ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ НАУКИ ИНСТИТУТ МАТЕМАТИКИ
ИМ. С. Л. СОБОЛЕВА СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ
АКАДЕМИИ НАУК

На правах рукописи

ГУСЬКОВ Георгий Константинович

ТРАНЗИТИВНЫЕ СОВЕРШЕННЫЕ КОДЫ И РАЗБИЕНИЯ

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата физико-математических наук

Новосибирск - 2013

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук

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

Официальные оппоненты: Дьячков Аркадий Георгиевич, доктор физико-математических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Московский государственный университет имени М. В. Ломоносова;

Фионов Андрей Николаевич, доктор технических наук, профессор, Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования Сибирский государственный университет телекоммуникаций и информатики, проректор по научной работе

Ведущая организация: Федеральное государственное бюджетное учреждение науки Институт проблем передачи информации им. А. А. Харкевича Российской академии наук

Защита состоится 18 декабря 2013 г. в 16 час. 00 мин. на заседании диссертационного совета Д 003.015.01 при Федеральном государственном бюджетном учреждении науки Институте математики им. С. Л. Соболева Сибирского отделения Российской академии наук по адресу: 630090, г. Новосибирск, пр. Академика Коптюга, 4, конференц-зал.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Института математики им. С. Л. Соболева Сибирского отделения Российской академии наук.

Автореферат разослан "____" октября 2013 г.

Учёный секретарь
диссертационного совета Д 003.015.01,
д.ф.-м.н. Ю. В. Шамардин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящей диссертации исследуются проблемы существования и перечисления объектов, находящихся на стыке алгебраической комбинаторики и теории кодов, исправляющих ошибки в канале связи с шумами.

Объект исследования настоящей работы – транзитивные коды над двоичным алфавитом, исправляющие одиночные ошибки, а также разбиения пространства всех двоичных векторов на совершенные коды.

Двоичные коды являются одним из основных объектов исследования теории кодирования и служат базой для дальнейшего развития современных цифровых технологий. С 1949 года, с фундаментальных работ К. Шеннона по теории информации, началось бурное развитие теории кодирования как самостоятельной научной дисциплины, наряду с криптологией и сжатием информации, без которых был бы невозможен сегодняшний уровень развития коммуникационных технологий.

Совершенный код, исправляющий одиночные ошибки, задаёт разбиение всего пространства на совокупность шаров радиуса 1 с центрами в кодовых словах. Из данного факта следует важное свойство совершенных кодов – их оптимальность, то есть, при заданной длине кода и кодовом расстоянии мощность всякого совершенного кода максимальна. Раздел теории кодирования, посвящённый построению и исследованию свойств совершенных кодов настолько богат, что, помимо свойств самих кодов, интерес представляют также методы их исследования. Заметим, что задача упаковки пространства шарами фиксированного радиуса важна с точки зрения целого ряда других математических дисциплин: комбинаторного анализа, криптологии, теории групп, теории графов, топологии. Таким образом, результаты теории кодирования могут быть использованы для решения задач в смежных областях дискретной математики. Например, коды с богатыми группами автоморфизмов могут быть использованы в криптографии.

Проблема исследования разбиений пространства $\mathbb{F}^n$ (векторного пространства длины n над $\mathrm{GF}(2)$ по отношению к метрике Хэмминга) на совершенные коды тесно связана с проблемой построения таких кодов и изучения их свойств, поскольку асимптотики двойных логарифмов (если они существуют) числа различных совершенных кодов и числа различных разбиений на такие коды совпадают. Здесь и далее будем рассматривать только логарифмы по основанию 2. Также следует упомянуть о том, что некоторые разбиения пространства $\mathbb{F}^n$ индуцируют раскраски векторов $\mathbb{F}^n$ на коды, связанные с оптоволоконными сетями. Кроме того, совершенные коды являются частным случаем так называемых ре-

гулярных разбиений, в англоязычной литературе известных также как equitable partitions, а в отечественной литературе больше известных как совершенные раскраски. Наряду с дистанционно регулярными графами и схемами отношений, совершенные раскраски являются популярными объектами алгебраической комбинаторики. Различные методы построения разбиений могут быть использованы для исследования их нетривиальных свойств, а также для построения новых кодов, в частности, совершенных (такие методы, например, описаны в работе [7]). Важность поиска новых методов построения кодов, а также методов их задания, объясняется, в частности, тем, что на их основе можно разрабатывать новые, более эффективные, методы передачи информации, или криптографические системы-коды.

Несмотря на значительные усилия ряда исследователей, многие вопросы теории совершенных кодов всё ещё остаются нерешёнными. Так, по-прежнему не найдена классификация совершенных q-значных кодов для q – степеней простого, $q \geq 2$. Согласно теореме В. А. Зиновьева и В. К. Леонтьева (см. [3, 4]), независимо доказанной Э. Тиетвайненом, нетривиальные совершенные q-значные коды длины n, исправляющие ошибки, существуют только при $n = (q^k - 1)/(q - 1)$, $k \geq 2$, и имеют кодовое расстояние 3; при $n = 23$ – 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, в то время как существует дважды экспоненциальное число неэквивалентных совершенных кодов с кодовым расстоянием 3. Классификация расширенных совершенных двоичных кодов длины 16 и совершенных двоичных кодов длины 15, была получена П. Остергардом и О. Поттоненом в 2009 г. в работе [14].

