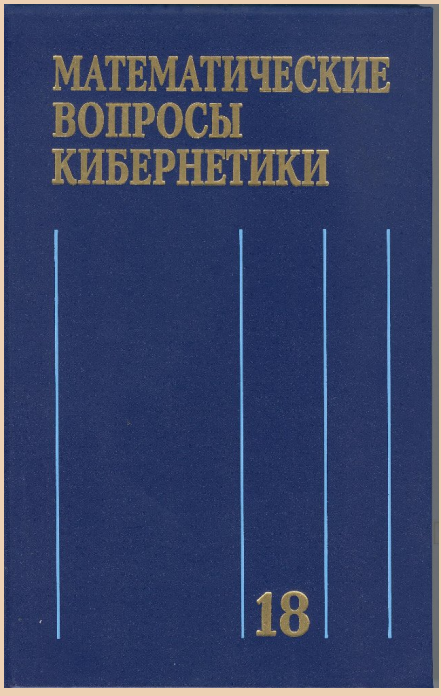
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 18



Ф. И. Соловьева

Обзор по совершенным кодам

Рекомендуемая форма библиографической ссылки: Соловьева Ф. И. Обзор по совершенным кодам // Математические вопросы кибернетики. Вып. 18. — М.: ФИЗМАТЛИТ, 2013. — С. 5–34. URL: http://library.keldysh.ru/mvk.asp?id=2013-5

ОБЗОР ПО СОВЕРШЕННЫМ КОДАМ*)

Ф. И. СОЛОВЬЕВА

(НОВОСИБИРСК)

Настоящий обзор посвящен совершенным кодам и смежным вопросам. Поскольку ранее был написан ряд обзоров по совершенным кодам (в основном на английском языке), см. [12, 103, 115, 154–156, 159–161], то в данном обзоре более подробно будут освещены некоторые результаты по совершенным кодам, полученные только за последние годы и не вошедшие в предыдущие обзоры. В этой работе мы лишь коснемся общих вопросов теории совершенных кодов: методов построения, описания свойств, нижних оценок числа таких кодов, связей теории совершенных кодов с другими областями математики и более подробно остановимся на вопросах изучения свойств совершенных кодов. Представленный вниманию читателя материал не претендует на полноту освещения всех областей теории совершенных кодов, отражает в основном результаты, полученные в лаборатории совершенных комбинаторных структур Института математики СО РАН за последние несколько лет, и отвечает в некотором смысле вкусам и воззрениям автора.

§ 1. Введение

Совершенные коды представляют собой один из наиболее интересных (как своими свойствами, так и методами, развитыми для их построения и исследования) математических предметов теории кодов, корректирующих ошибки. Код в пространстве F^n над полем Галуа $GF(q)$ по отношению к метрике Хэмминга называется *совершенным*, если совокупность шаров одинакового положительного радиуса, окружающих кодовые слова, задает разбиение пространства. Теория совершенных кодов на сегодняшний день является глубоко разработанной наукой, интенсивно развиваемой как в России, так и за рубежом. Несмотря на значительные усилия целого ряда исследователей, остается открытым множество проблем, связанных с совершенными кодами. По-прежнему остается нерешенной основная проблема классификации совершенных q-значных кодов для q — степеней простого. На сегодняшний день найдена только классификация двоичных совершенных кодов длины 15, а также расширенных совершенных двоичных кодов длины 16. Этот замечательный результат получен в 2009 г. П. Остергардом и О. Поттоненом в работе [129]: для $n = 15$ найдено 5983 неэквивалентных совершенных двоичных кодов длины 15, для $n = 16$ обнаружено 2165 неэквивалентных совершенных расширенных двоичных кодов длины 16. Известно,

*) Настоящая работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 12–01–00631-а).

что совершенные коды обладают целым рядом регулярных свойств. Плотная упакованность совершенных кодов предопределяет их оптимальность, т. е. максимальность мощности кода при заданной длине кода и кодовом расстоянии. Очевидно, что проблема упаковки шарами одного радиуса, — задача, важная как с точки зрения самой теории кодирования, так и с точки зрения целого ряда других математических дисциплин: комбинаторного анализа, теории групп, теории графов, комбинаторной топологии, геометрии, криптологии, синтеза схем.

Много усилий исследователей, особенно за последние пятнадцать лет, посвящено разработке методов построения и методов исследования свойств совершенных кодов.

К числу открытых проблем теории совершенных кодов относятся: проблема классификации совершенных кодов для любой допустимой длины $n > 15$, разработка прямых комбинаторных и итеративных методов построения и исследования свойств нелинейных совершенных и других, тесно связанных с ними, кодов; разработка методов построения транзитивных и пропелинейных (не обязательно совершенных) кодов, исследование спектральных свойств кодов, выяснение структуры i-компонент и α-компонент таких кодов и строения группы автоморфизмов произвольного совершенного кода, проблема построения и исследования разбиений пространства F^n на совершенные коды, проблема Этциона и Варди пересечения кодов. Следует отметить, что на сегодняшний день крайне недостаточно изучены совершенные коды полного ранга. Для исследования совершенных кодов используются традиционные методы и аппарат алгебраической и комбинаторной теории кодирования, комбинаторного анализа, теории графов, теории групп. Кроме того, применяются оригинальные методы комбинаторной теории кодирования, разработанные рядом авторов.

Следует подчеркнуть, что совершенные коды представляют собой удобный модельный объект для развития подходов к построению и исследованию свойств кодов с большими кодовыми расстояниями — многие из методов построения и изучения свойств совершенных двоичных кодов уже применены и успешно развиваются для кодов с другими параметрами, например, для равномерно упакованных кодов, кодов с параметрами кодов Рида—Маллера, четверичных кодов с метрикой Ли, q-значных, $q \geqslant 2$, кодов с метрикой Хэмминга, диаметральных совершенных кодов с метрикой Джонсона, для совершенных раскрасок, центрированных функций (см. ниже последний параграф) и др.

Опишем краткую структуру обзора: в параграфе 2 приводятся необходимые определения и понятия, параграф 3 посвящен методам построения совершенных кодов, в параграфе 4 обсуждаются транзитивные и пропелинейные коды, в параграфе 5 — разбиения пространства E^n на совершенные коды, параграф 6 посвящен q-значным совершенным кодам, в параграфе 7 обсуждается проблема пересечения двоичных совершенных кодов, параграф 8 посвящен некоторым метрическим свойствам совершенных кодов, параграф 9 — связи совершенных кодов с совершенными раскрасками, являющимися естественными обобщениями совершенных кодов, и, наконец, в последнем, 10-м, параграфе обсуждаются некоторые применения результатов, полученных для совершенных кодов, в других областях математики.

В данном обзоре опущено обсуждение результатов, полученных по строению групп автоморфизмов и групп симметрий совершенных кодов, см. [15, 55, 78, 79], метрической жесткости кодов, см. [1, 4, 13, 162], спектральных свойств совершенных кодов [19, 20], для полноты картины о конструкциях, строении совершенных кодов и кодов, близких к ним по ряду свойств, см. также опубликованные ранее обзоры [12, 103, 115, 154–156, 159–161].

§ 2. Необходимые определения и понятия

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

Подмножество пространства F^n всех q-значных векторов длины n над полем Галуа $GF(q)$, где q — степень простого числа, называется *q-значным кодом* C длины n. *Расстояние Хэмминга* $d(x, y)$ между векторами $x, y \in F^n$ определяется как число координат, в которых эти векторы различаются. Кодовое расстояние d кода C определяется как $d = min\, d(x, y)$ для любых различных кодовых слов $x, y \in C$. Элементы кода C называются *кодовыми словами*. Параметры q-значного кода C над полем Галуа $GF(q)$, где $q \geqslant 2$, — это тройка чисел n, $|C|$, d, где n — длина кода, $|C|$ — его мощность, d — кодовое расстояние (наименьшее расстояние по Хэммингу между различными кодовыми словами). Векторное пространство размерности n над $GF(2)$ обозначим через E^n.

Два кода $C, C' \subset F^n$ называются *изоморфными*, если существует подстановка $\pi \in S_n$ такая, что $C' = \pi(C) = \{\pi(x) : x \in C\}$, где S_n — симметрическая группа подстановок длины n. Коды $C, C' \subset F^n$ *эквивалентны*, если найдется изометрия пространства F^n, переводящая один код в другой, т. е. найдутся n подстановок $\tau_1, \ldots, \tau_n$ на q элементах поля Галуа F_q и подстановка $\pi \in S_n$ такие, что

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

Группа изометрий пространства F^n, переводящих произвольный код C длины n в себя, называется *группой автоморфизмов* $\mathrm{Aut}(C)$. Множество

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

называется *группой симметрий* кода C. Код C называется *транзитивным*, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Размерность линейной оболочки $< C >$ *приведенного* кода C (кода, содержащего нулевой вектор) называется *рангом* кода C. Совокупность *периодов* приведенного кода C, т. е. кодовых слов $x \in C$ таких, что $x + C = C$ называется *ядром* кода C.

Двоичный код C длины n называется *совершенным кодом, исправляющим одну ошибку* (далее, кратко — *совершенным*), если каждый вектор x из F^n находится на расстоянии 1 ровно от одного кодового слова C. *Система троек Штейнера* $STS(n)$ порядка n определяется как система сочетаний из n элементов по три такая, что каждая неупорядоченная пара элементов содержится в точности в одной тройке. Известно, что совокупность носителей кодовых слов веса 3 в любом приведенном двоичном совершенном коде C длины n определяет систему троек Штейнера порядка n, см. [122]. Другие определения будут приведены ниже при описании конкретных результатов. Широко известна теорема В. А. Зиновьева и В. К. Леонтьева [37–39], полученная независимо Э. Тиетвайненом [163], о том, что нетривиальные совершенные q-значные коды длины n, исправляющие ошибки, должны иметь те же самые параметры, что и один из кодов Хэмминга или Голея, т. е. такие коды существуют только при $n = (q^k - 1)/(q - 1)$, $k \geqslant 2$, и имеют кодовое расстояние 3 (коды с параметрами кодов Хэмминга, далее упоминаемые как совершенные); $n = 23$ — двоичный код Голея с кодовым расстоянием 7; $n = 11$ — троичный код Голея с кодовым расстоянием 5. Оба кода Голея и код Хэмминга любой допустимой длины единственны с точностью до эквивалентности. Ю. Л. Васильевым в 1962 г. [17] был открыт класс совершенных двоичных кодов, число неэквивалентных таких кодов оказалось дважды экспоненциальным. Тем самым была опровергнута гипотеза

Г. С. Шапиро и Г. Л. Злотника [153] о единственности существования совершенного двоичного кода (кода Хэмминга) для каждой допустимой длины.

Рассматриваются также отличные от полей Галуа алфавиты составной значности, не равной степени простого числа. Для таких алфавитов проблема существования совершенных кодов в общем случае все еще остается открытой.

Известно, что для кодовых расстояний, больших 5, усилиями целого ряда авторов было доказано, что совершенные коды не существуют, см., например, [30]. С. Голомб и Е. Познер [109] в 1964 г. показали несуществование совершенных кодов с расстоянием 3 длины $n = 7$ при размере алфавита, равном 6, и также, согласно теореме Х. Ленстры 1972 г., не существует групповых совершенных кодов. О несуществовании совершенных q-значных кодов, где q не является степенью простого числа, см. также обзор У. Хедена [115].

§ 3. Методы построения совершенных кодов

В теории совершенных кодов различают два основных метода построения кодов: свитчинговый и каскадный, а также их комбинирование. Как правило, свитчинговый метод — это прямой метод построения кодов, в то время как каскадный — всегда итеративный. Поскольку ранее каскадные методы были описаны достаточно подробно в обзорах [103, 115, 154, 156, 159, 160], и, кроме того, в последние годы не было открыто новых каскадных методов построения совершенных кодов, то в данном параграфе остановимся только на обсуждении некоторых свитчинговых методов построения совершенных кодов. Напомним кратко определения свитчинговых методов и их применение для исследования различных свойств как совершенных кодов, так и кодов, близких к ним по ряду свойств. Основная идея метода свитчинга состоит в следующем: в произвольном (не обязательно совершенном) коде C длины n из F^n рассмотрим некоторое подмножество M кодовых слов. Если найдется в F^n подмножество M', отличное от множества M, и множество

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

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

3.1. Метод α-компонент. Напомним основную идею метода α-компонент на примере совершенных двоичных кодов (из описания метода будет ясно, что, с точностью до некоторой модификации, он имеет место для любых q-значных кодов, $q \geqslant 2$, отличных от совершенных). Пусть C — произвольный совершенный двоичный код длины n и R — некоторое подмножество его кодовых слов. *Свитчингом* множества R в направлении i, где $i \in I = \{1, 2, \ldots, n\}$, назовем множество R', полученное из R сдвигом на вектор e_i веса один (с единицей только в i-й координате) всех его кодовых слов, и обозначим $R' = R \oplus e_i$. Множество R назовем *i-компонентой* кода C, если $K(R) = K(R \oplus e_i)$, где $K(R)$ — объединение шаров радиуса 1 с центрами в векторах R. Легко понять, что код $C' = (C \setminus R) \cup (R \oplus e_i)$ также является совершенным кодом. Будем говорить, что C' получен из кода C *свитчингом*. Пусть $\alpha \subseteq I$. Подмножество M кода C назовем *α-компонентой*, если для всех $i \in \alpha$ множество M является i-компонентой кода C. Понятие α-компоненты оказалось весьма полезным при построении новых классов совершенных кодов и исследовании свойств совершенных кодов.

