Кротов Денис Станиславович

Совершенные коды и n-арные квазигруппы: конструкции и классификация

Специальность 01.01.09 — дискретная математика
и математическая кибернетика

Автореферат
диссертации на соискание ученой степени
доктора физико-математических наук

Новосибирск — 2010

Работа выполнена в Учреждении Российской академии наук Институте математики им. С. Л. Соболева Сибирского отделения РАН

Официальные оппоненты: доктор физико-математических наук
Копытов Валерий Матвеевич

доктор технических наук
Федоренко Сергей Валентинович

доктор физико-математических наук
Черемушкин Александр Васильевич

Ведущая организация: Московский государственный университет имени М. В. Ломоносова

Защита состоится 23 марта 2011 г. в 15^{00} часов на заседании диссертационного совета Д 003.015.01 при Учреждении Российской академии наук Институте математики им. С. Л. Соболева СО РАН по адресу: 630090, Новосибирск, пр. Академика Коптюга, 4

С диссертацией можно ознакомиться в библиотеке ИМ СО РАН.

Автореферат разослан «9» 02 2011 года.

Ученый секретарь
диссертационного совета Д 003.015.01
при ИМ СО РАН, д.ф.-м.н. Шамардин Ю. В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В диссертации рассматриваются комбинаторные вопросы теории n-арных квазигрупп и 1-совершенных двоичных кодов. Доказаны признаки разделимости n-арных квазигрупп, получена характеризация класса n-арных квазигрупп порядка 4. Рассмотрены конструкции 1-совершенных двоичных кодов и построение из них кодов в троичном алфавите.

Актуальность темы. Объектами исследования настоящей работы являются 1-совершенные двоичные коды и n-арные квазигруппы, которые также известны как латинские гиперкубы (многомерное обобщение латинских квадратов) и эквивалентны максимально дистанционно разделимым (МДР) кодам с расстоянием 2. Оба класса объектов рассматриваются в метрическом пространстве Хэмминга H_q^n, носителем которого является множество $\{0,1,\ldots,q-1\}^n$ слов длины n алфавита $\{0,1,\ldots,q-1\}$, а расстояние между двумя словами есть число позиций, в которых эти слова различаются. Если q есть степень простого числа, H_q^n можно снабдить структурой векторного пространства над конечным полем $\mathrm{GF}(q)$, мы будем этим пользоваться в случае $q=2$. Пространство Хэмминга удобно также рассматривать как граф, в котором два слова соединены ребром тогда и только тогда, когда они отличаются только в одной позиции. Максимальную клику этого графа будем называть *линией* (линия состоит из q слов, совпадающих во всех позициях кроме одной), а вершину вместе с ее окрестностью — 1-шаром с центром в этой вершине. Множество слов в H_q^n называется 1-*совершенным кодом*, если каждый 1-шар содержит ровно одну кодовую вершину. Множество слов в H_q^n называется *МДР-кодом с расстоянием* 2, если каждая линия содержит ровно одну кодовую вершину. (Напомним, что кодовым расстоянием произвольного подмножества в H_q^n из двух или более вершин называется минимальное расстояние между двумя различными вершинами. Так, 1-совершенный код, если у него больше одной вершины, имеет расстояние 3.) Функция из $\{0,1,\ldots,q-1\}^n$ в $\{0,1,\ldots,q-1\}$ называется *n-арной квазигруппой порядка q*, если на каждой линии она принимает все q различных значений, каждое ровно по одному разу.

Если значение n-арной квазигруппы трактовать как дополнительный символ, то получится МДР-код с расстоянием 2.

Определения 1-совершенных кодов и МДР кодов в приведенной выше форме имеют определенную общность, которая в частности подчеркивает, что оба класса относятся к категории «точных» комбинаторных конфигураций. Эти классы кодов можно единообразно определить иначе: если удаление некоторого независимого множества вершин графа H_q^n приводит к регулярному графу степени $(q-1)^n-1$ или $(q-2)^n$, то это множество является 1-совершенным кодом или МДР-кодом с расстоянием 2 соответственно. Такая постановка близка к вопросам, изучаемым в алгебраической теории графов. На самом деле, как 1-совершенные коды, так и МДР-коды с расстоянием 2 являются важнейшими частными случаями так называемых регулярных разбиений, в англоязычной литературе известными также как equitable partitions (термин «equitable» в данном контексте не имеет удобного перевода), а на русском языке больше известными как совершенные раскраски. Наряду с дистанционно регулярными графами и схемами отношений, совершенные раскраски (equitable partitions) являются популярными объектами алгебраической комбинаторики, см. напр. [35], [46].

Отмеченная связь постановок была упомянута, чтобы подчеркнуть общую природу изучаемых объектов, к существу вопросов, рассматриваемых в диссертации, прямого отношения она не имеет. Для нас более важна конструктивная связь: существуют способы построения 1-совершенных кодов из n-арных квазигрупп, впервые предложенные К. Т. Фелпсом [65], [66], см. также [15], [52]. Поэтому результаты, полученные для n-арных квазигрупп, важны и для теории 1-совершенных кодов, к примеру, эта связь использовалась в работах [1], [31], [52], [16], [54].

Прежде чем перейти к рассмотрению классов 1-совершенных кодов и n-арных квазигрупп отдельно, отметим один общий для них вопрос, вопрос о числе объектов. Известно, что число 1-совершенных кодов в H_q^n растет дважды экспоненциально при росте n, если q есть степень простого числа, а $n = (q^m - 1)/(q - 1)$ (это необходимое для существования 1-совершенных кодов условие на n следует из известных соображений: мощность пространства должна делиться на мощность 1-шара),

то есть нижняя оценка на число кодов имеет вид $2^{2^{cn \pm o(n)}}$, где c — некоторая константа. В двоичном случае такая оценка, с $c = 1/2$, была установлена Ю. Л. Васильевым одновременно с открытием нелинейных 1-совершенных кодов [8], на случай произвольного q, равного степени простого числа, конструкция обобщена Дж. Шонхеймом [70]. Следует отметить, что существование совершенных кодов в H_q^n для q, не представимого в виде степени простого числа, является известной открытой проблемой в данной области; однако, если только существует хотя бы один такой код, известные методы позволяют построить коды для бесконечного числа значений n с тем же q [66], причем число таких кодов будет расти дважды экспоненциально по n. Известная верхняя оценка числа 1-совершенных кодов с точки зрения асимптотики двойного логарифма не отличается от числа всевозможных подмножеств H_q^n (в двоичном случае $2^{2^{n-\mathrm{const}\cdot\log n}}$, см. [1]). Улучшения нижних оценок в сериях работ [2], [20], [I], [V] (глава 6 диссертации), для двоичного случая, и [42], [17], [27], [18], [52], для кодов над q-значным алфавитом, важны больше с точки зрения понимания возможного строения совершенных кодов, чем в контексте проблемы асимптотики двойного логарифма числа кодов, хотя для $q > 3$ нижняя граница этой асимптотики была реально поднята [18], [52] (в последней работе для этого использовалась связь с n-арными квазигруппами).

Таким образом, основной проблемой является установить константу при n в асимптотике двойного логарифма числа 1-совершенных кодов (мощность алфавита q считается фиксированной). При этом даже существование такой константы не доказано, хотя противное и кажется фантастикой.

Ситуация с n-арными квазигруппами порядка $q > 3$ аналогична. Дважды экспоненциальное по n число квазигрупп составного порядка следует из известной конструкции сплетения n-арных квазигрупп (термин «сплетение» в данном случае никак не соотносится со сплетением групп), а для простых порядков, начиная с 5, установлено относительно недавно [56]. Для порядка меньше 4 проблема с числом n-арных квазигрупп тривиальна, поскольку существует только одна n-арная квазигруппа, с точностью до простых преобразований эквивалентности.

Верхнюю оценку числа объектов, с точки зрения асимптотики двойного логарифма, удается несколько улучшить по сравнению с числом всех функций, см. [26]. Однако в случае $q > 4$ асимптотики двойного логарифма нижней и верхней оценок числа n-арных квазигрупп порядка q, как и для 1-совершенных кодов, расходятся. Единственным *классом объектов, для которых проблема асимптотики двойного логарифма* числа решена, является класс n-арных квазигрупп порядка 4. Более того, существует и является одним из основных результатов диссертации характеризация этого класса и, как следствие, известна асимптотика самого числа объектов. (На самом деле, асимптотика получена В. Н. Потаповым ранее и опубликована в совместной статье [25].) Проблема оценки дважды экспоненциального числа комбинаторных объектов известна и в других разделах дискретной математики. Одним из примеров является класс бент-функций, которые определяются как булевы функции $\{0,1\}^n \to \{0,1\}$, на которых определенным образом заданная мера нелинейности достигает теоретической верхней границы. Бент-функции существуют при всех четных n, а нижняя и верхняя оценки их числа, как и для числа 1-совершенных двоичных кодов, имеют вид $2^{2^{n/2 \pm o(n)}}$ и $2^{2^{n \pm o(n)}}$ соответственно [36]. Таким образом, проблема оценок подобного рода достаточно широка, и осмысление способов ее решения — это дело будущего. Хочется подчеркнуть, что величины столь большого роста находятся за рамками интуитивного восприятия (по крайней мере автора диссертации), поэтому бывает трудно вообразить природу тех факторов, которые могли бы оказать существенное влияние на верхнюю и, кроме известных конструктивных подходов, нижнюю оценки. Трудность восприятия таких чисел приводит порой к тому, что для некоторых исследователей получение дважды экспоненциальной нижней оценки закрывает вопрос о числе объектов — это число по своей величине в каком-то смысле сравнимо с числом всех подмножеств пространства. На самом же деле нижняя оценка по сравнению с верхней остается почти ничем даже после логарифмирования.