Цель данной работы состоит в исследовании конструкций совершенных кодов и разбиений пространства $\mathbb{F}^n$ на совершенные коды, а также в применении этих конструкций для изучения свойств разбиений и кодов. В работе рассматриваются только двоичные коды и разбиения на такие коды.

Методика исследований. В диссертации используются традиционные методы и аппарат алгебраической и комбинаторной теории кодирования, комбинаторного анализа и теории t-схем. Для исследования предельно-транзитивных кодов использован метод локального анализа, восходящий к работам Ф. И. Соловьёвой [7].

Научная новизна. Все результаты, представленные в диссертации, являются новыми.

1. В диссертации продолжено развитие метода локального анализа из [7]. С его помощью установлено существование 5 бесконечных серий неэквивалентных предельно-транзитивных расширенных совершенных кодов. Для доказательства предельной транзитивности в работе предложено использовать свойства Паш-конфигураций систем троек Штейнера, соответствующих проверяемым совершенным кодам. Неэквивалентность кодов для каждой фиксированной длины была доказана с помощью сравнения значений их рангов и размерностей ядер. Впервые предельно-транзитивный код длины 16 был обнаружен С. А. Малюгиным[1] в 2004 г. С помощью системы компьютерной алгебры Magma[2] найдены все транзитивные расширенные совершенные коды длины 16, имеющие хотя бы одну нетранзитивную координату. Проверка кода на транзитивность заключалась в проверке на транзитивность соответствующей ему структуры инцидентности.

2. В диссертации впервые исследуется спектр рангов пропелинейных кодов. Для этого были использованы методы построения транзитивных кодов из [5], основанные на конструкциях Моллара и Васильева для совершенных кодов. Тот факт, что конструкция Моллара сохраняет пропелинейность исходных кодов, был доказан в [9]. Зависимость ранга результирующего кода от рангов исходных кодов для конструкции Моллара была доказана в [5]. С помощью системы компьютерной алгебры Magma впервые были обнаружены пропелинейные коды длин 15 и 31 полного ранга. В ходе компьютерных исследований рассматривались только нормализованные пропелинейные структуры, данное понятие было введено в [9].

3. Продолжено исследование транзитивных разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды, начатое в [6]. В данной диссертации впервые исследованы вершинно-транзитивные разбиения пространства $\mathbb{F}^n$. С помощью компьютерных исследований проверены транзитивность, 2-транзитивность и вершинная транзитивность 11 неэквивалентных разбиений длины 7, классифицированных К.Т. Фелпсом в [15]. Было показано, что конструкции транзитивных разбиений на двоичные коды, введённые в [6], могут применяться для построения 2-транзитивных и вершинно-транзитивных разбиений произвольной длины. Впервые получена нижняя оценка числа неэквивалентных разбиений для каждого из этих классов кодов. В качестве критерия неэквивалентности полученных разбиений использовались их матрицы пересечений, аналогичный метод

[1] *Малюгин С. А.* Частное сообщение — 2004.

[2] *Bosma W., Cannon J., Playoust C.* The Magma algebra system. I. The user language // J. Symbolic Comput. — 1997. — Vol. 24. — P. 235–265.

был применён в [8]. Была найдена зависимость матриц пересечений разбиений, полученных с помощью рассмотренных конструкций от матриц пересечений исходных разбиений.

4. С целью построения разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды малого ранга продолжено развитие свитчингового метода, предложенного С.В. Августиновичем и Ф.И. Соловьёвой в 1996 году для построения широкого класса двоичных совершенных кодов. Также предложена модификация конструкции разбиений на совершенные коды, основанная на конструкции Фелпса (см. [8]). Проведён сравнительный анализ семейств кодов, соответствующих данным конструкциям и показано, что нижняя оценка числа различных разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды малого ранга, полученная с помощью конструкции ijk-компонент, является лучшей на сегодняшний день для почти всех допустимых длин кодов.

Практическая и теоретическая ценность. Работа носит теоретический характер. Полученные в ней результаты могут быть применены в теории кодов, исправляющих ошибки: для дальнейшего исследования и построения новых классов двоичных кодов, для построения совершенных кодов полного ранга, кодов с большими кодовыми расстояниями, для исследования разбиений пространства $\mathbb{F}^n$ на коды.

Апробация работы. Все результаты диссертационной работы были апробированы на следующих конференциях: на XII международном симпозиуме по проблемам избыточности в информационных системах (С.-Петербург, Россия, 2009 г.); на VII молодёжной школе по дискретной математике и её приложениям (Москва, Россия, 2009 г.); на международной конференции по алгебраической комбинаторике и её приложениям ALCOMA-10 (Тырнау, Германия, 2010 г.); на международной конференции "Современные проблемы математики, информатики и биоинформатики" (Новосибирск, Россия, 2011 г.); на XXV конференции молодых учёных и специалистов "Информационные технологии и системы - 2012" (Петрозаводск, Россия); на международной конференции "Мальцевские чтения" (Новосибирск, Россия, 2012 г.); на международном симпозиуме по теории информации ISIT 2013 (Стамбул, Турция, 2013 г.).

Результаты работы докладывались на семинаре "Теория информации и теория кодирования" ИППИ РАН, на семинарах "Теория кодирования" и "Дискретный анализ" НГУ и Института математики СО РАН.

Основные результаты диссертации.

1. Получено (конструктивно) 5 бесконечных серий неэквивалентных предельно-транзитивных расширенных совершенных двоичных кодов любой возможной длины, начиная с шестнадцати.

