РОССИЙСКАЯ АКАДЕМИЯ НАУК
СИБИРСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ МАТЕМАТИКИ им. С. Л. Соболева

На правах рукописи
УДК 621.391.15

СОЛОВЬЕВА Фаина Ивановна

КОМБИНАТОРНЫЕ МЕТОДЫ ПОСТРОЕНИЯ И ИССЛЕДОВАНИЯ КОДОВ

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
доктора физико-математических наук

Новосибирск, 2008

Работа выполнена в Институте математики им. С. Л. Соболева СО РАН

Официальные оппоненты:	доктор физико-математических наук, профессор В. А. Зиновьев доктор физико-математических наук, профессор А. А. Нечаев, доктор технических наук, профессор Б. Я. Рябко
Ведущая организация:	Московский физико-технический институт (государственный университет)

Защита состоится 14 мая 2008 г. в 14 час. 00 мин. 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.

С диссертацией можно ознакомиться в библиотеке Института математики им. С. Л. Соболева СО РАН.

Автореферат разослан "____" апреля 2008 г.

Ученый секретарь
диссертационного совета,
д.ф.-м.н. Ю. В. Шамардин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Объект исследования настоящей диссертации – теория кодов, исправляющих случайные ошибки. Основные проблемы теории кодирования – разработка методов построения кодов, исследование свойств кодов, классификация кодов с заданными параметрами (длиной кода, его мощностью и кодовым расстоянием), разработка эффективных алгоритмов кодирования и декодирования. Теория кодирования имеет широкое применение на практике как средство экономной, удобной, быстрой и надежной передачи сообщений по линиям связи с различного вида шумами (телефон, телеграф, радио, телевидение, компьютерная, космическая связи и т. д.), что, безусловно, характеризует актуальность этой науки. С 1949 г., с фундаментальных работ К. Шеннона, началось бурное развитие теории кодирования как отдельной научной дисциплины, а также развитие таких тесно с нею связанных научных дисциплин, как сжатие информации и криптология.

Предмет исследования настоящей работы – комбинаторная и алгебраическая теория блоковых кодов, исправляющих случайные ошибки, новые комбинаторные методы построения и исследования таких кодов. Комбинаторная и алгебраическая теория блоковых кодов является важным разделом теории кодирования. В диссертации исследуются в основном двоичные нелинейные коды, среди них совершенные коды, коды с параметрами кодов Рида-Маллера, транзитивные коды; двоичные коды, содержащие схемы, системы Штейнера, MDS-коды. Большинство результатов, представленных в данной работе, получено для совершенных кодов или кодов, связанных с ними рядом свойств.

Актуальность разработки новых методов построения кодов и исследования их свойств (как известных кодов, так и построения новых кодов) в теории кодирования диктуется, прежде всего, задачами поиска кодов и такого их задания, которое позволит разработать более эффективные алгоритмы кодирования и декодирования с целью экономной передачи информации по каналам связи, а также применением таких кодов в криптографии. На практике зачастую используются линейные коды. Однако в последнее время в теории кодирования все большую актуальность приобретают нелинейные коды, например, транзитивные коды, среди них Z_2Z_4-

линейные, Z_4-линейные, их конструирование, классификация. Актуальность построения новых классов нелинейных кодов и изучения их свойств мотивирована следующими причинами. Во-первых, классы нелинейных кодов намного мощнее классов линейных кодов с теми же параметрами и, кроме того, часто линейный q-значный код с заданными параметрами единствен (как, например, код Хэмминга, двоичные коды Рида-Маллера). Во-вторых, за последние два десятилетия среди нелинейных кодов были открыты классы Z_4-линейных кодов, среди которых имеется много неэквивалентных кодов с фиксированными параметрами (например, коды Препараты, коды Кердока, коды с параметрами кодов Рида-Маллера). Кроме того, некоторые нелинейные коды имеют мощность, большую мощности линейных кодов той же длины и с тем же кодовым расстоянием (например, коды Препараты в два раза мощнее кодов БЧХ той же длины с расстоянием 5). Эти обстоятельства служат весомым основанием для поиска применения таких нелинейных кодов в криптографии в кодовых криптосистемах с открытыми ключами. Таким образом для нелинейных кодов возникают естественные математические (комбинаторные) задачи существования и описания (классификации) кодов с данными параметрами. Эти проблемы предусматривают, прежде всего, разработку методов построения кодов, а также методов исследования свойств классов кодов с заданными характеристиками (параметрами или свойствами).

Актуальность исследования совершенных кодов обусловлена следующими обстоятельствами. Совершенные коды представляют собой один из наиболее важных (как своими свойствами, так и методами, разработанными для их построения и исследования) предметов теории кодов, корректирующих ошибки. Код над полем Галуа $GF(q)$ называется *совершенным*, если совокупность шаров одного радиуса, окружающих кодовые слова, задает разбиение пространства. Теория совершенных кодов на сегодняшний день является глубоко разработанной наукой, интенсивно развиваемой как в России, так и за рубежом. Несмотря на значительные усилия целого ряда исследователей, остается открытым множество проблем, связанных с совершенными кодами. По-прежнему остается нерешенной основная проблема построения и перечисления совершенных q-значных кодов для q – степеней простого, не найдена клас-

сификация даже двоичных совершенных кодов длины 15, недостаточно изучены коды полного ранга, нет полного описания групп автоморфизмов совершенных кодов, структуры их i-компонент. Последние три проблемы непосредственно связаны с основной проблемой для совершенных кодов – проблемой их классификации. Известно, что совершенные коды обладают целым рядом регулярных свойств (см. их описание ниже при описании результатов диссертации). Плотная упакованность совершенных кодов предопределяет их оптимальность, т. е. максимальность мощности кода при заданной длине кода и кодовом расстоянии. Проблема упаковки шарами одного радиуса – задача, важная как с точки зрения самой теории кодирования, так и с точки зрения целого ряда других математических дисциплин: комбинаторного анализа, теории групп, теории графов, комбинаторной топологии, геометрии, криптологии, синтеза схем. Кроме того, совершенные коды представляют собой удобный модельный объект для развития подходов к построению и исследованию кодов с большими кодовыми расстояниями – многие из методов построения и изучения свойств совершенных двоичных кодов уже применены и успешно развиваются для кодов с другими параметрами, например, для равномерно упакованных кодов, кодов с параметрами кодов Рида-Маллера, четверичных кодов с метрикой Ли, q-значных, $q \geq 2$, кодов с метрикой Хэмминга, диаметральных совершенных кодов с метрикой Джонсона, для совершенных раскрасок, центрированных функций. Много усилий исследователей посвящено за последние десять лет разработке методов построения и методов исследования свойств совершенных кодов.

К числу открытых проблем (полное или частичное решение которых приводится в данной работе) относились: разработка прямых комбинаторных методов построения и исследования свойств нелинейных двоичных кодов, разработка методов построения транзитивных кодов, исследование метрической жесткости кодов, проблема классификации совершенных кодов, проблема Ф. Хергерта о существовании несистематических совершенных кодов, выяснение структуры i-компонент совершенных кодов и строения группы автоморфизмов таких кодов, проблема Т. Этциона и А. Варди построения и исследования разбиений q-значного n-мерного куба на совершенные коды.

Цель данной **работы** состоит в разработке новых комбинаторных методов построения двоичных нелинейных кодов, новых методов исследования свойств таких кодов и решении ряда открытых проблем теории кодирования с помощью этих методов.

Методика исследований. В диссертации используются традиционные методы и аппарат алгебраической и комбинаторной теории кодирования, комбинаторного анализа. Кроме того, применяются оригинальные методы комбинаторной теории кодирования, разработанные автором.

Научная новизна. Все результаты, представленные в диссертации, являются новыми. В работе представлено несколько принципиально новых комбинаторных методов построения двоичных кодов и исследования их свойств. Предложенные методы позволили решить серию открытых проблем теории корректирующих кодов.

1. В диссертации предложен новый комбинаторный (свитчинговый) метод построения и исследования нелинейных кодов, названный методом *α-компонент*. Этот метод применен к совершенным двоичным кодам и позволил сделать существенное продвижение в решении проблемы классификации совершенных двоичных кодов малых рангов. Используя его, удалось улучшить, впервые после более чем 30-летнего перерыва, нижнюю оценку Ю. Л. Васильева [5] для числа неэквивалентных совершенных кодов. Метод позволил получить дважды экспоненциальный по мощности класс неэквивалентных совершенных двоичных кодов. С помощью этого метода был решен ряд открытых проблем для совершенных кодов.

2. Разработаны новые свитчинговые методы построения транзитивных двоичных кодов. Предложен новый метод построения неэквивалентных четверичных кодов. Двоичные образы этих кодов под действием отображения Грея имеют параметры классических двоичных линейных кодов Рида-Маллера и обладают такими регулярными свойствами, как транзитивность, дистанционная регулярность. Построен новый класс неэквивалентных совершенных транзитивных кодов длины $n = 2^k - 1, k > 4$, таких кодов оказалось не менее $\lfloor k/2 \rfloor^2$. Аналогичный результат верен для расширенных совершенных транзитивных кодов.

3. Новым является комбинаторный метод локального анализа, разработанный для исследования структуры компонент двоичных совершенных кодов, а именно строения i-компонент характеристического графа произвольного совершенного кода. Этот метод позволил решить проблему существования неэквивалентных i-компонент максимальной мощности и построить новые классы кодов с максимальными по мощности связными i-компонентами для любой допустимой длины кода $n > 7$. Посредством этого метода была решена проблема построения неизоморфных замощений (сфер с пленками Мебиуса) с помощью специальных пар систем троек Штейнера порядка n для каждого $n \equiv 3 \pmod 6$.