n-Арные квазигруппы. Сам термин алгебраический и, строго говоря, обозначает пару (Σ, f), где Σ — некоторое множество, а f — n-арная операция такая, что в уравнении $x_0 = f(x_1, \ldots, x_n)$ значения любых n переменных из $x_0, x_1, \ldots, x_n$ всегда однозначно задают значение оставшейся

переменной. Как видно из названия, понятие n-арной, или многоместной (в англоязычной терминологии используются термины «polyadic» или «multary»), квазигруппы является обобщением понятия группы. Действительно, в случае $n = 2$ добавление аксиомы ассоциативности приводит к определению группы. Некоторое стандартное упрощение терминологии, которое используется в тексте диссертации, — называть n-арной квазигруппой саму операцию, как правило это не приводит к разночтениям. В случае конечного носителя Σ такие отображения также известны в комбинаторике как латинские гиперкубы порядка $q = |\Sigma|$ и часто, по аналогии с латинским квадратом (случай $n = 2$), интуитивно ассоциируются с n-мерной таблицей, $q \times q \times \ldots \times q$, заполненной символами алфавита Σ правильным образом — так, что в каждом ряду (линии) каждого из n базовых направлений все символы встречаются в точности по одному разу. Однако в некоторых случаях оказывается гораздо удобней работать с графиком $\{(x_0, x_1, \ldots, x_n) : x_0 = f(x_1, \ldots, x_n)\}$ n-арной квазигруппы, а не с самой операцией. В теории кодирования такие множества известны как МДР-коды с расстоянием 2. При рассмотрении графика n-арной квазигруппы вместо самой операции оказывается, что зависимая переменная наделена теми же «правами», что и все остальные, что делает многие формулировки более естественными, а доказательства более короткими. Однако в некоторых вопросах, например, при рассмотрении суперпозиции двух или более квазигрупп, функциональная форма все же оказывается необходимой, поэтому порой приходится использовать одновременно обе терминологии.

Фундаментальные результаты в алгебраической теории n-арных квазигрупп, которыми во многом определяется развитие этой теории начиная с 60-х годов прошлого века, принадлежат В. Д. Белоусову (см. напр. [6], [5]), начинавшему свою деятельность в этой области под руководством А. Г. Куроша. Отдельные классы многоместных операций со свойством однозначной обратимости изучались значительно раньше. Одной из первых работ является работа В. Дёрнте [41], положившая начало изучению n-арных групп (ассоциативных n-арных квазигрупп).

В последнее время возрастает интерес к n-арным квазигруппам как к комбинаторному объекту, что отчасти стимулируется возможными приложениями к теории кодирования и криптографии (см. напр. [71]), отча-

сти просто тем, что n-арные квазигруппы (латинские гиперкубы) являются очень естественным обобщением латинских квадратов — классических математических объектов, известных многим со школьной скамьи. В частности, появилось несколько работ с результатами по классификации латинских гиперкубов с малыми параметрами. В последней работе известных австралийских математиков Б. Мак-Кэя и Я. Уонлеса [63] получено число латинских n кубов порядка 4 до $n = 5$, порядка 5 до $n = 4$ и порядка 6 до $n = 3$, причем сосчитано также число классов эквивалентности для различных естественно определенных эквивалентностей, представители классов доступны на веб-ресурсе [62]. Продвинуться в бóльшие размерности при помощи переборных алгоритмов не представляется возможным на любых компьютерах, доступных в ближайшем будущем (напомним, что число объектов растет дважды экспоненциально). Число n-арных квазигрупп порядка 3 не было упомянуто не случайно. Существует только одна такая квазигруппа, с точностью до изотопии (перестановки элементов носителя независимо в каждом аргументе), а всего — $3 \cdot 2^n$. Это факт достаточно простой и, хотя самая ранняя из известных ссылок [44] (см. также [57, Corollary 13.25]) относится к последней декаде прошлого века, был известен намного раньше. Таким образом, *порядок 4 — первый нетривиальный порядок* с точки зрения n-арных квазигрупп. Именно этому порядку уделяется наибольшее внимание в диссертации и, хотя некоторые утверждения интересны в более общем контексте и применимы также и для других, не обязательно конечных, порядков, изначальной мотивацией и основным применением результатов исследований, описанных в первой части диссертации, в настоящий момент является классификация n-арных квазигрупп порядка 4.

В первой работе [I] автора диссертации 2000 года по n-арным квазигруппам порядка 4 нижняя оценка числа таких объектов устанавливается подсчетом числа изотопов n-арных квазигрупп, полученных сплетением квазигрупп порядка 2 (позже такие квазигруппы порядка 4 были названы полулинейными). После этого В. Н. Потапов сформулировал гипотезу, согласно которой *любая n-арная квазигруппа порядка 4 полулинейна или разделима*, то есть представима в виде бесповторной суперпозиции квазигрупп меньшей арности. В частности, из этого

следовало бы, что класс полулинейных n-арных квазигрупп асимптотически самый мощный, и нижняя оценка в [I] асимптотически точна. Несмотря на простоту формулировки и некоторые интуитивные соображения, на которых строилась гипотеза, найти короткое доказательство, по состоянию на текущий момент, не удалось. Полный текст имеющегося доказательства состоит из четырех статей [VII], [25], [IX], [X], каждая из которых представляет самостоятельное исследование, со своими подходами и терминологией и результатами, актуальность которых не ограничивается контекстом n-арных квазигрупп порядка 4. (Две статьи принадлежат автору диссертации, две написаны в соавторстве в В. Н. Потаповым. В диссертацию не вошла только работа [25], поскольку основная лемма, как и главный результат статьи — асимптотика числа n-арных квазигрупп порядка 4, — принадлежат В. Н. Потапову.) Промежуточным этапом исследования, который позволил ближе ознакомиться с предметом и разработать инструментарий, являлось получение верхних оценок числа квазигрупп порядка 4 [55], [25].

Возможно, утверждение о строении n-арных квазигрупп порядка 4 не прошло достаточную проверку временем и вниманием математической общественности, чтобы говорить о вероятности того, что более короткое решение не будет найдено в ближайшее время. Однако разработанная для текущего доказательства теория обладает достаточной степенью общности, чтобы быть интересной вне контекста n-арных квазигрупп порядка 4. Кроме того, обнаруживаются некоторые связи, которые косвенно указывают на то, что все действительно не так просто, как может показаться из формулировок теорем. Недавно В. Н. Потапов анонсировал следующее утверждение [68]: *(*) любая частичная n-арная квазигруппа порядка* 4, *значения которой заданы на* $\{0,1,2,3\}^{n-1} \times \{0,1\}$, *может быть дополнена до n-арной квазигруппы* $\{0,1,2,3\}^n \to \{0,1,2,3\}$. Этот факт имеет следующую эквивалентную формулировку: пусть множество вершин графа H_4^n разбито на два подмножества, порождающие регулярные подграфы степени n, тогда эти подграфы являются или не являются двудольными одновременно. Оказывается [54], подобным образом (в терминах одновременной двудольности элементов регулярного разбиения множества вершин графа Хэмминга) можно переформулировать и следующую проблему: *(**) каж-*

дый ли максимальный по мощности двоичный код длины $2^m - 3$ *с расстоянием* 3 *можно получить двукратным укорочением некоторого* 1*-совершенного кода длины* $2^m - 1$? Более того, как отмечено в [54], для некоторого подкласса кодов положительный ответ на вопрос (**) эквивалентен утверждению (*). В то же время в общем случае ответ на вопрос (**) отрицательный [64], контрпример был найден с использованием компьютера. Это говорит о том, что не существует общих аргументов, доказывающих (*), которые могли бы быть обобщены на (**), и для доказательства (*) нужен подход, использующий специфику именно этой задачи. И действительно, имеющееся доказательство [24] использует характеризацию n-арных квазигрупп порядка 4 и даже при этом достаточно трудоемко.

Вернемся к общим вопросам, касающимся n-арных квазигрупп. Важнейшую роль в их исследовании, как комбинаторных объектов, играет понятие разделимости. Разного вида редуцируемость бóльших объектов к меньшим рассматривается для многих классов математических объектов. Для класса многоместных квазигрупп, который замкнут относительно бесповторной суперпозиции, естественный вопрос представимости в виде такой суперпозиции возник на самом раннем этапе их исследования, как и вопрос существования неразделимых (не представимых в виде бесповторной суперпозиции) n-арных квазигрупп. Этот вопрос известен как одна из проблем В. Д. Белоусова (проблема номер 5 из монографии [5]) и решен для различных порядков в работах В. Д. Белоусова и М. Д. Сандика [6], Б. Р. Френкина [28], В. В. Борисенко [7], М. М. Глухова [9], М. А. Акивиса и В. В. Гольдберга [10], [11], [30], Кротова, В. В. Потапова и П. В. Соколовой [56]. Единственным известным в настоящее время способом строить неразделимые n-арные квазигруппы конечных порядков больше 3 является метод свитчинга, состоящий в локальной замене значений квазигруппы на некотором подмножестве области определения. (Следует заметить, что в алгебраической теории n-арных квазигрупп больше известно понятие приводимости, то есть представимости в виде бесповторной суперпозиции с тем же порядком переменных, что и в самой квазигруппе, см. напр. [5]. Это связано с тем, что порядок переменных существенен для выполнимости дополнительных алгебраических аксиом.) Крайне важным для пони-

мания структуры разделимых n-арных квазигрупп фактом является существование и в определенном смысле единственность канонического разложения в древовидную бесповторную суперпозицию неразделимых квазигрупп и групп, установленные А. В. Черемушкиным [29].

