3, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Глебов А.Н. (разделы 1.5, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Добрынин А.А. (разделы 1.4, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Мельников Л.С. (раздел 1.4)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Потапов В. Н. (раздел 1.1, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Августинович С.В. (раздел 1.3, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Токарева Н.Н. (разделы 1.2, 2)
с.н.с. ИМ СО РАН, к.ф.-м.н.	_____	Могильных И.Ю. (раздел 1.1, 1.3)
аспирант ИМ СО РАН	_____	Замбалаева Д.Ж. (раздел 1.5)
аспирант ИМ СО РАН	_____	Воробьев К.В. (раздел 1.3)
аспирант НГУ	_____	Коломеец Н.А. (раздел 1.2)

студент НГУ	_____	Валюженич А.А. (раздел 1.1)
Студент НГУ	_____	Паршина О.Г. (раздел 1.3)
Нормоконтролер	_____	Кравченко С.В.

Реферат

Отчет 35 с., 1 ч., 57 источников, 3 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: СОВЕРШЕННЫЕ РАСКРАСКИ; БУЛЕВЫ ФУНКЦИИ; БЕНТ-ФУНКЦИИ; ТЕОРИЯ КОДИРОВАНИЯ; ДИСТАНЦИОННО РЕГУЛЯРНЫЕ КОДЫ; ТЕОРИЯ ГРАФОВ; РАСКРАСКА ГРАФОВ; ДЕКОМПОЗИЦИЯ ГРАФОВ; ИНВАРИАНТЫ ГРАФОВ; 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 (методы эффективного кодирования и передачи информации, защита информации, анализ данных и распознавание образов, теория графов и ее приложения). 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 работы использовались классические и современные методы теории кодирования, методы теории графов, методы оптимизации и дискретного анализа, а также новые подходы, разработанные участниками проекта.

В результате фундаментальных поисковых исследований 3 этапа получены новые результаты мирового уровня.

1. Проведено исследование бент-функций на минимальном расстоянии от квадратичной бент-функции, получено описание всех таких бент-функций от $2k$ переменных.
2. Получен критерий, с помощью которого по параметрам совершенной 2-раскраски двоичного n-куба можно определить, является ли она кратным совершенным кодом заданного радиуса $r > 1$ некоторой кратности.
3. Доказано, что существуют сильно регулярные расширения графа Петерсена и графа решетки 3×3 с некоторыми параметрами и что не существует сильно регулярных расширений графов Шрикхандэ и Пэли.
4. Доказана NP-полнота задач разбиения последовательности векторов, содержащих конечное число элементов, по критерию минимума суммы квадратов расстояний.

5. 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.
6. Найден полиномиальный алгоритм для точной гармонической раскраски деревьев с большой максимальной степенью.
7. Получено исчерпывающее описание строения плоских графов в терминах звезд при младших вершинах. Опровергнута гипотеза Йендроля и Харанта.
8. Для $n \geq 425$ и $r < n$ описаны все n-вершинные гиперграфы с наибольшим числом ребер, не имеющие r-регулярных подграфов.
9. С точностью до логарифмического множителя найден порядок роста чисел Рамсея $R(3, K^r_t)$ в r-униформных гиперграфах (треугольники против клик) для всех $r \geq 3$.
10. Доказано, что аффинные функции – это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние.

Степень внедрения – результаты исследований по проекту используются в образовательном процессе Новосибирского государственного университета и Новосибирского государственного университета экономики и управления 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.

Значимость и эффективность 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 этапа 3 в последующих работах этого направления следует ожидать формирование эффективного инструментария для исследования проблем дискретной математики, использующего новые подходы и постановки задач.

По ряду направлений в ходе исследований получены новые фундаментальные результаты мирового уровня, доложенные на научных форумах и подготовленные к печати.

Обозначения и сокращения

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

НГУ – Новосибирский государственный университет.

НГУЭиУ – Новосибирский государственный университет экономики и управления.

Содержание

	Введение	8
1.	Поисковые исследования в области приложений бент-функций в криптографии и смежных областях, в теории кодирования информации, анализа структуры граф-моделей передачи информации и обработки данных	
1.1.	Экстремальные структуры и построение кодов	9
1.2.	Булевы функции с экстремальными свойствами (бент-функции)	14
1.3.	Совершенные раскраски и коды	15
1.4.	Раскраска графов и смежные вопросы	17
1.5.	Оптимизационные задачи на графах и сетях	20
1.6.	Сложностные вопросы анализа данных и распознавания образов	21
1.7.	Полученные результаты	23
2.	Подготовка научно-методических материалов для публикаций	25
3.	Показатели	25
4.	Заключение	26
5.	Список использованных источников	27
	Приложение А. Список публикаций исполнителей	31
	Приложение Б. Список сделанных исполнителями докладов	34
	Приложение В. Программа научных семинаров по 3 этапу проекта	35

Введение

Выполнение НИР по проекту направлено на проведение фундаментальных исследований в области теории кодирования и криптографии, обработке и передачи данных, анализа теоретико-графовых моделей в проблемах анализа структурных объектов. 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, теория графов и ее приложения). 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 3 включала поисковые исследования в области теории и приложений бент-функций в криптографии и смежных областях, в теории кодирования информации, анализа структуры граф-моделей передачи информации и обработки данных. По результатам исследований подготовлены научно-методические материалы для публикаций.

