На правах рукописи

ГОРКУНОВ Евгений Владимирович

ГРУППЫ АВТОМОРФИЗМОВ КОДОВ ХЭММИНГА И ИХ КОМПОНЕНТ

01.01.09 — дискретная математика и
математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск — 2010

Работа выполнена в Новосибирском государственном университете

Научный руководитель:
доктор физико-математических наук, профессор
Соловьёва Фаина Ивановна

Официальные оппоненты:
доктор физико-математических наук, профессор
Дьячков Аркадий Георгиевич,
кандидат физико-математических наук
Пережогин Алексей Львович

Ведущая организация:
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Защита состоится 10 ноября 2010 г. в 15 часов 00 минут на заседании диссертационного совета Д 003.015.01 при Институте математики им. С. Л. Соболева СО РАН по адресу: пр. Академика Коптюга, 4, Новосибирск, 630090.

С диссертацией можно ознакомиться в библиотеке Института математики им. С. Л. Соболева СО РАН и в библиотеке Новосибирского государственного университета.

Автореферат разослан 8 октября 2010 г.

Учёный секретарь диссертационного совета
доктор физико-математических наук Ю. В. Шамардин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Объектом исследования настоящей диссертации являются вопросы алгебраической и комбинаторной теории кодирования, касающиеся групп автоморфизмов кодов. Предмет исследования настоящей работы составляют изометрии метрического пространства, изометрии между его подпространствами, отображения, сохраняющие те или иные инварианты кодов, а также группы автоморфизмов кодов, исправляющих ошибки.

Пусть $\mathbb{F}_q^n$ — векторное пространство размерности n над конечным полем $\mathbb{F}_q = GF(q)$, называемое также *q-ичным кубом*. Снабжённый некоторой метрикой, этот куб образует метрическое пространство. В настоящей работе рассматриваются только пространства Хэмминга. *Расстояние Хэмминга* между двумя векторами $x, y \in \mathbb{F}_q^n$ определяется как число позиций, в которых x и y различаются. Произвольное подмножество $C \subseteq \mathbb{F}_q^n$ называется q-ичным *кодом* длины n, а его элементы — *кодовыми словами*. *Изометрия* — это преобразование метрического пространства, сохраняющее расстояние между любыми двумя его элементами. *Автоморфизмом* кода $C \subseteq \mathbb{F}_q^n$ называется изометрия пространства $\mathbb{F}_q^n$, отображающая код C в себя. Два кода C_1 и C_2 *эквивалентны*, если существует изометрия $\mathbb{F}_q^n$, отображающая эти коды друг в друга.

Актуальность исследований блочных кодов диктуется их широким практическим применением для надёжной передачи информации, её эффективной обработки, для восстановления целостности данных, которая может быть утрачена при длительном хранении или в результате старения носителя. Кроме того, результаты теории кодирования используются для решения задач в смежных областях дискретной математики, например, в криптографии, сжатии данных, обработке изображений, биоинформатике и др.

Группа автоморфизмов кода помогает детально прояснить внутреннюю структуру кода. Действуя на множестве кодовых слов, группа автоморфизмов кода позволяет понять, какие его части имеют одинаковое строение, а какие существенно различ-

ны. Обнаруженные структурные особенности имеют практическое применение в построении кодов с более лучшими структурными свойствами, в разработке более эффективных алгоритмов кодирования и декодирования. Помимо этого, знание группы автоморфизмов кода позволяет найти число кодов, ему эквивалентных. Код, обладающий большим количеством эквивалентных кодов, может быть использован в криптографических системах как секретный ключ. На основе знаний о группах автоморфизмов выполняется также классификация и систематизация кодов.

Таким образом, группы автоморфизмов кодов имеют актуальные приложения. Вместе с тем их исследование — нетривиальная, а подчас и трудная задача. В двоичном кубе $\mathbb{F}_2^n$, называемом также булевым, изометрии исчерпываются перестановками позиций координат и сдвигами пространства на вектор. В общем случае это не так. Если $q \geqslant 5$, то не все изометрии пространства $\mathbb{F}_q^n$ могут быть выражены в терминах операций поля.