2. Решена проблема рангов для пропелинейных совершенных двоичных кодов, за исключением случаев кодов полного ранга для длин $63, 127, 2047$ и кодов длины 127 предполного ранга.

3. Предложены конструкции транзитивных, 2-транзитивных и вершинно-транзитивных разбиений пространства $\mathbb{F}^n$ на совершенные коды для любой допустимой длины, получены нижние оценки числа неэквивалентных таких разбиений.

4. С помощью свитчинговой конструкции получена лучшая на сегодняшний день нижняя оценка числа разбиений двоичного n-мерного векторного пространства на совершенные коды длины $n \geq 31$.

Объем и структура диссертации. Диссертация состоит из введения, трёх глав, приложения и списка литературы (62 наименования), в конце приведён список публикаций автора по теме диссертации. Объем диссертации 116 страниц, включая 2 иллюстрации и 5 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Прежде чем перейти к обзору полученных в диссертации результатов, приведём необходимые определения и обозначения.

Расстояние Хэмминга $d(x, y)$ между двумя произвольными векторами x и y пространства $\mathbb{F}^n$ определяется как число координатных позиций, в которых эти векторы различаются. *Вес* вектора – это число его ненулевых координат. Произвольное подмножество пространства $\mathbb{F}^n$ называется двоичным кодом длины n. Векторы из $\mathbb{F}^n$, принадлежащие коду, называются кодовыми словами. Код C из $\mathbb{F}^n$ называется *совершенным двоичным кодом, исправляющим одиночные ошибки* (далее кратко *совершенным кодом*), если каждый вектор пространства $\mathbb{F}^n$ находится на расстоянии не больше 1 от некоторого единственного вектора из C. Как было отмечено ранее, такие коды существуют только при $n = 2^m - 1, \ m \geq 2$. Кодовым расстоянием кода называется наименьшее из расстояний Хэмминга между всеми его попарно различными кодовыми словами. Код, содержащий нулевое кодовое слово, называют *приведённым*. Код называется *линейным*, если он является подпространством $\mathbb{F}^n$. Линейный совершенный код называется *кодом Хэмминга*. Известно, что для фиксированного n код Хэмминга длины n единствен с точностью до изоморфизма.

Ядро приведённого кода C состоит из всех кодовых слов $x \in C$ таких, что $x + C = C$. Размерность линейной оболочки множества всех кодовых слов приведённого кода называется *рангом* кода. Размерность ядра и ранг приведённого кода C обозначаются через $k(C)$ и $r(C)$, соот-

ветственно. Известно, что ранг и размерность ядра кода Хэмминга равны $n-log(n+1)$, ранги совершенных (расширенных совершенных) кодов длины n (длины $n+1$) могут принимать значения от $n-log(n+1)$ до n. Здесь и далее log обозначает логарифм по основанию 2. Если ранг совершенного (расширенного совершенного) кода длины n (длины $N=n+1$) равен n, его называют кодом *полного ранга*.

Пусть C – произвольный совершенный код. Через $\mathrm{ST}(C)$ будем обозначать систему троек кода C, то есть $\mathrm{ST}(C)=\{u+v|u,v\in C : w(u+v)=3\}$. Соответственно, для произвольного расширенного совершенного кода C через $\mathrm{SQ}(C)$ будем обозначать систему четвёрок, то есть $\mathrm{SQ}(C)=\{u+v|u,v\in C : w(u+v)=4\}$.

Известно, что группа автоморфизмов пространства $\mathbb{F}^n$ исчерпывается всеми изометриями $\mathbb{F}^n$, каждая такая изометрия определяется подстановкой π на множестве координат и сдвигом на произвольный вектор $v\in\mathbb{F}^n$. *Группа автоморфизмов* $\mathrm{Aut}(\mathbb{F}^n)$ пространства $\mathbb{F}^n$ определяется как $\mathrm{Aut}(\mathbb{F}^n)=\{(v,\pi)\mid v\in\mathbb{F}^n,\ \pi\in S_n\}$, где S_n — симметрическая группа подстановок порядка n. Множество всех перестановок координатных позиций, сохраняющих код C, называется *группой симметрий* кода C и обозначается через $\mathrm{Sym}(C)$. *Группой автоморфизмов* $\mathrm{Aut}(C)$ кода C длины n называется группа изометрий пространства $\mathbb{F}^n$, переводящих код в себя. Говорят, что два произвольных кода C и D *эквивалентны*, если существует такая изометрия φ пространства $\mathbb{F}^n$, что $C=\varphi(D)$.

Код называется транзитивным, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Для приведённых кодов удобно использовать следующее определение транзитивного кода: для каждого кодового слова x из C найдётся подстановка π_x из S_n такая, что $(x,\pi_x)\in\mathrm{Aut}(C)$, то есть $x+C=\pi_x(C)$, где π_x может не принадлежать группе симметрий $\mathrm{Sym}(C)=\{\pi\in S_n\mid\pi(C)=C\}$ кода C. Таким образом, в транзитивном приведённом коде для любого его кодового слова x найдётся автоморфизм $(x,\pi_x)\in\mathrm{Aut}(C)$, переводящий слово x в нулевое кодовое слово. Легко видно, что оба этих определения эквивалентны.