1. Поисковые исследования в области приложений бент-функций в криптографии и смежных областях, в теории кодирования информации, анализа структуры граф-моделей передачи информации и обработки данных.

В рамках работ третьего 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. Экстремальные структуры и построение кодов.

1. 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 $n - k$. Этот результат анонсирован в [1]. Отметим, что известно несколько способов построения кодов Грея с различными свойствами, в частности, в [2, 3] построены гамильтоновы циклы с максимально равномерным (для фиксированной размерности) спектром. В [4] найден порядок логарифма числа различных кодов Грея в булевом n-кубе, а в [5] определена асимптотика логарифма этого числа (при $n \to \infty$).

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 работы 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.

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 [6-11].

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 $\varphi(a_i) = b_i\,xc_i$, 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*.

Пусть ω − бесконечное вправо непериодическое слово над алфавитом $\sum$. Тогда определим *бесконечную перестановку*, порождаемую словом ω, как упорядоченную тройку $\delta = \langle N, <_\delta, < \rangle$, 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 бесконечной перестановки было введено в [12], где, кроме того, исследовались свойства периодичности и низкая комбинаторная сложность перестановок. Понятие перестановки, порожденной бесконечным непериодическим словом, было введено Макаровым в [13]. В работе [14] тот же автор вычислил комбинаторную сложность перестановок, порожденных хорошо известным семейством слов Штурма. В работе [15] Уидмер вычислил комбинаторную сложность перестановки Туэ-Морса.

Нами 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* $n \geq L_\omega$.

Все функции, входящие в условие теоремы, определяются в работе [16].

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 [17], 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 $\{u; v; w\} \in T$. Будем говорить, 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 расстояние*. Два кода *эквивалентны*, если существует изометрия булева куба, отображающая один код в другой. Исследуется вопрос восстановления кодов с точностью до эквивалентности с использованием их метрических свойств [18-21]. 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 $(n – 1)/2$ [22].

Пусть C – приведенный двоичный код мощности k длины n. Упорядочим векторы из $\{0\} \times E^{k-1}$ некоторым образом и обозначим через $\alpha_0, \ldots, \alpha_{2^{k-1}-1}$ количество столбцов соответствующего вида в проверочной матрице кода C с нулевой верхней строкой. Зная размерности подкодов четной мощности кода C, можно составить $C_k^2 + C_k^4 + \ldots = 2^{k-1} - 1$ уравнений, связывающих величины $\alpha_1, \ldots, \alpha_{2^{k-1}-1}$. 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 [21]. 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 результат:

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

1.2 Булевы функции с экстремальными свойствами (бент-функции)

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 [23]. 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. Обзор работ и результатов по бент-функциям можно найти, например, в [24].

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. В работе построены бент-функции на минимально возможном расстоянии от квадратичной бент-функции. В [25] показано, что две бент-функции от $2k$ переменных находятся на расстоянии 2^k (минимальное расстояние между двумя различными бент-функциями) если и только если они отличаются на аффинном подпространстве размерности k и аффинны на нём. В данной работе описаны все бент-функции на минимальном расстоянии от квадратичной бент-функции, а также показано что число таких бент-функций от $2k$ переменных равно $2^k (2^1 + 1) \ldots (2^k + 1)$. Все квадратичные бент-функции аффинно эквивалентны функции $x_1x_{k+1} \oplus x_2x_{k+2} \oplus \ldots \oplus x_kx_{2k}$, которая принадлежит классу Мэйорана – МакФарланда. Поэтому рассматривалась и более общая задача нахождения нижней оценки числа бент-функций на минимальном расстоянии от произвольной бент-функции из класса Мэйорана – МакФарланда (теорема 3). Сформулирована гипотеза об оценке числа бент-функций на расстоянии 2^k 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.

1.3 Совершенные раскраски и коды

1. Раскраска вершин графа называется совершенной, если для каждой вершины цветовой набор её соседей зависит только от её цвета. Одной из проблем в этой области является изучение связи совершенных 2-раскрасок и k-кратных совершенных кодов двоичного гиперкуба. Основным полученным результатом является критерий, который по параметрам совершенной 2-раскраски определяет, является ли она k-кратным совершенным кодом.

Пусть H_n − это гиперкуб размерности n. Вершины куба – двоичные наборы длины n, они смежны, если их наборы отличаются ровно в одной координате. Весом $wt(y)$ вершины $y \in H_n$ называется число единиц её набора. Расстояние Хэмминга $d(x, y)$ между вершинами $x, y \in H_n$ − это число позиций, в которых x и y различны. Будем называть шаром радиуса r с центром в точке x множество $B(x, r) = \{y \in H_n \mid d(x, y) \le r\}$. Полиномом Кравчука степени r называется полином $P_r(x, n) = \sum_{i=0}^{r}(-1)^i \binom{x}{i}\binom{n-x}{r-i}$.

