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

На правах рукописи

УДК 519.725

Лось Антон Васильевич

Свитчинговые методы построения совершенных q-значных кодов

Специальность 01.01.09 — дискретная математика
и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Новосибирск, 2008

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

Научный руководитель:	кандидат физико-математических наук, доцент Ф. И. Соловьева
Официальные оппоненты:	доктор физико-математических наук, профессор В. А. Зиновьев
	кандидат физико-математических наук, доцент А. Л. Пережогин
Ведущая организация:	факультет ВМК МГУ имени М. В. Ломоносова

Защита состоится 14 мая 2008 г. в 16 часов 00 минут на заседании диссертационного совета Д 003.015.01 при Институте математики им. С. Л. Соболева СО РАН по адресу: пр. Академика Коптюга 4, г. Новосибирск, 630090.

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

Автореферат разослан 14 апреля 2008 г.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Объектом исследования настоящей работы являются блочные коды над недвоичным алфавитом, исправляющие случайные ошибки. В условиях современной жизни теория кодирования имеет широкое практическое применение в системах цифровой связи и в устройствах хранения информации.

Предметом исследования данной диссертации являются совершенные коды в алфавите из более чем двух символов. Код над полем Галуа $GF(q)$ называется *совершенным*, если совокупность шаров некоторого радиуса, окружающих кодовые слова, задает разбиение всего пространства. Согласно широко известной теореме В. А. Зиновьева и В. К. Леонтьева, полученной независимо Э. Титвайненом, см. [3, 4, 16], нетривиальные совершенные q-значные коды длины N существуют только при $N = (q^m - 1)/(q - 1)$, где m — любое натуральное число не меньшее двух, такие коды имеют кодовое расстояние 3 и исправляют одну ошибку; при $N = 23$ — это двоичный код Голея с кодовым расстоянием 7, а также при $N = 11$ — это троичный код Голея с кодовым расстоянием 5. Оба кода Голея единственны с точностью до эквивалентности. Совершенные коды представляют собой один из наиболее важных предметов теории блочных кодов, исправляющих ошибки, поскольку они обладают важным свойством — оптимальностью, т. е. при заданной длине кода и кодовом расстоянии мощность кода максимальна.

В качестве основных задач теории кодирования выделяют разработку методов построения кодов, исследование свойств кодов, разработку эффективных методов кодирования и декодирования. Несмотря на активные исследования целого ряда ученых в области теории кодирования, остается открытым множество проблем, связанных с совершенными кодами. Например, по-прежнему остается нерешенной основная проблема построения и перечисления совершенных q-значных кодов для q, равного степени простого числа. Эта проблема включает в себя разработку методов построения кодов, а также методов

исследования свойств отдельных классов кодов с заданными характеристиками (параметрами или свойствами).

Ряд задач теории кодирования являются важными и для других математических дисциплин: комбинаторного анализа, теории групп, теории графов, криптологии. Таковой, например, является проблема упаковки шарами одного радиуса. Кроме того, многие из методов построения и изучения свойств совершенных q-значных кодов применяются для кодов с другими параметрами, например, для кодов с большими кодовыми расстояниями, которые способны обнаруживать и исправлять большее число ошибок.

Самостоятельный интерес в теории кодирования представляют собой исследования различных свойств кодов таких, как изучение групп автоморфизмов кодов, исследование спектральных свойств кодов, построение и исследование разбиений q-значного n-мерного куба на коды, исследование рангов и ядер кодов, пересечения кодов.

Все результаты данного исследования верны и для двоичных кодов, но в этом случае они преобразуются в уже известные, поскольку особенность строения многозначных полей является для данного исследования существенно важным.

Цель данной работы состоит в разработке новых методов построения совершенных кодов над недвоичным алфавитом, исследовании свойств таких кодов.

Методика исследований. В диссертации используются известные методы и аппарат алгебраической и комбинаторной теории кодирования, комбинаторного анализа. Для исследования свойств кодов применены методы построения кодов, предложенные в диссертации.

Научная новизна. Все результаты, представленные в диссертации, являются новыми. В работе предложено три разных свитчинговых метода построения совершенных q-значных кодов, а также применение этих методов для исследования пере-

сечений совершенных q-значных кодов (проблема Т. Этциона и А. Варди).