Разделимости квазигрупп посвящены три из четырех глав первой части диссертации. Первоначально исследования ориентировались на описание n-арных квазигрупп порядка 4, которое можно считать главным результатом первой части диссертации. Однако результат главы 2 в представленном виде — завершенное утверждение, применимое к n-арным квазигруппам произвольного порядка (результаты, дополняющие теорию именно для произвольного порядка, получены в последней совместной работе [XI]) и полезное для исследования классов многоместных квазигрупп, замкнутых относительно взятия ретракта (ретракт многоместной квазигруппы получается при фиксации константами значений одного или более аргументов). Примеры использования полученного в главе 2 признака разделимости для характеризации классов n-арных квазигрупп приведены в главе 3.

Совершенные коды. Согласно широко известной теореме В. А. Зиновьева, В. К. Леонтьева и Э. Титвайнена [13], [14], [75], при q равном степени простого числа нетривиальные (т. е. $0 < r < n/2$) r-совершенные коды существуют только в следующих случаях:

– 1-совершенные коды в $H_q^{(q^m-1)/(q-1)}$ с параметрами кода Хэмминга, который является единственным с точностью до эквивалентности линейным кодом из этого класса. (Р. У. Хэмминг рассматривал только двоичные коды [49]; общая конструкция, как и коды Голея, предложена М. Дж. Е. Голеем в полустраничной заметке [47].) Однако при непростых q существуют групповые (то есть замкнутые относительно сложения, но не обязательно относительно умножения на скаляр) 1-совершенные коды, неэквивалентные коду Хэмминга [60]. Число же негрупповых 1-совершенных кодов оценивается снизу дважды экспоненциальным относительно размерности пространства числом, см. последние нижние оценки в [V], [52].

– Коды Голея: построенные М. Дж. Е. Голеем [47] 3-совершенный код в H_2^{23} и 2-совершенный код в H_3^{11}. Каждый из этих кодов является единственным с точностью до эквивалентности [39].

Вопрос существования q-значных совершенных кодов в случае, когда q не есть степень простого числа, является известной открытой проблемой в общей теории совершенных кодов. Известно, что не существует t-совершенных кодов при $t \notin \{1, 2, 6, 8\}$ [32] и при $t > 1$ в случае $q = 2^\alpha 3^\beta$ [4]; известно, что не существует групповых совершенных кодов [58]; известно, что не существует 1-совершенного кода в H_6^7 [48] (последнее следует из несуществования двух ортогональных латинских квадратов размера 6×6 [74]) — наименьших параметрах, удовлетворяющих необходимым условиям: $n - 1 \equiv 0 \bmod q$ (следствие из теоремы Ллойда для произвольного алфавита [58], [3], [12]) и $q^{(n-1)/q+1} \equiv 0 \bmod (n(q-1)+1)$ ([51], [69], следствие равномерной распределенности вершин 1-совершенного кода по подкубам размерности $(n-1)/q+1$).

Существование совершенных кодов исследуется и в отличных от хэмминговых метрических пространствах и графах. Ввиду применимости мощного аппарата алгебраической теории графов, особый интерес с этой точки зрения уделяется дистанционно-регулярным графам. Так, известная гипотеза Дельсарта [12] о несуществовании нетривиальных совершенных кодов в графах Джонсона на данный момент не решена (см. последнюю работу [43] на эту тему и библиографию в ней), в то время как аналогичный факт для графов Грассмана и графов билинейных форм доказан относительно давно Л. Чихарой [37] (другое доказательство представлено У. Дж. Мартином и З. Дж. Жу [61]).

В главе 7 диссертации рассматриваются совершенные коды с расстоянием 3 в пространстве троичных n-слов веса $n-1$ (то есть содержащих ровно один нуль). Такие коды были построены в работах М. Сванстрёма [73], [72], Дж. Ван Линта и Л. Толхьюзена [77] на основе смежных классов по двоичному коду Хэмминга. В работе автора диссертации [53], уже используя технику из теории нелинейных совершенных кодов, построено дважды экспоненциальное число совершенных троичных равновесных кодов. В главе 7 показано, что на основе смежных классов по коду Хэмминга можно строить как неэквивалентные совершенные коды, так и коды с новыми параметрами — оптимальные коды с расстоянием 5, — в пространстве троичных n-слов веса $n-1$. Заметим, что хотя рассматриваемое пространство, в отличие от случая равновесных

двоичных кодов, не обладает свойством дистанционной регулярности, равновесные q-значные коды являются достаточно популярными объектами в теории кодирования.

Как уже было отмечено, над конечными полями непростой мощности возможно существование неэквивалентных 1-совершенных кодов, замкнутых относительно покоординатного сложения. В двоичном случае такой код единственный — код Хэмминга. Однако при помощи отображения Грея $0 \to 00$, $1 \to 01$, $2 \to 11$, $3 \to 10$, при покоординатном действии являющимся изометрией между $n/2$-мерным четверичным пространством с метрикой Ли и n-мерным двоичным пространством Хэмминга, некоторые нелинейные коды представимы в виде образов линейных кодов над кольцом Z_4 [50] (такие коды принято считать Z_4 линейными, в смысле [50]) или над смешанным Z_2Z_4 алфавитом. Возможность представлять хорошие нелинейные двоичные коды как линейные над недвоичными алгебраическими структурами была впервые обнаружена А. А. Нечаевым в работах [21], [22]. В статье А. Р. Хэммонса и др. [50] для подобного представления использованы изометрические свойства отображения Грея. Идея использования масштабных изометрий для построения кодов была развита в работе А. А. Нечаева и Т. Хонольда [23]. 1-Совершенные и расширенные 1-совершенные двоичные коды, представимые при помощи кода Грея как линейные коды над Z_4 или смешанным Z_2Z_4 алфавитом, изучались в работе [11] и в работах Дж. Боргеса, К. Т. Фелпса и Дж. Рифы [34], [67], [33]; оказалось, что число таких неэквивалентных кодов растет примерно как логарифм от длины, и значения параметров, характеризующих «близость» к линейному коду (ранг — размерность линейной оболочки; размерность ядра — множества периодов), для них различные. В диссертации (глава 8) предложен способ построения расширенных 1-совершенных кодов из линейных кодов над кольцом Z_{2^k}. Использованное обобщение отображения Грея неоднозначно при $k > 2$, что позволяет сохранить плотность упаковки.

Цель работы: построение новых классов n-арных квазигрупп и кодов — 1-совершенных двоичных кодов, а также бесконечного класса оптимальных троичных равновесных кодов с новыми параметрами; ха-

рактеризация классов n-арных квазигрупп малого порядка и линейных аналогов расширенных 1-совершенных кодов над кольцами Z_{2^k}; обнаружение новых зависимостей внутри исследуемых классов объектов.

Методы исследования. В исследованиях используются традиционные методы и аппарат алгебраической и комбинаторной теории кодирования, теории графов, комбинаторного анализа, метод свитчинга, суть которого состоит в локальном изменении объекта с сохранением его основных параметров, а также разработанные автором методы, в частности анализа разделимости n-арных квазигрупп.

Научная новизна. Основные результаты диссертации являются новыми и состоят в следующем:

1) Доказаны признаки разделимости n-арных квазигрупп: для порядка 4 в терминах связности прообраза двух значений и для произвольного порядка в терминах максимальной арности неразделимого ретракта.

2) Получена характеризация n-арных квазигрупп порядка 4: любая n-арная квазигруппа порядка 4 является полулинейной или разделимой. Показано, что все n-арные квазигруппы порядков 5 и 7, бинарные ретракты которых изотопны циклической группе, являются разделимыми при $n \geq 4$.

3) Введено понятие свитчинговой разделимости графов, которая эквивалентна разделимости n-арных квазигрупп, построенных по этим графам определенным образом. Показано, что если при удалении любой вершины или любых двух вершин графа получается разделимый подграф, то сам граф является разделимым. С другой стороны, построена бесконечная серия неразделимых графов, у которых удаление любой вершины приводит к разделимому подграфу. Это дает пример неразделимых n-арных квазигрупп, все $(n-1)$-арные ретракты которых разделимы.

4) Доказано, что любой, в том числе нелинейный, двоичный код с расстоянием 3 всегда можно вложить в 1-совершенный код некоторой большей длины.

5) Предложен метод построения 1-совершенных кодов, дающий самый многочисленный из известных в настоящий момент класс 1-совершенных двоичных кодов.

6) Построен бесконечный класс диаметрально совершенных (как следствие, оптимальных) троичных равновесных кодов с расстоянием 5.