Подмножество вершин графа называется k-кратным совершенным кодом радиуса r, если шар радиуса r с центром в любой вершине этого подмножества содержит в точности k кодовых вершин. В случае $k = 1$ получаем классическое определение совершенного кода. Задача перечисления всех параметров n, r, при которых такие коды существуют, решена в [26, 27]. При произвольном k эта проблема ещё далека от решения. Подробнее о k-кратных совершенных кодах см. [28, 29].

Отображение $T : H_n \to \{1, 2, \ldots, k\}$ называется совершенной раскраской вершин куба в k цветов с матрицей параметров $(s_{ij})_{i,j\in\{1,\ldots,k\}}$, если оно сюръективно и для каждых i, j у любой вершины цвета i число соседей цвета j равно s_{ij}. 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. Не теряя общности, будем считать, что $b \ge c$. Рассматривается следующая задача: найти все такие параметры n, b, c, что соответствующая совершенная раскраска будет совершенным кодом некоторой кратности k. В данной работе получен критерий, который решает эту задачу.

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

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, мы заключаем, что $\forall m, l, r \in N : r \equiv 1 \pmod 2$ существуют кратные совершенные коды радиуса 1 при $n = 2^m l+1$ кратности $k = i \cdot l$ для всех $i \in \{1, \ldots, 2^m\}$, $i \equiv 1 \pmod 2$. 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 [30, 31]. 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.

2. Рассмотрим регулярный граф $G = (V, E)$. Для всякого кода (т.е. подмножества вершин) C определим дистанционное разбиение множества вершин этого графа относительно C: $V = \cup_{i=0,\ldots,p} C_i$, где $p = \max\{d(x, C): x \in C\}$ 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 $\{\gamma_j, \alpha_j, \beta_j : j = 0, \ldots, p\}$ 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 $J(n, w)$ [32,33]. Эти схемы включают в себя широко известные системы троек и четверок Штейнера. Здесь рассматриваются классические конструкции Оллтопа [34] 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: $D^1 = \{\Delta \cup (n+1) : \Delta \in D\}$, $D^2 = \{\{1, \ldots, n\} \setminus \Delta : \Delta \in D\}$. Рассмотрим случай, когда $n = 2w$. Опишем две конструкции Оллтопа [34]. Ниже $\bar{D}$ обозначает подмножество вершин графа $J(2w+1, w)$, дополнительное к D.

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 $\rho = 1$ 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 $\rho = 1$ 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 [35], 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).

1.4. 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. Например, в теоретических исследованиях проблемы распределения радиочастот в мобильных сетях связи возникают задачи о так называемых дистанционных раскрасках, в которых вершины на близких расстояниях не могут иметь 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 3 этапу получены следующие результаты:

1. 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:

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

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

2. 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 (Discrete Math. 308, 2008, 4435–4445) 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 Кюном и Остасом.

3. 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 $t > \max\{4^{15s2^{+s}}, (240s \log_2 s)^{8s \log 2 s + 1}\}$, 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 $t > C(s \log_2 s)^3$.

4. 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 $n = 2^k - 1$.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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 гипергра-

фов. 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 $R(3,K^r_t)$ 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.

10. В работе [36] 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

11. 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. 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 [37-45]. 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).

1.5. Оптимизационные задачи на графах и сетях

Рассмотрена 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 послед-

нее 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. Например, для симметричной задачи одного коммивояжера на максимум наилучший известный алгоритм имеет гарантированную асимптотическую оценку точности 25/33 [46], а для задачи о двух коммивояжерах на максимум – оценку точности 7/9 [47]. Для несимметричной задачи коммивояжера на максимум в работе [48] построен алгоритм с гарантированной оценкой точности 2/3. Нами получен аналогичный результат для задачи о двух коммивояжерах. А именно, для несимметричной задачи о двух коммивояжерах на максимум построен алгоритм, имеющий асимптотическую оценку точности 2/3 и оценку временной сложности $O(n^3)$, где n – число вершин графа. Как и алгоритм в [47], данный алгоритм основан на построении специальной раскраски ребер графа и на последующем выделении пары реберно непересекающихся частичных туров достаточно большого веса.

1.6. Сложностные вопросы анализа данных и распознавания образов

Исследовались дискретные экстремальные задачи выбора из последовательности векторов евклидова пространства, состоящей из конечного числа членов, подпоследовательности элементов близких по критерию минимума суммы квадратов расстояний при наличии ограничений на номера выбираемых векторов. Цель исследования – анализ алгоритмической сложности этих задач. Полученные результаты дополняют работу [49], где было установлено, что к числу NP-трудных задач относятся следующие тесно связанные между собой оптимизационные задачи кластерного анализа и выбора подмножества в конечном множестве векторов евклидова пространства.

Задача VS-1 (Vector Subset 1).