Непересекающиеся α-компоненты можно разбивать на компоненты меньшей мощности по разным направлениям. Это позволяет сдвигать сначала компоненты меньшей мощности, варьируя направления, затем полученные α-компоненты сдвигать по оставшимся неиспользованными направлениям из множества α. При этом получается новый класс совершенных кодов с теми же параметрами. Если число компонент равно T, то мощность этого класса не менее 2^T. Метод α-компонент оказался особенно подходящим в применении к коду Хэмминга (не обязательно двоичному), поскольку позволяет, разрушая групповую структуру кода Хэмминга, тем не менее следить за структурой нелинейного совершенного кода, получаемого в результате воздействия на код серии преобразований — свитчингов компонент.

Используя этот метод, в 1996 г. в работе [11] удалось впервые улучшить нижнюю оценку Ю. Л. Васильева [17]

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

$n = 2^m - 1, m > 3$, полученную в 1962 г. для числа различных совершенных двоичных кодов длины n, а именно было доказано, что количество различных совершенных двоичных кодов длины n не меньше, чем

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

Здесь и далее рассматриваем логарифмы только по основанию 2. Оценка достигается применением метода α-компонент к коду Хэмминга H длины n. Сначала разбиваем код Хэмминга H на ijk-компоненты, где (i, j, k) — произвольная тройка из системы троек Штейнера $STS(H)$ кода Хэмминга H, затем независимо каждую ijk-компоненту — на i-, j- или k-компоненты. Для построения класса кодов существенно использовались свойства $STS(H)$. При этом был проведен анализ свойств подмножеств с фиксированной координатой системы троек Штейнера кода Хэмминга. Именно он позволил итеративно препарировать код Хэмминга (сначала на подкоды большой мощности, затем меньшей) и применить к нему серии локальных преобразований — свитчингов компонент.

Фактически при этом была получена нижняя оценка числа совершенных кодов ранга не больше $n - \log(n+1) + 2$. С помощью этого метода построения кодов впервые, после Ю. Л. Васильева, была доказана *мощностным* способом неэквивалентность предложенных совершенных кодов ранее известным кодам (первый фактор в формуле (1) получается при варьировании i-компонент, второй фактор получен за счет варьирования ijk-компонент). Следует отметить, что прежде производились многочисленные, но безуспешные попытки улучшить оценку Ю. Л. Васильева.

Этот свитчинговый метод построения совершенных кодов и исследования их свойств дал возможность решить целую серию проблем, например, положительно решить проблему рангов и ядер (проблему Т. Этциона и А. Варди 1998 г. [106]), см. [14], для всех $n = 2^k - 1$, $k \geqslant 5$, кроме случая совершенного кода полного ранга длины 31 с размерностью ядра 21, который был закрыт У. Хеденом в [114]. Метод α-компонент позволил доказать существование разбиения множества всех двоичных векторов длины n на попарно неэквивалентные совершенные двоичные коды длины n с кодовым расстоянием 3, см. [16]. Следует подчеркнуть, что этот метод лег в основу развития метода i-компонент (см. описание ниже) и получил активное развитие в работах С. А. Малюгина [53, 54, 57–59], Д. С. Кротова [46], С. В. Августиновича и Д. С. Кротова [121].

В работе [53] С. А. Малюгин предложил сначала заменить произвольную ijk-компоненту в коде Хэмминга H на изоморфную ijk-компоненту, затем производить сдвиги i- и j-компонент. Эта модификация позволила обогатить

получаемый класс совершенных кодов по мощности. Затем этот метод был развит Д. С. Кротовым [46] также для совершенных кодов ранга опять-таки не больше $n-\log(n+1)+2$, дополнительно к методу α-компонент он применил известный обобщенный каскадный метод, см. [131], а также [168], что позволило получить следующую нижнюю оценку числа различных совершенных двоичных кодов:

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

Впоследствии, применяя многократно к коду Хэмминга длины n метод локальных автоморфизмов, С. В. Августинович и Д. С. Кротов, см. [121], получили лучшую на сегодняшний день нижнюю оценку числа различных совершенных кодов длины n неполного ранга. Метод локальных автоморфизмов, предложенный в этой работе, является дальнейшим развитием методов [17], [11], [53], [46]. Идея метода локальных автоморфизмов состоит в преобразованиях кода Хэмминга, состоящих в применении изометрий пространства E^n к частям кода таким образом, чтобы окрестности этих частей не менялись. Такие изометрии были названы *локальными автоморфизмами*. Всякий локальный автоморфизм действует на часть кода, не меняя ее окрестности. Поскольку имеется тесная взаимосвязь между совершенными двоичными кодами и расширенными совершенными двоичными кодами (число различных последних длины $n+1$ в два раза больше числа различных совершенных кодов для каждой допустимой длины n), нижняя оценка в работе сформулирована в терминах последних.

Теорема 1 [121]. *Число различных расширенных совершенных двоичных кодов длины* $n'=2^m$, $m\geqslant 4$ *не менее чем*

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

Следует отметить, что для совершенных двоичных кодов длины $n=2^m-1$ первые три наибольших фактора в нижней оценке С. В. Августиновича и Д. С. Кротова совпадают с нижней оценкой Д. С. Кротова (2). В этой же работе С. В. Августинович и Д. С. Кротов выдвинули гипотезу, что предложенная в теореме 1 оценка является асимптотически точной для числа N_n всех различных совершенных двоичных кодов длины n; фактически это должно означать, что почти все совершенные двоичные коды имеют неполный ранг.

Заметим, что на сегодняшний день полностью классифицированы все совершенные двоичные коды длины n ранга меньшего или равного $n-\log(n+1)+2$. Легко видно, что совершенные коды ранга $n-\log(n+1)+1$ — это класс нелинейных совершенных кодов, полученных из кода Хэмминга $H^{(n-1)/2}$ длины $(n-1)/2$ с помощью конструкции Васильева (см. конструкцию Ю. Л. Васильева в [17], а также ниже в параграфе 4) для произвольной нелинейной функции $\lambda: H^{(n-1)/2}\to\{0,1\}$. В 2004 г. в работе [84] было доказано, что все совершенные двоичные коды ранга $n-\log(n+1)+2$ могут быть получены с помощью конструкции Фелпса-1984 [131]. Асимптотика числа n-арных квазигрупп порядка 4 (или отвечающих им MDS-кодов, используемых в конструкции Фелпса-1984), полученная Д. С. Кротовым и В. Н. Потаповым в [49], с учетом [43], дает асимптотику числа совершенных кодов ранга $n-\log(n+1)+2$. Более того, в работе [50] Д. С. Кротов и В. Н. Потапов установили, что все совершенные коды длины n ранга $n-\log(n+1)+2$ могут быть получены многократными свитчингами i-компонент из кода Хэмминга той же длины. У. Хеден, см. [115], показал,

что все совершенные двоичные коды неполного ранга могут быть получены с помощью комбинированной конструкции Кротова [45].

Завершая данный параграф, напомним, что верхняя оценка числа различных совершенных двоичных кодов длины n имеет вид

$$N_n \leqslant 2^{2^{n-\frac{3}{2}\log n+\log\log(en)}},$$

см. [2]. Таким образом, разрыв между рекордной на сегодняшний день нижней оценкой и приведенной верхней оценкой все еще остается большим.

3.2. Метод i-компонент. Рассмотрим метод сдвига непересекающихся i-компонент. Метод свитчингов (последовательных сдвигов) i-компонент можно продемонстрировать следующим образом: в коде длины n для различных координат сдвигаются достаточно далекие компоненты, либо сначала в коде сдвигается некоторое специальным образом выбранное множество i-компонент, затем в полученном коде сдвигаются j-компоненты (и так далее) таким образом, что результирующий код, отличный от исходного или неэквивалентный ему, остается кодом с теми же параметрами — длиной, мощностью и кодовым расстоянием.

Метод сдвига непересекающихся i-компонент различных направлений, безусловно, тесно связан с методом α-компонент, но не является его частным случаем, поскольку имеются ситуации, когда метод i-компонент применим, а метод α-компонент — нет, и наоборот. Нетрудно видеть, что известный итеративный метод построения совершенных кодов Васильева [17] является методом i-компонент, для этого достаточно в конструкции Васильева взять произвольный код Васильева в качестве кода предыдущей кодовой размерности, см. подробные объяснения в работе [155]. Но следует отметить, что всякий раз при решении некоторой конкретной задачи методом i-компонент требуются дополнительные условия, вследствие чего этот метод фактически модифицируется в новую конструкцию кодов. Этот метод был независимо предложен в 1994 г. Т. Этционом и А. Варди [105] для перечисления спектра рангов нелинейных совершенных кодов, в 1995 г. К. Фелпсом и М. ЛеВаном [133] для описания спектра размерностей ядер нелинейных совершенных двоичных кодов длины $n \geqslant 15$, в 1996 г. С. В. Августиновичем и автором данной статьи для решения проблемы Ф. Хергерта 1985 г. существования несистематических совершенных двоичных кодов, см. [10]; о структурах i-компонент см. [18, 157].

Продемонстрируем этот метод на примере построения несистематического совершенного двоичного кода из кода Хэмминга. Доказать требуемое свойство (например, построить несистематические коды или i-компоненты максимальной мощности, неразложимые на компоненты меньшей мощности), имея в запасе только локально повторяющуюся одинаковую структурную часть кода, означает воссоздать строение всего объекта, сформированного из локальных фрагментов, суметь «склеить», имея только частичную информацию, весь код в целом или суметь перестроить код, являющийся глобально и локально однородным (например, код Хэмминга) таким образом, чтобы результирующий код, став нелинейным, обладал требуемыми свойствами и в целом и для фрагментов.

Т е о р е м а 2. *Для любого допустимого $n = 2^m$, $m > 7$, существует несистематический совершенный код длины n.*

Для доказательства этой теоремы в работе [10] были рассмотрены локальные преобразования кода Хэмминга длины n. Код Хэмминга можно униформизовать — он является систематическим, т. е. в пространстве E^n найдется такая $\log(n+1)$-мерная грань, что в каждой параллельной ей грани содержится в точности одно кодовое слово. Никакой несистематический код невозможно униформизовать в указанном смысле, т. е. какая бы $\log(n+1)$-мерная грань ни была выбрана в E^n, найдется грань, параллель-

ная ей, не содержащая кодовых слов и, соответственно, найдется параллельная грань, содержащая не менее двух кодовых слов. Для построения несистематических кодов, как правило, необходим достаточный «простор» в пространстве между кодовыми словами, какового нет для совершенного кода в силу его плотной упакованности. Отсутствие простора удалось компенсировать строго скорректированными свитчингами специальных подкодов кода Хэмминга, не нарушающими плотную упакованность результирующего кода. Для этого в работе [10] был разработан метод свитчингов (последовательных сдвигов) i-компонент: в коде Хэмминга длины n для различных i, $i = 1, \ldots, n$, были сдвинуты n достаточно далеких друг от друга i-компонент. При этом существенно использовались свойства специального вида подсистем системы троек Штейнера кода Хэмминга и свойства систем троек Штейнера полученного кода. Долгое время предполагалось, согласно гипотезе Ф. Хергерта 1985 г., см. [119], что все совершенные коды систематические. В 1996 г. в [10] было доказано, что существует класс несистематических совершенных двоичных кодов длины n для любого $n > 127$, где $n = 2^k - 1$.

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

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

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

Исследование структуры множества $ST(C)$ для произвольного совершенного кода C полезно также с точки зрения доказательства неэквивалентности двух совершенных кодов — два совершенных кода с системами троек разной мощности неэквивалентны.

Позднее метод свитчингов i-компонент был использован для построения класса совершенных кодов полного ранга с тривиальной группой автоморфизмов, состоящей только из двух векторов — нулевого $\mathbf{0}$ и единичного $\mathbf{1}$, и, следовательно, кода с тривиальным ядром, не являющегося систематическим для любого допустимого $n \geqslant 255$ (см. [89]) и систематического для любого допустимого $n \geqslant 31$ (см. [123]). Метод построения несистематических кодов получил дальнейшее развитие в следующих работах: К. Т. Фелпсом и М. ЛеВаном в работе [134] были построены несистематические коды для $n \leqslant 127$, А. М. Романовым в [69] — для $n = 15$. С. А. Малюгиным в [56] опубликован следующий результат.

Т е о р е м а 3. *Минимальное количество i-компонент, которые необходимо сдвинуть в коде Хэмминга длины $n \geqslant 15$ для получения несистематического кода длины n, не зависит от n и равно* 7.

В работе [60] С. А. Малюгин обобщил этот результат на q-значный случай, а именно, им были построены несистематические совершенные q-значные коды над конечными полями $GF(q)$ длины $n = (q^m - 1)/(q - 1)$ при $m \geqslant 4$ и $q \geqslant 2$, а также при $m = 3$ и при q, не являющимся простым числом. Показано, что при $q \neq 3, 5$ такие коды можно строить также сдвигами семи непересекающихся компонент, а при $q = 3, 5$ — сдвигами восьми непересекающихся компонент кода Хэмминга длины n (тем самым был получен ответ на вопрос К. Т. Фелпса и М. ЛеВана [134], поставленный для совершенных двоичных кодов). К. Т. Фелпс и М. ЛеВан [135], используя конструкцию [70] автора настоящей статьи, доказали в 1999 г., что существуют

совершенные коды длины 15, которые невозможно получить из кода Хэмминга методом свитчинга. Следует отметить, что в работах [32, 34] были перечислены все совершенные и совершенные расширенные коды длин 15 и 16 соответственно, кроме кодов полного ранга, равного 15. В [130] были перечислены все (многоразовые) свитчинговые классы совершенных кодов длины 15, их оказалось девять, один из которых имеет максимальную мощность, равную 5819, что представляет собой подавляющую часть от общего числа 5983 всех неэквивалентных совершенных кодов длины 15. Среди этих девяти классов обнаружено четыре спорадических класса, каждый состоящий только из одного кода.

Обзор свитчинговых конструкций, а также нетривиальных свойств, присущих всем совершенным кодам, полученных различными свитчинговыми методами, см. в [155, 159–161].