7) Представлено новое обобщение отображения Грея $\Phi : Z_{2^k}^n \to Z_2^{2^{k-1}n}$, связанное с известным обобщенным отображением Грея φ следующим образом: если взять два дуальных линейных Z_{2^k}-кода и построить из них двоичные коды, используя обобщения φ и Φ отображения Грея, то весовые нумераторы полученных двоичных кодов будут связаны тождеством Мак-Вильямс. Описаны классы кодов Адамара и расширенных 1-совершенных кодов, полученных из линейных Z_{2^k}-кодов при помощи старого и нового обобщенного отображения Грея.

Теоретическая и практическая ценность. Работа носит теоретический характер. Полученные в ней результаты могут быть использованы в различных разделах общей теории n-арных квазигрупп, теории кодирования, криптографии, стеганографии.

Апробация работы. Результаты работы докладывались на научных семинарах «Математические вопросы кибернетики» ММФ НГУ, «Теория информации и теория кодирования» ИППИ РАН, семинаре Кафедры безопасности информационных систем ГУАП, «Теория кодирования» и Общеинститутском семинаре Института математики им. С. Л. Соболева СО РАН, в Похангском государственном университете (г. Поханг, Республика Корея, цикл из 6 лекций), включены в список важнейших научных результатов ИМ СО РАН за 2006, 2008 и 2009 годы, прошли апробацию на следующих научных конференциях и совещаниях:

- Международные конференции по алгебраической и комбинаторной теории кодирования ACCT (2002 в Царском Селе, 2004 в Болгарии, 2006 в Звенигороде);

- Международная конференция по оптимальным кодам и смежным вопросам OC 2005 (Болгария);
- Международная конференция по кодированию и криптографии WCC 2001 (Париж);
- Международная конференция по схемам отношений, кодам и дизайнам Com^{2}MaC 2004 (Ю. Корея);
- Международная конференция «Coding Theory Days in St.-Petersburg» (2008, Санкт-Петербург);
- Конференция «Математика в современном мире» (2007, Новосибирск);
- IX международный семинар «Дискретная математика и ее приложения» (2007, Москва);
- VI сибирская научная школа-семинар «Компьютерная безопасность и криптография» SIBECRYPT (2007, Горно-Алтайск);
- Конференции «Дискретный анализ и исследование операций» DAOR (2000, 2004, Новосибирск).

Публикации. Основные материалы диссертации опубликованы в 12 статьях в журналах, рекомендованных ВАК. Работы [XI] и [X], результаты которых изложены в главах 2 (кроме раздела 2.2) и 3, написаны в неразделимом соавторстве с Владимиром Николаевичем Потаповым. Работы [IV] и [V] (главы 5 и 6) — в неразделимом соавторстве с Сергеем Владимировичем Августиновичем. По главам, результаты опубликованы: глава 1 — [VII]; глава 2 — [IX], [XI]; глава 3 — [X], раздел 3.5 в [XI]; глава 4 — [XII], [VIII]; глава 5 — [IV]; глава 6 — [I], [V]; глава 7 — [VI]; глава 8 — [II], [III]. Большинство результатов были предварительно опубликованы в трудах и тезисах конференций [XIII]–[XXII].

Структура и объем работы. Диссертация состоит из введения, двух частей, разбитых на восемь глав, и списка литературы (158 наименований, включая 22 работы автора по теме диссертации, приведенные в конце списка). Текст работы изложен на 225 страницах.

СОДЕРЖАНИЕ РАБОТЫ

В первой части диссертации рассматриваются n-арные квазигруппы.

Множество Σ с определенной на нем n-арной операцией $f : \Sigma^n \to \Sigma$ называется n-арной квазигруппой порядка $|\Sigma|$, если в равенстве $f(x_1, \ldots, x_n) = x_{n+1}$ любые n элементов из $x_1, \ldots, x_n, x_{n+1}$ однозначно задают оставшийся элемент. Саму функцию f при этом будем также называть *n-арной квазигруппой*.

n-Арная квазигруппа f называется *разделимой*, если существуют такие $m \in \{2, \ldots, n-1\}$, $(n-m+1)$-арная квазигруппа h, m-арная квазигруппа g и перестановка $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, что

$$f(x_1, \ldots, x_n) \equiv h(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)})$$

(т. е. f есть суперпозиция h и g). Если n-арная квазигруппа не является разделимой, то она называется *неразделимой*.

Если у n-арной квазигруппы f или у функции, обратной ей по некоторому аргументу, зафиксировать один или более аргументов, то мы получим квазигруппу некоторой меньшей арности k, называемую *ретрактом* n-арной квазигруппы f.

n-Квазигруппы f и g называются *изотопными*, если для некоторого набора $\bar{\tau} = (\tau_0, \tau_1, \ldots, \tau_n)$ перестановок носителя Σ выполняется тождество $f(x_1, \ldots, x_n) \equiv \tau_0^{-1} g(\tau_1 x_1, \ldots, \tau_n x_n)$.

n-Арная квазигруппа $f : \Sigma^n \to \Sigma$ порядка 4 называется *полулинейной*, если для некоторых $a, b \in \Sigma$ характеристическая функция $\chi_{a,b}$ прообраза $f^{-1}(\{a, b\})$ представима в виде

$$\chi_{a,b}(x_1, \ldots, x_n) = \chi_1(x_1) + \cdots + \chi_n(x_n) \bmod 2$$

для некоторых $\chi_1, \ldots, \chi_n : \Sigma \to \{0, 1\}$. Заметим, что для фиксированных $\chi_1, \ldots, \chi_n$ существуст ровно 2^n полулинейных n-арных квазигрупп с данной $\chi_{a,b}$. Им можно поставить в соответствие n-местные булевы функции, задающие выбор значений a или b (в точках, где $\chi_{a,b} = 1$) и среди двух оставшихся элементов Σ (в точках, где $\chi_{a,b} = 0$) на определенных 2^n наборах из Σ^n так, что на оставшихся наборах f определяется однозначно.

В главе 1 доказан признак разделимости n-арных квазигрупп порядка 4 в терминах связности графа смежности прообраза двух выбранных значений $a, b \in \Sigma$. Пусть $\Sigma = \{0, 1, 2, 3\}$. Множество $S \subset \Sigma^n$ назовем 2-МДР-кодом (двукратным МДР-кодом) длины n, если для любого $\bar{x} \in \Sigma$ и для любой координаты $i \in \{1, \ldots, n\}$ найдется ровно два элемента множества S, совпадающих с $\bar{x}$ во всех позициях кроме может быть i-й. Для множества $S \subset \Sigma^n$ через $G(S)$ будем обозначать граф на множестве S, в котором два набора из этого множества соединены ребром тогда и только тогда, когда они различаются ровно в одной позиции.

Теорема 1 (следствие 1.17). *Граф $G(S)$ 2-МДР-кода S не связен тогда и только тогда, когда характеристическая функция множества S есть бесповторная сумма характеристических функций 2-МДР-кодов меньших длин.*

Теорема 2 (следствие 1.24). *Пусть $f : \Sigma^n \to \Sigma$ — n-арная квазигруппа, $a, b \in \Sigma$, $a \neq b$, число компонент связности 2-МДР-кода $f^{-1}(\{a, b\})$ равно K и $k = 1 + \log_2 K$.*

(a) *Если $1 < k < n$, то n-арная квазигруппа f является разделимой.*

(b) *Если $k = n$, то n-арная квазигруппа f является полулинейной.*

В главе 2 доказан признак разделимости n-арных квазигрупп произвольного порядка в терминах разделимости ретрактов:

Теорема 3 (теорема 2.1). *Пусть f — неразделимая n-арная квазигруппа, $n \geq 4$. Тогда f имеет неразделимый $(n-1)$-арный или $(n-2)$-арный ретракт. Более того, если порядок n-арной квазигруппы f конечный и простой, то f имеет неразделимый $(n-1)$-арный ретракт.*

Другими словами, если все $(n-1)$- и $(n-2)$-ретракты n-арной квазигруппы разделимы, то сама квазигруппа также разделима. Для разделимости n-арной квазигруппы простого конечного порядка достаточно разделимости всех ее $(n-1)$-арных ретрактов.

В главе 3 с использованием признаков разделимости из предыдущих глав доказана характеризация n-арных квазигрупп порядка 4:

Теорема 4 (теорема 3.3). *Каждая n-арная квазигруппа порядка 4 является разделимой или полулинейной.*

В доказательстве использованы признаки разделимости из предыдущих глав. Кроме того, эти признаки использованы для характеризации интересного подкласса класса n-арных квазигрупп порядков 5 и 7. Будем говорить, что n-арная квазигруппа порядка k *сублинейная*, если все ее бинарные ретракты изотопны циклической группе Z_k.

Теорема 5 (теорема 3.9). *Все сублинейные n-арные квазигруппы порядка 5 разделимы при $n \geq 4$. Все сублинейные n-арные квазигруппы порядка 7 разделимы при $n \geq 3$.*

Заметим, что существует пример неразделимой сублинейной тернарной квазигруппы порядка 5.