Некоторую аналогию с двоичным случаем имеют линейные коды в $\mathbb{F}_q^n$. В группе автоморфизмов линейного кода имеются полулинейные симметрии пространства $\mathbb{F}_q^n$ и сдвиги на векторы. Полулинейные симметрии описываются при помощи операций поля $\mathbb{F}_q$ и его автоморфизмов из группы Галуа $\mathrm{Gal}(\mathbb{F}_q)$. Поскольку именно линейные или эквивалентные им коды используются на практике, то при рассмотрении автоморфизмов кодов часто имеет смысл ограничиться указанными видами преобразований. Однако при $q \geqslant 4$ все возможные композиции полулинейных симметрий и сдвигов на векторы порождают собственную подгруппу группы автоморфизмов пространства $\mathbb{F}_q^n$.

Существуют многочисленные примеры нетривиальных линейных кодов, которые имеют автоморфизмы, не являющиеся ни линейными, ни даже полулинейными. Кроме того, к настоящему времени построены классы нелинейных кодов, которые представляют интерес для практики. Среди этих кодов можно выделить, например, Z_2Z_4-линейные, Z_4-линейные, ДНК-коды и другие. Исследование групп автоморфизмов подобных кодов требует разработки новых методов.

В диссертации исследуются группы автоморфизмов кода Хэмминга над произвольным конечным полем, группы мономиальных автоморфизмов различных компонент кода Хэмминга, активно используемых при построении и изучении кодов. Строение этих компонент, как и всего кода Хэмминга, тесно связано с проективными геометриями над полями Галуа.

В некотором смысле, изометричные пространства, равно как и эквивалентные коды, устроены одинаково. Дело обстоит иначе, если рассматриваемый вопрос касается специфики того, как код вложен в объемлющее пространство. Например, среди кодов Адамара, которые изометричны друг другу по определению, имеется множество попарно неэквивалентных. Если любая изометрия, определённая в коде, продолжается до изометрии всего пространства, то код называется метрически жёстким. Вопросы, связанные с метрической жёсткостью кодов, являются частным случаем более общей проблемы восстановимости объекта по некоторой информации о нём. Иначе говоря, при рассмотрении объекта актуальным представляется поиск его инвариантов, которые бы определяли этот объект однозначно (с точностью до эквивалентности, изоморфизма и т. п.).

Цель настоящей работы состоит в исследовании и полном описании группы автоморфизмов q-ичного кода Хэмминга, а также его подкодов, называемых компонентами, которые играют существенную роль как в изучении свойств совершенных кодов над конечными полями, так и в построении таких кодов.

Методика исследований. В диссертации используются методы алгебраической теории кодирования и комбинаторного анализа. Для исследования строения групп автоморфизмов кода Хэмминга и его подкодов применён метод локального анализа, восходящий к работам Ф. И. Соловьёвой [14], а также аппарат конечных проективных геометрий.

Научная новизна. Все результаты, представленные в диссертации, являются новыми. Некоторые из кодов рассмотрены впервые. Разработана оригинальная техника исследования автоморфизмов линейного кода посредством анализа их действия на кодовые слова минимального веса. В частности, впервые

замечено, что кодовые слова линейного кода, имеющие минимальный вес и равные носители, должны быть коллинеарными. При исследовании автоморфизмов линейных кодов это положение имеет решающее значение наряду со строением всего множества кодовых слов минимального веса.

Кодовые слова веса 3 в коде Хэмминга образуют так называемую обобщённую систему троек Штейнера. Это означает, что для любой пары координат найдётся единственная тройка, содержащая эту пару. Зафиксировав, например, 1 в первой координате троек, можно проследить за действием произвольной изометрии на любое значение всякой другой координаты. Такая техника позволила исследовать симметрии кода Хэмминга и мономиальные автоморфизмы его компонент. В числе прочих рассмотрены p^s-компоненты, которые предложены как обобщение линейной и простой компонент кода Хэмминга.

Впервые исследована группа перестановочных автоморфизмов $\mathrm{PAut}(\mathcal{H})$ кода Хэмминга $\mathcal{H}$ при $q > 2$. Из ранее известных фактов (см. [18, теорема 7.1]) следует, что эта группа изоморфна стабилизатору множества столбцов проверочной матрицы кода $\mathcal{H}$ по действию группы $GL_m(q)$ умножением на эти столбцы. Прямой проверкой для кода Хэмминга с проверочной матрицей в канонической форме удалось показать, что этот стабилизатор равен унитреугольной группе $UT_m(q)$. Вместе с тем выяснилось, что если $\mathcal{H}_c$ — циклический код Хэмминга, то $\mathrm{PAut}(\mathcal{H}_c) \ncong UT_m(q)$, поскольку порядок циклической подгруппы $\mathrm{PAut}(\mathcal{H}_c)$, равный длине кода n, не делит $|UT_m(q)|$. Тем самым установлено, что разные коды Хэмминга неожиданно могут иметь неизоморфные группы перестановочных автоморфизмов несмотря на то, что все эти коды эквивалентны.