§ 4. Транзитивные и пропелинейные коды

В настоящем параграфе обсуждается связь транзитивных кодов с пропелинейными, часть результатов посвящена транзитивным кодам, другая часть — пропелинейным.

Всюду в этом параграфе полагаем, что нулевой вектор принадлежит коду. Пусть Π — отображение множества кодовых слов произвольного кода C в совокупность допустимых подстановок: $x \to \pi_x$ таких, что $(x, \pi_x) \in Aut(C)$, где $\pi_{(x,\pi_x)y} = \pi_x \pi_y$. Определим групповую операцию на коде C следующим образом:

$$x \star y = (x, \pi_x)y.$$

Код, оснащенный таким образом определенной операцией, называется *пропелинейной структурой* на C и обозначается $(C, \Pi, \star)$ и кратко $(C, \star)$, если не требуется информации о строении Π. Код называется *пропелинейным*, если он имеет пропелинейную структуру.

Из приведенного определения легко видно, что всякий пропелинейный код является транзитивным. В работе [96] доказана отделимость класса транзитивных кодов от пропелинейных, а именно, показано, что известный код Беста длины 10, мощности 40, с кодовым расстоянием 4 транзитивен, но не является пропелинейным. Однако этот вопрос остается открытым для транзитивных и пропелинейных совершенных (расширенных совершенных) кодов.

Ниже приведем несколько новых свитчинговых методов построения бесконечных классов пропелинейных двоичных кодов. Будучи примененными к совершенным кодам, эти методы позволили (конструктивно) доказать в [96], что существует квадратичное число неэквивалентных совершенных пропелинейных кодов длины $n = 2^k - 1, k > 4$ для любых рангов, варьирующихся от $n - \log(n+1)$ до $n - \frac{1}{4}\log(n+1)$. Аналогичный результат немедленно следует для расширенных совершенных пропелинейных кодов, полученных применением к пропелинейным кодам общей проверки на четность, поскольку нетрудно видеть, что расширение пропелинейного кода с помощью общей проверки на четность всегда дает пропелинейный код. Обратное, вообще говоря, неверно. Более того, известны примеры таких транзитивных кодов, что коды, полученные из них выкалыванием некоторой координаты, не являются транзитивными (пока неизвестно, являются ли эти коды пропелинейными). Назовем такие коды *предельно-транзитивными*. С. А. Малюгин (частное сообщение) обнаружил первый пример расширенного совершенного предельно-транзитивного кода длины 16 — каждый из

шестнадцати его выколотых совершенных кодов длины 15 не является транзитивным. Позднее, в 2012 г., Г. К. Гуськов (ученик автора обзора) и автор настоящей статьи перечислили все расширенные совершенные предельно-транзитивные коды длины 16 и обнаружили бесконечные серии предельно-транзитивных кодов, см. [29]. Следовательно, построение и исследование расширенных транзитивных кодов целесообразно проводить независимо от построения транзитивных кодов, не являющихся расширенными, аналогично для пропелинейных кодов. Экспоненциальное число попарно неэквивалентных совершенных расширенных пропелинейных двоичных кодов длины $4N$, $N=2^m$ малого ранга было получено в [97].

Кроме того, в этом параграфе обсуждается метод построения неэквивалентных Z_4-линейных кодов с параметрами классических кодов Рида—Маллера.

Транзитивные и пропелинейные объекты, обладая богатым набором симметрий, играют важную роль как в теории кодирования, так и в комбинаторике, теории групп, теории графов. Следует отметить, что по ряду свойств эти коды близки к линейным, и, по всей видимости, по этой причине количество таких кодов невелико. Однако для большинства оптимальных нелинейных кодов почти всегда можно найти транзитивные и/или пропелинейные коды с такими же параметрами. Например, двоичный образ (под действием отображения Грея) произвольного аддитивного (над кольцом $\mathbb{Z}_4$ или алфавитом $\mathbb{Z}_2\mathbb{Z}_4$) кода является пропелинейным кодом. На сегодняшний день известно много хороших двоичных нелинейных кодов, представимых в качестве линейных над кольцом $\mathbb{Z}_4$, среди них следует отметить подклассы кодов Препараты, Кердока, Дельсарта—Геталса, Геталса—Дельсарта, совершенных, Адамара, см. [63, 94, 98, 101, 113, 120, 127].

Несколько конструкций транзитивных кодов (не обязательно совершенных), в частности, базирующихся на конструкциях Васильева и Моллара, предложено в [71, 158]. Пропелинейные коды были определены в работе [143] и позднее исследованы в [96, 97, 144]. В [145] было доказано, что совершенные пропелинейные коды могут быть получены, используя конструкцию Васильева. В работе [96] доказано, что пропелинейные коды (не обязательно совершенные) могут быть получены, используя конструкцию Васильева, и пропелинейные коды, корректирующие одиночные ошибки (также не обязательно совершенные), — используя конструкцию Моллара. Остановимся подробнее на полученных в этой области результатах.

Пусть B и C — произвольные двоичные коды длины n с кодовыми расстояниями d_1 и d_2 соответственно, где d_1 нечетно. Пусть λ — произвольная функция из кода C в множество $\{0,1\}$, $|x| = x_1 + \ldots + x_n \pmod 2$, где $x=(x_1,\ldots,x_n)\in E^n$. Код

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

будем называть *кодом Васильева*, см. [17]. Он имеет длину $2n+1$, мощность $|B|\cdot|C|$ и кодовое расстояние $d=\min\{2d_1+1, d_2\}$.

Пусть $(C,\star)$ — пропелинейная структура на коде C. Гомоморфизм λ из $(C,\star)$ на Z_2 называется *пропелинейным гомоморфизмом* (или *пропелинейной функцией*).

Теорема 4 [96]. *Пусть $(C,\star)$ — пропелинейная структура на коде C длины n, пусть λ — пропелинейная функция из C в Z_2. Тогда код Васильева C^{2n+1} является пропелинейным кодом.*

Множество

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

где B и C — коды длины n с кодовыми расстояниями d_1 и d_2 соответственно, называется *кодом Плоткина* длины $2n$. Этот код имеет мощность $|B|\cdot|C|$ и кодовое расстояние $d=\min\{2d_1, d_2\}$.

Т е о р е м а 5 [96]. *Пусть C является произвольным пропелинейным кодом с параметрами $(n, |C|, d_2)$, B — таким линейным кодом с параметрами $[n, |B|, d_1]$, что для любого автоморфизма $(y, \pi) \in Aut(C)$ выполняется $\pi \in Sym(B)$. Тогда код Плоткина C^{2n} пропелинеен.*

Заметим, что пропелинейные двоичные коды, полученные с помощью предыдущих двух теорем, могут иметь большие кодовые расстояния.

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

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

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

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

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

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

называется двоичным *кодом Моллара* длины $n = tm + t + m$ с кодовым расстоянием 3 (см. [126]). Справедлива

Т е о р е м а 6 [96]. *Пусть P^t и C^m — произвольные двоичные пропелинейные коды длин t и m соответственно. Пусть f — пропелинейный гомоморфизм из кода C^t в F^m. Тогда код Моллара C^n является двоичным пропелинейным кодом длины $n = tm + t + m$, исправляющим одиночные ошибки.*

В работе [71] результаты, аналогичные приведенным в последних трех теоремах, были ранее получены для двоичных транзитивных кодов, не обязательно совершенных.

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

Т е о р е м а 7 [96]. *Число неэквивалентных совершенных пропелинейных кодов длины $n = 2^k - 1, k \geqslant 4$, имеющих ранги, варьирующиеся от $n - \log(n+1)$ до $n - \frac{1}{4}\log(n+1)$, не менее $\lfloor k/2 \rfloor^2$.*

Напомним, что в работе [71] результат, аналогичный приведенной теореме, был получен для совершенных транзитивных кодов.

Ранее было известно $\lfloor (k+1)/2 \rfloor$ совершенных аддитивных (над кольцом $\mathbb{Z}_4$ или алфавитом $\mathbb{Z}_2\mathbb{Z}_4$) кодов длины $n = 2^k - 1$, см. [99], аналогично для расширенных совершенных аддитивных кодов, см. [44, 120]. Нетрудно показать, что все эти коды являются пропелинейными и дистанционно инвариантными. С. А. Малюгиным в 2004 г., см. [58], перечислены все совершенные транзитивные коды длины 15 из одношагового свитчингового класса кода Хэмминга длины 15. В работе [96] доказано, что все эти коды являются пропелинейными. В 2009 г. П. Остергард и др. перечислили, см. [130], все совершенные транзитивные коды, их оказалось 201, и совершенные расширенные транзитивные коды (таких кодов 101) длин 15 и 16 соответственно. Нетривиальные свойства, а именно группы автоморфизмов, мощности систем троек кода, ранги, размеры ядер, строение компонент и другие свойства совокупности всех совершенных и расширенных совершенных

двоичных кодов длин 15 и 16 соответственно, исследованы в работе [130]. Но, к сожалению, конкретная информация, касающаяся строения и свойств совершенных и расширенных совершенных транзитивных кодов длин 15 и 16 соответственно, в данной работе не приводится; по этой причине таблицы с этими кодами и их свойствами были приведены в [112].

В работе [64] для каждого допустимого достаточно большого n В. Н. Потаповым было построено экспоненциальное число неэквивалентных расширенных совершенных транзитивных кодов длины $4n$. В [97] доказано, что все эти коды являются пропелинейными.

Т е о р е м а 8 [97]. *При $n \to \infty$ существует по крайней мере*

$$\frac{1}{8n^2\sqrt{3}}\, e^{\pi\sqrt{2n/3}}(1+o(1))$$

попарно неэквивалентных двоичных расширенных совершенных пропелинейных кодов длины $4n$, $n=2^m$ ранга $n-\log_2 n$.

Эти пропелинейные коды были получены с использованием конструкции Фелпса-1984, см. [131] (можно также использовать каскадную конструкцию [168], примененную для получения совершенных кодов), в которой используются классы смежностей кода Хэмминга и специального вида пропелинейные MDS коды (названные в [97] изотопно пропелинейными MDS кодами), весьма близкие по строению и свойствам к линейному MDS коду. Поскольку каждый из этих пропелинейных кодов длины n имеет ранг $n-\log_2 n$, т. е. ранг любого такого кода на единицу больше ранга кода Хэмминга такой же длины, следовательно, каждый такой пропелинейный код может быть описан, согласно [84], конструкцией Васильева. Для совершенных пропелинейных кодов вопрос о существовании экспоненциальной нижней оценки попарно неэквивалентных кодов остается пока открытым.

Для класса пропелинейных совершенных кодов естественно возникают вопросы о том, каковы спектры рангов и размерностей ядер. Кроме того, представляется интересным также исследовать проблему рангов и ядер: какие пары чисел (r,k) достижимы для ранга r и размерности ядра k для пропелинейных кодов произвольной длины n. Напомним, что проблема рангов и ядер для двоичных совершенных кодов была решена в работе [14] за исключением одного случая кодов длины 31 полного ранга с ядром размерности 21, который был закрыт У. Хеденом в [114]. Проблема спектра рангов пропелинейных совершенных кодов, а именно каковы допустимые ранги пропелинейных совершенных кодов, была решена, за исключением четырех частных случаев кодов малых длин, в работе [111]:

Т е о р е м а 9. *Для любого $n=2^m-1$, $m\geqslant 4$ и каждого натурального числа r, удовлетворяющего $n-\log(n+1)\leqslant r\leqslant n$, исключая случаи $n=r=63$; $n=127$, $r\in\{126,127\}$ и $n=r=2047$, существует совершенный пропелинейный код длины n ранга r.*

Авторы работы [111] полагают, что для оставшихся случаев также существуют пропелинейные совершенные коды полных рангов.

В статье [29] перечислены все расширенные совершенные предельно-транзитивные коды длины 16. Их оказалось всего 10 среди всех 101 расширенных совершенных транзитивных кодов длины 16. Для пяти из 10 таких кодов удалось построить бесконечные серии попарно неэквивалентных.

Т е о р е м а 10 [29]. *Для любого допустимого $N=2^m, m>3$, существует 5 попарно неэквивалентных расширенных совершенных предельно-транзитивных кодов длины N, т. е. таких кодов, что каждый из них, будучи выколотым по любой из N координатных позиций, не является совершенным транзитивным кодом.*

Завершим данный параграф обсуждением свитчингового метода построения для каждого r, $0\leqslant r\leqslant m$, класса четверичных линейных кодов $\mathscr{LRM}(r,m)$, двоичные образы которых под действием отображения Грея

являются двоичными кодами с параметрами классических двоичных линейных кодов Рида—Маллера $RM(r,m)$ порядка r. Эти коды также являются пропелинейными и дистанционно инвариантными.

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

Теорема 11 [72]. *Для любого r, $r \in \{0,1,\ldots,m\}$, $m \geqslant 1$, существует четверичный групповой код над кольцом Z_4 с параметрами*

$$(n = 2^{m-1},\ 2^k,\ d = 2^{m-r}),\ \textit{где}\ k = \sum_{i=0}^{r} \binom{m}{i}, \tag{3}$$

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

Этот класс кодов построен с помощью конструкции Плоткина, примененной к известным групповым кодам Рида—Маллера над кольцом Z_4. Дальнейшее расширение этого класса кодов было получено в работе [140], где была предложена модификация конструкции Плоткина для четверичных групповых кодов над кольцом Z_4. Конструкции Z_2Z_4-линейных кодов с параметрами выколотых кодов Рида—Маллера см. в статье Д. Пухоля и др. [138, 139].

Поскольку под действием отображения Грея двоичный образ любого из четверичных кодов является Z_4-линейным кодом, который является пропелинейным кодом, а с помощью теоремы 5 можно строить коды с параметрами кодов Рида—Маллера, то применение этой теоремы дает бесконечный класс пропелинейных двоичных кодов с параметрами кодов Рида—Маллера, которые уже могут не быть Z_4-линейными.