Кодовое слово x из нетранзитивного кода C, для которого не существует такой подстановки π_x, будем называть *нетранзитивным кодовым словом*. Координатную позицию транзитивного расширенного совершенного кода назовём *нетранзитивной*, если код, полученный её выкалыванием, нетранзитивен.

Во введении обосновывается актуальность темы диссертации, характеризуется новизна работы. Даётся краткий обзор полученных результатов по тематике диссертации. Приводится список основных результатов диссертации и объясняются связи между ними.

Первая глава диссертации посвящена исследованию транзитив-

ных совершенных и расширенных совершенных кодов. Задачу проверки объекта на транзитивность можно встретить и в других областях математики – например, поиск гамильтонова цикла в графах. Транзитивные коды по ряду свойств близки к линейным кодам, в частности, для приведённого транзитивного кода C верно следующее: $|\mathrm{Aut}(C)| = |C| \cdot |\mathrm{Sym}(C)|$. Данное обстоятельство позволяет сделать вывод о некотором богатстве групп автоморфизмов транзитивных кодов. Число транзитивных кодов, по всей вероятности, невелико, по сравнению с общим числом кодов с теми же параметрами. Тем не менее, для всякого оптимального нелинейного кода почти всегда можно найти транзитивный код с теми же параметрами. Например, двоичный образ (под действием отображения Грея) произвольного Z_4- или Z_2Z_4-линейного кода является транзитивным кодом.

Очевидно, что применение общей проверки на чётность позволяет получать из транзитивных совершенных двоичных кодов транзитивные расширенные совершенные двоичные коды. Обратное не всегда верно, в частности, в 2004 г. С. А. Малюгиным был обнаружен один транзитивный расширенный совершенный двоичный код длины 16, такой, что все коды, полученные из него выкалыванием любой координаты, являются нетранзитивными. Всякий транзитивный расширенный совершенный код произвольной допустимой длины, обладающий свойством, что все коды, полученные из него выкалыванием любой координаты, являются нетранзитивными, будем называть *предельно-транзитивным*. Иными словами, это код, все координаты которого нетранзитивны.

В разделе 1.1 решена задача классификации всех предельно-транзитивных кодов длины 16, а также доказано существование таких кодов для любой допустимой длины.

В разделе 1.1.1 приведены результаты, полученные в диссертации посредством дополнительных компьютерных исследований, проведённых с помощью системы компьютерной алгебры Magma. Для каждого транзитивного кода длины 15 и транзитивного расширенного кода длины 16 из [14] были вычислены ранг, размерность ядра, порядок группы симметрий, мощность множества $\mathrm{ST}(C)$ ($\mathrm{SQ}(C)$ – для расширенных кодов). Найдены[3] все транзитивные расширенные совершенные коды длины 16, имеющие хотя бы одну нетранзитивную координату.

Для построения бесконечной серии предельно-транзитивных кодов в разделе 1.1.2 использованы известные конструкции Васильева [2] и

[3] Guskov G. K., Solov'eva F. I. Properties of perfect transitive binary codes of length 15 and extended perfect transitive binary codes of length 16, 2012, http://arxiv.org/abs/1210.5940.

Плоткина [12].

Рассмотрим произвольный расширенный совершенный код C^N длины $N = 2^k$. Через C^{2N} обозначим расширенный код длины $2N$, полученный из него с помощью конструкции Плоткина. Введём обозначение $\mathcal{N}_N = \{1, 2, \ldots, N\}$. Через C_j^{N-1} обозначим код, полученный выкалыванием кода C^N по j-й координатной позиции, $j \in \mathcal{N}_N$. Пусть V_i^{2n+1} – код, полученный из совершенного кода C_i^n, $i \in \mathcal{N}_N$, $n = 2^k - 1$, $k \geq 3$, применением конструкции Васильева с функцией $\lambda \equiv 0$. Сравнение этих конструкций позволило обнаружить связь между кодами V_i^{2n+1} и C_j^{2n+1}, которая выражается в следующем утверждении

Лемма 1. *Для любого $j \in \mathcal{N}_{2N}$ найдётся $i \in \mathcal{N}_N$ такое, что код C_j^{2n+1} изоморфен коду Васильева V_i^{2n+1}.*

Для проверки нетранзитивности выколотых кодов был применён метод локального анализа из [7], а именно, были детально исследованы Паш-конфигурации систем троек Штейнера полученных совершенных кодов. Напомним, что *системой троек Штейнера* STS_n *порядка* n называется система сочетаний из n-элементного множества $\mathcal{N}_n = \{1, \ldots, n\}$ по три, называемых тройками, такая, что каждая неупорядоченная пара элементов содержится в точности в одной тройке. Известно (см. [12]), что множество кодовых слов веса 3 в приведённом совершенном коде C^n образует систему троек Штейнера (каждая тройка системы состоит из номеров ненулевых координат соответствующего кодового слова веса 3). Будем обозначать её через $\mathrm{STS}(C^n)$. *Паш-конфигурацией* для STS_n называется множество троек из STS_n, изоморфное множеству

$$\{(a, b, c), (a, y, z), (x, b, z), (x, y, c)\},$$

то есть, троек, попарно пересекающихся по одному элементу, а в объединении дающих шесть элементов. Известно, что число Паш-конфигураций $P(\mathrm{STS}_n)$ системы троек Штейнера STS_n порядка n является инвариантом, часто позволяющим устанавливать неэквивалентность двух систем троек Штейнера.