4. Решена проблема Ф. Хергерта – для каждого допустимого $n > 127$ доказано (конструктивно) существование класса несистематических совершенных двоичных кодов. Для этой цели был развит метод свитчинга компонент минимальной мощности, названный методом i-компонент (независимо для решения других проблем такой подход был применен немного раньше Т. Этционом и А. Варди в [24], а также К. Т. Фелпсом и М. ЛеВаном в [33]).

5. Предложен новый метод (i, α)-star (выявление локально-жестких фрагментов кодов, который также является методом локального анализа) для исследования метрической жесткости кодов. Посредством этого метода полностью выяснен вопрос о метрической жесткости q-значных совершенных кодов, $q \geq 2$, и некоторых классов MDS-кодов. Доказано, что при $n \geq k^4$ произвольный приведенный, т. е. содержащий нулевой вектор, двоичный код длины n, содержащий 2-(n, k, λ)-схему, является метрически жестким кодом.

6. Предложен новый комбинаторный метод (который также можно отнести к методу локального анализа) исследования группы автоморфизмов произвольного совершенного двоичного кода, основанный на тех фактах, что каждое кодовое слово совершенного кода связано со своей системой троек Штейнера, характеристический граф совершенного кода связен, код представляет собой замощение всех своих систем троек Штейнера – локальных фрагментов. Для этого потребовался также комбинаторный подход к изучению строения группы автоморфизмов кодовых систем троек Штейнера, что представляет самостоятельный интерес.

7. Предложены новые комбинаторные (каскадные и свитчинго-

вые) методы построения богатых классов разбиений Хэммингова пространства на совершенные коды и совершенные расширенные коды.

Практическая и теоретическая ценность. Работа носит теоретический характер. Полученные в ней результаты уже нашли применение в теории совершенных кодов, в теории Z_4-линейных кодов, для оптимальных кодов (кодов Препараты, Кердока). Разработанные в диссертации методы могут быть применены в теории корректирующих кодов для построения q-значных кодов, $q \geq 2$, кодов с большими кодовыми расстояниями, для исследования свойств кодов, в криптографии, комбинаторике, комбинаторной топологии, теории графов, а также при преподавании теории информации, см. [48].

Апробация работы. Все результаты работы прошли апробацию на следующих международных конференциях: на конференциях по алгебраической и комбинаторной теории кодирования ACCT-IV (Новгород, 1994 г.), ACCT-V (Созополь, Болгария, 1996 г.), ACCT-VI (Псков, 1998 г.), ACCT-VII (Банско, Болгария, 2000 г.); ACCT-VIII (Царское Село, 2002), ACCT-IX (Кранево, 2004), ACCT-X (Звенигород, 2006); на минисеминаре по упаковкам и покрытиям (Варшава, Польша, 1996 г.); на международном симпозиуме по теории информации (Ульм, Германия, 1997 г.); на международной конференции по теории информации (Килларни, Ирландия, 1998 г.); на международном симпозиуме, посвященном 60-летию профессора Р. Альсведе (Билефельд, Германия, 1998 г.); на международной конференции по геометрии и ее приложениям (Новосибирск, 2000); Сибирской конференции по исследованию операций SCOR-98 и SCOR-2000, на конференциях по дискретному анализу и исследованию операций DAOR-2002, 2004 (Новосибирск, 2002 г., 2004 г.); на международных конференциях по кодированию и криптографии WCC-1999, 2001, 2003 и 2007 г.г. (Париж, Франция), на конференции "Математика в современном мире" (Новосибирск, 2007). Результаты диссертации докладывались на семинарах "Дискретный анализ" НГУ и Института математики СО РАН, "Теория информации и теория кодирования" ИППИ РАН, "Дискретная математика" НГУ и ИМ СО РАН, на семинарах Мюнхен-

ского технического университета и университета Ульма (Германия, 1997 г.), в Билефельдском университете (Билефельд, Германия, 1998 г., 2003, 2007), в Институте математики Болгарской Академии Наук (София, Велико Тырново, Болгария, 1999 г.), в Линчепинском университете (Линчепинг, Швеция, 1999 г. и 2000 г.), в Королевском технологическом университете Стокгольма (Стокгольм, Швеция, 1999, 2000, 2001, 2002, 2004, 2006, 2007 г.), в Похангском университете (Поханг, Корея, 2003, цикл из 8 лекций). Все результаты были доложены на семинаре НГУ и Института математики СО РАН "Теория кодирования". Некоторые результаты диссертации включены в книгу Ж. Коэна с соавторами "Covering codes" и в "Handbook on coding theory". Результаты первой, третьей, четвертой (частично) глав диссертации были включены в цикл работ, занявших в 2002 г. первое место на конкурсе научных работ в ИМ СО РАН.

Публикации. По теме диссертации автором опубликовано 42 работы, см. [39]-[80], среди них одна монография по совершенным кодам и одно учебное пособие по теории кодирования, опубликованное под грифом УМО.

Основные результаты диссертации.

1. Предложен новый комбинаторный метод построения и исследования свойств кодов – метод α-компонент. Метод позволил построить обширный класс неэквивалентных совершенных двоичных кодов длины n, которых оказалось не менее

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 6^{2^{\frac{n+5}{4}-\log_2(n+1)}}.$$

2. Решена проблема Хергерта о существовании несистематических совершенных двоичных кодов длины n для каждого допустимого $n > 127$.

3. Предложено несколько свитчинговых методов построения бесконечных классов транзитивных кодов. Построено не менее $\lfloor k/2 \rfloor^2$ неэквивалентных совершенных транзитивных кодов длины $n = 2^k - 1, k > 4$. Аналогичный результат получен для расширенных совершенных транзитивных кодов. Построен класс неэквивалентных Z_4-линейных кодов длины $2^m, m > 3$, с параметрами клас-

сических кодов Рида-Маллера $RM(r, m)$ для любой допустимого n и любого $r \in \{1, \ldots, m-2\}$.

4. Предложен новый метод исследования свойств кодов, являющийся методом локального анализа. Посредством этого метода исследовано строение i-компонент произвольного совершенного кода. Решена (конструктивно) проблема существования неэквивалентных компонент максимальной мощности, вложимых в совершенные коды. Для каждого допустимого n построен класс совершенных кодов длины n с i-компонентами как неэкстремальной, так и максимально возможной мощностей.

5. Полностью решен вопрос о метрической жесткости q-значных совершенных кодов, $q \geq 2$, и некоторых классов MDS-кодов. Доказано также, что при $n \geq k^4$ произвольный приведенный код длины n, содержащий 2-(n, k, λ)-схему, является метрически жестким.

6. Решена (конструктивно) проблема существования неизоморфных неориентируемых двуцветных замощений (сфер с пленками Мебиуса) порядка n для каждого $n \equiv 3 \pmod 6$ и половины классов вычетов $n \equiv 1 \pmod 6$.

Личный вклад. Диссертационная работа представляет собой единый цикл многолетних исследований автора, объединенных не только предметами, но и методами изучения. В совместных работах соискателю принадлежат идеи новых методов кодирования (предложенных в этих работах) и методов исследования свойств кодов, ключевые моменты разработки этих методов, применение к решению открытых проблем теории кодирования. Отдельные элементы доказательств утверждений и теорем выполнены в соавторстве при непосредственном участии соискателя. Конфликт интересов с соавторами отсутствует.

На защиту выносятся новые комбинаторные методы построения двоичных нелинейных кодов, новые методы исследования свойств таких кодов, а также решение с помощью этих методов нескольких открытых проблем теории кодирования.

Объем и структура диссертации. Диссертация состоит из введения, шести глав и списка литературы (188 наименований), в

конце приведен список публикаций автора по теме диссертации. Объем диссертации – 202 страницы.

СОДЕРЖАНИЕ РАБОТЫ

При решении каждой из задач, рассмотренных в данной работе, был разработан оригинальный математический аппарат, который получил дальнейшее развитие (см. ниже описание результатов) и применение в теории кодирования. Особенность решенных задач определяется главным образом тем, что *локальное строение* исследуемого или конструируемого объекта (кода, блок-схемы, характеристического графа кода) однородно и регулярно, а *глобальное строение* специфично. Совершенные коды обладают целым рядом регулярных свойств, таких как дистанционная инвариантность; равномерная распределенность кодовых слов в пространстве по граням больших размерностей, антиподальность для двоичных совершенных кодов (помимо вершины x совершенному двоичному коду всегда принадлежит вершина $x + \mathbf{1}$, где $\mathbf{1}$ – вектор, все координаты которого равны единице); совокупности кодовых слов веса 3 совершенного двоичного кода C длины n, содержащего нулевой вектор, отвечает система троек Штейнера $STS(C)$ порядка n. На фоне этих однородных свойств в классе совершенных кодов неожиданно проявляются нерегулярные свойства, например, все совершенные коды длины $n \geq 15$ (и даже линейный совершенный код – код Хэмминга) не являются дистанционно-регулярными, существует богатый класс несистематических кодов, ранги и размерности ядер совершенных кодов варьируются от минимально возможных до максимальных, каждая конечная группа изоморфна группе симметрий некоторого совершенного кода, порядок групп автоморфизмов совершенных двоичных кодов длины n варьируется от 2 до порядка общей линейной группы $GL(\log(n+1), 2)$ (здесь и далее под log будем понимать логарифм по основанию 2), умноженной на мощность кода, а количество i-компонент (специального вида компонент связности характеристического графа совершенного кода) произвольного совершенного кода длины n – от 2 до $2^{\frac{n+1}{2}}/(n+1)$ и т. д. Обзоры по построению совершенных двоичных кодов и изучению их свойств см. в [23, 43, 60, 65, 66, 77, 80], q-значных – в [23].

Почти все методы построения совершенных кодов можно разбить схематично на два типа: каскадные и свитчинговые. Оба метода оказались плодотворными для исследования свойств кодов.