Напомним, что код Рида—Маллера $RM(r,m)$ порядка $r = m-2$ является совершенным расширенным кодом. Классификация $\mathbb{Z}_4$-линейных совершенных расширенных кодов дана Д. С. Кротовым в 2000 г. в [44], а классификация Z_2Z_4-линейных кодов совершенных кодов приведена К. Боргесом и Ж. Рифой в 1999 г. [99].

§ 5. Разбиения E^n на совершенные коды

К предыдущему параграфу непосредственно примыкает данный, где обсуждаются результаты, полученные по разбиениям пространства E^n на совершенные коды. Проблема перечисления разбиений пространства E^n на совершенные коды самым тесным образом взаимосвязана с проблемой перечисления всех совершенных кодов: асимптотики, если таковые существуют, двойных логарифмов числа различных совершенных кодов и числа различных разбиений пространства E^n на совершенные коды совпадают.

В [70] автором статьи были предложены два метода построения нетривиальных разбиений E^n на совершенные коды, один из которых каскадный, другой — свитчинговый (с использованием конструкции Ю. Л. Васильева), дающий дважды экспоненциальную нижнюю оценку числа различных разбиений. В работе [132] К. Т. Фелпс перечислил все неэквивалентные разбиения пространства E^7 на коды Хэмминга. Несмотря на то, что в E^7 существует единственный с точностью до изоморфизма линейный совершенный код — код Хэмминга, было обнаружено 11 таких разбиений (там же доказано,

что в E^8 существует 10 неэквивалентных разбиений на расширенные коды Хэмминга длины 8).

Приведем нижнюю оценку (лучшую на сегодняшний день) числа различных разбиений пространства E^n на совершенные коды, полученную свитчинговым методом ijk-компонент:

Теорема 12 [28]. *Для любого допустимого $n \geqslant 7$ число различных разбиений $\boldsymbol{P}_n$ пространства E^n на совершенные двоичные коды длины n удовлетворяет неравенству*

$$\boldsymbol{P}_n \geqslant 2^{2^{\frac{n-1}{2}}} \cdot 6^{2^{\frac{n-3}{4}}}.$$

Следствие 1. *Для любого допустимого $n = 2^m - 1$, $m \geqslant 5$, существует не менее $2^{2^{\frac{n-1}{2}}}$ неэквивалентных разбиений пространства E^n на совершенные двоичные коды длины n.*

Аналогичные оценки верны для числа различных расширенных совершенных двоичных кодов. Легко видно, что для получения этой нижней оценки достаточно нижнюю оценку числа разбиений на совершенные коды длины n возвести в квадрат (число различных расширенных совершенных кодов в два раза больше числа различных совершенных кодов). Таким образом число различных разбиений $\mathscr{R}_n$ пространства E^n, где $n = 2^m$, $m \geqslant 4$, на расширенные совершенные двоичные коды длины n удовлетворяет нижней оценке:

$$\mathscr{R}_n \geqslant 2^{2^{\frac{n}{2}}} \cdot 6^{2^{\frac{n+4}{4}}}.$$

Рассмотрим два произвольных разбиения пространства E^n на совершенные расширенные двоичные коды и их матрицу пересечений. Она дает мощности попарных пересечений кодов из этих разбиений. В этом параграфе приведем оценки снизу и сверху количества различных матриц пересечений, полученных из произвольных двух разбиений E^n на совершенные расширенные двоичные коды.

Для получения оценок числа различных и неэквивалентных матриц пересечений, полученных из произвольных двух разбиений пространства E^n на совершенные расширенные двоичные коды, рассматривались сначала различные разбиения пространства E^n, которые использовались для построения двух разбиений пространства E^{2n} (здесь $n = 2^k$). При этом использовался и развивался далее, с применением свитчингов латинских квадратов, каскадный способ построения совершенных расширенных кодов и разбиений из [70].

Для получения нижней оценки числа различных матриц пересечений двух разбиений пространства E^n на совершенные расширенные двоичные коды длины n потребовалось оценить число различных матриц пересечений латинских квадратов. Для этой цели посредством свитчингов (локальных перестроек) подматриц порядка 2×2 внутри пары латинских квадратов специального вида было сконструировано мощное множество различных матриц пересечения двух латинских квадратов. Были доказаны следующие теоремы.

Теорема 13. *Для любого $n = 2^k > 8$, число различных матриц пересечения двух латинских квадратов порядка n не меньше чем 2^{n^4}.*

Теорема 14. *Для $n = 2^k$, $k > 2$, число различных матриц пересечений разбиений пространства E^n на совершенные расширенные двоичные коды не меньше 2^{cn^2}, где c — положительная константа.*

Теорема 15. *Для $n = 2^k$, $k > 3$, число неэквивалентных матриц пересечений разбиений пространства E^n на совершенные расширенные двоичные коды не меньше $2^{c'n^2}$, где c' — положительная константа.*

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

Результаты теорем 13–15 по исследованию матриц пересечений разбиений пространства E^n на совершенные расширенные двоичные коды были получены в работе [88].

Проблема построения разбиений пространства E^n рассматривалась также в ряде других работ, например, Т. Этционом и А. Варди в работе [106], а также в работах Ж. Рифы, К. Боргеса, М. Виллануэвой, К. Т. Фелпса, К. Фернандес. Используя свитчинги компонент, из разбиения пространства E^n на совершенные коды, содержащего некоторый совершенный код, можно построить множество различных разбиений пространства E^n, содержащих, в частности, этот код, см., например, [95, 146]. Исследованию свойств разбиений пространства E^n на совершенные коды, построению разбиений, имеющих специальное алгебраическое строение, посвящены работы [95, 142, 145], см. также [106, 131, 146].

В статье [117] исследованы разбиения пространства E^n на классы смежностей попарно различных кодов Хэмминга длины n. Здесь же рассмотрено несколько конструкций разбиений $\mathscr{P}=\{\bar{H}_0, \bar{H}_1, \bar{H}_2, \ldots, \bar{H}_n\}$ пространства E^n на $n+1=2^m$ классов смежности $\bar{H}_i = H_i + e_i$ различных линейных кодов Хэмминга H_i длины n, $i \in N = \{0, 1, 2, \ldots, n\}$. Напомним, что $e_i \in E^n$ — вектор из E^n с 1 только в i-й координатной позиции, а $e_0 = \mathbf{0}^n$ — нулевой вектор длины n, т. е. $\bar{H}_0 = \bar{H}$. Такое разбиение называется *разбиением на непараллельные коды Хэмминга длины* n. В этой статье приведена нижняя оценка числа таких разбиений:

Т е о р е м а 16. *Для каждого* $n=2^m-1$, $m \geqslant 4$, *существует, по крайней мере,*

$$\frac{n! \cdot 1344^{\frac{(n+1)(n-7)}{8^2}}}{7! \cdot (8!)^{\frac{n-7}{8}} \cdot |\mathrm{GL}(\log_2((n+1)/8), 2)|}$$

различных разбиений E^n *на непараллельные коды Хэмминга длины* n.

Для $n=15$ существует, по крайней мере, $1,53 \cdot 2^{42}$ различных разбиений E^{15} на непараллельные коды Хэмминга длины 15.

В статье [73] приводятся два метода построения вершинно-транзитивных и 2-транзитивных разбиений пространства F^n на совершенные коды, а также нижние оценки числа неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений F^n на совершенные коды длины n.

§ 6. q-значные совершенные коды

В данном параграфе обсудим некоторые результаты последних лет, касающиеся совершенных q-значных кодов.

Метод α-компонент был развит А. В. Лосем (учеником автора статьи) в 2006 г. для q-значных совершенных кодов, см. [51], что позволило ему получить нижнюю оценку числа таких кодов, которая оставалась наилучшей до 2010 г. В работе [51] было предложено исследование свитчингов так называемых простых компонент q-значного кода Хэмминга. Конструкция позволила получить следующую нижнюю оценку числа $N_q(n)$ различных совершенных q-значных кодов длины $n=(q^m-1)/(q-1)$, $m \geqslant 2$:

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

Эта оценка получена за счет выделения в коде Хэмминга простых компонент. Простые компоненты впервые были рассмотрены в статье [136]. Известно, что простая компонента специального вида является минимальной, т. е. неразложимой на компоненты меньшей мощности.

В 2010 г. Д. С. Кротов и У. Хеден, см. [116], предложили обобщение конструкции Кротова [45] для q-значных совершенных кодов. Используя s-арные квазигруппы и комбинированную конструкцию Д. С. Кротова, они получили наилучшую на сегодняшний день нижнюю оценку числа различных совершенных q-значных кодов:

Т е о р е м а 17. *Для числа $N_q(n)$ различных совершенных q-значных кодов длины $n=(q^m-1)/(q-1)$, $m\geqslant 2$, справедливо:*

$N_3(n)\geqslant \exp\exp(\frac{\ln 3}{3}n-O(1))$;

$N_5(n)\geqslant \exp\exp(\frac{\ln 375}{15}n-O(1))$;

$N_q(n)\geqslant \exp\exp(\frac{\ln\sqrt{q4/4-q^3+3q^2/4}}{q}n-O(\ln n))$ *при нечетных* $q>5$;

$N_q(n)\geqslant \exp\exp(\frac{\ln(q^2/2)}{q}n-O(\ln n))$, *если* $q=2^m$, $m\geqslant 1$.

6.1. Группы автоморфизмов q-значных совершенных кодов. Несколько работ Е. В. Горкунова [24–26] (ученика автора статьи) посвящено исследованию строения группы автоморфизмов q-значных кодов Хэмминга и некоторых их подкодов. Напомним, что для двоичного кода Хэмминга строение группы автоморфизмов хорошо известно, см. [122]. В [24, 26] детально изучается строение группы автоморфизмов q-значных кодов Хэмминга, $q>2$. В отличие от двоичного случая, в случае $q>2$ ситуация значительно сложнее и здесь различают несколько видов групп автоморфизмов для кода. Наиболее объемлющая группа автоморфизмов $Aut(C)$ q-значного кода C — как и в двоичном случае, это группа изометрий всего пространства F^n, переводящих код в себя; группа перестановочных автоморфизмов является подгруппой подстановок из $Aut(C)$, переводящих код C в себя; группа мономиальных автоморфизмов — подгруппа группы автоморфизмов $Aut(C)$, автоморфизмы которой задаются умножением на мономиальную матрицу; и, наконец, группа симметрий кода C — подгруппа $Aut(C)$, сохраняющая веса кодовых слов. Следует отметить, что в двоичном случае последние три вида групп совпадают. В [24] изучены перестановочные группы автоморфизмов двух типичных q-значных кодов Хэмминга: кода Хэмминга, заданного проверочной матрицей в каноническом виде и циклического q-значного кода Хэмминга. Установлено, что они имеют неизоморфные перестановочные группы автоморфизмов, что представляется неожиданным, поскольку код Хэмминга единствен с точностью до эквивалентности. В [26] доказано, что любая симметрия произвольного q-значного кода Хэмминга полулинейна, тем самым получено описание группы автоморфизмов кода Хэмминга, $q>2$. Для этого было изучено воздействие таких симметрий на множество кодовых слов кода Хэмминга веса 3, что представляет самостоятельный интерес, поскольку такой объект является неполной блок-схемой с весьма регулярным строением.

В работе [25] Е. В. Горкуновым изучены группы мономиальных автоморфизмов различных компонент q-значного кода Хэмминга, дано описание мономиальных групп автоморфизмов линейной, простой компонент и также обобщения простой компоненты на подполем — компоненты кода Хэмминга, названной p^s-компонентой. Напомним, что эти компоненты представляют собой линейные оболочки множества кодовых слов веса три (кода Хэмминга) с фиксированной i-й координатой, равной единице, взятые над полем $GF(q)$, его простым подполем $GF(q)$ и любым подполем $GF(p^s)$ поля $GF(q)$ соответственно.

6.2. Разбиения пространства F^N на q-значные совершенные коды. Проблема перечисления всех разбиений пространства F^N на совершенные q-значные коды длины $N=(q^m-1)/(q-1)$, так же как и в двоичном случае, тесно связана с классической проблемой перечисления всех совершенных q-значных кодов. Очевидно, что достаточно изучать только различные разбиения, поскольку, зная оценку снизу числа различных разбиений, легко оценить снизу число неэквивалентных таких разбиений с учетом порядка группы автоморфизмов F^N. Конструкции разбиений часто оказываются полезными для построения новых классов q-значных кодов, в частности, совершенных, см. в работе [103, гл. 11] обзор конструкций совершенных q-значных кодов, где также обсуждается ряд конструкций, в основе которых лежат разбиения пространства F^N на совершенные коды. Следует отметить, что для $q>2$ известно не так много работ, посвященных построению разбиений пространства F^N на совершенные коды, двоичный же случай исследован существенно шире, см. предыдущий параграф.

Для любого числа $N=(q^m-1)/(q-1)$, где $q>2$ — степень простого числа, в работе [75] предложены две конструкции построения различных разбиений множества F^N всех q-значных векторов длины N на совершенные q-значные коды длины N. Первый метод базируется на некоторой модификации известной конструкции Шонхайма [152] и является обобщением метода построения разбиений пространства всех двоичных векторов на совершенные двоичные коды, где была использована широко известная конструкция Васильева [17], см. предыдущий параграф. Второй метод построения разбиений F^N с использованием простых компонент и латинских квадратов дает наилучшую на сегодняшний день нижнюю оценку числа таких разбиений:

Т е о р е м а 18. *Число различных разбиений пространства F^N, $q>2$, на совершенные q-значные коды не меньше чем*

$$((L(p))^{p^{r-1}})^{KN}\cdot(p!)^{K(1-N)-1}, \tag{4}$$

где $K=p^{n(2r-1)-r(m-1)}$, $q=p^r$.