В настоящей работе продолжено исследование инвариантов двоичных кодов, которое ранее проводилось рядом авторов. Одним из наиболее сильных оказался набор размерностей подкодов, см. [1, 4]. Здесь под размерностью кода понимается размерность минимальной грани булева куба, содержащей этот код. Оказалось, что этот инвариант избыточен для эквивалентности кодов и его можно ослабить, оставив лишь размерности подкодов чётной мощности. В итоге получены новые неулучшаемые достаточные условия эквивалентности двоичных кодов.

Практическая и теоретическая ценность. Работа носит теоретический характер. Полученные в ней утверждения и теоремы могут быть применены в теории кодов, исправляющих ошибки, а также в криптографии и комбинаторике. Изложенные в диссертации результаты могут оказаться полезными для классификации q-ичных совершенных кодов, для построения и исследования свойств q-ичных кодов с большими кодовыми расстояниями.

Апробация работы. Все результаты диссертации были доложены на следующих международных конференциях: 11-я и 12-я Международные конференции по алгебраической и комбинаторной теории кодирования (ACCT'2008, Пампорово, Болгария, 2008 г.; ACCT'2010, Новосибирск, 2010 г.); XVII Международная школа-семинар „Синтез и сложность управляющих систем“ им. ак. О. Б. Лупанова (Новосибирск, 2008 г.); XII Международный симпозиум по проблемам избыточности в информационных и управляющих системах (Redundancy 2009, Санкт-Петербург, 2009 г.); Мальцевские чтения 2009 и 2010 (Новосибирск, 2009, 2010 гг.); 32-я Конференция молодых учёных и специалистов „Информационные технологии и системы“ (ИТиС'09, Бекасово, Россия, 2009 г.); Международная конференция по вычислительным технологиям в разработке электротехники и электроники (SIBIRCON 2010, Иркутск, 2010 г.). Результаты, изложенные в диссертации, были представлены на семинарах Института математики им. С. Л. Соболева и НГУ „Теория кодирования“ и „Дискретный анализ“.

Публикации. Содержание диссертации отражено в 9 публикациях, в числе которых имеются 3 статьи в журналах, рекомендованных ВАК, и 5 работ в рецензируемых трудах международных и российских конференций.

Основные результаты диссертации.

1. Доказано, что все симметрии q-ичных кодов Хэмминга являются полулинейными. Получено описание группы автоморфизмов этих кодов.

2. Для q-ичного кода Хэмминга с проверочной матрицей в канонической форме показано, что его группа перестановоч-

ных автоморфизмов изоморфна унитреугольной группе. Обнаружены коды Хэмминга с неизоморфными группами перестановочных автоморфизмов.

3. Описана структура групп мономиальных автоморфизмов различных компонент q-ичного кода Хэмминга: простой, линейной и p^s-компоненты.

4. Доказано, что любая полусильная изометрия между произвольными двоичными кодами однозначно продолжается до изометрии булева куба. Показано, что этот результат имеет неулучшаемый характер.

Объём и структура диссертации. Диссертация состоит из введения, 3 глав и списка литературы (65 наименований), в конце приведён список публикаций автора по теме диссертации. Объём диссертации — 78 страниц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, приводятся основные определения, даётся краткий обзор ранее полученных результатов, связанных с группами автоморфизмов кодов.

Код, образующий подпространство размерности k в пространстве $\mathbb{F}_q^n$, называется *линейным* или $[n, k]$-кодом. Наименьшее ненулевое расстояние между кодовыми словами из C обозначается $d = d(C)$ и называется *кодовым расстоянием*.

Если шары фиксированного радиуса $t \geqslant 0$ с центрами в кодовых словах из C образуют разбиение пространства $\mathbb{F}_q^n$, то код называется *совершенным*. В. А. Зиновьев и В. К. Леонтьев [9], а также независимо А. Титвайнен [24] в точности указали набор параметров, которые может иметь нетривиальный совершенный код над $\mathbb{F}_q$: такой код либо исправляет одну ошибку, либо эквивалентен двоичному или троичному кодам Голея, исправляющим 3 или 2 ошибки соответственно.