В главе 4 вводится понятие свитчингой разделимости графа, которое, в рамках описанного способа построения n-арных квазигрупп по графам, соответствует разделимости n-арных квазигрупп. Граф $G = (V, E)$ назовем *свитчингово разделимым*, если $|V| \geq 4$ и для некоторого полного двудольного графа $K_{U,V\setminus U} = (V, E_{U,V\setminus U})$ граф $(V, E \triangle E_{U,V\setminus U})$ (известный как U-свитчинг графа G) несвязный, причем каждая компонента связности содержит не более чем $n-2$ вершины. Для графов доказывается теорема, аналогичная теореме 3 для квазигрупп:

Теорема 6 (теорема 4.2). *Если все подграфы, порожденные $n-1$ или $n-2$ вершинами графа G порядка n свитчингово разделимы, то G — свитчингово разделимый граф.*

Формально, этот факт является следствием теоремы 3. Но его доказательство значительно проще, хотя и повторяет общий ход рассуждений разделов 2.2 и 2.5. Кроме того, доказано следующее:

Теорема 7 (теорема 4.3). *Для любого нечетного n существует свитчингово неразделимый граф порядка n, у которого все порожденные подграфы порядка $n-1$ свитчингово разделимы.*

Следствием для n-арных квазигрупп является следующий факт:

Теорема 8 (теорема 4.15). *Для любого четного n и любого целого $k > 0$ существует неразделимая n-арная квазигруппа f порядка $4k$, все $(n-1)$-арные ретракты которой являются разделимыми.*

Для n-арной квазигруппы f обозначим через $\kappa(f)$ наибольшую арность ее неразделимого ретракта. Из теоремы 8 следует, что условия теоремы 3, в которой утверждается, что из $\kappa(f) \leq n-3$ следует разделимость n-арной квазигруппы f, не могут быть в общем случае расширены до $\kappa(f) \leq n-2$.

Во второй части диссертации рассматриваются 1-совершенные двоичные коды или расширенные 1-совершенные двоичные коды, получаемые из 1-совершенных добавлением к каждому кодовому слову еще одного символа, равного сумме по модулю два всех остальных, а также коды с другими параметрами, так или иначе связанные с двоичными совершенными. Напомним, что *весом* кодового слова называется число ненулевых символов в этом слове, *(n, M, d)-кодом* называется код длины (длины кодовых слов) n, мощности M и попарным расстоянием не меньше d между кодовыми словами.

<u>В главе 5</u> доказана следующая теорема:

Теорема 9 (теорема 5.4). *Любой двоичный код $C \subset \{0,1\}^m$ с расстоянием не меньше 3 является укорочением некоторого 1-совершенного кода $P(C)$ длины $n = 2^m$, т. е.*

$$C = \{\iota \in F^m | (\iota, 0^{n-m}) \in P(C)\}.$$

Другими словами, любой двоичный код с расстоянием не меньше 3 вкладывается в 1-совершенный код некоторой большей длины. Простыми следствиями этого факта являются классические теоремы о вложении так называемых частичных систем троек и четверок Штейнера в полные системы [76], [45] (см. также обзоры в [59], [38]).

<u>В главе 6</u> приводится конструкция 1-совершенных двоичных кодов, дающая рекордную нижнюю оценку их числа:

Теорема 10 (теорема 6.15). *Число $B(n-1)$ 1-совершенных двоичных кодов длины $n-1 = 2^m - 1$ удовлетворяет неравенству*

$$B(n-1) \geq \widetilde{K}_{LA}(n) \stackrel{\text{def}}{=} \frac{n!}{6\left(\frac{n}{4}!\right)^4} \prod_{k=2,4,8,\ldots,\frac{n}{4}} \left(\left(2 \cdot 2^{-\frac{n}{k}} \binom{k}{k/2}^{\frac{n}{k}} \right)^{2^{\frac{n}{2k}-1}} - \binom{k}{k/2}^{\frac{n}{k}} \cdot 2^{-\frac{n}{2k}} \right)^{2^{\frac{n}{2k}-\log\frac{n}{2k}-1}}$$

$$\sim \frac{n!}{6\left(\frac{n}{4}!\right)^4} \prod_{k=2,4,8,\ldots,\frac{n}{4}} \left(2 \cdot 2^{-\frac{n}{k}} \binom{k}{k/2}^{\frac{n}{k}} \right)^{2^{\frac{n}{k}-\log\frac{n}{k}-1}}$$

В частности, $\widetilde{K}_{LA}(32) \approx 2^{2363.79}$.

Предыдущая оценка [I] состояла из двух мультипликативных членов ($t = 1, 2$) формулы. Заметим, что про асимптотику двойного логарифма числа $B(n)$ эта теорема не говорит ничего нового, со времен пионерской работы Ю. Л. Васильева [8] с этой точки зрения улучшения получено не было (известно, что асимптотика не меньше $n/2$ и не больше n). Ценность новой оценки не в формуле, а в том, что в рамках современного понимания проблемы 1-совершенных кодов оценку не удается асимптотически улучшить (даже умножив на константу, что нельзя было сказать про все предыдущие оценки). Можно сформулировать гипотезу, что полученная нижняя оценка асимптотически точна. В пользу этой гипотезы говорит тот факт, что приведенная конструкция накрывает почти все коды, размерность линейной оболочки которых на 1 или 2 превышает размерность линейного 1-совершенного кода, что следует из характеризации таких кодов в терминах n-арных квазигрупп порядка 4 [31] и асимптотики числа таких квазигрупп [25].

В главе 7 рассмотрено построение равновесных троичных кодов при помощи смежных классов по линейному 1-совершенному двоичному коду, коду Хемминга. Для удобства вместо слов длины n с весом (числом ненулевых элементов) $n-1$ рассматривается множество X^n слов в алфавите $\{0, 1, *\}$, содержащих ровно один символ $*$ (иногда этот символ удобно трактовать как $\{0, 1\}$, а слова из X^n — как пару соседних двоичных слов, или ребро двоичного графа Хемминга). Для двух двоичных кодов P, Q обозначим $R(P, Q) \stackrel{\text{def}}{=} \{\bar{r} \in X^n \mid d(x, P) = d(x, Q) = 1\}$, где

$d(\cdot,\cdot)$ — расстояние Хемминга. Пусть $n = 2^m \geq 4$ и $\alpha_1, \alpha_2, ..., \alpha_n$ — все элементы множества $\{0,1\}^m$. Для любого $\beta \in \{0,1\}^m$ определим множества

$$H^0_\beta \stackrel{\text{def}}{=} \{(x_1, x_2, ..., x_n) \in \{0,1\}^n \mid \sum_{i=1}^n x_i = 0, \sum_{i=1}^n x_i\alpha_i = \beta\},$$

$$H^1_\beta \stackrel{\text{def}}{=} \{(x_1, x_2, ..., x_n) \in \{0,1\}^n \mid \sum_{i=1}^n x_i = 1, \sum_{i=1}^n x_i\alpha_i = \beta\},$$

которые являются смежными классами по расширенному коду Хемминга. Следующая теорема обобщает результат [72], [77], где для каждого $n = 2^m$ был построен только один $(n, 2^n, 3)$-код.

Теорема 11 (теорема 7.9, следствие 7.16). *Пусть $f : \{0,1\}^m \to \{0,1\}^m$ — линейный оператор, удовлетворяющий следующим свойствам:*
a) f — биекция,
b) $f + \mathrm{Id}$ — биекция.
Множество $C_{H,f} \stackrel{\text{def}}{=} \bigcup_{\beta\in\{0,1\}^m} R(H^0_\beta, H^1_{f(\beta)})$ является совершенным $(n, 2^n, 3)$-кодом в X^n.

Более того, при $m \geq 4$ существует два оператора $f', f'' : \{0,1\}^m \to \{0,1\}^m$, удовлетворяющие условиям a) и b), такие, что совершенные коды $C_{H,f'}$ и $C_{H,f''}$ неэквивалентны, то есть не получаются друг из друга применением одновременно ко всем кодовым словам перестановки координат и/или инверсиями $0 \leftrightarrow 1$ символов в выбранных координатах.

Функция $f : \{0,1\}^m \to \{0,1\}^m$ называется *ПСН* функцией (*почти совершенно нелинейной*), если для любой пары $(a; b) \neq (0^m; 0^m)$ элементов $\{0,1\}^m$ система уравнений

$$\begin{cases} x + y = a \\ f(x) + f(y) = b \end{cases}$$

либо не имеет решения, либо имеет ровно два решения $(x; y)$ (другими словами, образы четырех точек, образующих невырожденный параллелограмм, никогда не образуют параллелограмм). Обозначим

$$Q_f \stackrel{\text{def}}{=} \{(x_1, x_2, ..., x_n) \in \{0,1\}^n \mid \sum_{i=1}^n x_i = 1, \sum_{i=1}^n x_i f(\alpha_i) = 0^m\}$$

Теорема 12 (теорема 7.20). *Если* $f : \{0,1\}^m \to \{0,1\}^m$ — *взаимнооднозначная ПСН функция, то множество* $R(H^0_{0^m}, Q_f)$ *является* $(n = 2^m, 2^{2^m-m-1}, 5)$*-кодом в* X^n.

Хорошо известно, что взаимнооднозначные ПСН функции, или ПСН перестановки (APN permutations) существуют при всех нечетных $m \geq 3$. При $m = 4$ такой перестановки не существует, а их существование при бо́льших четных m долгое время являлось открытой проблемой. Недавно [40] был найден первый пример ПСН перестановки для $m = 6$. Таким образом, построена бесконечная серия кодов с расстоянием 5 в X^n, причем нетрудно доказать, что построенные коды оптимальны, то есть имеют максимальную мощность среди кодов с расстоянием 5 в том же пространстве.