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

$$F_1(\mathsf{C}) = \frac{1}{|\mathsf{C}|}\left\| \sum_{\mathbf{y} \in \mathsf{C}} \mathbf{y} \right\|^2 + \sum_{\mathbf{y} \in \mathsf{Y} \setminus \mathsf{C}} \| \mathbf{y} \|^2$$

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

Задача VS-2 (Vector Subset 2).

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

$$F_2(\mathsf{C}) = \sum_{\mathbf{y}\in\mathsf{C}} \| \mathbf{y} - \bar{\mathbf{y}}(\mathsf{C}) \|^2,$$

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

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

$$F_3(\mathsf{C}) = \sum_{\mathbf{y}\in\mathsf{C}} \sum_{\mathbf{z}\in\mathsf{C}} \| \mathbf{y} - \mathbf{z} \|^2$$

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

Задача MSSC-Case (Minimum Sum-of-Squares Clustering, special Case).

Дано: множество $\mathsf{Y} = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ векторов из R^q, натуральное число $M > 1$. *Найти*: разбиение множества Y на $J = N - M + 1$ непустых кластеров $\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_J$ такое, что мощность одного из кластеров равна M и

$$F_4(\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_J) = \sum_{j=1}^{J} \sum_{\mathbf{y}\in\mathsf{C}_j} \| \mathbf{y} - \bar{\mathbf{y}}(\mathsf{C}_j) \|^2 \to \min,$$

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

Для целевых функций задач VS-1, VS-2 и VS-3 выполняются следующие соотношения [1]:

$$F_2(\mathsf{C}) = \sum_{\mathbf{y}\in\mathsf{Y}} \| \mathbf{y} \|^2 - F_1(\mathsf{C}) = \frac{1}{2|\mathsf{C}|} F_3(\mathsf{C}). \qquad (1)$$

Поэтому 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 [1]

$$F_4(\mathsf{C}_1, \mathsf{C}_2, \ldots, \mathsf{C}_J) = F_2(\mathsf{C}_1), \qquad (2)$$

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. Доказано [49], что в форме верификации свойств сформулированные задачи NP-полны в сильном смысле.

Одна из возможных содержательных трактовок проблемы анализа данных, которая приводит к решению сформулированных задач, состоит в следующем [49]. 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 (см., например, [50-55] и цитированные там работы), 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. Полученные результаты

Здесь приводится список всех результатов, выполненных в ходе фундаментальных поисковых исследований на этапе 3 проекта (из этого списка в заключении указаны только результаты мирового уровня).

1. Проведено исследование бент-функций на минимальном расстоянии от квадратичной бент-функции, получено описание всех таких бент-функций от $2k$ переменных и показано, что их число равно $2^k (2^1 + 1) \ldots (2^k + 1)$. Найдена нижняя оценка числа бент-

функций на минимальном расстоянии от бент-функций из класса Мэйорана – Мак-Фарланда.

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.
3. Доказано, что аффинные функции – это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние.
4. Доказано существование такой размерности N, что если сформулированные выше необходимые условия на спектр являются достаточными для существования гамильтонова цикла с таким спектром в булевом N-мерном кубе, то эти условия являются достаточными и для любых размерностей n.
5. Установлено, что сложность реализации в классе обобщённых (троичных) π-схем троичного счётчика кратности 3, зависящего от трёх переменных, равна 18.
6. Получен критерий, с помощью которого по параметрам совершенной 2-раскраски двоичного n-куба можно определить, является ли она кратным совершенным кодом заданного радиуса $r > 1$ некоторой кратности.
7. Найдены условия, по которым можно определить, является ли маркированный морфизм сравнимым. Вычислена комбинаторная сложность перестановок, порожденных неподвижными точками сравнимых морфизмов.
8. Доказано, что существуют сильно регулярные расширения графа Петерсена и графа решетки 3×3 с некоторыми параметрами и что не существует сильно регулярных расширений графов Шрикхандэ, Пэли порядка 13 *и* $\overline{L(K6)}$.
9. Доказано, что размерности подкодов четной мощности двоичного кода образуют минимальный набор размерностей, определяющий код с точностью до эквивалентности.
10. 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 $\{\alpha_0 = 5, \beta_0 = 20, \gamma_1 = 8, \alpha_1 = 17\}$. Конструкции расширения полностью регулярных кодов применимы к кодам произвольной силы t (в отличие от варианта конструкций для блок-схем).
11. 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.
12. Найден полиномиальный алгоритм для точной гармонической раскраски деревьев с большой максимальной степенью.
13. Получено исчерпывающее описание строения плоских графов в терминах звезд при младших вершинах. Опровергнута гипотеза Йендроля и Харанта.

14. Для $n \geq 425$ и $r < n$ описаны все n-вершинные гиперграфы с наибольшим числом ребер, не имеющие r-регулярных подграфов.
15. С точностью до логарифмического множителя найден порядок роста чисел Рамсея $R(3, K^r_t)$ в r-униформных гиперграфах (треугольники против клик) для всех $r \geq 3$.
16. Построен новый 4-хроматический вершинно-критический граф Кёстера на 32 вершинах, образованный пересечением 7 кривых на плоскости.
17. Доказана NP-полнота нескольких актуальных задач разбиения последовательности векторов, содержащих конечное число элементов, по критерию минимума суммы квадратов расстояний.
18. Предложены 2-приближённые полиномиальные алгоритмы, а также точные псевдополиномиальные алгоритмы для ряда труднорешаемых задач поиска подпоследовательностей векторов.
19. Для несимметричной задачи о двух коммивояжерах на максимум построен алгоритм, имеющий асимптотическую оценку точности 2/3 и оценку временной сложности $O(n^3)$, где n – число вершин графа.