Среди направлений изучения кодов следует выделить следующие: методы построения, методы исследования свойств кодов, среди них свитчинговые и каскадные методы; классический вопрос изучения групп автоморфизмов кодов, исследование спектральных свойств кодов, изучение метрической жесткости кодов, построение и исследование разбиений q-значного n-мерного куба на коды (разбиения кодов с одними параметрами на коды с другими, но одной и той же длины), исследование рангов и ядер кодов, пересечения кодов. Исследование этих свойств кодов представляет собой самостоятельный интерес в теории кодирования, а также полезно для построения новых классов оптимальных кодов и решения задачи классификации кодов с данными параметрами.

Прежде чем перейти к обзору и анализу полученных результатов, приведем основные определения и обозначения.

Подмножество пространства F^n всех q-значных векторов длины n над полем Галуа $GF(q)$ по отношению к метрике Хэмминга называется *q-значным кодом* C длины n. Элементы кода C называются *кодовыми словами* или *векторами*. Параметры q-значного линейного кода C над полем Галуа $GF(q)$, $q \geq 2$, будем обозначать через $[n, M, d]_q$, где n – длины кода, M – его мощность, d – кодовое расстояние (наименьшее расстояние по Хэммингу между кодовыми словами). Для нелинейного кода C параметры будем обозначать через $(n, M, d)_q$, в двоичном случае q будем опускать. Векторное пространство размерности n над $GF(2)$ обозначим через E^n.

Два кода $C, C' \subset F^n$ называются *изоморфными*, если существует подстановка π такая, что $C' = \pi(C) = \{\pi(\mathbf{x}) : \mathbf{x} \in C\}$. Коды $C, C' \subset F^n$ *эквивалентны*, если найдется n подстановок $\tau_1, \ldots, \tau_n$ на q элементах поля Галуа F_q и подстановка π на n координатных позициях такие, что

$$C' = \{\pi(\tau_1(x_1), \tau_2(x_2), \ldots, \tau_n(x_n)) : (x_1, x_2, \ldots, x_n) \in C\}.$$

Расстояние Хэмминга $d(\mathbf{x}, \mathbf{y})$ между векторами $\mathbf{x}, \mathbf{y} \in F^n$ равно числу координат, в которых эти векторы различаются (далее век-

торы будем обозначать выделенными строчными латинскими буквами). Кодовое расстояние d определяется как $d = min\, d(\mathbf{x}, \mathbf{y})$ для любых различных кодовых слов $\mathbf{x}, \mathbf{y} \in C$. *Группой автоморфизмов* $\mathrm{Aut}(C)$ произвольного кода C длины n является группа изометрий пространства E^n, переводящих код в себя, т.е.

$$\mathrm{Aut}(C) = \{(v, \pi) \mid v + \pi(C) = C\}.$$

Множество

$$\mathrm{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$$

называется *группой симметрий* кода C. Код C *транзитивен*, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Размерность линейной оболочки $< C >$ кода C называется *рангом* кода C. Совокупность *периодов* кода C, т.е. кодовых слов $x \in C$ таких, что $x + C = C$ называется *ядром* кода C. Код мощности M (размерности $k = \log_q M$) длины n называется *систематическим*, если существуют такие k координатных позиций кода, что код, полученный из исходного выкалываем (удалением) оставшихся $n - \log_q M$ координат, совпадает со всем пространством E_q^k. *Системой троек Штейнера* $STS(n)$ порядка n называется система сочетаний из n элементов по три такая, что каждая неупорядоченная пара элементов содержится в точности в одной тройке. Другие определения целесообразно привести ниже при описании результатов диссертации.

Широко известна теорема В. А. Зиновьева и В. К. Леонтьева, полученная независимо Э. Тиетвайненом, см. [7, 8, 38], о том, что нетривиальные совершенные q-значные коды длины n, исправляющие ошибки, существуют только при $n = (q^k - 1)/(q - 1)$, $k \geq 2$, такие коды имеют кодовое расстояние 3 (далее упоминаемые как совершенные); при $n = 23$ – это двоичный код Голея с кодовым расстоянием 7, а также при $n = 11$ – троичный код Голея с кодовым расстоянием 5. Оба кода Голея единственны с точностью до эквивалентности. Ю. Л. Васильевым [5] в 1962 г. был открыт класс совершенных двоичных кодов, число неэквивалентных таких кодов оказалось дважды экспоненциальным. Тем самым была опровергнута гипотеза Г. С. Шапиро и Г. Л. Злотника [37] о единственности существования совершенного двоичного кода (кода Хэмминга) для

каждой допустимой длины. Для составных q известно, что для расстояний, больших 3, совершенные коды не существуют, и также не существуют совершенные коды с расстоянием 3 при $q = 6, n = 7$ и $n = 19$.

В первой главе приводятся новые свитчинговые методы построения кодов: метод α-компонент и метод последовательных сдвигов i-компонент. Основная идея метода свитчинга состоит в следующем: в произвольном коде C длины n рассмотрим некоторое подмножество M кодовых слов. Если найдется в F^n подмножество M', отличное от множества M такое, что множество

$$C' = (C \setminus M) \cup M'$$

является кодом с параметрами, совпадающими с параметрами кода C, то будем говорить, что код C' получен из кода C *свитчингом* множества M на множество M'. Результирующий код отличен или неэквивалентен исходному.

Рассмотрим основную идею метода α-компонент на примере совершенных кодов (из описания метода следует, что он имеет место для q-значных кодов, $q \geq 2$, отличных от совершенных). Пусть C – произвольный совершенный код длины n и R – некоторое подмножество его кодовых слов. *Свитчингом* множества R в направлении i, где $i \in I = \{1, 2, \ldots, n\}$, назовем множество R', полученное из R сдвигом на вектор e_i веса один (с единицей только в i-й координате) всех его кодовых слов, и обозначим его $R' = R \oplus e_i$. Множество R назовем *i-компонентой* кода C, если $K(R) = K(R \oplus e_i)$, где $K(R)$ – объединение шаров радиуса 1 с центрами в векторах R. Легко понять, что код $C' = (C \setminus R) \cup (R \oplus e_i)$ также является совершенным кодом. Будем говорить, что C' получен из кода C *свитчингом*. Пусть $\alpha \subseteq I$. Подмножество M кода C назовем *α-компонентой*, если для всех $i \in \alpha$ множество M является i-компонентой кода C. Понятие α-компоненты оказалось плодотворным при построении новых классов совершенных кодов и исследовании свойств совершенных кодов. Непересекающиеся α-компоненты можно разбивать на компоненты меньшей мощности по разным направлениям. Это позволяет сдвигать сначала компоненты меньшей мощности, варьируя направления, затем полученные α-компоненты сдвигать по

оставшимся неизрасходованными направлениям из множества α. При этом получается новый класс совершенных кодов с теми же параметрами. Если число компонент равно K, то мощность этого класса не менее 2^K. Метод α-компонент оказался особенно подходящим в применении к коду Хэмминга, поскольку позволяет, разрушая групповую структуру кода Хэмминга, следить за структурой нелинейного совершенного кода, получаемого вследствии серии свитчингов.

Используя этот метод, в 1996 г. удалось впервые улучшить нижнюю оценку Ю. Л. Васильева [5]

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}},$$

полученную в 1962 г. для числа различных совершенных двоичных кодов длины n, а именно, в параграфе 1.2 доказана

Теорема 2. Количество различных совершенных двоичных кодов длины n не менее, чем

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 6^{2^{\frac{n+5}{4}-\log_2(n+1)}}.$$

Оценка достигается применением метода α-компонент к коду Хэмминга H длины n. Сначала разбиваем код Хэмминга H на (i,j,k)-компоненты, где (i,j,k) – произвольная тройка из системы троек Штейнера $STS(H)$ кода Хэмминга H, затем независимо каждую (i,j,k)-компоненту – на i, j или k-компоненты. Для построения класса кодов существенно использовались свойства $STS(H)$. При этом проведен анализ свойств подмножеств с фиксированной координатой системы троек Штейнера кода Хэмминга. Именно он позволил итеративно препарировать код Хэмминга (сначала на подкоды большой мощности, затем меньшей) и применить к нему серии локальных преобразований – свитчингов компонент.

Фактически при этом была получена нижняя оценка числа совершенных кодов ранга не больше $n-\log(n+1)+2$. С помощью этого метода построения кодов впервые, после Ю. Л. Васильева, была доказана мощностным способом неэквивалентность предложенных кодов ранее известным кодам (первый фактор в формуле теоремы

2 получается при варьировании i-компонент, второй фактор получен за счет варьирования (i,j,k)-компонент). Следует отметить, что прежде производились многочисленные, но безуспешные, попытки улучшить оценку Ю. Л. Васильева.

Этот свитчинговый метод построения совершенных кодов и исследования их свойств дал возможность решить целую серию проблем, например, положительно решить проблему рангов и ядер (проблему Т. Этциона и А. Варди 1998 г.), см. [2], для всех $n = 2^k - 1$, $k \geq 5$, позволил доказать существование разбиения множества всех двоичных векторов длины n на попарно неэквивалентные совершенные двоичные коды длины n с кодовым расстоянием 3, см. [4], этот метод был развит для q-значных совершенных кодов, см. [12], что позволило получить наилучшую на сегодняшний день нижнюю оценку числа таких кодов, этот подход лег в основу развития метода i-компонент (см. описание ниже). Метод α-компонент получил активное развитие в работах С. А. Малюгина [13, 30], Д. С. Кротова [11], С. В. Августиновича и Д. С. Кротова [29]. В работе [13] С. А. Малюгин предложил сначала заменить произвольную (i,j,k)-компоненту в коде Хэмминга H на изоморфную (i,j,k)-компоненту, затем производить сдвиги i и j компонент. Эта модификация позволила обогатить получаемый класс совершенных кодов по мощности. Затем этот метод был развит Д. С. Кротовым [11] также для совершенных кодов ранга опять таки не больше $n - \log(n+1) + 2$, дополнительно к методу α–компонент он применил известный обобщенный каскадный метод К. Т. Фелпса-1984. Впоследствии, применяя многократно к коду Хэмминга длины n метод α–компонент, С. В. Августинович и Д. С. Кротов, см. [29], получили лучшую на сегодняшний день нижнюю оценку числа различных совершенных кодов длины n неполного ранга, первые три наибольших фактора в этой оценке совпадают с нижней оценкой Д. С. Кротова

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}.$$

Обзор свитчинговых конструкций и нетривиальных свойств совершенных кодов, полученных с помощью свитчингового подхода, см. в работах [43, 65, 77].