1. В диссертации предложено развитие свитчингового метода построения и исследования нелинейных кодов — метода $\widetilde{\alpha}$-компонент, который был предложен С. В. Августиновичем и Ф. И. Соловьевой в 1996 году и применен для построения широкого класса двоичных совершенных кодов.

2. Была предложена оригинальная модификация этого метода посредством так называемых конфигураций — перестановок, действующих на q элементах алфавита. Такие преобразования элементов q-значного алфавита значительно расширяют произвол в выборе сдвигаемого множества, не имеют аналогий в двоичном случае и позволяют получить более обширный класс совершенных кодов по сравнению с классом кодов, построенных методом свитчинга $\widetilde{\alpha}$-компонент.

3. Разработан новый метод свитчинга простых компонент для совершенных q-значных кодов над расширением простого поля, то есть при $q = p^r, r > 1$. Этот метод позволил получить широкий класс различных совершенных q-значных кодов и, как следствие, рекордную на сегодняшний день нижнюю оценку числа таких кодов. Показано, что в коде Хэмминга не существует i-компонент меньшей мощности, чем простая i-компонента специального вида. Этот факт свидетельствует о том, что полученная оценка не может быть существенно улучшена методом свитчинга компонент. Простые компоненты были введены К. Т. Фелпсом, Й. Рифой и М. Вилланувеой для исследования свойств специального вида линейных подкодов (p-ядер) q-значных кодов Хэмминга в работе [14].

4. Впервые исследована проблема пересечений совершенных нелинейных q-значных кодов, $q > 2$. Используя предложенные свитчинговые методы построения совершенных q-значных кодов, получен широкий спектр возможных пересечений таких кодов. Для любого допустимого $N = (q^m - 1)/(q - 1)$, где m — целое число, сконструированы также два кода, пересечение которых меньше, чем пересече-

ние, которое может быть получено применением свитчинговых методов.

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 q-значных кодов, для построения кодов с большими кодовыми расстояниями, для исследования свойств q-значных кодов; в криптографии (в схемах распределения секрета, см. [9]), комбинаторике. Возможно практическое применение для передачи информации по каналам связи, допускающим больше двух состояний сигнала, например, в оптоволоконных сетях.

Апробация работы. Все результаты работы были апробированы на следующих международных конференциях: на конференциях по алгебраической и комбинаторной теории кодирования ACCT-IX (Кранево, Болгария, 2004 г.), ACCT-X (Звенигород, 2006 г.); на конференции по дискретному анализу и исследованию операций DAOR-2004 (Новосибирск, 2004 г.); на конференции по оптимальным кодам и смежным областям OC'2005 (Пампорово, Болгария, 2005 г.); на международной конференции "Математика в современном мире" (Новосибирск, 2007 г.). Результаты диссертации докладывались на семинаре "Теория информации и теория кодирования" ИППИ РАН, на семинаре "Синтез управляющих систем" мехмата МГУ, на семинаре "Дискретная математика и математическая кибернетика" факультета ВМК МГУ, на семинаре "Дискретный анализ" Института математики СО РАН. Все результаты были доложены на семинаре НГУ и Института математики СО РАН "Теория кодирования".

Публикации. Основное содержание диссертации отражено в 6 печатных работах. Среди них 3 работы в журналах из перечня ВАК, 3 работы в рецензируемых трудах международных конференций.

Основные результаты диссертации.

1. Для совершенных q-значных кодов, $q > 2$, развит свитчинговый метод построения и исследования свойств кодов, известный как метод $\widetilde{\alpha}$-компонент.

2. Предложена модификация метода свитчинга компонент q-значного, $q > 2$, кода Хэмминга посредством конфигураций. Такие преобразования присущи q-значным, $q > 2$, кодам и не имеют аналогов в двоичном случае.

3. Предложен комбинаторный метод построения и исследования свойств q-значных кодов, для $q = p^r, r > 1$ – метод свитчинга простых компонент. Метод позволил построить обширный класс различных совершенных q-значных кодов длины $N = qn + 1 = (q^m - 1)/(q - 1)$, которых оказалось не менее

$$(p!)^{q^{n(\frac{2r-1}{r})-(m-1)}} \cdot (q+1)^{q^{\frac{n-1}{q}-(m-2)}}.$$

4. Исследована проблема пересечения нелинейных совершенных q-значных кодов. С помощью метода свитчинга простых компонент получен широкий ряд возможных пересечений таких кодов. Показано, что существуют подвижные множества мощности меньшей, чем минимальная i-компонента кода Хэмминга.