2. Подготовка научно-методических материалов для публикаций.

По результатам исследований по третьему этапу опубликовано 13 статей, приняты к публикации 12 статей и отправлено в журналы 13 статей исполнителей проекта. Сделано 3 доклада на международных и 4 доклада на отечественных научных конференциях. Статьи опубликованы и приняты к публикации в ведущих зарубежных и российских изданиях, среди которых такие журналы как «Дискретный анализ и исследование операций», «Graphs and Combinatorics», «Combinatorics, Probability and Computing», «Random Structures and Algorithms», «Discrete Applied Mathematics», «Discrete Mathematics», «J. Automata, Languages and Combinatorics», «Journal of Graph Theory», «Discussione Mathematicae. Graph Theory». В печати находится учебное пособие по криптографии для студентов НГУ.

3. Показатели

3.1. Количество подготовленных и опубликованных статей:

Вышло из печати 13 статей, приняты к печати 12 статей, отправлено в журналы 13 статей (см. Приложение А).

3.2. Количество сделанных докладов:

Сделано 3 доклада на международных и 4 доклада на отечественных научных конференциях (см. Приложение Б).

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

Аспирантка Д.Ж. Замбалаева после защиты диссертации принята на работу в Лабораторию дискретных экстремальных задач Института математики им. С.Л. Соболева СО РАН (зав. лаб. д.ф.-м.н. Э.Х. Гимади).

3.4. Проведено 13 научных семинаров по теме исследований (см. Приложение В).

4. Заключение

В процессе выполнения работ по этапу 3 НИР получены следующие результаты мирового уровня.

1. Проведено исследование бент-функций на минимальном расстоянии от квадратичной бент-функции, получено описание всех таких бент-функций от $2k$ переменных.
2. Получен критерий, с помощью которого по параметрам совершенной 2-раскраски двоичного n-куба можно определить, является ли она кратным совершенным кодом заданного радиуса $r > 1$ некоторой кратности.
3. Доказано, что существуют сильно регулярные расширения графа Петерсена и графа решетки 3×3 с некоторыми параметрами и что не существует сильно регулярных расширений графов Шрикхандэ и Пэли.
4. Доказана NP-полнота задач разбиения последовательности векторов, содержащих конечное число элементов, по критерию минимума суммы квадратов расстояний.
5. 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.
6. Найден полиномиальный алгоритм для точной гармонической раскраски деревьев с большой максимальной степенью.
7. Получено исчерпывающее описание строения плоских графов в терминах звезд при младших вершинах. Опровергнута гипотеза Йендроля и Харанта.
8. Для $n \geq 425$ и $r < n$ описаны все n-вершинные гиперграфы с наибольшим числом ребер, не имеющие r-регулярных подграфов.

9. С точностью до логарифмического множителя найден порядок роста чисел Рамсея $R(3, K^r_t)$ в r-униформных гиперграфах (треугольники против клик) для всех $r \geq 3$.
10. Доказано, что аффинные функции – это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние.

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 13 научных семинаров.

По результатам 3 этапа НИР представляется целесообразным продолжение работ.

5. Список использованных источников

1. Потапов В. Н. О спектрах гамильтоновых циклов в булевом n-кубе // Мат. XVII междунар. школы-семинара «Синтез и сложность управляющих систем» (Новосибирск, 27 окт. – 1 ноябр. 2008 г.) – Новосибирск: Ин-т матем. СО РАН, 2008. – С. 137–140.
2. Bhat G. S., Savage C. D. Balanced Gray codes // Electron. J. Comb. – 1996. – Vol.3, paper 25.
3. Suparta I. N. A simple proof for the existence of exponentially balanced Gray codes // Electron. J. Comb. – 2005. – Vol. 12, note 19.
4. Feder T., Subi C. Nearly tight bounds on the number of Hamiltonian circuits of the hypercube and generalizations // Inform. Process. Lett. – 2009. – Vol. 109, N 5. – P. 267–272.
5. Пережогин А. Л., Потапов В. Н. О числе гамильтоновых циклов в булевом кубе // Дискрет. анализ и исслед. операций. Сер. 1. – 2001. – Т. 8, № 2. – С. 52–62.
6. Рычков К. Л. Модификация метода В. М. Храпченко и применение её к оценкам сложности π-схем для кодовых функций // Дискрет. анализ. Вып. 42. – 1985. – С. 91–98.
7. Рычков К. Л. О нижних оценках сложности параллельно-последовательных контактных схем, реализующих линейные булевы функции // Сиб. журн. исслед. операций. – 1994. – Т. 1, №4. – С. 33–52.
8. Рычков К. Л. О сложности обобщённых контактных схем // Дискрет. анализ и исслед. операций. – 2009. – Т. 16, № 5. – С. 78–87.
9. Рычков К. Л. Нижняя оценка сложности реализации в классе π-схем q-ичного счётчика кратности q // Дискрет. анализ и исслед. операций. – 2010. – Т. 17, № 6. – С. 68–76.
10. Храпченко В. М. О сложности реализации линейной функции в классе π-схем // Мат. заметки. – 1971. – Т. 9, № 1. – С. 35–40.