<u>В главе 8</u> рассматриваются двоичные коды, в том числе расширенные 1-совершенные, построенные из линейных кодов над кольцом Z_{2^k}. Для того, чтобы сформулировать результаты главы, нам понадобится несколько определений.

Пусть $m = 2^{k-1}$. Пусть $A \subset Z_2^m$ есть $(m, 2m, m/2)$-код Адамара и $A = \{a_0, a_1, \ldots, a_{2m-1}\}$, где a_0 есть слово из всех нулей и $a_i + a_{i+m}$ есть слово из всех единиц для каждого i от 0 до $m-1$. Определим *обобщенное отображение Грея* $\varphi : Z_{2m}^n \to Z_2^{mn}$ следующим правилом:

$$\varphi(x_1, \ldots, x_n) \stackrel{\text{def}}{=} (a_{x_1}, \ldots, a_{x_n}).$$

Известно [23], что φ является изометричным вложением пространства Z_{2m}^n со специально определенной метрикой в в mn-мерное двоичное пространство Хемминга.

Далее, пусть $\{H_0, \ldots, H_{2m-1}\}$ — разбиение Z_2^m на расширенные 1-совершенные $(m, 2^m/2m, 4)$-коды (например, в качестве H_0 мы можем взять расширенный код Хемминга, а в качестве остальных частей — смежные классы по нему). Более того, будем полагать, что H_0 содержит слово из всех нулей $\bar{0}$ и четность весов кодовых слов из H_j совпадает с четностью j.

Определим отображение $\Phi : Z_{2m}^n \to 2^{Z_2^{mn}}$ по правилу

$$\Phi(x_1, \ldots, x_n) \stackrel{\text{def}}{=} H_{x_1} \times \ldots \times H_{x_n}.$$

Для $C \subseteq Z_{2m}^n$, положим $\Phi(\mathcal{C}) \stackrel{\text{def}}{=} \bigcup_{\bar{x}\in\mathcal{C}} \Phi(\bar{x})$.

Линейные коды $\mathcal{C}, \mathcal{C}' \subseteq Z_{2m}^n$ называются *дуальными* друг другу, если $\mathcal{C}' = \{\bar{x} \mid \forall \bar{y} \in \mathcal{C} : \bar{x} \cdot \bar{y} = 0\}$, где $(x_1, ..., x_n) \cdot (y_1, ..., y_n) \stackrel{\text{def}}{=} x_1y_1 + \ldots + x_ny_n$. *Весовым нумератором* двоичного кода $C \subset \{0,1\}^N$ называется многочлен

$$W_C(X,Y) = \sum_{i=0}^{N} w_{C,i} X^{N-i} Y^i,$$

где $w_{C,i}$ — число слов кода C веса i. Известно [19], что весовые нумераторы дуальных двоичных кодов C и C' связаны тождеством Мак-Вильямс

$$W_{C'}(X,Y) = |C|^{-1} W_C(X+Y, X-Y).$$

Любые два кода C, C', для которых это тождество верно, называются *формально дуальными.*

Теорема 13 (теорема 8.10). *Пусть $\mathcal{C}$ и $\mathcal{C}'$ — дуальные линейные Z_{2^k}-коды. Тогда двоичные коды $\varphi(\mathcal{C})$ и $\Phi(\mathcal{C}')$ формально дуальны.*

Пусть $n = 2^r$ и $I = (i_1, \ldots, i_k)$ — набор неотрицательных целых чисел, удовлетворяющий равенству $1i_1 + 2i_2 + \ldots + ki_k = r$. Пусть $\bar{b}_1, \ldots, \bar{b}_n \in Z_{2^k}^{1+i_1+\ldots+i_k}$ — все элементы множества $\{1\} \times (2^{k-1}Z_{2^k})^{i_1} \times (2^{k-2}Z_{2^k})^{i_2} \times \ldots \times (2^0 Z_{2^k})^{i_k}$, упорядоченные лексикографически. Определим линейный $Z_{2^k}^n$-код

$$\mathcal{H}_I \stackrel{\text{def}}{=} \{\bar{h} = (h_1, \ldots, h_n) \in Z_{2^k}^n \mid \sum_{j=1}^{n} h_j \bar{b}_j = B_I \bar{h}^T = \bar{0}\},$$

дуальный ему код обозначим через $\mathcal{D}_I$.

Теорема 14 (теоремы 8.14, 8.17). *Код $\Phi(\mathcal{H}_I)$ является двоичным $(nm, 2^{nm}/2nm, 4)$-кодом, т. е. расширенным 1-совершенным кодом. Код $\varphi(\mathcal{D}_I)$ является двоичным $(n2^{k-1}, n2^k, n2^{k-2})$-кодом, т. е. кодом Адамара.*

Теорема 15 (теорема 8.21). *Если $\mathcal{H}$ — линейный $Z_{2^k}^n$-код такой, что двоичный код $\Phi(\mathcal{H})$ является расширенным 1-совершенным кодом, то $\mathcal{H}$ эквивалентен одному из кодов $\mathcal{H}_I$, т. е. получается из него перестановкой координат и умножением некоторых координат на константы.*

Список литературы

[1] *Августинович С. В.* Об одном свойстве совершенных двоичных кодов // *Дискрет. анализ и исслед. операций. Сер. 1.* — 1995. — Т. 2, № 1. — С. 4–6. http://mi.mathnet.ru/da450.

[2] *Августинович С. В., Соловьева Ф. И.* Построение совершенных двоичных кодов последовательными сдвигами $\bar{a}$-компонент // *Проблемы передачи информации.* — 1997. — Т. 33, № 3. — С. 15–21. http://mi.mathnet.ru/ppi374.

[3] *Бассалыго Л. А.* Обобщение теоремы Ллойда на произвольный алфавит // *Проблемы управления и теории информации.* — 1973. — Т. 2, № 2. — С. 133–137.

[4] *Бассалыго Л. А., Зиновьев В. А., Леонтьев В. К., Фельдман Н. И.* Несуществование совершенных кодов для некоторых составных алфавитов // *Проблемы передачи информации.* — 1975. — Т. 11, № 3. — С. 3–13. http://mi.mathnet.ru/ppi1590.

[5] *Белоусов В. Д.* n-Арные квазигруппы. — Кишинев: Штиинца, 1972.

[6] *Белоусов В. Д., Сандик М. Д.* n-арные квази-группы и лупы // *Сибирский математический журнал.* — 1966. — Т. 7, № 1. — С. 31–54.

[7] *Борисенко В. В.* Неприводимые n-квазигруппы на конечных множествах составного порядка // Квазигруппы и лупы. — Кишинев: Штиинца, 1979. — Т. 51 из *Мат. Исслед.* — С. 38–42.

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

[9] *Глухов М. М.* О многообразиях (i, j)-приводимых n-квазигрупп // Сети и квазигруппы. — Кишинев: Штиинца, 1976. — Т. 39 из *Мат. Исслед.* — С. 67–72.

[10] *Гольдберг В. В.* Об инвариантной характеристике некоторых условий замыкания в тернарных квазигруппах // *Сибирский математический журнал.* — 1975. — Т. 16, № 1. — С. 29–43.

[11] *Гольдберг В. В.* О приводимых, групповых и $(2n + 2)$-эдричных $(n + 1)$-тканях многомерных поверхностей // *Сибирский математический журнал.* — 1976. — Т. 17, № 1. — С. 44–57.

[12] *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования: Пер. с англ. Библиотека Кибернетического Сборника. — М.: Мир, 1976. — 136 с.

[13] *Зиновьев В. А., Леонтьев В. К.* О совершенных кодах // *Проблемы передачи информации.* — 1972. — Т. 8, № 1. — С. 26–35. http://mi.mathnet.ru/ppi772.

[14] *Зиновьев В. А., Леонтьев В. К.* Несуществование совершенных кодов над полями Галуа // *Проблемы управления и теории информации.* — 1973. — Т. 2, № 2. — С. 123–132.

[15] *Зиновьев В. А., Лобстейн А.* Об обобщенных каскадных конструкциях совершенных двоичных нелинейных кодов // *Проблемы передачи информации.* — 2000. — Т. 36, № 4. — С. 59–73. http://mi.mathnet.ru/ppi495.

[16] *Кротов Д. С., Потапов В. Н.* О свитчинговой эквивалентности n-арных квазигрупп порядка 4 и совершенных двоичных кодов // *Проблемы передачи информации.* — 2010. — Т. 46, № 3. — С. 22–28. http://mi.mathnet.ru/ppi2019.

[17] *Лось А. В.* Построение совершенных q-значных кодов последовательными сдвигами $\tilde{\alpha}$-компонент // *Проблемы передачи информации.* — 2004. — Т. 40, № 1. — С. 40–47. http://mi.mathnet.ru/ppi122.

[18] *Лось А. В.* Построение совершенных q-ичных кодов свитчингами простых компонент // *Проблемы передачи информации.* — 2006. — Т. 42, № 1. — С. 34–42. http://mi.mathnet.ru/ppi35.

[19] *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки: Пер. с англ. — М.: Связь, 1979. — 744 с.

[20] *Малюгин С. А.* О нижней оценке числа совершенных двоичных кодов // *Дискрет. анализ и исслед. операций. Сер. 1.* — 1999. — Т. 6, № 4. — С. 44–48. http://mi.mathnet.ru/da327.