В работе найдена рекуррентная формула для числа Паш-конфигураций системы троек Штейнера кода Васильева V_i^{2n+1}. Оказалось, что оно зависит только от числа Паш-конфигураций системы троек Штейнера исходного кода C_i^n:

$$P(STS(V_i^{2n+1})) = 8 \cdot P(STS(C_i^n)) + |STS(C_i^n)| + 2 \cdot \binom{n}{2}. \qquad (1)$$

В результате исследования свойств десяти неэквивалентных предельно-транзитивных расширенных совершенных кодов длины 16, обнаружено, что восемь из них таковы, что для любого направления $i \in \mathcal{N}_{16}$,

в нетранзитивном выколотом коде C_i^n, $n = 15$, найдётся такое нетранзитивное слово y, что системы троек Штейнера кодов C_i^n и $C_i^n + y$ имеют различное число Паш-конфигураций. Используя лемму 1, доказано, что, при подстановке таких кодов в конструкцию Плоткина (см. [12]), это свойство сохраняется, то есть верна

Лемма 4. *Для любого $N = 2^k$, $k \geq 4$, существует не менее 8 различных транзитивных расширенных совершенных кодов длины N таких, что для любого из этих кодов C^N для всякого направления $i \in \mathcal{N}_N$, в выколотом коде C_i^n, $n = N-1$, найдётся такое нетранзитивное слово y, что $P(STS(C_i^n)) \neq P(STS(C_i^n + y))$.*

Используя зависимость (1), лемму 4 и результаты компьютерных исследований, представленные в приложении, доказана

Теорема 1. *Для любого допустимого $N > 16$ существует не менее пяти неэквивалентных предельно-транзитивных расширенных совершенных кодов длины N. При $N = 16$ существует 10 неэквивалентных таких кодов.*

Неэквивалентность кодов доказывалась с помощью сравнения соответствующих им пар значений *(ранг, размерность ядра)*, используя подход из [5].

Применяя конструкцию Плоткина, каждый из восьми различных предельно-транзитивных расширенных совершенных кодов длины 16, обладающих описанным в лемме 4 свойством, можно продолжить до бесконечной серии. Таким образом, верно

Следствие 1. *Для любого допустимого $N > 16$ существует не менее 8 различных предельно-транзитивных расширенных совершенных кодов длины N.*

В разделе 1.2 решается задача нахождения всех значений, которые могут принимать ранги транзитивных совершенных кодов, то есть, решается проблема спектра рангов транзитивных совершенных кодов.

Из статьи [5] известно, что если в конструкцию Васильева с функцией $\lambda \equiv 0$ подставить код длины n, то разница между рангом полученного кода длины $2n + 1$ и рангом кода Хэмминга длины $2n + 1$ (так называемая *прибавка ранга*, см. [5]) остаётся той же, какой она была для исходного кода и кода Хэмминга длины n. Таким образом, с помощью конструкции Васильева с нулевой функцией λ из кода полного ранга длины n (то есть, ранга n) можно получить лишь код длины $2n + 1$ ранга на единицу меньше полного ранга. Однако, используя нелинейные функции λ специального вида, ранг результирующего кода можно увеличить до полного, с сохранением транзитивности кода. В качестве таких функций λ можно рассматривать пропелинейные функции и, соответственно, решать проблему рангов для пропелинейных кодов. Поскольку, по опре-

делению, всякий пропелинейный код является транзитивным, как следствие, будет решена проблема рангов и для транзитивных совершенных кодов.

Понятие *пропелинейного кода* (от латинского *prope – близко, почти*) было впервые введено Дж. Рифой с соавторами в 1989 г. Как известно, множество $\mathrm{Aut}(\mathbb{F}^n)$ всех автоморфизмов пространства $\mathbb{F}^n$ образует группу под действием операции композиции: $(u,\pi)\circ(v,\tau) = (u+\pi(v),\pi\tau)$ для всех $(u,\pi),(v,\tau) \in Aut(\mathbb{F}^n)$, здесь и далее $\pi\tau(x) = \pi(\tau(x))$ для $x \in \mathbb{F}^n$.

Пусть для кода C задано *означивание* Π кодовых слов подстановками: $x \mapsto \pi_x$: $(x,\pi_x) \in Aut(C)$, такое что $\pi_{(x,\pi_x)y} = \pi_x\pi_y$. Через $\Pi(C)$ обозначим множество всех подстановок, соответствующих словам из кода C. Определим групповую операцию на C вида $x \star y = (x,\pi_x)y$. Код с такой операцией называется *пропелинейной структурой* на C и обозначается $(C,\Pi,\star)$ или, кратко, $(C,\star)$, если не требуется информация об означивании Π. Код называется *пропелинейным*, если на нём определена пропелинейная структура. Очевидно, что любой пропелинейный код транзитивен. В 2001 г. Дж. Рифа с соавторами показали, что пропелинейные совершенные коды могут быть получены применением конструкции Васильева, а также конструкции Моллара, доказательство последнего факта см. в [9].

В разделе 1.2.1 с помощью системы компьютерной алгебры Magma доказано существование пропелинейных кодов полного ранга длин 15 и 31. Ранее в [9] было доказано существование пропелинейных совершенных кодов длины 15 любого допустимого ранга, за исключением полного ранга.