На защиту выносятся новые свитчинговые методы построения совершенных q-значных кодов и применение этих методов для исследования пересечений таких кодов (проблема Т. Этциона и А. Варди).

Объем и структура диссертации. Диссертация состоит из введения, трех глав и списка литературы (36 наименований), в конце приведен список публикаций автора по теме диссертации. Объем диссертации — 64 страницы.

СОДЕРЖАНИЕ РАБОТЫ

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

Пусть V_q^N — N-мерное векторное пространство над полем Галуа $GF(q)$, где q — степень простого числа. В пространстве V_q^N фиксирован некоторый базис и задана *метрика Хэмминга*. Под расстоянием $d(x, y)$ между двумя произвольными векторами x и y пространства подразумевается число координат, в которых они различаются. *Вес* вектора $z \in V_q^N$ — это число его ненулевых координат. Произвольное подмножество C такого пространства является q-значным кодом. Код в V_q^N называется *совершенным q-значным кодом длины N с расстоянием 3* (далее просто *совершенным кодом*), если $|C| = q^{N-\log_q(qN-N+1)}$ и расстояние между любыми двумя *кодовыми словами* (так в дальнейшем будем называть элементы кода) не менее 3. Эти условия эквивалентны плотной упаковке пространства V_q^N шарами единичного радиуса с центрами в кодовых словах.

Код C *линеен*, если он является подпространством V_q^N. Совершенный линейный код в пространстве V_q^N называется *кодом Хэмминга*. Будем обозначать его через $\mathcal{H}_q^N$.

Всюду далее полагаем $N = qn + 1$, $n = (q^{m-1} - 1)/(q - 1)$ и $m \geq 2$.

В настоящей диссертации предложено три новых метода построения совершенных q-значных кодов, последовательно улучшавших нижнюю оценку числа различных совершенных q-значных кодов. Все три метода различаются между собой и могут найти применение для построения и исследования q-значных кодов, необязательно совершенных.

Во введении обосновывается актуальность темы диссертации, характеризуется новизна работы, обсуждаются трудности, сопутствующие исследованию q-значных кодов в отличии от изучения двоичных кодов. Дается краткий обзор ранее известных конструкций совершенных q-значных кодов. Приводится список основных результатов диссертации и обосновывается тесная связь между ними.

В первой главе приводится описание свитчингового метода построения совершенных q-значных кодов, который является обобщением для q-значного случая способа построения двоичных совершенных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент, предложенного в 1996 г. С. В. Августиновичем и Ф. И. Соловьевой в [1]. Этот метод был усовершенствован посредством дополнительных преобразований, не имеющих аналогов в двоичном случае. Приведены нижние оценки числа различных совершенных q-значных кодов, построенных описанными методами.

В параграфе 1.1 вводятся ключевые понятия для данного исследования: подвижное множество, i-компонента и $\widetilde{\alpha}$-компонента, сдвиг множества, множество R_i. Приведем определения этих понятий.

Пусть C произвольный q-значный код длины N, M — некоторое подмножество его кодовых слов.

Пусть $\mathcal{F}(M)$ множество, полученное с помощью некоторого преобразования $\mathcal{F}$ векторов множества M, причем множества M и $\mathcal{F}(M)$ не совпадают. Множество M называется *подвижным множеством кода* C, если множество

$$C' = (C \backslash M) \cup \mathcal{F}(M)$$

является q-значным кодом с теми же параметрами.

Согласно [15], *сдвигом множества* M *по направлению* i, $i \in \{1, 2, \ldots, N\}$, на элемент a, где a — ненулевой элемент поля $GF(q)$, называется множество $M' = \{x + ae_i | x \in M\}$, где e_i — вектор длины N с нулевыми координатами, кроме i-й, равной 1, то есть $M' = M + ae_i$, здесь ae_i означает покомпонентное произведение вектора e_i на элемент a.

Множество M называется *i-компонентой совершенного кода* C, если код $C' = (C \backslash M) \cup (M + ae_i)$ является совершенным кодом.