Далее термин *совершенный* означает код с кодовым расстоянием 3, то есть исправляющий одну ошибку. Из условия

плотной упаковки (разбиения пространства $\mathbb{F}_q^n$ шарами радиуса 1), такой код имеет длину $n = \frac{q^m-1}{q-1}$. Единственным линейным совершенным кодом является код Хэмминга. Тем не менее, существует множество нелинейных совершенных q-ичных кодов, впервые построенных Ю. Л. Васильевым [8] для $q = 2$, а позднее — многими другими авторами для $q = p^r \geqslant 2$ (см., например, лекции Ф. И. Соловьёвой [22]).

А. А. Марков в 1956 г. показал [12], что группа изометрий пространства $\mathbb{F}_q^n$ представляет собой полупрямое произведение

$$\mathrm{Aut}(\mathbb{F}_q^n) = S_n \leftthreetimes S_q^n = \left\{(\pi;\sigma) \mid \pi \in S_n,\, \sigma \in S_q^n\right\}.$$

Иначе говоря, каждая изометрия $\mathbb{F}_q^n$ представляется в виде пары $(\pi;\sigma)$, где подстановка $\pi \in S_n$ переставляет координаты вектора $x \in \mathbb{F}_q^n$, в то время как $\sigma = (\sigma_1, \ldots, \sigma_n)$ есть набор, в котором каждая подстановка $\sigma_i \in S_q$ действует на элементах поля $\mathbb{F}_q$ и в соответствии с этим изменяет значение координаты x_i. Набор σ называется *конфигурацией*.

В этих терминах *группой автоморфизмов* кода C называется группа $\mathrm{Aut}(C)$ изометрий пространства $\mathbb{F}_q^n$, отображающих код C в себя. Автоморфизмы вида (π, ε), где ε — тождественная конфигурация, образуют подгруппу $\mathrm{PAut}(C) \leqslant \mathrm{Aut}(C)$, называемую *группой перестановочных* автоморфизмов кода C.

Автоморфизм $\mathbb{F}_q^n$, заданный умножением векторов на мономиальную матрицу, называется *мономиальным*. Группа мономиальных автоморфизмов кода C обозначается $\mathrm{MAut}(C)$.

Стабилизатор нулевого вектора в группе $\mathrm{Aut}(C)$ назовём *группой симметрий* кода C и обозначим через $\mathrm{Sym}(C)$. Отметим, что для двоичных кодов $\mathrm{Sym}(C) = \mathrm{MAut}(C) = \mathrm{PAut}(C)$. Кроме того, изометрия $\mathbb{F}_q^n$ является симметрией тогда и только тогда, когда она сохраняет вес произвольного вектора.

Поскольку сдвиг линейного кода $C \subseteq \mathbb{F}_q^n$ на принадлежащий ему вектор даёт в результате тот же самый код, то легко доказать известное соотношение $\mathrm{Aut}(C) \cong \mathrm{Sym}(C) \leftthreetimes C$. Таким образом, в группе автоморфизмов линейного кода существенную часть представляют его симметрии.

Напомним, что функция $f\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ называется *полулинейной* с сопутствующим автоморфизмом $\gamma \in \mathrm{Gal}(\mathbb{F}_q)$, если

для любых $\alpha, \beta \in \mathbb{F}_q$ и $x, y \in \mathbb{F}_q^n$ выполняется

$$f(\alpha x + \beta y) = \gamma(\alpha) f(x) + \gamma(\beta) f(y).$$

Группа полулинейных симметрий $[n, n-m]$-кода с кодовым расстоянием $d \geqslant 3$ изоморфна некоторой подгруппе общей полулинейной группы $\Gamma L_m(q) = \mathrm{Gal}(\mathbb{F}_q) \leftthreetimes GL_m(q)$. В частности, хорошо известно, что группа полулинейных симметрий кода Хэмминга $\mathcal{H}$ длины $n = \frac{q^m-1}{q-1}$ изоморфна группе $\Gamma L_m(q)$, см. [18, теорема 7.2].