Здесь же, в главе 1, приводится метод сдвига непересекающихся

i-компонент. Этот подход, примененный к коду Хэмминга, позволил решить проблему Ф. Хергерта 1985 г. о существовании несистематических совершенных кодов. Доказать требуемое свойство (например, построить несистематические коды или i-компоненты максимальной мощности, см. ниже результаты главы 3), имея в запасе только локально повторяющуюся одинаковую картину, означает воссоздать структуру объекта, сформированного из локальных фрагментов, суметь "склеить", имея только частичную информацию, весь предмет в целом или суметь перестроить код, являющийся глобально и локально однородным (например, код Хэмминга) таким образом, чтобы результирующий код, став нелинейным, обладал требуемыми свойствами и в целом и для фрагментов.

Для решения проблемы Ф. Хергерта 1985 г. потребовались локальные преобразования кода Хэмминга длины n. Код Хэмминга можно униформизовать – он является систематическим, т. е. в n-кубе найдется такая $\log(n+1)$-мерная грань, что в каждой параллельной ей грани содержится в точности одно кодовое слово. Никакой несистематический код невозможно униформизовать в указанном смысле, т. е. какая бы $\log(n+1)$-мерная грань ни была выбрана в n-кубе, найдется грань, параллельная ей, не содержащая кодовых слов и, соответственно, найдется параллельная грань, содержащая не менее двух кодовых слов. Для построения несистематических кодов, как правило, необходим достаточный "простор" в пространстве между кодовыми словами, какового нет для совершенного кода в силу его плотной упакованности. Отсутствие простора было компенсировано строго скорректированными свитчингами специальных подкодов кода Хэмминга, не нарушающими плотную упакованность результирующего кода. Для этого был разработан метод свитчингов (последовательных сдвигов) i-компонент: в коде Хэмминга длины n для различных i, $i = 1, \ldots, n$, были сдвинуты n достаточно далеких i-компонент. При этом существенно использовались свойства специального вида подсистем системы троек Штейнера кода Хэмминга и свойства систем троек Штейнера полученного кода. Долгое время предполагалось, согласно гипотезы Ф. Хергерта 1985 г., см. [28], что все совершенные коды систематические.

В главе 1 доказана

Теорема 3. Существует класс несистематических совершенных двоичных кодов длины n для любого $n > 127$, где $n = 2^k - 1$.

Существенную роль в проверке несистематичности построенного кода сыграл метод локального анализа окрестностей кодовых слов полученного совершенного кода – систем троек Штейнера $ST(\mathbf{x})$ кодовых слов (это множество таких троек (i, j, k), что $\mathbf{x} \oplus \mathbf{y} \in C$, где вершине $\mathbf{y} \in C$ отвечает тройка (i, j, k), здесь $\mathbf{x} \in C$) и в особенности $STS(H)$ кода Хэмминга H. Нетрудно видеть, что $ST(\mathbf{x}) = STS(\mathbf{x} \oplus C)$. Определим систему троек кода C следующим образом

$$ST(C) = \bigcup_{\mathbf{x} \in C} ST(\mathbf{x}).$$

Систему троек назовем *полной*, если она содержит всевозможные тройки координат. Оказалось, что построенный код имеет полную систему троек.

Результаты этой главы получены совместно с С. В. Августиновичем (см. [54, 42, 55, 40]).

Метод сдвига непересекающихся i-компонент различных направлений, безусловно, тесно связан с методом α-компонент, но не является его частным случаем, поскольку имеются ситуации, когда метод i-компонент применим, а метод α-компонент – нет, и наоборот. Нетрудно видеть, что известный итеративный метод построения совершенных кодов Васильева является методом i-компонент, для этого достаточно в конструкции Васильева взять произвольный код Васильева в качестве кода предыдущей кодовой размерности, см. также [65]. Но всякий раз при решении конкретной задачи методом i-компонент требуются дополнительные условия, вследствие чего этот метод модифицируется в новую конструкцию кодов. Этот метод был независимо предложен Т. Етционом и А. Варди [24] для перечисления спектра рангов нелинейных совершенных кодов, К. Т. Фелпсом и М. ЛеВаном [33] для описания спектра размерностей ядер нелинейных совершенных кодов длины $n \geq 15$. Позднее этот метод был использован для построения класса совершенных кодов полного ранга с тривиальной группой автоморфизмов и, следовательно, с тривиальным ядром (см. [57]).

Метод построения несистематических кодов получил дальнейшее развитие в следующих работах: были построены несистемати-

ческие коды для $n \leq 127$ К. Т. Фелпсом и М. ЛеВаном в работе [34], А. М. Романовым для $n = 15$; С. А. Малюгиным в [15] опубликован результат о том, что минимальное количество i-компонент, которые необходимо сдвинуть в коде Хэмминга длины n для получения несистематического кода, не зависит от n и равно 7. К. Т. Фелпс и М. ЛеВан [35], используя конструкцию [39] автора диссертации, доказали в 1999 г., что существуют совершенные коды длины 15, которые невозможно получить из кода Хэмминга методом свитчинга. Следует отметить, что на сегодняшний день перечислены все совершенные и совершенные расширенные коды длин 15 и 16 соответственно, кроме кодов полного ранга, равного 15, см. работы [9, 16]. Обзор конструкций, а также нетривиальных свойств, присущих всем совершенным кодам, полученных методом свитчингов, см. в [65, 77, 80].

Вторая глава посвящена разработке методов построения и исследования транзитивных кодов. В этой главе приводится новых несколько новых свитчинговых методов построения бесконечных классов транзитивных двоичных кодов. Будучи примененными к совершенным кодам, эти методы позволили (конструктивно) доказать, что существует не менее $\lfloor k/2 \rfloor^2$ неэквивалентных совершенных транзитивных кодов длины $n = 2^k - 1, k > 4$. Аналогичный результат справедлив для расширенных совершенных транзитивных кодов. Кроме того, в этой главе приведен метод построения неэквивалентных Z_4-линейных кодов с параметрами классических кодов Рида-Маллера для любых допустимых параметров этих кодов.

Транзитивные объекты, обладая богатым набором симметрий, играют важную роль как в теории кодирования, так и в комбинаторике, теории групп, теории графов. Следует отметить, что по ряду свойств транзитивные коды близки к линейным кодам и, по всей видимости, по этой причине количество таких кодов невелико. Однако для большинства оптимальных нелинейных кодов почти всегда можно найти транзитивные коды с такими же параметрами. Например, двоичный образ (под действием отображения Грея) произвольного аддитивного кода является транзитивным кодом.

Пусть B и C – произвольные двоичные коды длины n с кодовыми расстояниями d_1 и d_2 соответственно, где d_1 нечетно. Пусть

λ – произвольная функция из кода C в множество $\{0,1\}$, $|x| = x_1 + \ldots + x_n (\mathrm{mod}\, 2)$, где $x = (x_1, \ldots, x_n) \in E^n$. Код

$$C^{2n+1} = \{(x, |x| + \lambda(y), x + y) \mid x \in B, y \in C\}$$

будем называть *кодом Васильева*, см. [5]. Он имеет длину $2n+1$, мощность $|B| \cdot |C|$ и кодовое расстояние $d = \min\{2d_1 + 1, d_2\}$.

Теорема 4. Пусть C является произвольным транзитивным кодом с параметрами $(n, |C|, d_2)$, B – таким линейным кодом с параметрами $[n, |B|, d_1]$ с нечетным кодовым расстоянием d_1, что для любого автоморфизма $(y, \pi) \in \mathrm{Aut}\,(C)$ выполняется $\pi \in \mathrm{Sym}\,(B)$. Тогда код Васильева C^{2n+1}, для которого $\lambda \equiv 0$, является транзитивным.

Множество

$$C^{2n} = \{(x, x + y) \mid x \in B, y \in C\}$$

называется *кодом Плоткина* длины $2n$, он имеет мощность $|B| \cdot |C|$ и кодовое расстояние $d = \min\{2d_1, d_2\}$.

Нетрудно видеть, что расширение транзитивного кода с помощью общей проверки на четность всегда дает транзитивный код. Обратное, вообще говоря, неверно. Более того, известны примеры таких транзитивных кодов, что коды, полученные из них выкалыванием некоторой координаты, не являются транзитивными. Следовательно, построение и исследование расширенных транзитивных кодов целесообразно проводить независимо от построения транзитивных кодов, не являющихся расширенными.

Теорема 5. Пусть C является произвольным транзитивным кодом с параметрами $(n, |C|, d_2)$, B – таким линейным кодом с параметрами $[n, |B|, d_1]$, что для любого автоморфизма $(y, \pi) \in \mathrm{Aut}\,(C)$ выполняется $\pi \in \mathrm{Sym}\,(B)$. Тогда код Плоткина C^{2n} транзитивен.