Пусть $\widetilde{\alpha} \subseteq \{1, 2, \ldots, N\}$. Множество M называется *$\widetilde{\alpha}$-компонентой совершенного кода* C, если для всех $i \in \widetilde{\alpha}$ множество M является i-компонентой кода C.

Подпространство, порождённое совокупностью вершин веса 3 кода $\mathcal{H}_q^N$ с единичной i-й координатой, обозначим через R_i. Известно, см. [13], что множество R_i является i-компонентой.

Впервые свитчинговый метод построения совершенных двоичных кодов был предложен Ю. Л. Васильевым в 1962 году, см. [2]. В 1968 году Дж. Шонхайм, см. [15], предложил свитчинговую конструкцию для построения совершенных q-значных кодов. Следующее утверждение раскрывает механизм *свитчингового метода* (от английского: *switching — сдвиг, обмен*), который предложен для q-значного случая в [13], (см. также [10]). Однако следует различать свитчинговый метод, описанный здесь, от изложенного в [13], так как мы не ограничиваемся сдвигом только i-компонент, а сдвигаем (так же, как в [1]) ещё и специального вида ijk-компоненты.

Итак, рассмотрим произвольный совершенный код C длины N. Пусть $M_{i_1}^1, M_{i_2}^2, \ \dots \ , M_{i_k}^k$ попарно непересекающиеся подмножества кода C такие, что $M_{i_s}^s$ являются i_s-компонентами кода C, причём $i_1, i_2, \ \dots \ , i_k \in \{1, 2, \dots, N\}$ не обязательно все различны.

Утверждение.(См [13].) Пусть C произвольный совершенный код длины $N = (q^m - 1)/(q - 1)$, $m \geq 2$. Тогда для любого ненулевого элемента a_s поля $GF(q)$ множество

$$C' = (C \setminus \bigcup_{s=1}^{k} M_{i_s}^s) \cup (\bigcup_{s=1}^{k} (M_{i_s}^s + a_s \cdot e_{i_s}))$$

является совершенным q-значным кодом длины N.

В параграфе 1.2 рассмотрено разбиение q-значного кода Хэмминга на классы смежности линейной $\widetilde{\alpha}$-компоненты, а также на классы смежности i-, j- и k-компонент. Эти утверждения позволяют доказать Теорему 1 о том, что код, построенный из q-значного кода Хэмминга методом свитчинга $\widetilde{\alpha}$-компонент, является совершенным.

Основная идея метода свитчинга $\widetilde{\alpha}$-компонент заключается в следующем. Сначала для каждой $\widetilde{\alpha}$-компоненты выбираем свое направление i из множества направлений $\widetilde{\alpha}$ и делаем свитчинг, то есть сдвигаем все i-компоненты в каждой $\widetilde{\alpha}$-компоненте на произвольный элемент поля $GF(q)$, затем производим свитчинг полученных новых $\widetilde{\alpha}$-компонент, делая сдвиги по неиспользованным из множества $\widetilde{\alpha}$ направлениям. В итоге результирующий код остается кодом с теми же параметрами, но отличным или даже неэквивалентным исходному.

Параграф 1.3 посвящен получению нижней оценки числа различных совершенных q-значных кодов, описанных конструкцией Теоремы 1. Поскольку построенные коды не все различны, для их сравнения вводится понятие функции сдвига. Функция сдвига f_c определяет, на какие элементы поля $GF(q)$ и в каких направлениях следует сдвигать кодовые слова кода Хэмминга, чтобы получить код C. Каждый совершенный код однозначно определяется своей функцией сдвига, причём несовпадающие коды имеют разные функции.

В параграфе 1.3 доказана

Теорема 2. Количество $F_q(N)$ различных совершенных q-значных кодов длины N не меньше, чем

$$q^{q^{n-(m-1)}} \cdot (3q)^{q^{\frac{n-1}{q}-(m-2)}}. \qquad (1)$$

Эта оценка улучшает ранее известную нижнюю оценку Б. Линдстрема, см. [12].

А. М. Романов в 2004 г., см. [5], для построения совершенных q-значных кодов использовал связь столбцов проверочной матрицы кода Хэмминга с проективной геометрией, впервые примененную для построения совершенных q-значных кодов К. Т. Фелпсом и М. Виллануевой в [13]. Это позволило расширить класс совершенных q-значных кодов и получить новую нижнюю оценку, оценка А. М. Романова отличается от (1) тем, что вместо 3 во втором мультипликативном члене стоит (q+1).