При $q \in \{2, 3\}$ имеем $\mathrm{Sym}(\mathbb{F}_q^n) = \mathrm{MAut}(\mathbb{F}_q^n)$, так что справедливы соотношения

$$\mathrm{Sym}(\mathcal{H}) \cong GL_m(q) \ \text{ и } \ \mathrm{Aut}(\mathcal{H}) \cong GL_m(q) \leftthreetimes \mathcal{H}.$$

При $q \geqslant 4$ полулинейные симметрии пространства $\mathbb{F}_q^n$ порождают собственную подгруппу группы $\mathrm{Sym}(\mathbb{F}_q^n)$. Возникает естественный вопрос, будет ли при любом $q \geqslant 4$ выполняться соотношение

$$\mathrm{Aut}(\mathcal{H}) \cong \Gamma L_m(q) \leftthreetimes \mathcal{H}.$$

В настоящей диссертации даётся положительный ответ на этот вопрос.

В **первой главе** представлены результаты исследования автоморфизмов q-ичного кода Хэмминга.

В параграфе 1.1 приводятся определения группы автоморфизмов кода, а также некоторых её подгрупп. Указываются связи между автоморфизмами кодов, подстановками симметрической группы и матрицами над конечными полями. Необходимо отметить, что используемое в настоящей работе определение группы автоморфизмов кода согласуется с определением И. Константинеску и В. Хайзе [17] и отличается от традиционного, включая в рассмотрение все изометрии пространства $\mathbb{F}_q^n$. Такой подход представляется целесообразным, в особенности для изучения автоморфизмов нелинейных кодов, практическое применение которых становится всё более актуальным.

В параграфе 1.2 излагаются известные факты о строении групп автоморфизмов линейных кодов. Также здесь содержатся замечания, раскрывающие характер действия полулинейных симметрий на векторы пространства $\mathbb{F}_q^n$.

В параграфе 1.3 исследуется группа перестановочных автоморфизмов q-ичных кодов Хэмминга, где $q > 2$. В отличие от случая двоичных кодов перестановочные автоморфизмы пространства $\mathbb{F}_q^n$ при $q \geqslant 3$ образуют собственную подгруппу его группы симметрий. Поэтому группа перестановочных автоморфизмов q-ичного кода представляет самостоятельный интерес.

Рассматривается код Хэмминга длины $n = \frac{q^m-1}{q-1}$ с проверочной матрицей в каноническом виде, то есть столбцы которой имеют 1 в качестве первого ненулевого элемента и которую можно построить для любого целого $m \geqslant 2$. Доказано, что группа перестановочных автоморфизмов такого кода изоморфна унитреугольной группе матриц $UT_m(q)$ (теорема 5). Показано, что группа перестановочных автоморфизмов циклического кода Хэмминга не может быть изоморфна $UT_m(q)$ (утверждение 1). Как следствие, получено, что при $q > 2$ группы перестановочных автоморфизмов различных кодов Хэмминга могут быть неизоморфны друг другу (следствие 1).

Говоря неформально, перестановочные автоморфизмы вращают пространство $\mathbb{F}_q^n$ вокруг прямой $x_1 = \ldots = x_n$. Результаты параграфа 1.3 показывают, что при $q > 2$ коды Хэмминга имеют различную симметрию относительно этой прямой.

В параграфе 1.4 доказано, что любая симметрия кода Хэмминга над полем $\mathbb{F}_q$ является полулинейной. Это доказательство проводится методом локального анализа, систематически разработанным Ф. И. Соловьёвой [14]. Он состоит в том, что сначала исследование рассматриваемого вопроса проводится на локальном фрагменте кода, например, на множестве кодовых слов веса 3. Затем проверка выполнимости обнаруженных свойств тем или иным образом распространяется на весь код.

В силу того, что симметрии пространства $\mathbb{F}_q^n$ сохраняют вес любого вектора, справедливо соотношение $\mathrm{Sym}(\mathcal{H}) \leqslant \mathrm{Sym}(T)$, где $T \subset \mathcal{H}$ — подкод, образованный тройками кода Хэмминга. Доказано, что все симметрии множества троек T полулинейны (леммы 5–7). Отсюда следует полулинейность симметрий кода Хэмминга. Таким образом получено описание группы автоморфизмов q-ичных кодов Хэмминга (теорема 6).

Результаты первой главы опубликованы в [25,27,31,33].