11. Храпченко В. М. Об одном методе получения нижних оценок сложности π-схем // Мат. заметки. – 1971. – Т. 10, № 1. – С. 83–92.
12. Fon-Der-Flaass D.-G., Frid A.E. On periodicity and low complexity of infinite permutations // European J. Combin. 2007. Vol. 28, N 8. P. 2106-2114.
13. Makarov M. A. On permutations generated by infinite binary words // Sib. Elektron. Mat. Izv. 2006. Vol. 3. Pp. 304-311.
14. Makarov M.A. On the permutations generated by the Sturmian words // Sib. Math. J. 2009. Vol. 50, N 3. P. 674-680.
15. Widmer S. Permutation complexity of the Thue-Morse word // Adv. in Appl. Math. 2010.
16. Valuzhenich A. Permutation complexity of the fixed points of some uniform binary morphisms // EPTCS 63 (2011), Proceedings of WORDS 2011. P. 257-264.
17. Брауэр А.Е., ван Линт И.Х. Сильно регулярные графы и частичные геометрии. / Киберн. сб. № 24, С. 186–229, М.: Наука, 1987.
18. Августинович С. В., Соловьёва Ф. И. К метрической жесткости двоичных кодов // Пробл. передачи информ. – 2003. – Т. 39, вып. 2. – С. 23–28.
19. Могильных И.Ю. О слабых изометриях кодов Препараты // Пробл. передачи информ. – 2009. – Т. 45, вып. 2. – С. 78–83.
20. Августинович С. В. О сильной изометрии бинарных кодов // Дискретн. анализ и исслед. операций. Сер. 1. – 2000. – Т. 7, № 3. – С. 3–5.
21. Горкунов Е. В., Августинович *С. В.* О восстановлении двоичных кодов по размерностям их подкодов // Дискретн. анализ и исслед. операций. – 2010. – Т. 17, № 5. – С. 15–21.
22. Kelly P. J. A congruence theorem for trees // Pacific Journal of Mathematics . – 1957. – Vol. 7. – P. 961–968.
23. Rothaus O. On bent functions // J. Comb. Theory, Ser. A.– 1976.– Vol. 20, N 3.–P. 300–305.
24. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения // Saarbrucken, Germany: Lambert Acad. Publ., 2011. – 180 с.
25. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика.– 2009. – № 4. – С. 5–21.
26. Зиновьев В. А., Леонтьев В. К. О совершенных кодах // Препринт / ИППИ АН СССР. – 1972. – Т. 1. – С. 26–35.
27. Tietavainen A. On the nonexistence of perfect codes over the finite fields // SIAM J. Appl. Math. – 1973. – Vol. 24. – P. 88–96.
28. Cohen G. D., Honkala I. S., Litsyn S. N., Lobstein A. C. Covering codes. – Amsterdam: Elsevier, 1997. – 542 p.

29. van Wee G. J. M., Cohen G. D., Litsyn S. N. A note on perfect multiple coverings of the Hamming space // IEEE Trans. Inf. Theory. – 1991. – Vol. 37, N 3. – P. 678–682.
30. Воробьев К. В., Фон-Дер-Флаасс Д. Г. О совершенных 2-раскрасках гиперкуба // Сиб. электрон. мат. изв. – 2010. – Т. 7. – С. 67–75.
31. Потапов В. Н. О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Сиб. электрон. мат. изв. – 2010. – Т. 7. – С. 372–382.
32. Avgustinovich S.V., Mogilnykh I.Yu. Perfect 2-colorings of Johnson graphs J(6; 3) and J(7; 3) // LNCS, Springer. 2008. Vol. 5228. P. 11–19.
33. Delsarte P. An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. V. 10. P. 1–97.
34. Alltop W.O. Extending t-designs // Journal of Combinatorial Theory. Ser. A. 1975. Vol. 18, 2. P. 177–186
35. Avgustinovich S.V., Mogilnykh I.Yu. On completely regular codes in Johnson graphs J(2w+1,w) with covering radius 1 // Proc. Twelfth Intern. workshop on Algebraic Combinatorial Coding Theory (ACCT-2010), P. 20–26. September 5–11, 2010, Novosibirsk, Russia.
36. Harant J., Jendrol S. On the existence of specific stars in planar graphs // Graphs Combin. 2007,Vol. 23, P.529–543
37. 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.
38. 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.
39. 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.
40. Koester G. Bemerkung zu einem Problem von Grötzsch // Wiss.Z.Univ.Halle,1984,V.33, P.129.
41. Koester G. 4–critical 4–valent planar graphs constructed with crowns. // Math. Scand., 1990, V. 67, P. 15–22.
42. Dobrynin A.A., Mel'nikov L.S. Counterexamples to Grötzsch–Sachs–Koester's conjecture. // Discrete Math., 2006, V. 306, N. 6, P. 591–594.
43. 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.
44. Dobrynin A.A., Mel'nikov L.S. 4–chromatic edge critical Grötzsch–Sachs graphs. // Discrete Math. - 2009 - Vol. 309, n. 8 - P.2564-2566.