В разделе 1.2.2, на основании этих результатов, для кодов малых длин, используя конструкцию Васильева с функцией $\lambda \equiv 0$, а для кодов длин, начиная с 255 – конструкцию Моллара [13] с функцией $f \equiv 0$, по индукции доказана

Теорема 5. *Для любого $n = 2^m - 1, m \geq 4$ и произвольного r, такого, что $n - \log(n+1) \leq r \leq n$, кроме случаев $n = r = 63$; $n = 127$, $r \in \{126, 127\}$ и $n = r = 2047$, существует пропелинейный совершенный двоичный код длины n ранга r.*

Результаты первой главы опубликованы в [19, 20, 22, 26, 27].

Во второй главе данной работы проводится исследование транзитивных разбиений пространства $\mathbb{F}^n$ на совершенные коды, начатое в [6]. Изучение совершенных кодов, как уже упоминалось, неразрывно связано с изучением разбиений пространства $\mathbb{F}^n$ на совершенные коды. Некоторые свойства кодов справедливы для разбиений. Одним из таких свойств является транзитивность. *Группой автоморфизмов произволь-*

ного разбиения $P^n = \{C_0, C_1, \ldots, C_n\}$ *пространства* $\mathbb{F}^n$ *на совершенные коды* $C_0, C_1, \ldots, C_n$, $\bigcup\limits_{i=0}^{n} C_i = \mathbb{F}^n$, называется группа изометрий пространства $\mathbb{F}^n$, переводящих разбиение P^n в себя. *Разбиение* P^n называется *k-транзитивным*, $1 \leq k \leq n$, если для любой пары упорядоченных подмножеств $\{i_1, \ldots, i_k\}$ и $\{j_1, \ldots, j_k\}$ из $\mathcal{N}_n$ существует автоморфизм σ из $Aut(P^n)$ такой, что $\sigma(C_{i_t}) = C_{j_t}, t = 1, \ldots, k$. При $k = 1$ разбиение P^n называется *транзитивным*. Если же рассмотреть кодовые слова кодовэлементов разбиения, можно определить более сильное свойство. Разбиение P^n назовём *вершинно-транзитивным*, если для любых двух кодовых слов $u \in C_i,\ v \in C_j$ существует автоморфизм σ из $\mathrm{Aut}(P^n)$ такой, что $\sigma(u) = v$. При этом, если $i = j$ для любого $i \in \mathcal{N}_n$, то получим вершинно-транзитивное разбиение на транзитивные коды (например, на классы смежности кода Хэмминга). Далее будем говорить, что *разбиение имеет длину* n, если оно состоит из кодов длины n.

В разделе 2.1 приведены вспомогательные утверждения и определения, необходимые для доказательства неэквивалентности полученных разбиений.

В разделе 2.2 представлены две конструкции транзитивных разбиений на совершенные коды. Доказано, что они сохраняют свойства вершинной транзитивности, транзитивности и также 2-транзитивности.

В разделе 2.3, используя утверждения из раздела 2.1 и ряд комбинаторных соображений, подсчитаны нижние оценки числа неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений пространства $\mathbb{F}^n$ на совершенные коды.

Теорема 10. *Для любого* $n \geq 2^k - 1$, $k > 20$, *число неэквивалентных транзитивных разбиений* $\mathbb{F}^n$ *на совершенные коды удовлетворяет следующей нижней оценке:* $R_{n;trans} > n + 1$.

Теорема 11. *Справедливо*

a) Для любого $n \geq 2^m - 1$, $m > 20$, *число* $R_{n;vertex-trans}$ *неэквивалентных вершинно-транзитивных разбиений* $\mathbb{F}^n$ *на совершенные коды длины* n *удовлетворяет следующей нижней оценке:* $R_{n;vertex-trans} > \frac{n+1}{2}$.

b) Для любого $n \geq 2^m - 1$, $m > 20$, *число* $R_{n;2-trans}$ *неэквивалентных 2-транзитивных разбиений* $\mathbb{F}^n$ *на совершенные коды длины* n *удовлетворяет:* $R_{n;2-trans} > \frac{n+1}{3}$.

Для малых значений длин кодов $n \leq 2^{20} - 1$ с помощью этого метода удалось получить только следующие нижние оценки:

Утверждение 1. *Для любого* $n \geq 2^m - 1$, *где* $3 \leq m \leq 20$, *число неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений* $\mathbb{F}^n$ *на совершенные коды удовлетворяет следующим нижним оценкам соответственно:*

a) $R_{n;trans} \geq \frac{n+1}{2}$; *b)* $R_{n;vertex-trans} \geq \frac{n+1}{3}$; *c)* $R_{n;2-trans} \geq \frac{n+1}{4}$.

Результаты второй главы опубликованы в [17, 23].

В третьей главе изучаются и анализируются три конструкции различных разбиений пространства $\mathbb{F}^n$ на совершенные коды малого ранга с целью получения нижней оценки числа таких различных разбиений. Данная проблема связана с проблемой подсчёта числа различных совершенных двоичных кодов. Напомним, что, как известно, асимптотики двойных логарифмов (при условии, что они существуют) числа различных совершенных двоичных кодов и числа различных разбиений на такие коды совпадают. Причина подробного изучения разбиений малого ранга состоит в том, что на сегодняшний день в наилучшей нижней оценке числа различных совершенных двоичных кодов, полученной в статье [11], первые три сомножителя определяются именно совершенными кодами ранга не больше $n - \log(n+1) + 2$.

В разделе 3.1 изучается конструкция из работы 2004 г. [16], основанная на конструкции Васильева (она также использовалась в [10], но с некоторыми ограничениями).