[21] *Нечаев А. А.* Функции «след» в кольце Галуа и помехоустойчивые коды // Тезисы сообщений V Всесоюзн. симп. по теории колец, алгебр и модулей. — Новосибирск, Россия: 1982. — С. 97.

[22] *Нечаев А. А.* Код кердока в циклической форме // *Дискретная математика.* — 1989. — Т. 1, № 4. — С. 123–139. http://mi.mathnet.ru/dm948.

[23] *Нечаев А. А., Хонольд Т.* Полновесные модули и представления кодов // *Проблемы передачи информации.* — 1999. — Т. 35, № 3. — С. 18–39. http://mi.mathnet.ru/ppi450.

[24] *Потапов В. Н.* О дополняемости частичных n-квазигрупп порядка 4 // *Математические труды.* — 2010. — Подано в печать.

[25] *Потапов В. Н., Кротов Д. С.* Асимптотика числа n-квазигрупп порядка 4 // *Сибирский математический журнал.* — 2006. — Т. 47, № 4. — С. 873–887. http://mi.mathnet.ru/smj902.

[26] *Потапов В. Н., Кротов Д. С.* О числе n-арных квазигрупп конечного порядка // *Дискретная математика.* — 2010. — Принято в печать.

[27] *Романов А. М.* О разбиениях q-ичных кодов хемминга на непересекающиеся компоненты // *Дискрет. анализ и исслед. операций. Сер. 1.* — 2004. — Т. 11, № 3. — С. 80–87. http://mi.mathnet.ru/da114.

[28] *Фрейкин Б. Р.* О приводимости и сводимости в некоторых классах n-группоидов. II. — Кишинев: Штиинца, 1972. — Т. 7:1(23) из *Мат. Исслед.* — С. 150–162.

[29] *Черемушкин А. В.* Каноническая декомпозиция n-арных квазигрупп // Исследование операций и квазигрупп. — Кишинев: Штиинца, 1988. — Т. 102 из *Мат. Исслед.* — С. 97–105.

[30] *Akivis M. A., Goldberg V. V.* Solution of Belousov's problem // *Discuss. Math., Gen. Algebra Appl.* — 2001. — Vol. 21, no. 1. — Pp. 93–103.

[31] *Avgustinovich S. V., Heden O., Solov'eva F. I.* The classification of some perfect codes // *Des. Codes Cryptography.* — 2004. — Vol. 31, no. 3. — Pp. 313–318. — DOI: 10.1023/B:DESI.0000015891.01562.c1.

[32] *Best M. R.* Perfect codes hardly exist // *IEEE Trans. Inf. Theory.* — 1983. — Vol. 29, no. 3. — Pp. 349–351. — DOI: 10.1109/TIT.1983.1056677.

[33] *Borges J., Phelps K. T., Rifà J.* The rank and kernel of extended 1-perfect Z_4-linear and additive non-Z_4-linear codes // *IEEE Trans. Inf. Theory.* — 2003. — Vol. 49, no. 8. — Pp. 2028–2034. — DOI: 10.1109/TIT.2003.814490.

[34] *Borges J., Rifà J.* A characterization of 1-perfect additive codes // *IEEE Trans. Inf. Theory.* — 1999. — Vol. 45, no. 8. — Pp. 1688–1697. — DOI: 10.1109/18.771247.

[35] *Brouwer A. E., Cohen A. M., Neumaier A.* Distance-Regular Graphs. — Berlin: Springer-Verlag, 1989.

[36] *Carlet C.* Boolean Functions for Cryptography and Error-Correcting Codes // Boolean Models and Methods in Mathematics, Computer Science,

and Engineering / Ed. by Y. Crama, L. Hammer. — Cambridge Univ. Press, 2010. — Vol. 134 of *Encycl. Math. Appl.* — Pp. 257–397.

[37] *Chihara L.* On the zeros of the askey–wilson polynomials, with applications to coding theory // *SIAM J. Math. Anal.* — 1987. — Vol. 18, no. 1. — Pp. 191–207. — DOI: 10.1137/0518015.

[38] *Colbourn C. J., Rosa A.* Triple Systems. — Oxford: Clarendon Press, 1999.

[39] *Delsarte P., Goethals J. M.* Unrestricted codes with the Golay parameters are unique // *Discrete Math.* — 1975. — Vol. 12, no. 3. — Pp. 211–224. — DOI: 10.1016/0012-365X(75)90047-3.

[40] *Dillon J. F.* APN polynomials: An update. — Fq9, International Conference on Finite Fields and their Applications. — 2009. — http://mathsci.ucd.ie/~gmg/Fq9Talks/Dillon.pdf.

[41] *Dörnte W.* Untersuchungen über einen verallgemeinerten Gruppenbegrieff // *Mathematische Zeitschrift.* — 1928. — Vol. 29. — Pp. 1–19.

[42] *Etzion T.* Nonequivalent q-ary perfect codes // *SIAM J. Discrete Math.* — 1996. — Vol. 9, no. 3. — Pp. 413–423.

[43] *Etzion T., Schwartz M.* Perfect constant-weight codes // *IEEE Trans. Inf. Theory.* — 2004. — Vol. 50, no. 9. — Pp. 2156–2165. — DOI: 10.1109/TIT.2004.833355.

[44] *Finizio N. J., Lewis J. T.* Enumeration of maximal codes // *Congr. Numer.* — 1994. — Vol. 102. — Pp. 139–145.

[45] *Ganter B.* Finite partial quadruple systems can be finitely embedded // *Discrete Math.* — 1974. — Vol. 10, no. 2. — Pp. 397–400. — DOI: 10.1016/0012-365X(74)90130-7.

[46] *Godsil C. D.* Algebraic Combinatorics. — New York: Chapman and Hall, 1993.

[47] *Golay M. J. E.* Notes on digital coding // *Proc. IRE.* — 1949. — Vol. 37, no. 6. — P. 657. — DOI: 10.1109/JRPROC.1949.233620.

[48] *Golomb S. W., Posner E. C.* Rook domains, latin squares, and error-distributing codes // *IEEE Trans. Inf. Theory.* — 1964. — Vol. 10, no. 3. — Pp. 196–208. — DOI: 10.1109/TIT.1964.1053680.

[49] *Hamming R. W.* Error detecting and error correcting codes // *Bell Syst. Tech. J.* — 1950. — Vol. 29, no. 2. — Pp. 147–160.

[50] *Hammons A. R., Jr, Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.* The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes // *IEEE Trans. Inf. Theory.* — 1994. — Vol. 40, no. 2. — Pp. 301–319. — DOI: 10.1109/18.312154.

[51] *Heden O.* A Study of Mixed Perfect Codes: Thesis / University of Stockholm. — Stockholm,, 1977.

[52] *Heden O., Krotov D. S.* On the structure of non-full-rank perfect q-ary codes // *Adv. Math. Commun.* — 2010. — Accepted. Eprint version: http://arXiv.org/abs/1001.0001.

[53] *Krotov D. S.* Inductive constructions of perfect ternary constant-weight codes with distance 3 // *Probl. Inf. Transm.* — 2001. — Vol. 37, no. 1. — Pp. 1–9. — DOI: 10.1023/A:1010424208992.

[54] *Krotov D. S.* On the binary codes with parameters of doubly-shortened 1-perfect codes // *Des. Codes Cryptography.* — 2010. — Vol. 57, no. 2. — Pp. 181–194. — DOI: 10.1007/s10623-009-9360-5.

[55] *Krotov D. S., Potapov V. N.* On the reconstruction of n-quasigroups of order 4 and the upper bounds on their number // Proc. the Conference Devoted to the 90th Anniversary of Alexei A. Lyapunov. — Novosibirsk, Russia: 2001. — October. — Pp. 323–327. — http://www.sbras.ru/ws/Lyap2001/2363.

[56] *Krotov D. S., Potapov V. N., Sokolova P. V.* On reconstructing reducible n-ary quasigroups and switching subquasigroups // *Quasigroups Relat. Syst.* — 2008. — Vol. 16, no. 1. — Pp. 55–67.

[57] *Laywine C. F., Mullen G. L.* Discrete Mathematics Using Latin Squares. — Wiley, New York, 1998.

[58] *Lenstra Jr H. W.* Two theorems on perfect codes // *Discrete Math.* — 1972. — Vol. 3, no. 1-3. — Pp. 125–132. — DOI: 10.1016/0012-365X(72)90028-3.

[59] *Lindner C. C.* A survey of embedding theorems for Steiner sysrems // Topics on Steiner Systems / Ed. by C. C. Lindner, A. Rosa. — North-Holland, 1980. — Vol. 7 of *Ann. Discrete Math.* — Pp. 175–202.

[60] *Lindström B.* On group and nongroup perfect codes in q symbols // *Math. Scand.* — 1969. — Vol. 25. — Pp. 149–158. — http://www.mscand.dk/article.php?id=1942.

[61] *Martin W. J., Zhu X. J.* Anticodes for the grassman and bilinear forms graphs // *Des. Codes Cryptography.* — 1995. — Vol. 6, no. 1. — Pp. 73–79. — DOI: 10.1007/BF01390772.

[62] *McKay B. D., Wanless I. M.* Combinatorial data. Latin cubes and hypercubes. — http://cs.anu.edu.au/~bdm/data/latincubes.html.