Пусть P^t и C^m – произвольные двоичные коды длин t и m соответственно с кодовыми расстояниями не менее 3, содержащие нулевые векторы. Пусть

$$x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{t1}, \ldots, x_{tm}) \in E^{tm}.$$

Функции $p_1(x)$ и $p_2(x)$, определенные следующим образом

$$p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_t) \in E^t, \;\; p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m,$$

где $\sigma_i = \sum_{j=1}^{m} x_{ij}$ и $\sigma'_j = \sum_{i=1}^{t} x_{ij}$, называются *обобщенными проверками на четность*. Пусть f – произвольная функция из P^t в E^m. Множество

$$C^n = \{(x, y + p_1(x), z + p_2(x) + f(y)) \mid x \in E^{tm}, y \in P^t, z \in C^m\}$$

называется двоичным *кодом Моллара* длины $n = tm + t + m$ с кодовым расстоянием 3 (см. [31]). В параграфе 2.2.3 главы 2 доказана следующая

Теорема 6. Пусть P^t и C^m – произвольные двоичные транзитивные коды длин t и m соответственно. Тогда код Моллара C^n, для которого $f \equiv \mathbf{0}^m$, является двоичным транзитивным кодом длины $n = tm + t + m$.

Все три приведенных выше метода построения транзитивных двоичных кодов допускают построение совершенных транзитивных кодов длины n для любой допустимой длины разных рангов, начиная от минимально возможного, равного размерности кода Хэмминга длины n до $n - \frac{1}{4}\log(n+1)$. Были получены следующие результаты:

Теорема 7. Число неэквивалентных совершенных транзитивных кодов длины $n = 2^k - 1, k \geq 4$ не менее $\lfloor k/2 \rfloor^2$.

Теорема 8. Для любого $n = 16^l - 1, l \geq 1$, и каждого натурального числа δ, удовлетворяющего $1 \leq \delta \leq \frac{3}{4}\log(n+1)$, существует совершенный транзитивный код длины n ранга $n - \log(n+1) + \delta$.

Ранее было известно $\lfloor (k+1)/2 \rfloor$ совершенных аддитивных кодов длины $n = 2^k - 1$, см. [22] (аналогично для расширенных совершенных аддитивных кодов, см. [11]). Нетрудно показать, что все эти коды являются транзитивными и дистанционно инвариантными. Малюгиным в 2004 г. перечислены все совершенные транзитивные коды длины 15 из свитчингового класса кода Хэмминга длины 15. В работе [18] В. Н. Потаповым для каждого n было построено экспоненциальное число неэквивалентных расширенных транзитивных

совершенных кодов длины $4n$ ранга на единицу больше ранга кода Хэмминга такой же длины.

Здесь же, в главе 2, в параграфе 2.4, приводится свитчинговый метод построения для каждого r, $0 \leq r \leq m$, класса четверичных линейных кодов $\mathcal{LRM}(r,m)$, двоичные образы которых под действием отображения Грея являются двоичными кодами с параметрами классических двоичных линейных кодов Рида-Маллера $RM(r,m)$ порядка r. Эти коды являются транзитивными и дистанционно-регулярными. На сегодняшний день известно много хороших двоичных нелинейных кодов, представимых в качестве линейных над кольцом $\mathbb{Z}_4$, среди них следует отметить подклассы кодов Препараты, Кердока, Дельсарта-Геталса, Геталса-Дельсарта, совершенных, Адамара, см. [17, 26].

Напомним определение двоичного кода Рида-Маллера. Пусть $v = (v_1, \ldots, v_m)$ – вектор, пробегающий пространство $\mathbb{Z}_2^m$. Пусть $r \in \{0, 1, \ldots, m\}$, $m \geq 1$. Рассмотрим все булевы функции, равные многочленам, степень которых не превосходит r. *Двоичный код Рида-Маллера* $RM(r,m)$ *порядка* r определяется как линейная оболочка множества всех векторов длины 2^m, отвечающих значениям таких булевых функций. В главе 2 доказан следующий результат.

Теорема 9. Для любого r, $r \in \{0, 1, \ldots, m\}$, $m \geq 1$, существует четверичный линейный код с параметрами

$$(n = 2^{m-1},\ 2^k,\ d = 2^{m-r}),\ \text{где}\ k = \sum_{i=0}^{r} \left(\begin{array}{c} m \\ i \end{array} \right), \qquad (1)$$

чей образ под действием отображения Грея является двоичным кодом с параметрами кода Рида-Маллера $RM(r,m)$ порядка r. При каждом $r \in \{1, \ldots, m-2\}$, $m \geq 4$, существуют неэквивалентные четверичные коды.

Поскольку под действием отображения Грея двоичный образ любого из четверичных кодов является Z_4-линейным кодом, который является транзитивным кодом, то применение теоремы 5 дает бесконечный класс транзитивных двоичных кодов с параметрами кодов Рида-Маллера, которые уже могут не быть Z_4-линейными. Результаты этой главы опубликованы в работах [76, 78, 47, 49].

Полное решение проблемы пересечения произвольных двух аддитивных, в частности четверичных (т. е. перечисление всех возможных мощностей кодов, равных пересечению аддитивных кодов), совершенных кодов было дано в работе [36]. Были найдены верхняя и нижняя оценки этих мощностей, для любого допустимого числа между этими оценками были построены коды, дающие в пересечении код мощности, равной этому числу, описана аддитивная структура этих кодов.

В третьей главе предложен метод локального анализа для исследования строения i-компонент совершенных двоичных кодов, примененный также для решения проблемы двуцветного замощения замкнутых неориентируемых поверхностей. Основная идея метода локального анализа, разработанного в диссертации, состоит в изучении и анализе локальных фрагментов кодов (или блок-схем, зачастую это системы троек Штейнера), в последующем в неоднократном изменении этих фрагментов кодов с целью построения новых кодов и контроля за их свойствами или изучения свойств классов кодов.

Изучение структуры, а также спектра мощностей i-компонент важно для решения основной проблемы теории совершенных кодов – проблемы их перечисления и классификации. Известно, что верхняя и нижняя оценки числа m неразложимых (не разбивающихся на компоненты меньшей мощности) i-компонент произвольного совершенного кода длины n, $n = 2^s - 1$, удовлетворяют неравенству

$$2 \leq m \leq 2^{\frac{n+1}{2}}/(n+1).$$

Обе оценки точны, см. [5, 19, 20]. Мощность неразложимых i-компонент варьируется от $2^{(n-1)/2}$ до $2^{n-1}/(n+1)$. Согласно [6, 19], для совершенных кодов длины n (для всех допустимых $n > 7$) существуют i-компоненты неэкстремальной мощности. В работе [53] для любого $n > 7$ был предложен совершенный код длины n с i-компонентами различных структур и мощностей.

В этой главе для каждого допустимого n предлагается класс совершенных кодов длины n с i-компонентами как максимально возможной, так и неэкстремальной мощностей.

В параграфе 3.2 доказана

Теорема 12. Существует класс совершенных кодов длины n с неразложимыми i-компонентами мощности

$$(k+1)2^{n-k}/(n+1)$$

для каждого $n = 2^s - 1, s > 2$ и $k = 2^r - 1$, где $r = 2, \ldots, s-1$.

Основным результатом этой главы является следующая

Теорема 13. Для каждого $n = 2^s - 1, s > 3$, существуют неизоморфные i-компоненты максимальной мощности, принадлежащие различным совершенным кодам длины n.

При построении i-компонент, имеющих максимально возможную мощность, а также при построении i-компонент, не являющихся минимальными, важным моментом явилось следующее обстоятельство: оказалось существенным обеспечить связность этих множеств (как специальных компонент характеристического графа совершенного кода), их экстремальность и протяженность в n-кубе. Факт связности также важен для выяснения того обстоятельства, что i-компонента *неразложима*, т. е. не разбивается на i-компоненты меньшей мощности. На сегодняшний день в литературе не известны другие методы построения компонент совершенных кодов, кроме случая кодов длины 15. Для этого случая К. Т. Фелпс и М. Д. ЛеВан в [35] доказывают связность компонент совершенного кода длины 15, используя компьютер. При доказательстве Теоремы 13 посредством метода локального анализа строятся классы кодов с протяженными связными i-компонентами для любой допустимой длины кода $n > 7$. Особенные трудности возникают при построении неизоморфных i-компонент максимальной мощности, равной половине размера всего совершенного кода, поскольку приходится, учитывая максимальность, "склеивать" большое количество локально одинаковых фрагментов подкодов, максимальное Хэммингово расстояние в которых равно только 6. Получение этой совокупности i-компонент еще раз убеждает в нетривиальности задачи перечисления всех совершенных кодов, а также в некоторой ограниченности возможностей свитчингового подхода, который эффективно работает для линейных компонент кода Хэмминга, хотя в то же время существует много других более сложно устроенных компонент совершенных кодов.

Следует также отметить, что методы построения обоих классов кодов с i-компонентами максимально возможной и неэкстремальной мощностей совпадают и представляют собой одновременное комбинирование каскадного [39] и свитчингового [5] методов построения совершенных кодов. При этом снова используются структурные свойства систем троек Штейнера совершенных кодов Хэмминга, лежащих в основе каскадного метода построения результирующих кодов, предложенного автором диссертации в 1981 г., см. [39]. Использование метода локального анализа, с учетом свойств этих специальным образом выбранных систем троек Штейнера, позволило обеспечить связность i-компонент полученного кода, а также найти количество этих компонент.

Эти результаты опубликованы в работах [59, 61, 63, 64, 71].

Вторая половина третьей главы посвящена (конструктивному) решению проблемы существования неизоморфных замощений неориентируемых поверхностей парами систем троек Штейнера порядка n для каждого $n \equiv 3 \pmod 6$ и половины классов вычетов $n \equiv 1 \pmod 6$ (известно, что системы троек Штейнера существуют при $n \equiv 1, 3 \pmod 6$). Эта проблема тесно связана с широко известной в теории графов проблемой нитей, успешно решенной Г. Рингелем и Дж. У. Т. Янгсом в 1968 г. Проблема нитей касается исследования триангулированных вложений (необязательно двухцветных) полного графа в замкнутые поверхности. В отличие от проблемы нитей, проблема существования неизоморфных замощений состоит в построении и перечислении триангулированных *двухцветных* вложений полного графа в замкнутые поверхности. Сопоставим каждой тройке (i, j, k) из системы троек Штейнера порядка n (кратко $STS(n)$) топологический треугольник с вершинами i, j и k. Склеивание по одноименным сторонам треугольников, отвечающих специального вида паре непересекающихся $STS(n)$ позволяет получить черно-белое замощение некоторой замкнутой поверхности. Существование неизоморфных замощений ориентируемых поверхностей (сфер с ручками) было решено С. П. Боннонгтоном с соавторами, см. [21].