В параграфе 1.4 описана модификация метода свитчинга $\widetilde{\alpha}$-компонент за счет конфигураций (перестановок, действующих на элементах поля $GF(q)$), такие преобразования не имеют аналогий в двоичном случае, поскольку в случае двоичного алфавита перестановка вырождается в обмен элементов 0 и 1.

Использование конфигураций демонстрирует следующее

Утверждение. Пусть $\mathcal{H}_q^N$ — q-значный код Хэмминга длины $N = (q^m-1)/(q-1)$, $m \geq 2$. Тогда для любой перестановки π на множестве $\{0, 1, \ldots, q-1\}$ множество

$$C' = (\mathcal{H}_q^N \backslash R_i) \cup \pi(R_i)$$

является совершенным q-значным кодом.

Следует отметить, что определение свитчинга в этом параграфе уже отличается от приведенного в параграфе 1.1, ранее речь шла о свитчинге (в терминах настоящего определения) по циклической перестановке длины q.

В этом параграфе доказана теорема о том, что коды, построенные с помощью описанной конструкции, являются совершенными.

В параграфе 1.5 получена нижняя оценка числа различных совершенных q-значных кодов, построенных модифицированным методом свитчинга $\widetilde{\alpha}$-компонент кода Хэмминга.

Теорема 4. Число $F_q(N)$ различных совершенных q-значных кодов длины $N = qn+1$, $n = (q^{m-1}-1)/(q-1)$ не меньше, чем

$$(q!)^{q^{n-(m-1)}} \cdot 3^{q^{\frac{n-1}{q}-(m-2)}}. \qquad (2)$$

В доказательстве теоремы также учитывалось, что при построении не все коды получаются различными. Сравнивая с оценкой А. М. Романова [5], отметим, что оценка (2) лучше за счет первого главного мультипликативного члена.

Результаты первой главы опубликованы в работах [17] и [18].

Вторая глава посвящена описанию развития свитчингового подхода к q-значному коду Хэмминга. Предложенная в этой главе конструкция позволяет для произвольной допустимой длины получить нижнюю оценку числа различных совершенных q-значных кодов, являющуюся на сегодняшний день лучшей. Оценка получается за счет свитчингов в коде Хэмминга специального вида компонент, называемых простыми компонентами (определение см. ниже).

В параграфе 2.1 и далее рассматривается поле Галуа $GF(q)$, где q — степень простого и не равно простому, то есть $q = p^r$, $r > 1$. В таком случае поле $GF(q)$ содержит простое подполе $GF(p)$ с элементами от 0 до $p-1$ и возникает понятие простой i-компоненты.

Рассмотрим i-компоненту R_i кода Хэмминга $\mathcal{H}_q^N$. Компонента R_i является подпространством над полем $GF(q)$ кода $\mathcal{H}_q^N$, $q = p^r$, $r > 1$. Подпространство над подполем $GF(p)$, порожденное совокупностью векторов веса 3 с единичной i-й координатой, обозначим через P_i и назовем простой компонентой. То есть множеству P_i принадлежат векторы, полученные всевозможными линейными комбинациями с коэффициентами из подполя $GF(p)$ векторов, порождающих компоненту R_i. Такие компоненты, как было сказано выше, ввели К. Т. Фелпс, Ж. Рифа и М. Виллануева в работе [14].

Также в этом параграфе рассмотрена связь $(m-1)$-мерной проективной геометрии $PG(m-1,q)$ со столбцами проверочной матрицы q-значного кода Хэмминга, см. [13]. Приведено новое, отличное от известного в литературе, доказательство с помощью несложных законов проективной геометрии того факта, что ijk-компонента является L-компонентой, где L — прямая в проективной геометрии $PG(m-1,q)$, содержащая $q+1$ точку. То есть ijk-компонента является i-компонентой по одному из $q+1$ возможных направлений.