Основываясь на классификации неэквивалентных разбиений длины 7, приведённой К. Т. Фелпсом в [15] (таких разбиений оказалось всего 11), легко подсчитать число различных разбиений $\mathbb{F}^7$ на совершенные коды длины 7:

Утверждение 2. *Существует* $\mathcal{M}_7 = 27360 > 1.66 \cdot 2^{14}$ *различных разбиений* $\mathbb{F}^7$ *на совершенные коды длины* 7.

На основе этого утверждения доказана

Лемма 18. *Число* $\mathcal{M}_{15}$ *различных разбиений* $\mathbb{F}^{15}$ *на совершенные коды ранга не больше* 12 *удовлетворяет следующей нижней оценке:* $\mathcal{M}_{15} > 2^{147}$.

Утверждение 2 и лемма 18 позволяют сделать вывод, что полученная ранее, см. [1, 16], нижняя оценка числа $\mathcal{M}_n$ различных разбиений пространства $\mathbb{F}^n$ на совершенные коды длины $n, n > 15$, справедлива для всех допустимых длин $n \geq 7$: $\mathcal{M}_n > 2^{2^{\frac{n-1}{2}}} \cdot 2^{2^{\frac{n-3}{4}}}$.

В разделе 3.2 изучается каскадная конструкция, являющаяся частным случаем каскадного метода построения разбиений, введённого в 2001 г. в статье [8], и исследуется класс разбиений $\mathbb{F}^n$ ранга не более $n - \log(n+1) + 2$.

Основываясь на известных асимптотиках числа различных расширенных кодов Хэмминга и числа четверичных MDS кодов, доказана

Теорема 13. *Для числа* $\mathcal{M}_N$ *различных разбиений* $\mathbb{F}^N$ *на расширенные совершенные коды длины* $N \geq 16$ *ранга не больше* $N - \log N + 1$

верна следующая нижняя оценка: $\mathcal{M}_N \geq 2^{2^{\frac{N}{2}-1}} \cdot 2^{2^{\frac{N}{4}+\log 7}} \cdot 3^{2^{\frac{N}{4}+\log(N+8)-2}} \cdot 2^{\frac{N}{2}\cdot\left[\log\frac{N}{4e}\right]-2\log^2\frac{N}{4}-\log\frac{N}{4}+2}$.

Извлекая квадратный корень из оценки теоремы 13, получим нижнюю оценку числа различных разбиений $\mathbb{F}^n$ малого ранга

Следствие 4. *Для числа $\mathcal{M}_n$ различных разбиений $\mathbb{F}^n$ на совершенные коды длины $n \geq 15$ ранга не больше $n - \log(n+1) + 2$ верна следующая нижняя оценка*: $\mathcal{M}_n \geq 2^{2^{\frac{n-3}{2}}} \cdot 2^{2^{\frac{n-3}{4}+\log 7}} \cdot 3^{2^{\frac{n-11}{4}+\log(n+9)}} \cdot 2^{\frac{n+1}{4}\cdot\left[\log\frac{n+1}{4e}\right]-\log^2\frac{n+1}{4}-\frac{1}{2}\cdot\log\frac{n+1}{4}+1}$.

В разделе 3.3 изучается конструкция, основанная на методе ijk-компонент. Впервые аналогичная конструкция была предложена в 2007 г. в работе [1] для построения разбиений на попарно неэквивалентные совершенные коды, но не было исследовано многообразие возможных конструируемых разбиений и не был проведён подсчёт числа различных разбиений. Результирующие разбиения имеют ранг не больше $n-\log(n+1)+2$. С помощью данного метода получена следующая нижняя оценка числа различных разбиений пространства $\mathbb{F}^n$ на совершенные коды малого ранга:

Теорема 14. *Число $\mathcal{M}_n$ различных разбиений пространства $\mathbb{F}^n$ на совершенные коды длины n ранга не больше $n-\log(n+1)+2$ удовлетворяет следующей нижней оценке*

$$\mathcal{M}_n \geq 2^{2^{\frac{n-1}{2}}} \cdot 6^{2^{\frac{n-3}{4}}}$$

для любого допустимого $n \geq 7$.

Результаты третьей главы опубликованы в [18, 21, 24, 25].

В приложениях A, B, C диссертации приводятся результаты компьютерных исследований, проведённых как с помощью системы компьютерной алгебры Magma, так и с помощью компьютерной программы автора диссертации (см. приложение C в диссертации для главы 2).

Результаты раздела 1.2 получены совместно с И. Ю. Могильных и Ф. И. Соловьёвой, см. [20, 27]. Результаты раздела 3.3 и компьютерные исследования с использованием системы компьютерной алгебры Magma были проведены автором диссертации. Остальные результаты получены совместно с Ф. И. Соловьёвой.

Автор выражает глубокую искреннюю признательность своему научному руководителю д.ф.-м.н. проф. Ф. И. Соловьёвой, под руководством которой была выполнена эта работа.

Литература

1. *Августинович С. В., Соловьёва Ф. И., Хеден О.* О разбиениях n-куба на неэквивалентные совершенные коды // Пробл. передачи информ. — 2007. — Т. 43, № 4. — С. 45–50.

2. *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. — М: Физматгиз. — 1962. — № 8. — С. 337–339.

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

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

5. *Соловьёва Ф. И.* О построении транзитивных кодов // Проблемы передачи информации. — 2005. — Вып. 3. — С. 23–31.