Теорема 14. Для каждого $n \equiv 3 \pmod 6$ доказано существование неизоморфных замощений неориентируемых поверхно-

стей (сфер с пленками Мебиуса) парами систем троек Штейнера порядка n.

Теорема 15. Для любого $n \equiv 3 \pmod 6$, $n \geq 19$ существует не менее $2^{(n-1)(n-3)/6}$ неизоморфных неориентируемых замощений порядка $3n-2$.

Следствие. Существуют неэквивалентные замощения неориентируемой замкнутой поверхности (сферы с $(n-3)(n-4)/6$ пленками Мебиуса) посредством пар систем троек Штейнера порядка n для половины классов вычетов $n \equiv 1 \pmod 6$.

Следует отметить идейную аналогию и параллелизм результата о замощениях и основного результата главы 3 о построении неизоморфных i-компонент максимально возможной мощности. В обоих ситуациях имеем пару нетривиальных структур, которые в объединении дают совершенную структуру (в случае замкнутых поверхностей также имеем в некотором смысле "совершенность", а именно сферу с ручками Мебиуса, которая не является псевдосферой, т. е. не получается склеиванием нескольких сфер с ручками Мебиуса и (или) отождествлением некоторого количества точек поверхности), в обоих ситуациях необходимо обеспечить связность характеристических графов специального вида и, наконец, в основе каждой из этих конструкций лежит пара непересекающихся систем троек Штейнера специального вида (следует отметить, что пары STS, использованные для построения максимальных i-компонент и замощений различны). Кроме того, в обоих случаях для построения этих совершенных структур использовался метод локального анализа, а именно, исследовались свойства локальной структуры каждого из этих объектов (в случае замощений таким свойством является свойство цикличности, которое должно выполняться для каждого элемента $i \in N = \{1, 2, \ldots, n\}$ обоих систем троек Штейнера порядка n), затем склеивание этих локальных фрагментов позволило построить объекты в целом: в одном случае совершенных кодов с максимально мощными i-компонентами, в другом – "совершенных" замощений двумерных многообразий.

Четвертая глава настоящей диссертации посвящена вопросам метрической жесткости широкого класса двоичных кодов и неко-

торых классов q-значных кодов, $q > 2$. Вопросы жесткости метрических подпространств представляют собой достаточно популярную область в геометрии. Понятие метрической жесткости тесно и естественно связано с широко известным понятием жесткости в геометрии, см., например, [27]). В дискретной математике возникает ряд специфических особенностей при рассмотрении понятия метрической жесткости.

Код C называется *метрически жестким*, если каждая изометрия $\phi : C \to F^n$ по отношению к метрике Хэмминга расширяема до изометрии всего пространства F^n (напомним, что здесь F^n – векторное пространство над полем Галуа $GF(q)$ характеристики $q \geq 2$).

В 1994 г. С. В. Августиновичем, см. [1], доказано, что все совершенные двоичные коды длины $n > 15$ являются метрически жесткими. Два кода C_1, C_2 *слабо изометричны*, если существует такое отображение $J : C_1 \to C_2$, что равенство $d(\mathbf{x}, \mathbf{y}) = 3, \mathbf{x}, \mathbf{y} \in C_1$, справедливо тогда и только тогда, когда $d(J(\mathbf{x}), J(\mathbf{y})) = 3$. В 1998 г. С. В. Августиновичем, см. [1], доказано, что любые два слабо изометричных совершенных двоичных кода эквивалентны.

Пусть R – произвольное метрическое пространство с достаточно богатой группой автоморфизмов. Два метрических подпространства R_1 и R_2 из R эквивалентны, если существует автоморфизм I из группы автоморфизмов пространства R такой, что $I(R_1) = R_2$. Достаточно часто все проблемы относительно метрических пространств изучаются с точностью до эквивалентности. Рассмотрим ситуацию, когда важна только структура метрического подпространства, но не способ, как метрическое подпространство вложено в пространство R. Исследование такой ситуации, имея ввиду только эквивалентность, крайне затруднительно. Подход с учетом изометрии позволяет преодолевать все возникающие трудности. Описанная ситуация имеет место как в геометрии (см. [27]), так и в дискретной математике (см. [1, 10, 58, 62]).

Код из F^n над $GF(q)$ называется (n, k) *MDS-кодом* (maximal-distance separable – максимально-дистанционно разделимым), если его параметры достигают границы Синглтона: $d = n - k + 1$, где n – длина кодового слова, $k = \log_q M$ – размерность кода, M – мощность кода, d – кодовое расстояние кода C.

В этой главе методом $(i, \alpha)-star$ (выявлением локально-жестких

фрагментов кодов), предложенным в диссертации, доказаны следующие утверждения:

Теорема 19. Все q-значные $(n, n-1)$ MDS-коды являются метрически жесткими за исключением двух кодов длины 3 и одного кода длины 4.

Теорема 20. Все совершенные коды с кодовым расстоянием 3 над $GF(q)$ являются метрически жесткими за исключением двоичного кода Хэмминга длины 7 и троичного кода Хэмминга длины 4.

В параграфе 4.1 доказано, что двоичный четно-весовой код длины n является метрически жестким тогда и только тогда, когда $n \neq 4$. В параграфе 4.2 выяснено, что q-значные $(q, 2)$ и $(q+1, 2)$ MDS-коды метрически жесткие, если и только если $q = 2$.

Метрическую жесткость кодов удается доказать, исследуя локально-жесткие подкоды q-значных совершенных кодов и MDS-кодов. Эти подкоды являются в некотором смысле аналогами подмножеств систем троек Штейнера совершенного двоичного кода с фиксированной координатой.

Определим *2-(n, k, λ)-схему* на множестве N как систему k-элементных подмножеств (блоков) из N такую, что каждое неупорядоченное двухэлементное подмножество из N содержится в точности в λ блоках схемы.

Теорема 21. При $n \geq k^4$ произвольный приведенный двоичный код, содержащий 2-(n, k, λ)-схему, является метрически жестким кодом.

Класс таких кодов включает все семейства равномерно упакованных кодов достаточно большой длины, удовлетворяющих условию $d - \rho \geq 2$, где d – кодовое расстояние и ρ – радиус покрытия. Известно, что множество равномерно упакованных кодов содержит $(d-\rho)$-схемы (и, следовательно, 2-схемы) и включает БЧХ-коды с расстоянием 5 и 7, коды Препараты, коды Геталса с расстоянием 7, расширенные совершенные коды.

Последняя теорема получена совместно с С. В. Августиновичем, см. [46], остальные результаты этой главы получены совместно с С. В. Августиновичем, В. Хайзе и Т. Хонольдом, см. [58, 62].

Пятая глава посвящена исследованию групп автоморфизмов совершенных кодов и систем троек Штейнера. Известный результат К. Т. Фелпса [32] о том, что каждая конечная группа изоморфна группе перестановочных автоморфизмов некоторого совершенного кода к сожалению не позволяет прояснить строение полной группы автоморфизмов произвольного совершенного кода длины $n = 2^k - 1$, $k > 3$ и оценить ее порядок, поскольку полная группа автоморфизмов содержит группу симметрий только в качестве подгруппы. Систематическое исследование групп автоморфизмов совершенных кодов было начато в работах [57, 30], до этого изучались только группы симметрий кодов, что оправдано лишь для линейных двоичных кодов. Автором диссертации (совместно с С. В. Августиновичем), см. [57], было доказано (конструктивно) существование класса совершенных двоичных кодов с тривиальной группой автоморфизмов для любого $n = 2^k - 1$, $n > 127$. Эти коды оказались *несистематическими*. С. А. Малюгин [30] доказал существование класса *систематических* кодов с тривиальной группой автоморфизмов для любого $n = 2^k - 1, n \geq 31$. Для кодов длины 15 вопрос существования таких кодов пока остается открытым.

Хорошо известно, что группы симметрий кода Хэмминга H длины n и расширенного кода Хэмминга длины $n + 1$ (с одной проверочной координатой) изоморфны полной линейной $GL(\log(n+1), 2)$ и полной аффинной $GA(\log(n + 1))$ группам соответственно. Для кода Хэмминга H длины n справедливо

$$|Aut(H)| = |GL(\log(n + 1), 2) \times Ker(H)| =$$

$$2^{n-\log(n+1)} n(n - 1)(n - 3)(n - 7) \dots (n - (n - 1)/2).$$

Порядок группы автоморфизмов совершенного кода оказался тесно связанным с порядком группы автоморфизмов его системы троек Штейнера. В 2000 г., в работах [67, 68, 44], автором диссертации совместно с С. Т. Топаловой было доказано, что порядок группы автоморфизмов произвольного нелинейного совершенного двоичного кода с расстоянием 3 не превосходит порядка группы автоморфизмов кода Хэмминга той же длины. Для получения этого результата потребовалось развить комбинаторную технику для получения аналогичного результата для порядков групп автоморфизмов систем троек Штейнера. Там же была получена верх-

няя оценка порядка группы автоморфизмов произвольной системы Штейнера $S(t, t+1, n)$.

Развивая далее этот подход, была доказана в параграфе 5.2 следующая теорема

Теорема 23. Если порядок группы автоморфизмов произвольной системы троек Штейнера порядка n равен порядку полной линейной группы $GL(\log(n+1), 2)$, то эта система хэммингова и с точностью до изоморфизма единственна.