Два q-значных кода назовем *аффинно эквивалентными*, если существует изометрия пространства F^N, отображающая один код в другой с помощью перестановки координатных позиций в композиции со сдвигом на некоторый вектор пространства F^N. Следует отметить, что при $q=2$ и $q=3$ определения эквивалентности и аффинной эквивалентности совпадают. В статье [52] получен следующий результат, обобщающий аналогичный результат для совершенных двоичных кодов из [16].

Т е о р е м а 19. *Для всех $N=(q^m+1)/(q-1)$, $q=p^r>2$, $m\geqslant 4$, существует разбиение пространства F^N на попарно аффинно неэквивалентные совершенные q-значные коды длины N.*

§ 7. Проблема пересечения кодов

Проблема пересечения q-значных кодов состоит в следующем: *какие возможны мощности пересечения $\eta(C_1,C_2)$ двух кодов C_1 и C_2 длины N?* Этот вопрос был впервые сформулирован в 1994 г. Т. Этцион и А. Варди в работе [105] для совершенных двоичных кодов, см. также [106]. Число $\eta(C_1,C_2)$ называется числом пересечения кодов C_1 и C_2. Т. Этцион и А. Варди предложили полное решение проблемы пересечения двоичных кодов Хэмминга, нашли наименьшее пересечение для совершенных двоичных кодов любой допустимой длины, которое состоит всего из двух кодовых слов, а также получили возможные пересечения совершенных двоичных кодов, используя свитчинги i-компонент двоичных кодов Хэмминга (см. [106]).

С. Бар-Яшалом и Т. Этцион в 1997 г. решили проблему пересечения для любых, не обязательно совершенных, q-значных циклических кодов (см. [91]), $q \geqslant 2$.

В 2005 г. в статье [85] установлено, что для любых двух чисел k_1 и k_2 таких, что

$$1 \leqslant k_i \leqslant 2^{(n+1)/2-\log(n+1)},$$

$i = 1, 2$, существуют совершенные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, удовлетворяющие

$$\eta(C_1, C_2) = 2k_1k_2.$$

В 2006 г. в [86] доказано, что для всякого четного k_3, удовлетворяющего неравенствам $0 \leqslant k_3 \leqslant 2^{n+1-2\log(n+1)}$, найдутся совершенные коды C_1 и C_2 длины $n = 2^m - 1$, $m \geqslant 4$, такие, что

$$\eta(C_1, C_2) = k_3.$$

Следует отметить, что число кодовых слов в пересечении любых двух совершенных двоичных кодов всегда четно и удовлетворяет согласно [106] неравенствам

$$0 \leqslant \eta(C_1, C_2) \leqslant 2^{n-\log(n+1)} - 2^{(n-1)/2}, \tag{5}$$

причем верхняя оценка является достижимой. Сравнивая результаты работ [106], [85] и [86], убеждаемся, что результаты статьи [86] покрывают достаточно большую часть интервала (5), но не перекрывают результатов работы [85].

В 2010 г. в [118] впервые приводится улучшение верхней оценки Этциона и Варди (5): пусть C и D — произвольные совершенные двоичные коды длины $n \geqslant 15$. Тогда

$$0 \leqslant \eta(C, D) \leqslant 2^{n-\log(n+1)} - 2^{(n-1)/2} - 2(2n - 15). \tag{6}$$

Пересечение двух различных совершенных двоичных кодов, равное $2^{n-\log(n+1)} - 2^{(n-1)/2}$, представляет собой «спорадическое» значение.

В работе [118] с помощью компьютерных вычислений также построен широкий класс значений $\eta(C, D)$ для совершенных двоичных кодов C и D длины $n = 15$. Кроме того, методом α-компонент для $n > 15$ был найден новый спектр чисел пересечения для совершенных двоичных кодов C и D длины n.

Дальнейшее улучшение верхней оценки (6) было получено В. Н. Потаповым, см. [66], с использованием следующей идеи: можно показать, что двоичный вектор длины 2^n, отвечающий характеристической функции произвольного совершенного кода длины n, вложим в двоичный код Рида—Маллера $RM(r, n)$ порядка $r = (n-1)/2$ (это следует из неравенства Зигенталлера и того факта, что совершенный код C имеет, согласно [67] и [104], корреляционную иммунность, равную $(n+1)/2$). Напомним, что булевозначная функция от n переменных называется корреляционно-иммунной порядка m, если ее единицы равномерно распределены по граням размерности $n - m$. Далее достаточно рассмотреть сумму по модулю два характеристических функций двух произвольных совершенных двоичных кодов длины n и, применив к коду Рида—Маллера $RM((n-1)/2, n)$ теорему Касами и Токуры о спектре весов от d до $2d$ произвольного кода Рида—Маллера, имеющего расстояние d (см. [122], теорема 11 главы 15), можно доказать следующую теорему.

Т е о р е м а 20 [66]. *Пусть C и D — произвольные совершенные двоичные коды длины $n \geqslant 15$. Тогда*

$$0 \leqslant \eta(C, D) \leqslant 2^{n-\log(n+1)} - 3 \times 2^{(n+1)/2}/4.$$

Пересечение двух различных совершенных двоичных кодов, равное $2^{n-\log(n+1)}-2^{(n-1)/2}$, *представляет собой «спорадическое» значение.*

И. Ю. Могильных и автор данной статьи заметили, что, рассмотрев описанные ранее (см. выше в этом параграфе) числа пересечения совершенных двоичных кодов, используя данный подход, можно сделать вывод о том, какие именно веса кода Рида—Маллера $RM((n-1)/2, n)$ являются ненулевыми. Согласно теореме МакЭлиса (см. [122], теорема 12 главы 15) известно, что веса кодовых слов кодов Рида—Маллера $RM((n-1)/2, n)$ делятся на 4.

Таким образом оказалось, что проблема пересечения совершенных двоичных кодов непосредственно связана с проблемой описания весовых спектров кодов Рида—Маллера, которая, как широко известно, все еще остается нерешенной для $RM(r, m)$ при $r \geqslant 3$.

Что касается q-значных кодов, $q > 2$, то для них условие четности пересечения выполняется не обязательно, в частности, пересечение троичных кодов не всегда является четным. Более того, существуют совершенные троичные коды Хэмминга длины 4, пересечение которых составляет единственное кодовое слово. Такие коды могут быть заданы следующими проверочными матрицами:

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}, \qquad H_2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \end{bmatrix}.$$

В работе [74] исследуются пересечения q-значных совершенных кодов. Доказано, что существуют два q-значных совершенных кода C_1 и C_2 длины $N = qn + 1$ такие, что

$$|\, C_1 \cap C_2 \,| = k \cdot |P_i|/p$$

для каждого $k \in \{0, \ldots, p \cdot K - 2, p \cdot K\}$, где $q = p^r$, p — простое, $r \geqslant 1$, $n = \dfrac{q^{m-1}-1}{q-1}$, $m \geqslant 2$, $|P_i| = p^{nr(q-2)+n}$, $K = p^{n(2r-1)-r(m-1)}$. Показано также, что существуют два q-значных совершенных кода длины N, пересекающиеся по $p^{nr(q-3)+n}$ кодовым словам.

В 2008 г. в статье [137] К. Т. Фелпс и М. Виллануэва исследовали пересечения кодов Адамара. В статье [148] (см. также [149]) полностью решена проблема пересечения аддитивных (Z_4 и Z_2Z_4-линейных), расширенных и нерасширенных совершенных кодов. В этой работе были найдены верхняя и нижняя оценки этих мощностей, для любого допустимого числа в пределах этих оценок были построены коды, дающие в пересечении код мощности, равной этому числу. Более того, была охарактеризована структура абелевых групп — пересечений таких кодов, а также приведены конструкции всех возможных кодов-пересечений этих совершенных кодов. Аналогичный результат был получен для аддитивных (Z_4 и Z_2Z_4-линейных) кодов Адамара (дуальных кодов к Z_4 и Z_2Z_4-линейным совершенным кодам соответственно) в работе [150].

§ 8. Метрические свойства совершенных и близких к ним кодов

В теории совершенных кодов изучаются различные метрические и структурные свойства такие, как, например, вопросы вложимости кодов, восстановления кодов по заданным их частям. В этом параграфе рассмотрим несколько результатов за последние годы, посвященных таким исследованиям для совершенных кодов и ряда других двоичных кодов, в частности, кодов Препараты.

Вопросам изучения восстановимости кода по частям и исследованию разных проблем, связанных с изометриями кодов, были посвящены работы [61, 125] 2009 г. В этих статьях продолжены исследования, начатые в работах [1, 3, 5, 13]. В [61] исследуются вопросы восстановления произвольного кода Препараты (см. также [107]), в работе [125] — расширенного совершенного кода по графам минимальных расстояний этих кодов. Ранее в [3] С. В. Августинович исследовал аналогичный вопрос для совершенных двоичных кодов.

В статье [27] С. В. Августинович и Е. В. Горкунов продолжили изучение вопросов восстановления произвольных двоичных кодов по заданным их частям. Отображение двоичного кода, сохраняющее граневую размерность любого его подкода (т. е. размерность минимальной грани двоичного пространства, содержащей этот подкод), называется *сильной изометрией*. Отображение двоичного кода, сохраняющее граневую размерность любого его подкода четной мощности называется *полусильной изометрией*. В 2010 г. в работе [27] доказана

Теорема 21. *Всякая полусильная изометрия, отображающая один двочный код в другой, продолжаема до изометрии всего пространства.*

В статье [9] получено обобщение этой теоремы на q-значный случай.

В работе [22] вводится понятие реконструктивного множества в пространстве E^n (в терминах преобразования Фурье). В этой работе получена характеризация реконструктивных множеств, являющихся линейными подпространствами. Установлены необходимые и достаточные условия реконструктивности сферы в E^n. Кроме того, приведено достаточное условие реконструктивности двух концентрических сфер в пространстве E^n. В статье [23] А. Ю. Васильева исследует собственные функции пространства E^n. Получена формула, связывающая локальные распределения произвольной такой функции в паре ортогональных граней. Доказано, что при выполнении определенных условий собственная функция восстанавливается, частично или полностью, по своим значениям на сфере.

Рассмотрим несколько результатов диссертационной работы Д. С. Кротова [48], посвященных исследованию совершенных двоичных кодов и n-арных квазигрупп, последние известны в литературе также как латинские гиперкубы, являющиеся многомерными обобщениями латинских квадратов. Эти квазигруппы эквивалентны MDS-кодам (максимально дистанционно разделимым кодам — кодам, достигающим известной границы Синглтона) с расстоянием 2 и играют важную роль в построении совершенных кодов. Результаты по MDS-кодам см. подробнее в [48].

Д. С. Кротовым решена проблема дуальности для Z_{2^k}-линейных двоичных кодов, а именно, найдена связь между весовыми энумераторами двоичных образов дуальных линейных кодов над Z_{2^k}. Им построены ко-Z_{2^k}-линейные и Z_{2^k}-линейные коды с параметрами расширенных совершенных кодов и кодов Адамара. В [47, 48] Д. С. Кротовым приводится конструкция с дважды экспоненциальным числом совершенных троичных равновесных кодов; 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 $n-1$.

В статье [50] доказано, что множество s-арных квазигрупп порядка 4 является свитчингово связным для любого фиксированного n. Использование теоремы С. В. Августиновича и др. [84] о характеризации совершенных кодов малого ранга $n - \log(n+1) + 2$ посредством s-арных квазигрупп порядка 4 позволило доказать, что множество совершенных двоичных кодов длины n ранга не более чем $n - \log(n+1) + 2$ является свитчингово связным.

Следовательно, любой такой код можно получить из любого другого, в частности, кода Хэмминга, многократным применением свитчингов.

Помимо нижней оценки, полученной С. В. Августиновичем и Д. С. Кротовым (см. выше раздел 3.1) для совершенных двоичных кодов, в диссертации [48] приводится следующий результат 2009 г. этих же авторов (см. также оригинальную работу [87]):

Т е о р е м а 22. *Произвольный двоичный код C длины m, исправляющий одну ошибку, вложим в совершенный двоичный код длины $n=2^m-1$ такой, что при фиксации последних $n-m$ координат нулями из него получается код C.*

Этот результат обобщает классические теоремы К. Треш 1971 г. и Б. Гантера 1974 г. о вложении частичных систем троек и четверок Штейнера в полные системы троек и четверок Штейнера большего порядка соответственно. Напомним, что совокупность слов веса 3 произвольного совершенного кода, содержащего нулевой вектор, образует систему троек Штейнера; аналогично, совокупность слов веса 4 любого расширенного совершенного кода, содержащего нулевой вектор, образует систему четверок Штейнера. *Системой четверок Штейнера* $SQS(n)$ порядка n называется система сочетаний из n элементов по четыре такая, что каждая неупорядоченная тройка элементов содержится в точности в одной четверке.

В следующих работах исследуются вопросы вложимости систем троек (четверок) Штейнера малого ранга в совершенные (расширенные совершенные) коды.

В статье [169] В. А. Зиновьева и Д. В. Зиновьева посредством каскадных методов доказано, что любая система троек Штейнера порядка n ранга $n-\log(n+1)+2$ вложима в некоторый совершенный код длины n, при этом не указывается ранг этого совершенного кода. В [36] указано точное число таких систем троек Штейнера. В работе [35] изучен следующий случай, а именно вопрос вложимости систем троек Штейнера порядка n ранга $n-\log(n+1)+3$ в совершенные коды. В статье получен результат, аналогичный результату работы [169], при этом показано, что ранги совершенных кодов, содержащих эти системы троек, не могут быть больше, чем $n-\log(n+1)+6$.

