ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 1**

УДК 621.391.15

© 2019 г. **Ж. Боржес[1], Ж. Рифа[1], В.А. Зиновьев[2]**

О ПОЛНОСТЬЮ РЕГУЛЯРНЫХ КОДАХ

Представлен обзор результатов по полностью регулярным кодам. Рассмотрены известные свойства, взаимосвязи с другими комбинаторными структурами, а также методы построения таких кодов. Обсуждена также проблема существования и известные результаты для некоторых частных случаев. Кроме того, представлены несколько новых результатов о полностью регулярных кодах с радиусом покрытия $\rho = 2$ и о расширении полностью регулярных кодов.

DOI: 10.1134/S0134347519010017

§ 1. Введение

В 1959 г. Шапиро и Злотник [1] доказали, что двоичные совершенные коды полностью регулярны (этот термин тогда не использовался). Позднее, в 1971 г., Семаков, Зиновьев и Зайцев [2] доказали, что коды Препараты, расширенные коды Препараты и расширенные совершенные коды полностью регулярны (этот термин также не использовался). В 1973 г. Дельсарт [3] ввел термин *полностью регулярный код* в метрике Хэмминга. Такие коды обладают достаточно плотной упаковкой в пространстве; к ним относятся совершенные и расширенные совершенные коды [2], равномерно упакованные коды [2,4,5], коды, полученные их расширением [2], а также полностью транзитивные коды [6–9]. Известные полностью регулярные коды – это, например, коды Хэмминга, Голея, БЧХ (длины $2^{2m+1} - 1$ с расстоянием $d = 5$) и два кода Адамара (длины 11 и 12). Комбинаторные свойства полностью регулярных кодов позволяют установить различные взаимосвязи с другими комбинаторными конфигурациями, такими как дистанционно регулярные графы, схемы отношений и t-схемы. Всеобъемлющим текстом об этих взаимосвязях является монография Брауэра, Коэна и Ньюмайера [10, гл. 11], дополненная обзором ван Дама, Кулена и Танаки [11]. Таблицу параметров возможных полностью регулярных кодов конечной длины и их массивов пересечений, построенную Куленом, Кротовым и Мартином, можно найти в [12]. В недавней работе [13] Кулен, Ли, Мартин и Танака рассмотрели и классифицировали класс так называемых арифметических полностью регулярных кодов.

Известно, что полностью регулярные коды существуют для произвольно большого радиуса покрытия (см., например, прямое построение кодов с линейно растущим радиусом покрытия в работе Соле [6]). Однако не известно ни одного нетривиального полностью регулярного кода с большим кодовым расстоянием, более того, не известно полностью регулярного кода с минимальным расстоянием $d > 8$ и более чем двумя кодовыми словами. В 1973 г. несуществование неизвестных совершенных

[1] Работа выполнена при частичной финансовой поддержке гранта Испании TIN2016-77918-P (AEI/FEDER, UE).

[2] Работа выполнена в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

кодов над конечными полями было независимо доказано Титвайненом в [14] и Зиновьевым и Леонтьевым в [15]. Аналогичный результат для квазисовершенных равномерно упакованных кодов был получен в 1975 г. Геталсом и ван Тилборгом [4, 5] (бесконечные семейства таких кодов были исключены ранее в [2]). Для частного случая двоичных линейных полностью транзитивных кодов в 2001 г. Боржес, Рифа и Зиновьев [16, 17] доказали несуществование таких кодов для $d > 8$, имеющих более двух кодовых слов. В 1992 г. Ньюмайером [18] была высказана естественная гипотеза о том, что единственным полностью регулярным кодом, имеющим более двух кодовых слов, с минимальным расстоянием $d \geqslant 8$ является двоичный расширенный код Голея. Однако Боржес, Рифа и Зиновьев [19] нашли контрпример к гипотезе Ньюмайера. Точнее, они доказали, что половина совершенного двоичного кода Голея, составленная из слов четного веса, также является полностью регулярным кодом с минимальным расстоянием $d = 8$. Тем не менее существование нетривиальных неизвестных полностью регулярных кодов с $d \geqslant 9$ является главной открытой проблемой в этой области. В настоящем обзоре мы рассматриваем полностью регулярные коды только для конечных длин и с конечным числом кодовых слов (о полностью регулярных кодах в бесконечных решетках см., например, работу [20] и библиографию в ней). Также рассмотрены полностью регулярные коды в схемах Джонсона $J(n, w)$. Обсуждена проблема существования совершенных кодов в таких схемах, поставленная еще Дельсартом [3] в 1973 г., и приведены известные результаты по полностью регулярным кодам, совершенным раскраскам и полностью регулярным схемам в схеме Джонсона $J(n, w)$.