В параграфе 2.2 описан метод свитчинга простых компонент. Главное отличие от конструкции из параграфа 1.4 состоит

в том, что теперь в каждой i-компоненте R_i выделяются простые i-компоненты, что позволяет делать большее число свитчингов уже для каждой простой i-компоненты в отдельности. И в том и в другом случае свитчинги производятся по перестановкам, но в конструкции из параграфа 1.4 перестановки действуют на всех q элементах поля $GF(q)$, где $q = p^r, r > 1$, теперь же только на p элементах простого подполя $GF(p)$. Доказана теорема о том, что множество, построенное из q-значного кода Хэмминга с помощью описанного метода, является совершенным q-значным кодом.

Предлагаемый здесь метод построения q-значных совершенных кодов является развитием метода свитчинга компонент q-значного кода из главы 1.

В параграфе 2.3 доказана для любой допустимой длины N нижняя оценка числа различных совершенных q-значных кодов, при $q = p^r, r > 1$.

Теорема 6. Число $F_q(N)$ различных совершенных q-значных кодов длины $N = \frac{q^m-1}{q-1}$ не меньше, чем

$$(p!)^{q^{n\cdot(\frac{2r-1}{r})-(m-1)}} \cdot (q+1)^{q^{\frac{n-1}{q}-(m-2)}}.$$

Данная оценка является на сегодняшний день лучшей. Более того в параграфе 2.1 доказано утверждение о том, что простая компонента специального вида является минимальной. Это свойство простых компонент означает, что приведенная выше оценка не может быть существенно улучшена с помощью свитчингов такого типа компонент.

Результаты второй главы опубликованы в работах [19] и [20].

В третьей главе исследована проблема пересечения q-значных совершенных кодов: *какие возможны мощности пересечения $\eta(C_1, C_2)$ двух совершенных кодов C_1 и C_2 длины N?* Эта проблема была поставлена Т. Этционом и А. Варди в 1998

году в работе [11]. Там же они предложили полное решение проблемы пересечения двоичных кодов Хэмминга, нашли наименьшее пересечение для совершенных двоичных нелинейных кодов любой допустимой длины, которое состоит из двух кодовых слов, а также получили возможные пересечения совершенных двоичных кодов, используя простые свитчинги двоичных кодов Хэмминга. С. В. Августинович, У. Хеден, Ф. И. Соловьева (см. [6] и [7]) существенно продвинулись в решении проблемы пересечения для двоичных нелинейных кодов. В [7] доказано, что для всякого четного t, удовлетворяющего неравенствам

$$0 \leq t \leq 2^{n+1-2\log(n+1)}$$

найдутся совершенные двоичные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geq 4$, такие что $\eta(C_1, C_2) = t$. С. Е. Бар-Яшалом и Т. Этцион решили проблему пересечения для любых необязательно совершенных q-значных циклических кодов (см. [8]), $q \geq 2$.

В параграфе 3.1 приводится более короткое, чем в [8], доказательство существования возможных мощностей пересечения q-значных кодов Хэмминга. Техника, развитая в этом параграфе для изучения пересечений линейных q-значных кодов Хэмминга, существенно использовалась для исследования пересечений произвольных нелинейных q-значных кодов одинаковой длины.

В параграфе 3.2 описывается свитчинговый способ построения совершенных q-значных кодов, имеющих различные непустые пересечения с исходным кодом Хэмминга. Приведен спектр пересечений q-значных совершенных кодов, полученный сдвигами простых компонент.

Теорема 8. Для любого $k \in \{0, \ldots, p \cdot K - 2, p \cdot K\}$ существуют два q-значных совершенных кода $\mathcal{H}_q^N$ и C длины $N = nq + 1$ такие, что $\eta(\mathcal{H}_q^N, C) = k \cdot |P_i|/p$, где $|P_i| = p^{nr(q-2)+n}$, $q = p^r$.

В параграфе 3.3 с помощью комбинирования модификации конструкции Шонхайма из [15], методов свитчинга i-компонент и простых компонент, а также циклического сдвига координатных позиций кодов были доказаны Теоремы 9 (с помощью i-компонент) и 10 (с помощью простых компонент) о том, что для произвольной допустимой длины $N = (q^m - 1)/(q - 1)$, $m \geq 1$, существуют два совершенных q-значных кода, пересечение которых меньше, чем минимальное непустое пересечение совершенных кодов той же длины, достигаемое сдвигами простых компонент, см. теорему 8.