В статье [42] Д. И. Ковалевской (ученицей автора обзора) и автором настоящей статьи с помощью свитчингового подхода дана классификация класса систем троек Штейнера $STS(n)$ порядка $n=2^r-1$, $r>3$, ранга $n-\log(n+1)+2$, совпадающего с совокупностью $STS(n)$, вложимых в совершенные двоичные коды длины n, имеющих такой же ранг. В этой же работе приведены верхняя и нижняя оценки для числа таких различных систем троек Штейнера порядка n. Кроме того, приведены описание и нижняя оценка числа различных систем троек Штейнера порядка n ранга не менее $n-\log(n+1)+2$, не вложимых в совершенные двоичные коды длины n такого же ранга. Результаты, аналогичные полученным в работе [42], также с помощью свитчингового подхода, получены в статьях [40, 41] для систем четверок Штейнера. В статье [31] доказано, что любая система четверок Штейнера порядка N, $N\geqslant 16$, ранга $N-\log N$ вложима в некоторый расширенный совершенный код длины N такого же ранга, а именно — в некоторый расширенный код Васильева. В [42] аналогичный результат получен для систем троек Штейнера порядка n ранга $n-\log(n+1)+1$, а именно показано, что такая система вложима в совершенный код длины n такого же ранга и этим кодом является код Васильева.

Напомним, что ранее В. Д. Тончев нашел точное число систем троек и четверок Штейнера порядков n и $N=n+1$ соответственно, имеющих малый ранг $n-\log(n+1)+1$ в работах [164, 165]. В статье [33] В. А. Зиновьевым

и Д. В. Зиновьевым были классифицированы и перечислены все различные системы четверок Штейнера порядка $N = 2^r$ ранга не больше $N - \log N + 1$ (безотносительно вложимости в совершенные коды), доказано, что все такие системы разрешимы.

§ 9. Совершенные раскраски

В последнее время исследованию совершенных раскрасок уделяется большое внимание и, по-видимому, настала пора посвятить описанию и анализу результатов, касающихся совершенных раскрасок, отдельный обзор, см., например, список публикаций в работах, упомянутых в данном параграфе.

Раскраска вершин графа в k цветов называется *совершенной* с матрицей параметров $S = \{S_{ij}\}$, если для любых двух цветов i и j каждая вершина цвета i имеет ровно $S = \{S_{ij}\}$ соседей цвета j. Для случая дистанционно регулярных графов понятие совершенной раскраски обобщает очень важное в теории кодирования понятие полностью регулярного кода, введенного Ф. Дельсартом в 1973 г. Напомним, что подмножество вершин графа называется *полностью регулярным кодом*, если для любой вершины y рассматриваемого графа число кодовых слов на расстоянии i от нее зависит лишь от i и расстояния от вершины y до кода C.

Была доказана серия теорем о совершенных раскрасках — естественного обобщения совершенных кодов (следует отметить, что совершенные коды можно всегда интерпретировать на языке совершенных раскрасок). В первую очередь, упомянем предтечу данных исследований — работу [2] 1995 г. С. В. Августиновича, где доказано, что произвольный совершенный код длины n, содержащий нулевой вектор, однозначно востанавливается по совокупности своих кодовых слов веса $(n-1)/2$. В 2003 г. С. В. Августиновичем и А. Ю. Васильевой в [6] приведены явные формулы восстановления центрированной функции или совершенного кода по значениям в среднем слое пространства E^n; в [7], см. также [90], доказано, что в E^n все значения центрированной функции в шаре радиуса $k \leqslant (n+1)/2$ однозначно вычисляются по ее радиальным суммам относительно вершин соответствующей сферы. *Радиальная сумма* относительно некоторого вектора пространства E^n определяется как сумма значений функции в наименьшей грани, содержащей этот вектор и центр сферы.

Множество перестановок

$$Sim_k(f) = \{\pi \in S_n \mid f(x) = f(\pi(x)),\ x \in W_k\}$$

назовем *группой симметрий центрированной функции f в k-м слое пространства E^n*. Справедливо следующее утверждение.

Теорема 23 [7]. *Пусть n нечетно, f — 0-центрированная функция в E^n. Тогда*

$$Sim_0(f) \geqslant Sim_1(f) \geqslant \ldots \geqslant Sim_{(n-1)/2}(f).$$

В частности, эта теорема верна для совершенных двоичных кодов и из нее вытекает

Следствие 2. *Группа симметрий произвольного совершенного двоичного кода длины n изоморфна группе симметрий совокупности его кодовых слов веса $(n-1)/2$.*

В работах [21, 166] А. Ю. Васильевой введены понятия локального и межвесового спектров произвольной раскраски (разбиения) пространства E^n как аналога и расширения понятия весового спектра кода. Здесь

же установлена взаимосвязь локальных спектров совершенной раскраски в двух ортогональных гранях пространства E^n и исследованы свойства межвесового спектра. На этой основе доказано новое метрическое свойство произвольной совершенной раскраски, а именно ее сильная дистанционная регулярность. Как следствие, получены аналогичные свойства полностью регулярных кодов.

Для произвольной собственной функции пространства E^n А. Ю. Васильевой в [167] получена взаимосвязь между ее локальными спектрами в двух ортогональных гранях. Получены условия, при которых собственная функция восстанавливается, целиком либо частично, по своим значениям в вершинах сферы.

Связь совершенных раскрасок пространства E^n и корреляционно-иммунных функций малой плотности исследуется В. Н. Потаповым в статье [65]. См. также работы [81, 82, 108] Д. Г. Фон-Дер-Флаасса, посвященные совершенным раскраскам пространства E^n и корреляционно-иммунным функциям.

Диссертации С. А. Пузыниной [68] и И. Ю. Могильных [62] непосредственно примыкают с изучению обобщений совершенных кодов и посвящены исследованию совершенных раскрасок бесконечной прямоугольной решетки и графов Джонсона соответственно. В работе [8] С. В. Августиновичем и др. перечислены параметры всех дистанционно регулярных раскрасок бесконечной квадратной решетки.

В работе [66] В. Н. Потаповым исследованы мощности компонент совершенных раскрасок, корреляционно-иммунных и бент-функций (множеств единиц этих функций), см. также выше теорему 20. Напомним, что бент-функциями называются булевы функции, максимально удаленные от множества линейных функций. *Компонентой функции* называется множество векторов, на котором функция отличается от другой функции с теми же параметрами. Показано, что для совершенных раскрасок, корреляционно-иммунных и бент-функций мощность компоненты в промежутке между 2^k и 2^{k+1} может принимать только значения вида $2^{k+1} - 2^p$, где p варьируется между 0 и k, а $2k$ — минимальная мощность компоненты для комбинаторного объекта с теми же параметрами. Для бент-функций доказано существование компонент любой мощности из данного спектра. Для совершенных раскрасок с некоторыми параметрами и корреляционно-иммунных функций найдены компоненты некоторых из указанных выше мощностей.

§ 10. Некоторые применения совершенных кодов

Результаты, полученные для совершенных кодов, с успехом применяются в теории кодирования для развития методов построения кодов с большими кодовыми расстояниями и исследования их свойств, например, для двоичных кодов с параметрами кодов Рида—Маллера, см. [70, 72, 139, 140] и параграфы 4 и 7 выше (напомним, что проблема пересечения совершенных двоичных кодов оказалась напрямую связанной с проблемой описания весовых спектров кодов Рида—Маллера, которая все еще не решена для $RM(r, m)$ при $r \geqslant 3$), для кодов Препараты, кодов Кердока, см. [76, 77, 80], MDS-кодов (см. [48] и список публикаций в этой работе) для диаметральных совершенных кодов с метрикой Джонсона и аналогов совершенных кодов в пространствах Грассмана, см. [83], пространствах Джонсона, см. [110, 124] и [62], а также список публикаций в работе [62]. Об аналогах совершенных кодов в других экзотических метриках можно найти информацию в [48].

Как было показано в параграфе 5, разбиения пространства E^n на совершенные коды достаточно хорошо изучены. Методы построения разбиений могут оказаться полезными для исследования разбиений простран-

ства E^n на коды, которые индуцируют раскраски, связанные с устойчивостью оптоволоконных сетей, см., например, [128]. Другой мотивацией исследования и построения разбиений пространства E^n на коды (не обязательно совершенные) является связь разбиений с проблемой построения и перечисления совершенных раскрасок, связанных с полностью регулярными кодами, partition designs, equitable partitions, см. работы Д. Г. Фон-Дер-Флааса [81, 82, 108], С. А. Пузыниной [68], И. Ю. Могильных [62].

В криптографии совершенные q-значные, $q > 2$, коды Хэмминга были использованы Г. Р. Блекли и Г. А. Кабатянским, см. [93], для создания совершенных схем разделения секретов. В статьях [141, 147] Ж. Рифа с соавторами предложили использование в стеганографии Z_2Z_4-линейных совершенных кодов.

Специального вида пересечения двоичных кодов Хэмминга, определяющие двоичные линейные коды длины $n = 2^m - 1$, размерности $n - 2m$ (где m нечетно) с кодовым расстоянием 5, задают широко известные в криптографии биективные APN-функции (почти совершенно нелинейные функции), которые имеют применение в S-блоках стандартов шифрования данных, см., например, [92, 102]. В работе [151] исследуются пересечения кодов Хэмминга, не имеющих подкодов Хэмминга с одинаковыми носителями или, что эквивалентно, соответствующие этим кодам проективные геометрии не имеют общих плоскостей. Среди таких классов пересечений кодов Хэмминга (которые в действительности задают коды с кодовым расстоянием как минимум 4) обнаружены как определяющие APN-функции, так и не задающие таковых, но последние также могут представлять интерес с точки зрения приложений в криптографии в силу своих экстремальных геометрических свойств. При $m \leqslant 4$ такие функции не существуют. Отметим, что до недавнего времени в случае кодов длины $2^m - 1$, $m > 4$ четного, было неизвестно существование биективных APN-функций. Недавно, см. [100], была обнаружена первая биективная APN-функция для четного m, равного 6.

СПИСОК ЛИТЕРАТУРЫ

1. Августинович С. В. О неизометрии совершенных бинарных кодов // Труды Института математики СО РАН. — 1994. — Т. 74. — С. 3–5.
2. Августинович С. В. Об одном свойстве совершенных бинарных кодов // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 1. — С. 4–6.
3. Августинович С. В. К строению графов минимальных расстояний совершенных бинарных $(n, 3)$-кодов // Дискретный анализ и исследование операций. Сер. 1. — 1998. — Т. 5, № 4. — С. 3–5.
4. Августинович С. В. О сильной изометрии бинарных кодов // Дискретный анализ и исследование операций. Сер. 1. — 2000. — Т. 7, № 3. — С. 3–5.
5. Августинович С. В. Комбинаторные и метрические свойства совершенных кодов и раскрасок. Канд. дисс. — Новосибирск, 2000.
6. Августинович С. В., Васильева А. Ю. Вычисление центрированной функции по ее значениям на средних слоях булева куба // Дискретный анализ и исследование операций. Сер. 1. — 2003. — Т. 10, № 2. — С. 3–16.
7. Августинович С. В., Васильева А. Ю. Теоремы восстановления для центрированных функций и совершенных кодов // Сибирский матем. журнал. — 2008. — Т. 49, № 3. — С. 1–6.
8. Августинович С. В., Васильева А. Ю., Сергеева И. В. Дистанционно регулярные раскраски бесконечной квадратной решетки // Дискретный анализ и исследование операций. — 2011. — Т. 18, № 3. — С. 3–10.
9. Августинович С. В., Горкунов Е. В. Восстановление кодов по коэффициентам корреляции их подкодов // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 6. — С. 3–8.
10. Августинович С. В., Соловьева Ф. И. О несистематических совершенных двоичных кодах // Проблемы передачи информации. — 1996. — Т. 32, вып. 3. — С. 47–50.
11. Августинович С. В., Соловьева Ф. И. Построение совершенных бинарных кодов последовательными сдвигами α-компонент // Проблемы передачи информации. — 1997. — Т. 33, вып. 3. — С. 15–21.