45. 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.
46. Van Zuylen A.. Multiplying Pessimistic Estimators: Deterministic Approximation of Max TSP and Maximum Triangle Packing // Computing and Combinatorics, 1Annual Intern. Conf. (COCOON 2010). Nha Trang, Vietnam, July 19–21, 2010. Proceedings. LNCS, V. 6196. P. 60–69.
47. 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.
48. Kaplan H., Lewenstein M., Shafrir N., Sviridenko M. Approximation algorithms for asymmetric TSP by decomposing directed regular multigraphs. // Proc. of the 44th Ann. IEEE Symp. on Foundations of Computer Science (FOCS), 2003. P. 56–65.
49. Кельманов А.В., Пяткин А.В. NP-полнота некоторых задач выбора подмножества векторов // Дискретный анализ и исследование операций. 2010. Т.17, №5. С. 37-45.
50. Кельманов А.В., Хамидуллин С.А. Апостериорное обнаружение заданного числа одинаковых подпоследовательностей в квазипериодической последовательности // Журн. вычисл. математики и мат. физики, 2001, Т.41, № 5, С. 807-820.
51. Гимади Э.Х., Кельманов А.В., Кельманова М.А. Хамидуллин С.А. Апостериорное обнаружение в числовой последовательности квазипериодического фрагмента при заданном числе повторов // Сиб. журн. индустр. математики. 2006. Т.9 №1(25). С.55-74.
52. Кельманов А.В., Михайлова Л.В. Совместное обнаружение в квазипериодической последовательности заданного числа фрагментов из эталонного набора и ее разбиение на участки, включающие серии одинаковых фрагментов // Журн. вычисл. математики и мат. физики, 2006, Т.46, №1, С. 172-189.
53. Кельманов А.В., Михайлова Л.В. Хамидуллин С.А. Об одной задаче поиска упорядоченных наборов фрагментов в числовой последовательности // Дискретный анализ и исследование операций. 2009. Т.16. № 4. С. 31-46.
54. Kel'manov A.V., Jeon B. A Posteriori Joint Detection and Discrimination of Pulses in a Quasiperiodic Pulse Train//IEEE Transactions on Signal Processing, 2004,Vol.52, No.3, P.1-12.
55. Kel'manov A.V., Khamidullin S.A. An Algorithm for Recognition of a Vector Alphabet Generating a Sequence with a Quasi-Periodic Structure // Pattern Recognition and Image Analysis. 2010. Vol. 20, No.4, pp. 451-458.
56. Papadimitriou C.H. Computational Complexity. New-York: Addison-Wesley, 1994. 523P.
57. Garey M. R., Johnson D. S. Computers and Intractability: A Guide to the Theory of NP-Completeness. San Francisco: Freeman, 1979. 314 P.

Приложение А. Список публикаций исполнителей.

Опубликованные статьи в журналах и трудах конференций.

1. 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.
2. 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.
3. 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.
4. С.В. Августинович, Ю.Л. Васильев, К.Л. Рычков. Формульная сложность тернарной линейной функции // Дискретн. анализ и исслед. операций. 2012. Т.19, № 3. С. 3–12.
5. 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.
6. Tokareva N.N. Duality between bent functions and affine functions // Discrete Mathematics, V. 312. (2012), P. 666-670.
7. 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.
8. 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.
9. Kostochka A.V., Yancey M. Large rainbow matchings in edge-colored graphs // CPC, Vol. 21, 2012, P. 255-263.
10. 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.
11. 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.
12. 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.
13. А.В. Кельманов, С.М. Романченко. Псевдополиномиальные алгоритмы для некоторых труднорешаемых задач поиска подмножества векторов и кластерного анализа // Автоматика и телемеханика. 2012. № 2, С. 156-162.

Статьи и учебные пособия, принятые в печать.