Используя группы автоморфизмов систем троек Штейнера, окружающих каждое кодовое слово кода, учитывая связность характеристического графа совершенного кода и то, что код "склеен" из своих систем троек Штейнера, с использованием метода локального анализа была доказана

Теорема 24. Порядок группы автоморфизмов произвольного совершенного двоичного кода длины n меньше порядка группы автоморфизмов кода Хэмминга той же длины.

Аналогичная теорема верна для групп автоморфизмов расширенных совершенных кодов.

Результаты опубликованы в [67, 44, 45] и получены совместно с С. Т. Топаловой.

Аналогичный результат был независимо получен С. А. Малюгиным в работе [14].

Исследования групп автоморфизмов были продолжены в работе [3].

В шестой главе исследуются разбиения пространства E^n на совершенные коды, а также матрицы пересечений, отвечающие разбиениям совершенных расширенных двоичных кодов. Проблема перечисления разбиений n-куба на совершенные коды непосредственно связана с проблемой перечисления всех совершенных кодов, поскольку количество различных таких разбиений тесно связано с числом различных совершенных кодов: двойные логарифмы этих чисел асимптотически равны. В [39] автором диссертации были предложены два метода построения нетривиальных разбиений E^n на совершенные коды, один из которых каскадный, другой – свитчинговый (с использованием конструкции Ю. Л. Васильева).

В этой главе приводится нижняя оценка, см. [77, 48] (лучшая на сегодняшний день) числа различных разбиений пространства E^n на совершенные коды, полученная свитчинговым методом:

Теорема 25. Для любого допустимого $n \geq 31$ число различных разбиений $\mathbf{P}_n$ пространства E^n на совершенные коды длины n удовлетворяет неравенству

$$\mathbf{P}_n \geq 2^{2^{(n-1)/2}}.$$

Рассмотрим два произвольных разбиения n-куба E^n на совершенные расширенные двоичные коды и их матрицу пересечений. Она дает мощности попарных пересечений кодов из этих разбиений. В этой главе производится подсчет снизу и сверху количества различных матриц пересечений, полученных из произвольных двух разбиений n-куба E^n на совершенные расширенные двоичные коды.

Для получения оценок числа различных и неэквивалентных матриц пересечений, полученных из произвольных двух разбиений n-куба E^n на совершенные расширенные двоичные коды рассматриваются сначала различные разбиения E^n, которые используются для построения двух разбиений E^{2n} (здесь $n = 2^k$). При этом используется и развивается далее с использованием свитчингов латинских квадратов каскадный способ построения совершенных расширенных кодов и разбиений из [39].

Для получения нижней оценки числа различных матриц пересечений двух разбиений E^n на совершенные расширенные двоичные коды потребовалось оценить число различных матриц пересечений латинских квадратов. Для этой цели посредством свитчингов (локальных перестроек) подматриц порядка 2×2 внутри пары латинских квадратов специального вида (т. е. снова используя метод локального анализа) было сконструировано мощное множество различных матриц пересечения двух латинских квадратов. В параграфе 6.4 были доказаны следующие теоремы

Теорема 29. Для любого $n = 2^k > 8$, число различных матриц пересечения двух латинских квадратов порядка n не меньше чем 2^{n^4}.

Теорема 30. Для $n = 2^k, k > 2$, число различных матриц пересечений разбиений E^n на совершенные расширенные двоичные коды не меньше 2^{cn^2}, где c – положительная константа.

Теорема 31. Для $n = 2^k, k > 3$, число неэквивалентных матриц пересечений разбиений E^n на совершенные расширенные двоичные коды не меньше $2^{c'n^2}$, где c' – положительная константа.

В параграфе 6.5 доказано, что число неэквивалентных матриц пересечений разбиений E^n на совершенные расширенные двоичные коды не больше $2^{c''n^3}$, где n достаточно велико и c'' – положительная константа.

Проблема построения разбиений E^n рассматривалась также в ряде других работ, например, Т. Етционом и А. Варди в работе [25], а также в работах Ж. Рифы, К. Боргеса, М. Виллануевой, К. Фернандес.

Результаты по исследованию матриц пересечений разбиений пространства на совершенные расширенные двоичные коды были получены совместно с С. В. Августиновичем и А. Лобстейном [70, 72].

Автор считает своим приятным долгом выразить искреннюю и глубокую признательность всем своим соавторам и коллегам за плодотворное и увлекательное сотрудничество, а также А. В. Кельманову за ряд ценных замечаний, позволивших улучшить текст настоящего автореферата.

Список литературы

[1] *Августинович С. В.* Комбинаторные и метрические свойства совершенных кодов и раскрасок, Канд. дисс., Новосибирск, 2000. 33 с.

[2] *Августинович С. В., Соловьева Ф. И., Хеден У.* О проблеме рангов и ядер совершенных кодов // Пробл. передачи информ. 2003. Т. 39. N. 4. С. 341–345.

[3] *Августинович С. В., Соловьева Ф. И., Хеден У.* О структуре группы симметрий кодов Васильева // Пробл. передачи информ. 2005. Т. 41. N. 2. С. 105–112.

[4] *Августинович С. В., Соловьева Ф. И., Хеден У.* О разбиениях n-куба на неэквивалентные совершенные коды // Пробл. передачи информ. 2007. Т. 43. N. 4. С. 45–50.

[5] *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М: Наука, 1962. Вып. 8. С. 337–339.

[6] *Васильев Ю. Л., Соловьева Ф. И.* Кодообразующие факторизации n-мерного единичного куба и совершенных двоичных кодов // Пробл. передачи информ. 1997. Т. 33. Вып. 1. С. 64–74.

[7] *Зиновьев В. А., Леонтьев В. К.* О совершенных кодах, (Препринт/ ИППИ АН СССР). 1972. Вып. 1. С. 26–35.

[8] *Зиновьев В. А., Леонтьев В. К.* Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Вып. 2. С. 123–132.

[9] *Зиновьев В. А., Зиновьев Д. В.* Двоичные расширенные совершенные коды длины 16 ранга 14 // Пробл. передачи информ. 2006. Т. 42. N. 2. С. 63–80.

[10] *Кабатянский Г. А., Левенштейн В. И.* О границах для упаковок на сфере и в пространстве // Пробл. передачи информ. 1978. Т. 14. N. 1. С. 1–17.

[11] *Кротов Д. С.* Конструкции плотно упакованных кодов и нижние оценки их числа, Канд. дисс., Новосибирск, 2000. 64 с.

[12] *Лось А. В.* Построение совершенных q-ичных кодов свитчингами простых компонент // Пробл. передачи информ. 2006. Т. 42. N. 1. С. 34–42.

[13] *Малюгин С. А.* О нижней оценке числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6. N. 1. С. 44–48.

[14] *Малюгин С. А.* О порядке группы автоморфизмов совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7. N. 4. С. 91–100.

[15] *Малюгин С. А.* Несистематические совершенные двоичные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2001. Т. 8. N. 1. С. 55–76.

[16] *Малюгин С. А.* О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискрет. анализ и исслед. операций. Сер. 1. 2006. Т. 13. N. 1. С. 77–98.

[17] *Нечаев А. А.* Коды Кердока в циклической форме // Дискретн. Матем. 1989. V. 1. № 4. P. 123–139.

[18] *Потапов В. Н.* О нижней оценке числа транзитивных совершенных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2006. Т. 13. N. 4. С. 49–59.

[19] *Соловъева Ф. И.* О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных систем. Новосибирск: Ин-т математики СО АН СССР. 1988. Вып. 47. С. 66–88.

[20] *Соловъева Ф. И.* Точные границы связности кодообразующих д.н.ф., Препринт N 10. Новосибирск: Институт математики СО РАН, 1990. С. 15.

[21] *Bonnigton C. P., Grannell M. J., Griggs T. S., Širáň J.* Exponential Families of Non-Isomorphic Triangulations of Complete Graphs // J. Combin. Theory. Ser. B. 2000. V. 78. № 2. P. 169–184.

[22] *Borges J., Rifa J.* A characterization of 1-perfect additive codes // IEEE Trans. Inform. Theory. 1999. V. 45. № 5. P. 1688–1697.

[23] *Cohen G., Honkala I., Lobstein A., Litsyn S.* Covering codes, Elsevier, 1998.

[24] *Etzion T., Vardy A.* Perfect binary codes: constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40. N. 3. P. 754–763.

[25] *Etzion T., Vardy A.* On perfect codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11. N. 2. P. 205–223.

[26] Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A. and Solé P., "The Z_4-linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, V. 40. P. 301–319, 1994.

[27] *Herburt I., Ungar S.* Rigid sets of dimension $n-1$ in R^n // Geom. Dedicata. 1999. V. 76. P. 331–339.

[28] *Hergert F.* Algebraische Methoden fur Nichtlineare Codes, Thesis Darmstadt. 1985.

[29] *Krotov D. S., Avgustinovich S. V.* On the number of 1-perfect binary codes: a lower bound // IEEE Trans. Inform. Theory, V. 54. N. 4. 2008. P. 1760–1765.

[30] *Malyugin S. A.* Perfect codes with trivial automorphism group, Proc. Second Int. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria. June. 1998. P. 163–167.

[31] *Mollard M.* A generalized parity function and its use in the construction of perfect codes // SIAM J. Alg. Disc. Meth. 1986. V. 7. N. 1. P. 113–115.

[32] *Phelps K. T.* Every finite group is the automorphism group of some perfect code // J. Combin. Theory, series A. 1986. V. 43 N. 1. P. 45–51.

[33] *Phelps K. T., LeVan M. J.* Kernels of nonlinear Hamming codes // Des., Codes and Cryptography. 1995. V. 6. P. 247–257.