Во **второй главе** исследуются группы мономиальных автоморфизмов различных компонент q-ичного кода Хэмминга. Компоненты кода Хэмминга — это специальные его подкоды, которые могут быть сдвинуты по некоторой фиксированной координате i, в результате чего из кода Хэмминга получается другой совершенный код с теми же параметрами. Конструирование совершенных кодов сдвигами линейных компонент получило название метода i-компонент и восходит к работам Ю. Л. Васильева, который первым обнаружил нелинейные совершенные двоичные коды [8].

В настоящей диссертации рассматриваются компоненты кода Хэмминга, образованные линейной оболочкой множества его кодовых слов веса три с 1 в фиксированной i-й координате, которая (оболочка) взята над полем $\mathbb{F}_q$, его простым подполем $\mathbb{F}_p$ или, более общо, над произвольным подполем $\mathbb{F}_{p^s} \leqslant \mathbb{F}_q$. Такие компоненты называются соответственно линейными, простыми или p^s-компонентами.

На основе сдвигов линейных компонент С. В. Августинович и Ф. И. Соловьёва [6] разработали новый метод построения совершенных кодов, названный методом $\tilde{\alpha}$-компонент. Развитием указанных подходов для случая q-ичных кодов ($q > 2$) стал метод простых компонент, используя который, А. В. Лось [11] построил богатое семейство совершенных кодов. Перечисленные методы оказались также весьма плодотворными для изучения структурных свойств совершенных кодов, см., например, работы К. Т. Фелпса и др. [20, 21], Ф. И. Соловьёвой и А. В. Лося [15, 16] и других авторов.

Таким образом, компоненты кода Хэмминга активно применяются при решении важной задачи теории кодирования — при построении кодов с предписанными свойствами, например, совершенных кодов с тривиальными группами автоморфизмов.

В работе [7] доказано, что группа перестановочных автоморфизмов линейной компоненты двоичного кода Хэмминга длины $N = 2^m - 1$ изоморфна полупрямому произведению $S_n \leftthreetimes S_2^n$, где $n = 2^{m-1} - 1$.

В параграфе 2.1 приведены известные связи между кодом Хэмминга и конечными проективными геометриями. Эти связи позволяют использовать язык проективных геометрий для

изложения результатов, а также иллюстрируют строение рассматриваемых компонент. Доказано, что линейная компонента кода Хэмминга представляется в виде прямой суммы подкодов Хэмминга размерности $q-1$ (лемма 8). Каждому из этих подкодов в проективной геометрии соответствует одна из прямых, проходящих через фиксированную точку.

Параграф 2.2 содержит описание группы мономиальных автоморфизмов линейной компоненты q-ичного кода Хэмминга (теорема 7). Линейная компонента допускает перестановки своих подкодов Хэмминга, а также независимые друг от друга мономиальные автоморфизмы, действующие на эти подкоды и оставляющие на месте i-ю координату кодовых слов.

В параграфе 2.3, наряду с простыми компонентами кода Хэмминга, рассматриваются p^s-компоненты этого кода. Обобщение идей предыдущего параграфа позволило раскрыть структуру группы мономиальных автоморфизмов p^s-компонент (теорема 8).

Результаты второй главы опубликованы в [26,30,32].

В **третьей главе** рассматриваются вопросы, связанные с восстановлением двоичных кодов. Возможности восстановления объекта по некоторой его части или по некоторой информации о нём представляют не только теоретический интерес, но также могут иметь ценность и с практической точки зрения. Какие параметры математического объекта, какие его инварианты определяют этот объект однозначно (возможно, с точностью до эквивалентности, изоморфизма и т. п.)? Трудно указать область математики, в которой бы изучение подобных вопросов не являлось актуальным.

Естественный подход к восстановлению кодов состоит в использовании их метрических свойств. Однако, как уже было отмечено выше, наличие изометрии между кодами не гарантирует их однозначного задания, даже с точностью до эквивалентности. Напомним, что если любая изометрия, определённая в вершинах кода, продолжается до изометрии всего пространства, то код называется метрически жёстким. Для некоторых классов кодов проблема метрической жёсткости была изучена и разрешена рядом авторов, см., например, [3,5,23].