12. Августинович С.В., Соловьева Ф.И. Новые конструкции и свойства совершенных кодов // Труды Междунар. конференции по дискретному анализу и исследованию операций, Новосибирск, Россия, Июнь, 2000. — С. 5–10.
13. Августинович С.В., Соловьева Ф.И. О метрической жесткости двоичных кодов // Проблемы передачи информации. — 2003. — Т. 39, вып. 2. — С. 63–68.
14. Августинович С.В., Соловьева Ф.И., Хеден У. О проблеме рангов и ядер совершенных кодов // Проблемы передачи информации. — 2003. — Т. 39, вып. 4. — С. 341–345.
15. Августинович С.В., Соловьева Ф.И., Хеден У. О структуре группы симметрий кодов Васильева // Проблемы передачи информации. — 2005. — Т. 41, вып. 2. — С. 105–112.
16. Августинович С.В., Соловьева Ф.И., Хеден У. О разбиениях n-куба на неэквивалентные совершенные коды // Проблемы передачи информации. — 2007. — Т. 43, вып. 4. — С. 45–50.
17. Васильев Ю.Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. вып. 8. — М: Наука, 1962. — С. 337–339.
18. Васильев Ю.Л., Соловьева Ф.И. Кодообразующие факторизации n-мерного единичного куба и совершенных двоичных кодов // Проблемы передачи информации. — 1997. — Т. 33, вып. 1. — С. 64–74.
19. Васильева А.Ю. Спектральные свойства совершенных двоичных $(n, 3)$-кодов // Дискретный анализ и исследование операций. — 1995. — Т. 2, № 2. — С. 16–25.
20. Васильева А.Ю. Спектральные свойства совершенных двоичных кодов. Канд. дисс. — Новосибирск, 1999.
21. Васильева А.Ю. Локальные и межвесовые спектры вполне регулярных кодов и совершенных раскрасок // Проблемы передачи информации. — 2009. — Т. 45, вып. 2. — С. 84–90.
22. Васильева А.Ю. О реконструктивных множествах вершин в булевом кубе // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 1. — С. 3–16.
23. Васильева А.Ю. Локальные распределения и восстановление собственных функций гиперкуба // Проблемы передачи информации. — 2013. — Т. 49, вып. 1. — С. 37–45.
24. Горкунов Е.В. Группа перестановочных автоморфизмов q-ичного кода Хэмминга // Проблемы передачи информации. — 2009. — Т. 45, № 4. — С. 18–25.
25. Горкунов Е.В. Мономиальные автоморфизмы линейной и простой компонент кода Хэмминга // Дискретный анализ и исследование операций. Сер. 1. — 2010. — Т. 17, № 1. — С. 11–33.
26. Горкунов Е.В. Группа автоморфизмов q-ичного кода Хэмминга // Дискретный анализ и исследование операций. Сер. 1. — 2010. — Т. 17, № 6. — С. 50–55.
27. Горкунов Е.В., Августинович С.В. О восстановлении двоичных кодов по размерностям их подкодов // Дискретный анализ и исследование операций. Сер. 1. — 2010. — Т. 17, № 5. — С. 15–21.
28. Гуськов Г.К. О разбиениях двоичного векторного пространства на совершенные коды // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 2. — С. 15–25.
29. Гуськов Г.К., Соловьева Ф.И. О предельно-транзитивных расширенных совершенных кодах // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 5. — С. 31–44.
30. Зиновьев В.А. Комбинаторные методы построения и анализа нелинейных корректирующих кодов. Докт. дисс. — Москва, 1988.
31. Зиновьев В.А., Зиновьев Д.В. О кодах Васильева длины $n = 2^m$ и удвоение систем Штейнера $S(n, 4, 3)$ заданного ранга // Проблемы передачи информации. — 2006. — Т. 42, вып. 1. — С. 13–33.
32. Зиновьев В.А., Зиновьев Д.В. Двоичные расширенные совершенные коды длины 16 ранга 14 // Проблемы передачи информации. — 2006. — Т. 42, вып. 2. — С. 63–80.
33. Зиновьев В.А., Зиновьев Д.В. О разрешимости систем Штейнера $S(v = 2^m, 4, 3)$ ранга $r \leqslant v - m + 1$ над F^2 // Проблемы передачи информации. — 2007. — Т. 43, вып. 1. — С. 39–55.
34. Зиновьев В.А., Зиновьев Д.В. Двоичные совершенные и расширенные совершенные коды длины 15 и 16 с рангами 13 и 14 // Проблемы передачи информации. — 2010. — Т. 46, вып. 1. — С. 20–24.
35. Зиновьев В.А., Зиновьев Д.В. Структура систем троек Штейнера $S(2^{m-1}, 3, 2)$ ранга $2^{m-m} + 2$ над F_2 // Проблемы передачи информации. — 2013. — Т. 49, № 3. — С. 40–56.
36. Зиновьев В.А., Зиновьев Д.В. Письмо в редакцию // Проблемы передачи информации. — 2013. — Т. 49, № 2. — С. 107–111.
37. Зиновьев В.А., Леонтьев В.К. О совершенных кодах // Проблемы управления и теории информации. — 1972. — Вып. 1. — С. 26–35.

38. Зиновьев В.А., Леонтьев В.К. Теорема о несуществовании совершенных кодов над полями Галуа. Препринт ИППИ АН СССР. — М., 1973.
39. Зиновьев В.А., Леонтьев В.К. Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. — 1973. — вып. 2. — С. 123–132.
40. Ковалевская Д.И., Соловьева Ф.И. О системах четверок Штейнера малого ранга, вложимых в расширенные совершенные двоичные коды // Дискретный анализ и исследование операций. — 2012. — Т. 19, № 5. — С. 47–62.
41. Ковалевская Д.И., Соловьева Ф.И. Системы четверок Штейнера малых рангов и расширенные совершенные двоичные коды // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 4. — С. 46–64.
42. Ковалевская Д.И., Соловьева Ф.И., Филимонова Е.С. О системах троек Штейнера малого ранга, вложимых в совершенные двоичные коды // Дискретный анализ и исследование операций. — 2013. — Т. 20, № 3. — С. 3–25.
43. Кротов Д.С. Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискретный анализ и исследование операций. Сер. 1. — 2000. — Т. 7, № 2. — С. 47–53.
44. Кротов Д.С. Z_4-линейные совершенные коды // Дискретный анализ и исследование операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 78–90.
45. Кротов Д.С. Комбинированная конструкция совершенных двоичных кодов // Проблемы передачи информации. — 2000. — Т. 36, вып. 4. — С. 74–79.
46. Кротов Д.С. Конструкции плотно упакованных кодов и нижние оценки их числа. Канд. дисс. — Новосибирск, 2000.
47. Кротов Д.С. Индуктивные конструкции совершенных троичных равновесных кодов // Проблемы передачи информации. — 2001. — Т. 37, вып. 1. — С. 3–11.
48. Кротов Д.С. Совершенные коды и n-арные квазигруппы: конструкции и классификация. Докт. дисс. — Новосибирск, 2010.
49. Кротов Д.С., Потапов В.Н. Асимптотика числа n-квазигрупп порядка 4 // Сибирский матем. журнал. — 2006. — Т. 47. № 4. — С. 873–887.
50. Кротов Д.С., Потапов В.Н. О свитчинговой эквивалентности n-арных квазигрупп порядка 4 и совершенных двоичных кодов // Проблемы передачи информации. — 2010. — Т. 46, вып. 3. — С. 22–28.
51. Лось А.В. Построение совершенных q-ичных кодов свитчингами простых компонент // Проблемы передачи информации. — 2006. — Т. 42, вып. 1. — С. 34–42.
52. Лось А.В., Соловьева Ф.И. О разбиениях пространства F_q^N на аффинно неэквивалентные совершенные q-значные коды // Siberian Electronical Mathematical Reports. — 2010. — Т. 7. — С. 425–434.
53. Малюгин С.А. О нижней оценке числа совершенных двоичных кодов // Дискретный анализ и исследование операций. Сер. 1. — 1999. — Т. 6, № 1. — С. 44–48.
54. Малюгин С.А. О перечислении совершенных двоичных кодов длины 15 // Дискретный анализ и исследование операций. Сер. 1. — 1999. — Т. 6, № 2. — С. 48–73.
55. Малюгин С.А. О порядке группы автоморфизмов совершенных двоичных кодов // Дискретный анализ и исследование операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 91–100.
56. Малюгин С.А. Несистематические совершенные двоичные коды // Дискретный анализ и исследование операций. Сер. 1. — 2001. — Т. 8, № 1. — С. 55–76.
57. Малюгин С.А. Транзитивные совершенные коды длины 15 // Труды конф. «Дискретный анализ и исследование операций». — Новосибирск: Изд-во Ин-та математики — 2004. — С. 96.
58. Малюгин С.А. О классах эквивалентности совершенных двоичных кодов длины 15. Препринт № 138. — Новосибирск: Институт математики СО РАН, 2004. — С. 34.
59. Малюгин С.А. О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискретный анализ и исследование операций. Сер. 1. — 2006. — Т. 13, № 1. — С. 77–98.
60. Малюгин С.А. О несистематических совершенных кодах над конечными полями // Дискретный анализ и исследование операций. Сер. 1. — 2009. — Т. 16. — С. 44–63.
61. Могильных И.Ю. О слабых изометриях кодов Препараты // Проблемы передачи информации. — 2009. — Т. 45, вып. 2. — С. 78–83.
62. Могильных И.Ю. Совершенные раскраски графов Джонсона. Канд. дисс. — Новосибирск, 2010.
63. Нечаев А.А. Коды Кердока в циклической форме // Дискретная математика. — 1989. — Т. 1, № 4. — С. 123–139.
64. Потапов В.Н. О нижней оценке числа транзитивных совершенных кодов // Дискретный анализ и исследование операций. Сер. 1. — 2006. — Т. 13, № 4. — С. 49–59.
65. Потапов В.Н. О совершенных раскрасках булева n-куба и корреляционно-иммунных функциях малой плотности // Siberian Electronical Mathematical Reports. — 2010. — Т. 7. — С. 372–382.

66. Потапов В.Н. Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Проблемы передачи информации. — 2012. — Т. 48, №1. — С. 54–63.
67. Пулатов А.К. О геометрических свойствах и схемной реализации подгрупп в E^n // Методы дискретного анализа в теории кодов и схем. — Новосибирск: Ин-т математики СО АН СССР. — 1973. — вып. 23. — С. 32–37.
68. Пузынина С.А. Совершенные раскраски бесконечной прямоугольной решетки // Канд. дисс. — Новосибирск, 2008.
69. Романов А.М. О несистематических совершенных кодах длины 15 // Дискретный анализ и исследование операций. — 1997. — Т. 4, № 4. — С. 75–78.
70. Соловьева Ф.И. О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. — Новосибирск: Ин-т математики СО АН СССР. — 1981. — вып. 37. — С. 65–76.
71. Соловьева Ф.И. О построении транзитивных кодов // Проблемы передачи информации. — 2005. — Т. 41, вып. 3. — С. 23–31.
72. Соловьева Ф.И. О Z_4-линейных кодах с параметрами кодов Рида—Маллера // Проблемы передачи информации. — 2007. — Т. 43, вып. 1. — С. 41–47.
73. Соловьева Ф.И., Гуськов Г.К. О построении вершинно-транзитивных разбиений n-куба на совершенные коды // Дискретный анализ и исследование операций. Сер. 1. — 2010. — Т. 17, № 3. — С. 84–100.
74. Соловьева Ф.И., Лось А.В. О пересечениях q-значных совершенных кодов // Сибирский матем. журнал. — 2008. — Т. 49, № 2. — С. 464–474.
75. Соловьева Ф.И., Лось А.В. О построении разбиений F_q^n на совершенные q-значные коды // Дискретный анализ и исследование операций. — 2009. — Т. 16, № 3. — С. 63–73.
76. Соловьева Ф.И., Токарева Н.Н. О дистанционной нерегулярности кодов Препараты // Сибирский матем. журнал. — 2007. — Т. 48, № 2. — С. 408–416.
77. Соловьева Ф.И., Токарева Н.Н. Дистанционная регулярность кодов Кердока // Сибирский матем. журнал. — 2008. — Т. 49, № 3. — С. 668–681.
78. Соловьева Ф.И., Топалова С.Т. О группах автоморфизмов совершенных двоичных кодов и систем троек Штейнера // Проблемы передачи информации. — 2000. — Т. 36, вып. 4. — С. 53–58.
79. Соловьева Ф.И., Топалова С.Т. Совершенные двоичные коды и системы троек Штейнера с максимальными порядками групп автоморфизмов // Дискретный анализ и исследование операций. Сер. 1. — 2000. — Т. 7, № 4. — С. 101–110.
80. Токарева Н.Н. О компонентах кодов Препараты // Проблемы передачи информации. — 2004. — Т. 40, вып. 2. — С. 63–69.
81. Фон-Дер-Флаасс Д.Г. Совершенные 2-раскраски гиперкуба //Сибирский матем. журнал. — 2007. — Т. 48 — С. 923–930.
82. Фон-Дер-Флаасс Д.Г. Совершенные 2-раскраски 12-мерного куба // Siberian Electronical Mathematical Reports. — 2007. — Т. 4. — С. 292–295.
83. Ahlswede R., Aydinian H., Khachatrian L. On perfect codes and related concepts // Des., Codes and Cryptogr. — 2001. — V. 22. — P. 221–237.
84. Avgustinovich S. V., Heden O., Solov'eva F. I. The classification of some perfect codes // Des., Codes and Cryptogr. — 2004. — V. 31, №3. — P. 313–318.
85. Avgustinovich S. V., Heden O., Solov'eva F. I. On intersections of perfect binary codes // Bayreuther Mathematische Schriften. — 2005. — V. 71. — P. 8–13.
86. Avgustinovich S. V., Heden O., Solov'eva F. I. On intersection problem for perfect binary codes // Des., Codes and Cryptogr. — 2006. — V. 39. — P. 317–322.
87. Avgustinovich S. V., Krotov D.S. Embedding in a perfect code // J. Comb. Des. — 2009. — V. 17, № 5. — P. 419–423.
88. Avgustinovich S.V., Lobstein A., Solov'eva F.I. Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory. — 2001. — V. 47, № 4. — P. 1621–1624.
89. Avgustinovich S.V., Solov'eva F.I. Perfect binary codes with trivial automorphism group // Proc. of Int. Workshop on Information Theory. — 1998. — P. 114–115.
90. Avgustinovich S. V., Vasil'eva A.Yu. Testing sets for perfect codes // Lecture Notes in Computer Science. — 2006. — V. 4123. — P. 938–940.
91. Bar-Yahalom S.E., Etzion T. Intersection of isomorphic linear codes // Journal of Combin. Theory. Series A 80. — 1997. — P. 247–256.
92. Berger T. P., Canteaut A., Charpin P., Laigle-Chapuy Y. On Almost Perfect Nonlinear Functions Over F_2^n // IEEE Trans. Inform. Theory. — 2006. — V. 52, №9. — P. 4160–4170.