Параграф 3.4 посвящен построению различных разбиений пространства V_q^N на совершенные q-значные коды для любой допустимой длины $N = (q^m - 1)/(q - 1)$, используя конструкцию совершенных q-значных кодов Шонхайма [15] и технику свитчингового метода простых компонент из параграфа 2.2. Доказана

Теорема 11. Для любого $N = qn + 1$, $q = p^r$, существует не менее

$$p^{p^{rn+\log r}}$$

различных разбиений пространства V_q^N на совершенные q-значные коды длины N.

Результаты этой главы получены совместно с Ф. И. Соловьевой, опубликованы в [21] и [22].

Автор выражает глубокую искреннюю благодарность и признательность научному руководителю к.ф.-м.н., доценту Ф. И. Соловьевой, под руководством которой была выполнена эта работа.

Список литературы

[1] *Августинович С. В., Соловьева Ф. И.* Построение совершенных бинарных кодов последовательными сдвигами

$\widetilde{\alpha}$-компонент // Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 15–21.

[2] *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М: Наука, 1962. Вып. 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] *Романов А. М.* О разбиениях q-значных кодов Хэмминга на непересекающиеся компоненты // Дискрет. анализ и исслед. операций. 2004. Т. 11. № 3. С. 80–87.

[6] *Avgustinovich S. V., Heden O., Solov'eva F. I.* On intersections of perfect binary codes // Bayreuther Mathematische Schriften. 2005. No. 74. P. 1–6.

[7] *Avgustinovich S. V., Heden O., Solov'eva F. I.* On intersection problem for perfect binary codes // Des. Codes Cryptogr. 2006. V. 39. No. 3. P. 317–322.

[8] *Bar-Yahalom S. E., Etzion T.* Intersection of isomorphic linear codes // Journal of Comb. Theory, Series A. 1997. V. 80. No. 1. P. 247–256.

[9] *Blakley G. R., Kabatianski G. A.* When perfect secret sharing schemes with veto exist, Sixth Int. Workshop "Algebraic and Combinatorial Coding Theory", Pskov, Russia. September. 1998. P. 30–33.

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

[11] *Etzion T., Vardy A.* Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11. No. 2. P. 205–223.

[12] *Lindström B.* On group and nongroup perfect codes in q symbols // Math. Scand. 1969. V. 25. P. 149–158.

[13] *Phelps K. T., Villanueva M.* Ranks of q-ary 1 perfect codes // Des. Codes Cryptogr. 2002. V. 27. No. 1–2. P. 139–144.

[14] *Phelps K. T., Rifá J., Villanueva M.* Kernels of q-ary 1 perfect codes // Proc. Int. Workshop on Coding and Cryptography, March 2003, Versailles (France), P. 375–382.

[15] *Schönheim J.* On linear and nonlinear single-error-correcting q-ary perfect codes // Information and Control. 1968. V. 12. No. 1. P. 23–26.

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

Публикации автора по теме диссертации

[17] *Лось А. В.* Построние совершенных q-значных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Пробл. передачи информ. 2004. Т. 40. Вып. 1. С. 33–39.

[18] Construction of perfect q-ary codes // Proc. Ninth Int. Workshop "Algebraic and Combinatorial Coding Theory" Bulgaria (Kranevo). June 2004. P. 272–276.

[19] *Los' A. V.* Construction of perfect q-ary codes by switchings of simple components // Proc. of Int. Workshop on Optimal codes and related topics. Pamporovo, Bulgaria. June. 2005. P. 226–231.

[20] *Лось А. В.* Построение совершенных q-значных кодов свитчингами простых компонент // Пробл. передачи информ. 2006. Т. 42. № 1. С. 34–42.

[21] *Solov'eva F. I., Los' A. V.* On intersections of q-ary perfect codes // Proc. Tenth Int. Workshop "Algebraic and Combinatorial Coding Theory". Zvenigorod, Russia. September, 3–9. 2006. P. 244–247.

[22] *Соловьева Ф. И., Лось А. В.* О пересечениях q-значных совершенных кодов // Сиб. мат. журнал. 2008. Т. 49. № 2. С. 465–475.

Лось Антон Васильевич

Свитчинговые методы построения совершенных
q-значных кодов

Автореферат диссертации
на соискание ученой степени
кандидата физико-математических наук

Подписано в печать 02.04.08. Формат 60x84 1/16.
Усл. печ. л. 1,2. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ N 60.

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