Помимо попарных расстояний между кодовыми словами, которые сохраняются при изометрии, в качестве инвариантов для восстановления двоичного кода рассматривались следующие: граф минимальных расстояний, например, в работах [2, 13,19]; множество вершин, находящихся на фиксированном расстоянии p друг от друга, как в работе [10]; попарные расстояния между тройками вершин, которые порождают соответствующие тройки натуральных чисел [1].

В параграфе 3.1 приводится краткий обзор результатов, касающихся восстановимости кодов, графов, булевых функций и т. п. Одним из наиболее сильных инвариантов двоичного кода оказался набор размерностей его подкодов. Здесь под размерностью кода понимается размерность минимальной грани булева куба, содержащей этот код. Отображение кода в $\mathbb{F}_2^n$, сохраняющее размерность любого его подкода, называется *сильной изометрией*. В работе [4] доказано, что любая сильная изометрия однозначно расширяется до изометрии всего булева куба.

В параграфе 3.2 показано, что набор размерностей подкодов, как инвариант, избыточен, а именно: для восстановления двоичного кода с точностью до эквивалентности достаточно знать размерности всех его подкодов чётной мощности (теорема 9). Глава завершается примерами, показывающими неулучшаемый характер изложенных достаточных условий эквивалентности двоичных кодов.

Результаты третьей главы получены совместно с С. В. Августиновичем и опубликованы в работах [28, 29].

Автор выражает искреннюю благодарность и всестороннюю признательность научному руководителю профессору Ф. И. Соловьёвой за постоянное внимание к работе, плодотворные дискуссии, ценные замечания, поддержку и вдохновение.

Список литературы

[1] *Абдурахманов Ж. К.* О геометрической структуре кодов, исправляющих ошибки: Дис. ... канд. физ.-мат. наук: 01.01.09. — Ташкент, 1991. — 66 с.

[2] *Августинович С. В.* К строению графов минимальных расстояний совершенных бинарных $(n, 3)$-кодов // Дискретн. анализ и исслед. операций. Сер. 1. — 1998. — Т. 3, № 5. — С. 3–5.

[3] *Августинович С. В.* Об изометричности плотно упакованных бинарных кодов // Тр. Ин-та математики / РАН. Сиб. отд-ние. — 1994. — Т. 27: Дискретный анализ. — С. 3–5.

[4] *Августинович С. В.* О сильной изометрии бинарных кодов // Дискретн. анализ и исслед. операций. Сер. 1. — 2000. — Т. 7, № 3. — С. 3–5.

[5] *Августинович С. В., Соловьёва Ф. И.* К метрической жесткости двоичных кодов // Пробл. передачи информ. — 2003. — Т. 39, вып. 2. — С. 23–28.

[6] *Августинович С. В., Соловьёва Ф. И.* Построение совершенных двоичных кодов последовательными сдвигами $\tilde{\alpha}$-компонент // Пробл. передачи информ. — 1997. — Т. 33, вып. 3. — С. 15–21.

[7] *Августинович С. В., Соловьёва Ф. И., Хеден У.* О структуре группы симметрий кодов Васильева // Пробл. передачи информ. — 2005. — Т. 41, вып. 2. — С. 42–49.

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

[9] *Зиновьев В. А., Леонтьев В. К.* Несуществование совершенных кодов над полями Галуа. — М., 1972. — 10 с. — (Препр. / АН СССР. Ин-т пробл. передачи информ.; № 1).

[10] *Красин В. Ю.* О слабых изометриях булева куба // Дискретн. анализ и исслед. операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 26–32.

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

[12] *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. — М.: МЦНМО, 2003. — С. 70–93.

[13] *Могильных И. Ю.* О слабых изометриях кодов Препараты // Пробл. передачи информ. — 2009. — Т. 45, вып. 2. — С. 78–83.

[14] *Соловьёва Ф. И.* Комбинаторные методы построения и исследования кодов: Дис. ... докт. физ.-мат. наук: 01.01.09. — Новосибирск, 2008. — 202 с.

[15] *Соловьёва Ф. И., Лось А. В.* О пересечениях q-значных совершенных кодов // Сиб. мат. журнал. — 2008. — Т. 49, вып. 2. — С. 464–474.

[16] *Соловьёва Ф. И., Лось А. В.* О построении разбиений $\mathbb{F}_q^N$ на совершенные q-значные коды // Дискретн. анализ и исслед. операций. — 2009. — Т. 16, № 3. — С. 63–73.