[63] *McKay B. D., Wanless I. M.* A census of small Latin hypercubes // *SIAM J. Discrete Math.* — 2008. — Vol. 22, no. 2. — Pp. 719–736. — DOI: 10.1137/070693874.

[64] *Östergård P. R. J., Pottonen O.* Two optimal one-error-correcting codes of length 13 that are not doubly shortened perfect codes // *Des. Codes Cryptography.* — 2010. — To appair.

[65] *Phelps K. T.* A general product construction for error correcting codes // *SIAM J. Algebraic Discrete Methods.* — 1984. — Vol. 5, no. 2. — Pp. 224–228. — DOI: 10.1137/0605023.

[66] *Phelps K. T.* A product construction for perfect codes over arbitrary alphabets // *IEEE Trans. Inf. Theory.* — 1984. — Vol. 30, no. 5. — Pp. 769–771. — DOI: 10.1109/TIT.1984.1056963.

[67] *Phelps K. T., Rifà J.* On binary 1-perfect additive codes: Some structural properties // *IEEE Trans. Inf. Theory.* — 2002. — Vol. 48, no. 9. — Pp. 2587–2592. — DOI: 10.1109/TIT.2002.801474.

[68] *Potapov V. N.* On completion of latin hypercuboids of order 4 // Proc. Twelfth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT 2010. — Novosibirsk, Russia: 2010. — September. — Pp. 251–255.

[69] *Roos C.*: Preprint: Delft, the Netherlands, 1979.

[70] *Schönheim J.* On linear and nonlinear single-error-correcting q-ary perfect codes // *Inform. Contr.* — 1968. — Vol. 12, no. 1. — Pp. 23–26. — DOI: 10.1016/S0019-9958(68)90167-8.

[71] *Shcherbacov V. A.* Quasigroups in cryptology: E-print 1007.3572: arXiv.org, 2010. — Available at http://arxiv.org/abs/1007.3572.

[72] *Svanström M.* A class of perfect ternary constant-weight codes // *Des. Codes Cryptography.* — 1999. — Vol. 18, no. 1-3. — Pp. 223–230. — DOI: 10.1023/A:1008361925021.

[73] *Svanström M.* Ternary Codes with Weight Constraints: Dissertation 572 / Linköping University. — 1999.

[74] *Tarry G.* Le problème des 36 officers // *Comptes Rendu de l'Association Française pour l'Avancement de Science Naturel (National Academy of Sciences).* — 1900, 1901. — Vol. 1, 2. — Pp. 122–123, 170–203.

[75] *Tietäväinen A.* On the nonexistence of perfect codes over finite fields // *SIAM J. Appl. Math.* — 1973. — Vol. 24. — Pp. 88–96.

[76] *Treash C.* The completion of finite incomplete Steiner triple systems with applications to loop theory // *J. Comb. Theory, Ser. A.* — 1971. — Vol. 10, no. 3. — Pp. 259–265. — DOI: 10.1016/0097-3165(71)90030-6.

[77] *van Lint J., Tolhuizen L.* On perfect ternary constant-weight codes // *Des. Codes Cryptography.* — 1999. — Vol. 18, no. 1-3. — Pp. 231–234. — DOI: 10.1023/A:1008314009092.

Публикации автора по теме диссертации

[I] *Кротов Д. С.* Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // *Дискрет. анализ и исслед. операций. Сер. 1.* — 2000. — Т. 7, № 2. — С. 47–53. http://mi.mathnet.ru/da261.

[II] *Кротов Д. С.* Z_4-линейные совершенные коды // *Дискрет. анализ и исслед. операций. Сер. 1.* — 2000. — Т. 7, № 4. — С. 78–90. http://mi.mathnet.ru/da281.

[III] *Krotov D. S.* Z_{2^k}-Dual binary codes // *IEEE Trans. Inf. Theory.* — 2007. — Vol. 53, no. 4. — Pp. 1532–1537. — DOI: 10.1109/TIT.2007.892787.

[IV] *Avgustinovich S. V., Krotov D. S.* Embedding in a perfect code // *J. Comb. Des.* — 2009. — Vol. 17, no. 5. — Pp. 419–423. — DOI: 10.1002/jcd.20207.

[V] *Krotov D. S., Avgustinovich S. V.* On the number of 1-perfect binary codes: A lower bound // *IEEE Trans. Inf. Theory.* — 2008. — Vol. 54, no. 4. — Pp. 1760–1765. — DOI: 10.1109/TIT.2008.917692.

[VI] *Krotov D. S.* On diameter perfect constant-weight ternary codes // *Discrete Math.* — 2008. — Vol. 308, no. 14. — Pp. 3104–3114. — DOI: 10.1016/j.disc.2007.08.037.

[VIII] *Krotov D. S.* On irreducible n-ary quasigroups with reducible retracts // *Eur. J. Comb.* — 2008. — Vol. 29, no. 2. — Pp. 507–513. — DOI: 10.1016/j.ejc.2007.01.005.

[VII] *Krotov D. S.* On decomposability of 4-ary distance 2 MDS codes, double-codes, and n-quasigroups of order 4 // *Discrete Math.* — 2008. — Vol. 308, no. 15. — Pp. 3322–3334. — DOI: 10.1016/j.disc.2007.06.038.

[IX] *Krotov D. S.* On reducibility of n-ary quasigroups // *Discrete Math.* — 2008. — Vol. 308, no. 22. — Pp. 5289–5297. — DOI: 10.1016/j.disc.2007.08.099.

[X] *Krotov D. S., Potapov V. N.* n-Ary quasigroups of order 4 // *SIAM J. Discrete Math.* — 2009. — Vol. 23, no. 2. — Pp. 561–570. — DOI: 10.1137/070697331.

[XI] *Krotov D. S., Potapov V. N.* On connection between reducibility of an n-ary quasigroup and that of its retracts // *Discrete Math.* — 2011. — Vol. 311, no. 1. — Pp. 58–66. — DOI: 10.1016/j.disc.2010.09.023

[XII] *Кротов Д. С.* О связи свитчинговой разделимости графа и его подграфов // *Дискрет. анализ и исслед. операций.* — 2010. — Т. 17, № 2. — С. 46–56. http://mi.mathnet.ru/da605.

Труды конференций и тезисы

[XIII] *Krotov D. S.* Z_4-linear Hadamard and extended perfect codes // WCC2001, International Workshop on Coding and Cryptography. — Elsevier B.V., 2001. — Vol. 6 of *Electron. Notes Discrete Math.* — Pp. 107–112. — DOI: 10.1016/S1571-0653(04)00161-1.

[XIV] *Krotov D. S.* On decomposition of $(n, 4^{n-1}, 2)_4$ MDS codes and double-codes // Proc. Eighth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT-VIII. — Tsarskoe Selo, Russia: 2002. — September. — Pp. 168–171.

[XV] *Krotov D. S.* On decomposability of distance 2 MDS codes // Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT'2004. — Kranevo, Bulgaria: 2004. — June. — Pp. 247–253.

[XVI] *Krotov D. S.* Z_{2^k}-duality, Z_{2^k}-linear Hadamard codes, and co-Z_{2^k}-linear extended perfect codes // Proc. Fourth Int. Workshop on Optimal Codes and Related Topics. — Pamporovo, Bulgaria: 2005. — June. — Pp. 205–213.

[XVII] *Krotov D. S.* On irreducible n-quasigroups with reducible $(n-1)$-ary retracts // Proc. Tenth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT-10. — Zvenigorod, Russia: 2006. — September. — Pp. 157–160.

[XVIII] *Krotov D., Avgustinovich S.* On the number of 1-perfect binary codes: a lower bound // Proc. Tenth Int. Workshop on Algebraic and Combinatorial Coding Theory ACCT-10. — Zvenigorod, Russia: 2006. — September. — Pp. 161–164.

[XIX] *Avgustinovich S. V., Krotov D. S.* Embedding in a perfect code // Coding Theory Days in St.Petersburg. — St.Petersburg: 2008. — September. — Pp. 37–39.

[XX] *Krotov D. S., Avgustinovich S. V.* On the number of perfect binary codes. A lower bound // Proc. the conference "Discrete Analysis and Operations Research" DAOR'2004. — Novosibirsk, Russia: 2004. — June–July. — P. 95. — http://www.math.nsc.ru/conference/DAOR'04/daor04.pdf.

[XXI] *Кротов Д. С., Потапов В. Н.* Описание n-арных квазигрупп порядка 4 // «Математика в современном мире». Российская конференция, посвященная 50-летию Института математики им. С. Л. Соболева СО РАН. Тезисы докладов. — Новосибирск: 2007. — Сент. — С. 36. — http://math.nsc.ru/conference/conf50/Abstracts.pdf.

[XXII] *Кротов Д. С., Потапов В. Н.* О приводимости n-арных квазигрупп и свитчинговой разделимости графов // IX Международный семинар «Дискретная математика и ее приложения», посвященный 75-летию со дня рождения академика О. Б. Лупанова. Тезисы докладов. — Москва: 2007. — Июнь. — С. 432–434.

Кротов Денис Станиславович

Совершенные коды и n-арные квазигруппы: конструкции и классификация

Автореферат
диссертации на соискание ученой степени
доктора физико-математических наук

Подписано в печать 28.12.2010. Формат 60x84 1/16.
Усл. печ. л. 2,0. Уч.-изд. л. 2,0. Тираж 100 экз. Заказ № 169

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