93. Blakley G.R., Kabatianski G.A. When perfect secret sharing schemes with veto exist // Proc. Sixth Int. Workshop on Algebraic and Comb. Coding Theory. — 1998. — P. 30–33.
94. Borges J., Fernandes C., Phelps K.T. Quaternary Reed-Muller codes // IEEE Trans. Inform. Theory. — 2005. — V. 51, №7. — P. 2686–2691.
95. Borges J., Fernandez C., Rifá J., Villanueva M. Constructions of 1-perfect partitions on the n-cube $(Z/2)^n$ // Technical report PIRDI 1/01, ETSE. — 2001.
96. Borges J., Mogilnykh I. Yu., Rifa J., Solov'eva F. I. Structural properties of binary propelinear codes // Advances in Math. Commun. — 2012. — V. 6, №3. — P. 329–346.
97. Borges J., Mogilnykh I. Yu., Rifa J., Solov'eva F. I. On the number of nonequivalent propelinear extended perfect codes // The Electronic J. of Combinatorics. — 2013. — V. 20, № 2. — P. 37–50.
98. Borges J., Phelps K.T., Rifá J., Zinoviev V.A. On $\mathbb{Z}_4$-Linear Preparata-Like and Kerdock-Like Codes // IEEE Trans. Inform. Theory. — 2003. — V. 49, №11. — P. 2834–2843.
99. Borges J., Rifá J. A characterization of 1-perfect additive codes // IEEE Trans. Inform. Theory. — 1999. — V. 45, №5. — P. 1688–1697.
100. Browning K.A., Dillon J.F., McQuistan M.T., Wolfe A.J. An APN Permutation in Dimension Six // Contemporary Mathematics. — 2010. — V. 518 — P. 33–42.
101. Calderbank A.R., Cameron P.J., Kantor W.M., Seidel J.J. $\mathbb{Z}_4$-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets // Proc. London Math. Soc. — 1997. — V. 75. — P. 436–480.
102. Carlet C., Charpin P., Zinoviev V. Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems // Des. Codes and Cryptogr. — 1998. — V. 15, №2. — P. 125–156.
103. Cohen G., Honkala I., Lobstein A., Litsyn S. Covering codes. — Elsevier, 1998.
104. Delsarte P. Bounds for unrestricted codes by linear programming // Philips Res. Report. — 1972. — №27. — P. 272–289.
105. Etzion T., Vardy A. Perfect binary codes: constructions, properties and enumeration // IEEE Trans. Inform. Theory. — 1994. — V.40, №3. — P. 754–763.
106. Etzion T., Vardy A. On perfect codes and tilings: problems and solutions // SIAM J. Discrete Math. — 1998. — V. 11, №2. — P. 205–223.
107. Fernandez-Cordoba C., Phelps K. T. On the minimum distance graph of an extended Preparata code // Des., Codes and Cryptogr. — 2010. — V. 57, №2. — P. 161–168.
108. Fon-Der-Flaass D.G. A bound of correlation ummunity // Siberian Electronical Mathematical Reports. — 2007. — V. 4. — P. 133–135.
109. Golomb S.W., Posner E.C. Rook domains, latin squares, affine and error distributing codes // IEEE Trans. Inform. Theory. — 1964. — V. 10. — P. 196–208.
110. Gordon D.M. Perfect single error-correcting codes in th Johnson scheme // IEEE Trans. Inform. Theory. — 2006. — V. 52. — P. 4670–4672.
111. Guskov G.K., Mogilnykh I.Yu., Solov'eva F.I. Ranks of propelinear perfect binary codes // Siberian electronic Mathematical Reports. — 2013. — V. 10. — P. 443–449.
112. Guskov G. K., Solov'eva F. I. Properties of perfect transitive binary codes of length 15 and extended perfect transitive binary codes of length 16, 2012, *ArXiv*, http://arxiv.org/abs/1210.5940
113. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P. The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes // IEEE Trans. Inform. Theory. — 1994. — V. 40, №2. — P. 301–319.
114. Heden O. A full rank perfect code of length 31 // Des., Codes Cryptogr. — 2006. — V. 38, №1.— P. 125–129.
115. Heden O. A survey of perfect codes // Advances Math. Commun. — 2008. — V. 2, №2. — P. 223–247.
116. Heden O., Krotov D.S. On the structure of non-full-rank perfect q-ary codes // Advances in Math. of Communications. — 2011. — V. 5, №2. — P. 149–156.
117. Heden O., Solov'eva F.I. Partitions of F^n into nonparallel Hamming codes // Advances Math. Commun. — 2009. — V. 3, №4. — P. 385–397.
118. Heden O., Solov'eva F.I., Mogilnykh I.Yu. Intersections of perfect binary codes // Proc. of 2010 IEEE Region Intern. Conference on Computational Technologies in Electrical and Electronics Engeneering SIBIRCON 2010 — 2010. — P. 52–54.
119. Hergert F. Algebraische Methoden fur Nichtlineare Codes // Thesis Darmstadt. — 1985.
120. Krotov D.S. $\mathbb{Z}_4$-linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography WCC 2001. — Paris. — 2001. — P. 329–334.
121. Krotov D.S., Avgustinovich S.V. On the number of 1-perfect binary codes: A lower bound // IEEE Trans. Inf. Theory. — 2008. — V. 54, №4. — P. 1760–1765.

122. MacWilliams F.G., Sloane N.J.A. The theory of error correcting codes. — New York: North-Holland. — 1977. — 744 p. [Имеется перевод: Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. — М.: Связь, 1979. — 744 с.]
123. Malyugin S.A. Perfect codes with trivial automorphism group // Proc. Second Int. Workshop on Optimal Codes and Related Topics. — 1998. — P. 163–167.
124. Martin W.J. Completely regular subsets. Ph. D. Dissertation. — Univ. Waterloo, 1992.
125. Mogilnykh I.Yu., Östergård P.R.J., Pottonen O., Solov'eva F.I. Reconstructing extended perfect binary one-error-correcting codes from their minimum distance graphs // IEEE Trans. Inform. Theory. — 2009. — V. 55. — P. 2622–2625.
126. Mollard M. A generalized parity function and its use in the construction of perfect codes // SIAM J. Alg. Disc. Meth. — 1986. — V. 7, №1. — P. 113–115.
127. Nechaev A.A., Kuzmin A.S. $\mathbb{Z}_4^n$-linearity, two approaches// Proc. of Fourth Int. Workshop on Algebraic and Comb. Coding Theory. — 1996. — P. 112–115.
128. Östergård P.R.J. On a hypercube coloring problem // J. Combin. Theory Ser. A. — 2004. — V. 108. — P. 199–204.
129. Östergård P.R.J., Pottonen O. The Perfect Binary One-Error-Correcting Codes of Length 15: Part I — Classification // IEEE Trans. Inform. Theory. — 2009. — V. 55. — P. 4657–4660.
130. Östergård P.R.J., Pottonen O., Phelps K.T. The Perfect Binary One-Error-Correcting Codes of Length 15: Part II — Properties // IEEE Trans. Inform. Theory. — 2010. — V. 56. — P. 2571–2582.
131. Phelps K.T. A General Product Construction for Error Correcting Codes // SIAM J. Algebraic Discrete Methods. — 1984. — V. 5. — P. 224–228.
132. Phelps K.T. An enumeration of 1-perfect binary codes of length 15 // Australian Journal of Combin. — 2000. — V. 21. — P. 287–298.
133. Phelps K.T., LeVan M. Kernels of nonlinear Hamming codes // Des., Codes and Cryptogr. — 1995. — V. 6. — P. 247–257.
134. Phelps K.T., LeVan M. Nonsystematic perfect codes // SIAM Journal of Discrete Math. — 1999. — V. 12, №1. — P. 27–34.
135. Phelps K.T., LeVan M. Switching equivalence classes of perfect codes // Des., Codes and Cryptogr. — 1999. — V. 16, №2. — P. 179–184.
136. Phelps K.T., Rifá J., Villanueva M. Kernels of q-ary 1 perfect codes // Proc. Int. Workshop on Coding and Cryptography. — 2003. — P. 375–381.
137. Phelps K.T., Villanueva M. Intersection of Hadamard codes // IEEE Trans. Inform. Theory. — 2008. — V. 53, №5. — P. 1924–1928.
138. Pujol J., Rifá J. Additive Reed-Muller codes, Proc. of Int. Symp. on Inform. Theory. — 1997. — P. 508.
139. Pujol J., Rifá J., Ronguillo L. Construction of Additive Reed-Muller Codes // Lecture Notes in Computer Science. — 2009. — V. 5527, P. 223–226.
140. Pujol J., Rifá J., Solov'eva F. I. Construction of Z4-Linear Reed-Muller Codes // IEEE Trans. Inform. Theory. — 2009. — V. 55, №1. — P. 99–104.
141. Rifá H., Rifá J., Ronquillo L. Z2Z4-additive perfect codes in steganography // Advances Math. Commun. — 2011.— V. 5, T 3. — P. 425–433.
142. Rifá J. Well-ordered Steiner triple systems and 1-perfect partitons of the n-cube // SIAM J. Discrete Math. — 1999. — V. 12, №1. — P. 35–47.
143. Rifa J., Basart J. M., Huguet L. On completely regular propelinear codes // Proc. 6th Int. Conference AAECC-6 — 1989. — V. 357 LNCS. P. 341–355.
144. Rifa J., Pujol J. Translation invariant propelinear codes // IEEE Trans. Inform. Theory. — 1997. — V. 43. — P. 590–598.
145. Rifá J., Pujol J., Borges J. 1-Perfect uniform and distance invariant partitions // Applicable Algebra in Engineering, Communucation and Computing. — 2001. — V. 11. — P. 297–311.
146. Rifá J., Vardy A. On partitions of space into perfect codes // Workshop on Coding and Information Integrity. — 1997.
147. Rifá J., Ronquillo L. Product Perfect Z2Z4-linear codes in steganography // In Proceedings of the 2010 International Symposium of Information Theory and its Applications Publication on-line. — 2010. — P. 696–701.
148. Rifá J., Solov'eva F.I., Villanueva M. On the intersection of additive perfect codes // IEEE Trans. Inform.Theory. — 2008. — V. 54, №3. — P. 1346–1356.
149. Rifá J., Solov'eva F. I., Villanueva M. On the intersection of additive extended and non-extended perfect codes // Proc. Int. Workshop on Coding and Cryptography. — 2007. — P. 333–341.
150. Rifá J., Solov'eva F. I., Villanueva M. On the intersection of Z2Z4-additive Hadamard codes // IEEE Trans. Inform. Theory. — 2009. — V. 55, №4. — P. 1766–1774.

151. Riſá J., Solov'eva F. I., Villanueva M. Intersection of Hamming codes avoiding Hamming subcodes // Des., Codes and Cryptogr. — 2012. — V. 62, №2. — P. 209–223.
152. Schönheim J. On linear and nonlinear single-error-correcting q-nary 1-perfect codes // Inform. Control. — 1986. — V. 12. — P. 23–26.
153. Shapiro G.S., Slotnik D.L. On the mathematical theory of error correcting codes // IBM J. Res. and Devel. — 1959. — V. 3, № 1. — P. 25–34 [Имеется перевод: Шапиро Г.С., Злотник Д.Л. К математической теории кодов с исправлением ошибок // Кибернетич. сб. вып. 5. — М.: Изд-во иностр. лит., 1962. — С. 7–32.]
154. Solov'eva F.I. Constructions of perfect binary codes . Preprint 98-042, Universität Bielefeld, Sonderforschungsbereich 343 Discrete Structuren in der Mathematik. — 1998. P. 12.
155. Solov'eva F.I. Switchings and perfect codes // Numbers, Information and Complexity. — Kluwer Academic Publisher. — 2000. — P. 311–314.
156. Solov'eva F.I. Perfect binary codes: bounds and properties // Discrete Math. — 2000. — V. 213. — P. 283–290.
157. Solov'eva F.I. Structure of i-components of perfect binary codes // Discrete Appl. Math. — 2001. — V. 111, №1–2. — P. 189–197.
158. Solov'eva F.I. On transitive codes // Proc. of Int. Workshop on Discrete Analysis and Operation Research. — 2004. — P. 99.
159. Solov'eva F. I. On perfect codes and related topics, Com^{2}Mac // Lecture Note Series 13 — Pohang 2004.
160. Solov'eva F.I. On perfect binary codes // Discrete Appl. of Math. — 2008. — V. 156, №9. — P. 1488–1498.
161. Solov'eva F. I. Switching Methods for Error-Correcting Codes // Aspects of Network and Information Security. Series D: Information and Communication Security. — IOS Press. — 2008. — V. 17. — P. 333–342.
162. Solov'eva F.I., Avgustinovich S.V., Honold T., Heise W. On the extendability of code isometries // J. of Geometry. — 1998. — V. 61. — P. 3–16.
163. Tietäväinen A. On the nonexistence of perfect codes over finite fields. // SIAM J. Appl. Math. — 1973. — V. 24. — P. 88–96.
164. Tonchev V. D. A mass formula for Steiner triple systems $STS(2^n-1)$ of 2-rank 2^n-n // Journal of Combin. Theory. — 2001. — Series A, V. 95. — P. 197–208.
165. Tonchev V. D. A formula for the number of Steiner quadruple systems on 2^n points of 2-rank 2^n-n // Journal of Combin. Designs. — 2003. — № 11. — P. 260–274.
166. Vasil'eva A. Yu. Local and Interweight Spectra of completely regular codes and perfect colourings // 10'th Int. Workshop «Algebraic and Combinatorial Coding Theory». — 2006. — P. 161–164.
167. Vasil'eva A. Yu. Local Distribution and Reconstruction of Hypercube Eigenfunctions // Twelth Int. Workshop «Algebraic and Combinatorial Coding Theory». — 2010. — P. 292–297.
168. Zinoviev V.A. On Generalized Concatenated Codes // Colloquia Mathematica Societatis Janos Bolyai. — 1975. — V. 16 — P. 587–592.
169. Zinoviev V.A., Zinoviev D.V. Steiner Triple Systems $S(2^m-1,3,2)$ of Rank 2^m-m+1 over F_2 // Problems of Inform. Transm. — 2012. — V. 48, №2. — P. 102–126.

Поступило в редакцию: первый вариант 21.I.2011,
окончательный вариант 2.XI.2013.