[34] *Phelps K. T., LeVan M. J.* Non-systematic perfect codes // SIAM Journal of Discrete Mathematics. 1999. V. 12. N. 1. P. 27–34.

[35] *Phelps K. T., LeVan M. J.* Switching equivalence classes of perfect codes // Des., Codes and Cryptogr. 1999. V. 16. N. 2. P. 179–184.

[36] *Rifa J., Solov'eva F. I., Villanueva M.* On the intersection of additive perfect codes // IEEE Trans. Inform. Theory, V. 54. N. 3. 2008. P. 1346–1356.

[37] *Shapiro G. S., Slotnik D. L.* On the mathematical theory of error correcting codes // IBM J. Res. and Devel. 1959. V. 3. N. 1. P. 25–34. (Русский перевод:*Шапиро Г. С., Злотник Д. Л.* К математической теории кодов с исправлением ошибок // Кибернетический сб. М.: Изд-во иностр. лит., 1962. Вып. 5. С. 7–32.)

[38] *Tietäväinen A.* On the nonexistence of perfect codes over finite fields. // SIAM J. Appl. Math. 1973. V. 24. P. 88-96.

Публикации автора по теме диссертации

[39] *Соловьева Ф. И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Новосибирск: Ин-т математики СО АН СССР. 1981. Вып. 37. С. 65–76.

[40] *Августинович С. В., Соловьева Ф. И.* О несистематических совершенных двоичных кодах // Пробл. передачи информ. 1996. Т. 32. Вып. 3. С. 47–50.

[41] *Соловьева Ф. И.* Системы троек Штейнера и проблема нитей, Второй Сибирский конгресс по прикладной и индустриальной математике (ИНПРИМ–96). Новосибирск, 25–30 июня, 1996. С. 125–126.

[42] *Августинович С. В., Соловьева Ф. И.* Построение совершенных бинарных кодов последовательными сдвигами α-компонент // Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 15–21.

[43] *Августинович С. В., Соловьева Ф. И.* Новые конструкции и свойства совершенных кодов, Труды Междунар. конференции по дискретному анализу и исследованию операций, Новосибирск, Россия, Июнь. 2000. С. 5–10.

[44] *Соловьева Ф. И., Топалова С. Т.* О группах автоморфизмов совершенных двоичных кодов и систем троек Штейнера // Пробл. передачи информ. 2000. Т. 36. Вып. 4. С. 53–58.

[45] *Соловьева Ф. И., Топалова С. Т.* Совершенные двоичные коды и системы троек Штейнера с максимальными порядками групп автоморфизмов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7. N. 4. С. 101–110.

[46] *Августинович С. В., Соловьева Ф. И.* О метрической жесткости двоичных кодов // Пробл. передачи информ. 2003. Т. 39. Вып. 2. С. 63–68.

[47] *Соловьева Ф. И.* О построении транзитивных кодов // Пробл. передачи информ. 2005. Т. 41. Вып. 3. С. 23–31.

[48] *Соловьева Ф. И.* Введение в теорию кодирования, учебное пособие, Изд. Новосибирского гос. университета, г. Новосибирск, 2006, 123 с.

[49] *Соловьева Ф. И.* О Z_4-линейных кодах с параметрами кодов Рида-Маллера // Пробл. передачи информ. 2007. Т. 43. Вып. 1. С. 41–47.

[50] *Соловьева Ф. И.* Замощения неориентируемых поверхностей системами троек Штейнера // Пробл. передачи информ. 2007. Т. 43. Вып. 3. С. 54–65.

[51] *Соловьева Ф. И.* Построение замощений неориентируемых поверхностей системами троек Штейнера, Труды конференции "Математика в современном мире", 17-23 сентября 2007. Новосибирск, С. 286–287.

[52] *Solov'eva F. I.* A combinatorial construction of perfect binary codes, Proc. of Fourth Int. Workshop on Algebraic and Comb. Coding Theory. Novgorod, Russia. September. 1994. P. 171–174.

[53] *Avgustinovich S. V., Solov'eva F. I.* On projections of perfect binary codes, Proc. Seventh Joint Swedish-Russian Workshop on Information Theory, St.-Petersburg, Russia. June. 1995. P. 25–26.

[54] *Avgustinovich S. V., Solov'eva F. I.* Construction of perfect binary codes by sequential translations of the i-components, Proc. of Fifth Int. Workshop on Algebraic and Comb. Coding Theory. Sozopol, Bulgaria. June. 1996. P. 9–14.

[55] *Avgustinovich S. V., Solov'eva F. I.* Existence of nonsystematic perfect binary codes, Proc. of Fifth Int. Workshop on Algebr. and Comb. Coding Theory, Sozopol, Bulgaria, June. 1996. P. 15–19.

[56] *Avgustinovich S. V., Solov'eva F. I.* Structural properties of perfect binary codes, Proc. of Int. Symp. on Inform. Theory, Ulm, Germany. 1997. P. 456.

[57] *Avgustinovich S. V., Solov'eva F. I.* Perfect binary codes with trivial automorphism group, Proc. of Int. Workshop on Information Theory, Killarney, Ireland. June. 1998. P. 114–115.

[58] *Solov'eva F. I., Avgustinovich S. V., Honold T., Heise W.* On the extendability of code isometries // J. of Geometry. 1998. V. 61. P. 3–16.

[59] *Solov'eva F. I.* On components of perfect binary codes, Preprint 98-041, Universität Bielefeld, Sonderforschungsbereich 343 Discrete Structuren in der Mathematik. 1998. 8 p.

[60] *Solov'eva F. I.* Constructions of perfect binary codes, Preprint 98-042, Universität Bielefeld, Sonderforschungsbereich 343 Discrete Structuren in der Mathematik. 1998. 12 p.

[61] *Solov'eva F. I.* Cardinality of i-components of perfect codes, Proc. of Siberian conference on Operation Research, Russia, Novosibirsk. 1998. P. 139.

[62] *Solov'eva F. I., Avgustinovich S. V., Honold T., Heise W.* Metrically rigid codes, Proc. Sixth Int. Workshop on Algebraic and Comb. Coding Theory. Pskov, Russia. September. 1998. P. 215–219.

[63] *Solov'eva F. I.* Components on perfect binary codes, Proc. of 1998 Optimal codes Workshop, Sozopol. Bulgaria. 1998. P. 188–192.

[64] *Solov'eva F. I.* Perfect binary codes components, Proc. of Workshop on Coding and Cryptography WCC'99. Paris, France. January. 1999. P. 29–32.

[65] *Solov'eva F. I.* Switchings and perfect codes, Numbers, Information and Complexity, Kluwer Academic Publisher. 2000. 311–314.

[66] *Solov'eva F. I.* Perfect binary codes: bounds and properties // Discrete Math. 2000. V. 213. P. 283–290.

[67] *Solov'eva F. I., Topalova S. T.* On the automorphism groups of perfect binary codes, Proc. Seventh Int. Workshop on Algebr. and Comb. Coding Theory. Bansko, Bulgaria. June. 2000. P. 283–287.

[68] *Solov'eva F. I., Topalova S. T.* On the automorphism groups of Steiner Systems, Proc. of Int. Workshop on Discrete Analiz and Operation Research, Novosibirsk, Russia. June. 2000. P. 90.

[69] *Avgustinovich S. V., Solov'eva F. I.* On the rigidity of binary codes, Proc. of Int. Conference "Geometry and applications", Novosibirsk, Russia. March. 2000. P. 16–17.

[70] *Avgustinovich S. V., Lobstein A., Solov'eva F. I.* Partitions by perfect binary codes, using concatenation and latin qsuares, Proc. Seventh Int. Workshop on Algebraic and Comb. Coding Theory. Bansko, Bulgaria. June. 2000. P. 45–50.

[71] *Solov'eva F. I.* Structure of i-components of perfect binary codes // Discrete Appl. Math. 2001. V. 111. N. 1-2. P. 189–197.

[72] *Avgustinovich S. V., Lobstein A., Solov'eva F. I.* Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory. 2001. V. 47. N. 4. P. 1621–1624.

[73] *Solov'eva F. I., Avgustinovich S. V.* On the metrical rigidity of binary codes, Proc. of Workshop on Coding and Cryptography WCC'2001, Paris, France. January. 2001. P. 35–42.

[74] *Solov'eva F. I.* Automorphism groups of perfect codes, Proc. of EWM Intern. Workshop on Groups and Graphs, Varna, Bulgaria. August. 2002. P. 95–100.

[75] *Solov'eva F. I.* Tilings of closed surfaces by Steiner triple systems, Proc. of Workshop on Coding and Cryptogr. WCC'2003, Versaille, France. March. 2003. P. 425–431.

[76] *Solov'eva F. I.* On transitive codes, Proc. of Int. Workshop on Discrete Analysis and Operation Research, Novosibirsk, Russia. June. 2004. P. 99.

[77] *Solov'eva F. I.* On perfect codes and related topics, Com^{2}Mac Lecture Note Series 13, Pohang 2004. 80 p.

[78] *Solov'eva F. I.* Some constructions of transitive codes, Proc. of Int. Workshop on Optimal codes and related topics. Pamporovo, Bulgaria. June. 2005. P. 254–260.

[79] *Solov'eva F. I.* Designs and perfect codes // Lecture Notes in Computer Science, V. 4123. November. 2006. P. 1104–1105.

[80] *Solov'eva F. I.* On perfect binary codes // Discrete Appl. Math., to appear.

Соловьева Фаина Ивановна

Комбинаторные методы построения и исследования кодов

Автореферат диссертации
на соискание ученой степени
доктора физико-математических наук

Подписано в печать 02.04.08. Формат 60x84 1/16.
Усл. печ. л. 2,44. Уч.-изд. л. 2,0. Тираж 120 экз. Заказ N 58.

Отпечатано в ООО "Омега Принт"
пр. Ак. Лаврентьева, 6, Новосибирск 630090