6. *Соловьёва Ф. И.* О транзитивных разбиениях n-куба на коды // Проблемы передачи информации. — 2008. — Т. 44, № 4. — С. 27–35.

7. *Соловьёва Ф. И.* Комбинаторные методы построения и исследования кодов (докторская диссертация). – 2008. — 202 С.

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

9. *Borges J., Mogilnykh I. Yu., Rifà J. K., Solov'eva F. I.* Structural properties of binary propelinear codes // Advances in Math. of Commun. — 2012. — Vol. 6, N 3. — P. 329–346.

10. *Heden O., Solov'eva F. I.* Partitions of $\mathbb{F}^n$ into nonparallel Hamming codes // Advances in Math. of Communications. — 2009. — Vol. 3, N 4. — P. 385–397.

11. *Krotov D. S., Avgustinovich S. V.* On the number of 1-perfect binary codes: A lower bound // IEEE Trans. Inf. Theory. — 2008. — Vol. 54, N 4. — P. 1760–1765.

12. *MacWilliams F. G., Sloane N. J. A.* The theory of error correcting codes // New York: North-Holland. — 1977. — P. 744. (Русский перевод: Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. // Москва: Связь. — 1979. — 744 С.)

13. *Mollard M.* A generalized parity function and its use in the construction of perfect codes // SIAM J. Alg. Discrete Math. — 1986. — Vol. 7, N 1. — P. 113–115.

14. *Östergård P. R. J., Pottonen O.* The Perfect Binary One-Error-Correcting Codes of Length 15: Part I – Classification // IEEE Trans. Inform. Theory. — 2009. — Vol. 55. — P. 4657–4660. Codes at arXiv:0806.2513v3.

15. *Phelps K.T.* An enumeration of 1-perfect binary codes // Australas. J. Comb. — 2000. — Vol. 21. — P. 287–298.

16. *Solov'eva F. I.* On perfect codes and related topics // *Com*^{2}*Mac* Lecture Note Series13. — Pohang. — 2004. — 80 P.

Публикации автора по теме диссертации

Публикации в научных журналах

17. *Соловьёва Ф. И., Гуськов Г. К.* О построении вершинно-транзитивных разбиений n-куба на совершенные коды // Дискретный анализ и исследование операций. — 2010. – Т. 17, № 3. — С. 84 – 100.

18. *Гуськов Г. К.* О разбиениях двоичного векторного пространства на совершенные коды // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 2. — С. 15–25.

19. *Гуськов Г. К., Соловьёва Ф. И.* О предельно-транзитивных расширенных совершенных кодах // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 5. — С. 31–44.

20. *Guskov G. K., Mogilnykh I. Yu., Solov'eva F. I.* Ranks of propelinear perfect binary codes // Siberian Electronic Mathematical Reports. — 2013. — Vol. 10. — P. 443–449.

Труды конференций

21. *Гуськов Г. К.* О числе различных разбиений куба E^{15} на совершенные двоичные коды // Материалы 47 Международной научной студенческой конференции "Студент и научно-технический прогресс". — Новосибирский государственный университет. — 2009. — 235 с. — С. 160.

22. *Гуськов Г.К., Соловьева Ф.И.* О рангах и ядрах совершенных двоичных транзитивных кодов. // Материалы VII молодежной школы по дискретной математике и её приложениям, М. Изд-во ИПМ РАН. — Москва, 18-23 мая 2009. — Часть I. — С. 23-28.

23. *Solov'eva F.I., Guskov G.K.* On vertex-transitive and 2-transitive partitions of $\mathbb{F}^n$ into perfect codes // Proc. XII Int. Symposium on problems of Redundancy in Information and Controls Systems. St.-Petersburg, Russia. — May, 26-30, 2009. — P. 104–108.

24. *Гуськов Г. К., Соловьева Ф.И.* О разбиениях n-куба на совершенные двоичные коды // Международная конференция "Современные проблемы математики, информатики и биоинформатики" (ISBN 978-5-905569-03-6). Россия, Новосибирск, 11 - 14 октября, 2011. — С. 65. — http://conf.nsc.ru/files/conferences/Lyap100/fulltext/74556/74659/Guskov.Soloveva.LowerBoundPartitions.pdf

25. *Гуськов Г. К., Соловьёва Ф. И.* Об одной каскадной конструкции разбиений n-куба на совершенные двоичные коды // Тр. международной конф. "Информационные технологии и системы". Россия, Петрозаводск, 19 - 25 августа. — М: ИППИ РАН. — 2012. — С. 124–128.

26. *Гуськов Г. К., Соловьёва Ф. И.* Существование расширенных совершенных транзитивных в узком смысле кодов // Мальцевские чтения — 12-16 ноября 2012. — Новосибирск. – С. 25.

27. *Guskov G. K., Mogilnykh I. Yu., Solov'eva F. I.* Rank Spectrum of Propelinear Perfect Binary codes // IEEE International Symposium on Information Theory (ISBN 978-1-4799-0445-7). Istanbul, Turkey. — July 7-12, 2013. — P. 879–881.

Гуськов Георгий Константинович

Транзитивные совершенные коды и разбиения

Автореферат диссертации
на соискание учёной степени
кандидата физико-математических наук

Подписано в печать 23.10.13. Формат 60x84 1/16.
Усл. печ. л. 1,2. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ N 58.

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