[17] *Constantinescu I., Heise W.* On the consept of code-isomorphy // J. Geom. — 1996. — V. 57. — P. 63–69.

[18] *Huffman W. C.* Codes and groups // Handbook of coding theory. — Amsterdam, New York: Elsevier Science, 1998. — P. 1345–1440.

[19] *Mogilnykh I. Yu., Östergård P. R. J., Pottonen O., Solov'eva F. I.* Reconstructing extended perfect binary one-error-correcting codes from their minimum distance

graphs // IEEE Trans. Inform. Theory — 2009. — V. 55. — P. 2622–2625.

[20] *Phelps K. T., Rifà J., Villanueva M.* Kernels and p-kernels of p^r-ary 1-perfect codes // Designs, Codes and Cryptography. — 2005. — V. 37, № 2. — P. 243–261.

[21] *Phelps K. T., Villanueva M.* Ranks of q-ary 1-perfect codes // Designs, Codes and Cryptography. — 2002. — V. 27, № 1–2. — P. 139–144.

[22] *Solov'eva F. I.* On perfect codes and related topics. — Pohang: Pohang University of Science and Technology, 2004. — 80 p. — (Com^{2}MaC Lecture Note Series; 13).

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

[24] *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

[25] *Горкунов Е. В.* Группа перестановочных автоморфизмов q-ичного кода Хэмминга // Пробл. передачи информ. — 2009. — Т. 45, вып. 4. — С. 18–25.

[26] *Горкунов Е. В.* Мономиальные автоморфизмы линейной и простой компонент кода Хэмминга // Дискретн. анализ и исслед. опер. — 2010. — Т. 17, № 1. — С. 11–33.

[27] *Горкунов Е. В.* Связь между перестановочными автоморфизмами кода Хэмминга и коллинеациями проективной геометрии // Материалы XVII Межд. школы-семинара „Синтез и сложность управляющих систем“

им. ак. О. Б. Лупанова (Новосибирск, Россия. 27 октября – 1 ноября, 2008). — Новосибирск: Изд-во Института математики, 2008. — С. 30–32.

[28] *Горкунов Е. В., Августинович С. В.* О восстановлении двоичных кодов по размерностям их подкодов // Дискретн. анализ и исслед. опер. — 2010. — Т. 17, № 5. — С. 15–21.

[29] *Avgustinovich S. V., Gorkunov E. V.* On redundancy of strong isometries of binary codes // Proc. IEEE Int. Conference on Computational Technologies in Electrical and Electronics Engineering (Irkutsk, Russia. July 11–15, 2010). — Piscataway: IEEE, 2010. — P. 50–51.

[30] *Gorkunov E. V.* Monomial automorphisms of linear components of the Hamming code // Proc. XII Int. Symposium on Probl. of Redundancy in Information and Control Systems (Saint-Petersburg, Russia. May 26–30, 2009). — Saint-Petersburg: Saint-Petersburg State University of Aerospace Instrumentation, 2009. — P. 76–80.

[31] *Gorkunov E. V.* On permutation automorphism groups of q-ary Hamming codes // Proc. 11th Int. Workshop on Algebraic and Combinatorial Coding Theory (Pamporovo, Bulgaria. June 16–22, 2008). — Sofia: Inst. of Math. and Informatics, 2008. — P. 119–124.

[32] *Gorkunov E. V.* On the monomial automorphism group of p^s-components in the q-ary Hamming code // Сб. трудов 32-й Конф. молодых учёных и специалистов „Информационные технологии и системы“ (Бекасово, Россия. 14–18 декабря 2009). — М.: Ин-т пробл. передачи информ., 2009. — С. 390–395.

[33] *Gorkunov E. V.* Symmetries of a q-ary Hamming code // Proc. 12th Int. Workshop on Algebraic and Combinatorial Coding Theory (Novosibirsk, Russia. Sept. 5–11, 2010). — Novosibirsk: Sobolev Inst. of Math., 2010. — P. 144–149.

Горкунов Евгений Владимирович

Группы автоморфизмов кодов Хэмминга и их компонент

Автореферат диссертации
на соискание учёной степени
кандидата физико-математических наук

Подписано в печать 30.09.2010	Формат 60 x 84 1/16
Печать офсетная	Усл. печ. л. 1.0
Заказ №	Тираж 100 экз.

Редакционно-издательский центр НГУ
ул. Пирогова, 2, Новосибирск, 630090