1. Borodin O.V., Ivanova A.O. Acyclic 4-choosability of planar graphs with no 4- and 5-cycles // J. Graph Theory, DOI 10.1002/jgt.21647.
2. Воробьев К. В. Кратные совершенные коды в гиперкубе. гиперкубе // Дискретный анализ и исследование операций, 2012. Т.19.
3. Dobrynin A.A., Mel'nikov L.S. 4-chromatic Grotzsch-Sachs graphs generated by circles in the plain // Discuss. Math. Graph Theory.
4. Добрынин А.А. Разложение индекса Винера для гексагональных цепей // Прикладные информационные технологии. – Изд. НГУЭиУ.
5. Kostochka A.V., Milans K. Coloring clean and K_4-free circle graphs // A special volume "Geometric Graph Theory".
6. Kostochka A.V., Yu G. Graphs containing every 2-factor // Graphs and Combinatorics.
7. Kostochka A.V., Mubayi D., Verstraete J. On independent sets in hypergraphs // Random Structures and Algorithms.
8. Kostochka A.V., Kumbhat M., Luczak T. Conflict-free colorings of uniform hypergraphs with few edges // Combinatorics, Probability and Computing.
9. Balogh J., Kostochka A.V., Raigorodskii A. Coloring some finite sets in R^n // Discuss. Math. Graph Theory.
10. Akbari S., Kim S.-J., Kostochka A.V. Harmonious coloring of trees with large maximum degree // Discrete Math.
11. Кельманов А.В., Романченко С.М., Хамидуллин С.А. Приближённые алгоритмы для некоторых труднорешаемых задач поиска подпоследовательности векторов // Дискретный анализ и исследование операций.
12. Токарева Н. Н. Криптография. Краткий курс // Учебное пособие. Издательство Новосибирского государственного университета, в печати 2012. 231 страница.

Статьи, сданные в журналы.

1. Borodin O.V., Ivanova A.O. Acyclic 4-choosability of planar graphs without adjacent short cycles // Discrete Math.
2. Borodin O.V. Ivanova A.O. Edge 2-distance coloring of planar graph // Discuss. Math. Graph Theory.
3. Borodin O.V., Kostochka A.V. Defective 2-colorings of sparse graphs//J. Combin. Theory.

4. Kostochka A.V. On almost (k–1)-degenerate (k+1)-chromatic graphs and hypergraphs // Discrete Math.
5. Kostochka A.V., Pfender F., Yancey M. Large rainbow matchings in large graphs // Electronic J. Comb.
6. Kim S.-J., Kostochka A.V. Maximum hypergraphs without regular subgraphs // Discrete Appl. Math.
7. Kim S.-J., Kostochka A.V., West D.B., Wu H., Zhu X. Decomposition of sparse graphs into forests and a graph with dounded degree // J. Graph Theory.
8. Borodin O.V., Kostochka A.V., Yancey M. On 1-improper 2-coloring of sparse graphs // Discrete Math.
9. Kostochka A.V., Prince N. On $K_{s,t}$-minors in graphs with given average degree, II // Discrete Math.
10. Kostochka A.V. $K_{s,t}$-minors in (s+t)-chromatic graphs, II // J. Graph Theory.
11. Kostochka A.V., Mubayi D. , Verstraete J. Hypergraph Ramsey numbers: triangles versus cliques // JCTA.
12. Couturier J.-F., Golovach P., Kratsch D., Liedloff M., Pyatkin A.V. Colorings with few colors: counting, enumeration and combinatorial bounds // Theory of Computing Systems.
13. Кельманов А.В., Романченко С.М., Хамидуллин С.А. Точные псевдополиномиальные алгоритмы для некоторых труднорешаемых задач поиска подпоследовательности векторов // Журнал вычислительной математики и математической физики.

Приложение Б. Список сделанных исполнителями докладов.

На всероссийских конференциях и семинарах.

Секционные доклады.

1. 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.
2. Валюженич А.А. Комбинаторная сложность перестановок, порожденных неподвижными точками кодов // Международная (43-я Всероссийская) молодежная школа-конференция «Современные проблемы математики», 29 января - 5 февраля 2012 г., Екатеринбург, Россия.
3. 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.
4. 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.

На международных конференциях и семинарах.

Пленарные доклады.

1. Kostochka A.V. Workshop on the hypergraph Turan problem. Oberwolfach, Germany, April, 2012.
2. Kostochka A.V. Workshop on probabilistic methods in combinatorics, Birmingham Univ., Birmingham, UK, March, 2012.
3. Kostochka A.V. 1080-th AMS Meeting at George Washington Univ. Washington, DC, March, 2012.

Приложение В. Программа научных семинаров по 3 этапу проекта.

1. С.В. Августинович

   Об антиподальных графах.

2. Е.В. Горкунов, С.В. Августинович

   О восстановлении q-значных кодов.

3. А.А. Валюженич

   Перестановочная сложность неподвижных точек сравнимых морфизмов.

4. И.Ю. Могильных

   Антиподальные дистанционно регулярные графы.

5. В.Н. Потапов

   О подвижных множествах.

6. А.А.Добрынин, Л.С. Мельников

   О графах Кестера на 32 вершинах.

7. В.Н. Потапов

   О совершенных 2-раскрасках в q-значном гиперкубе.

8. И.Ю. Могильных

   Индуцированные совершенные раскраски в двудольных графах.

9. А.В. Кельманов, Хандеев В.И.

   2-приближенный полиномиальный алгоритм для решения одной задачи кластерного анализа

10. С.В. Августинович

    Обобщенный алгоритм Визинга построения совершенных раскрасок.

11. А.В. Косточка

    Независимые множества в униформных гиперграфах.

12. А.В. Косточка

    Уточнение теоремы Хайнала и Корради.

13. А.В. Косточка

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

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