План обзора выглядит следующим образом. В § 2 введены основные понятия и приведены предварительные результаты по полностью регулярным кодам в схемах Хэмминга. В конце рассмотрены некоторые необходимые условия существования полностью регулярных кодов, а также расширения таких кодов. Затем § 3 посвящен полностью транзитивным кодам, которые являются частным случаем полностью регулярных кодов. В § 4 приводятся известные результаты по полностью регулярным кодам в схемах Джонсона. Наконец, в § 5 собраны различные методы построения полностью регулярных кодов в схемах Хэмминга.

§ 2. Предварительные результаты о полностью регулярных кодах

2.1. Полностью регулярные и связанные с ними коды. Мы будем рассматривать только коды над конечными полями $\mathbb{F}_q = GF(q)$, где q – степень простого числа, с метрикой Хэмминга. Множество всех векторов пространства $\mathbb{F}_q^n$ с отношениями эквивалентности R_i, $i = 0, 1, \ldots, n$, задаваемыми условием $(x, y) \in R_i$, если и только если $d(x, y) = i$ (где $d(x, y)$ – число позиций, в которых x и y различны), называется *схемой отношений Хэмминга* или просто *схемой Хэмминга* и обозначается $H(q, n)$. Для кодов над кольцами часто используется метрика Ли. Во многих случаях такие коды можно рассматривать как двоичные коды, полученные с помощью известного отображения Грея. Следовательно, их можно рассматривать как двоичные коды с расстоянием Хэмминга. Как обычно, для кода $C \subset \mathbb{F}_q^n$ используются обозначения n, d, e и ρ для его длины, минимального расстояния, радиуса упаковки (или корректирующей способности) и радиуса покрытия соответственно. Если C – линейный код, то через k обозначается его размерность (или число информационных символов). Используются стандартные обозначения $(n, M, d)_q$ для q-ичного кода длины n и мощности (или числа его кодовых слов) M с минимальным расстоянием d. Если код линейный, то вместо мощности указывается его размерность, и код обозначается через $[n, k, d]_q$. Код с радиусом упаковки e часто называется e-кодом. Если необходимо указать также радиус покрытия ρ, то обозначения будут выглядеть как $(n, M, d; \rho)_q$ для нелинейного кода и $[n, k, d; \rho]_q$ для линейного. Для двоичного случая ($q = 2$) индекс q опускается. Если не оговорено противное, всегда предполагается,

что код C является дистанционно инвариантным, т.е. его весовой спектр не зависит от выбора нулевого слова [21]. Для линейного $[n,k,d]_q$-кода C дуальный к нему $[n,n-k,d^\perp]_q$-код $C^\perp$ определяется следующим образом:

$$C^\perp = \{x \in \mathbb{F}_q^n : \langle x \cdot y\rangle = 0 \text{ для каждого } y \in C\},$$

где через $\langle x \cdot y\rangle$ обозначено внутреннее произведение векторов x и y в $\mathbb{F}_q^n$.

Напомним несколько простых общеизвестных операций над кодами, позволяющих получить новые коды из уже известных. Для двоичного кода C длины n с минимальным расстоянием $d = 2e+1$ обозначим через C^* код, полученный из C добавлением еще одной проверочной позиции (*общей проверки на четность*). Код C^* (*расширение* кода C) имеет уже длину $n^* = n+1$, минимальное расстояние $d^* = 2e+2$ и ту же мощность $M^* = M$. Для q-ичного кода C расширение означает код, полученный добавлением еще одной позиции к каждому кодовому слову, так чтобы в результирующем коде для каждого кодового слова сумма в $\mathbb{F}_q$ его координат равнялась нулю. Для кода C длины n назовем *i-выколотым кодом* код, полученный из C удалением i-й позиции из всех слов кода C. Если же координата i не указана, то предполагается, что параметры результирующего кода не зависят от выбора позиции i. Назовем *a-укороченным кодом* код, полученный из C выбором всех кодовых слов, имеющих элемент a в фиксированной координате, и затем удалением этой координаты. Аналогичным образом скажем, что код получен укорочением кода C, если его параметры не зависят от выбора a. В более общем случае для векторов $x_1,\dots,x_r$ длины $j < n$ скажем, что код получен $\{x_1,\dots,x_r\}$-укорочением кода C, если он получен фиксированием некоторых j позиций кодовых слов, выбором всех слов C, совпадающих на этих позициях с одним из векторов $x_1,\dots,x_r$, и затем отбрасыванием j фиксированных позиций. Таким образом, результирующий код имеет длину $n-j$ и расстояние

$$d' \geqslant d - \max_{\substack{i,i' \in \{1,\dots,r\}\\ i \neq i'}} d(x_i, x_{i'}).$$

Для двоичного кода C обозначим через $\mathrm{Aut}(C)$ его группу автоморфизмов, т.е. множество перестановок координат, которые не меняют данный код (как множество его кодовых слов). Для q-ичного случая используются мономиальные перестановки, когда координаты кодовых слов также умножаются на ненулевые элементы поля $\mathbb{F}_q$. Скажем, что код C *тривиален*, если он имеет мощность $M = |C| \leqslant 2$ или совпадает со всем пространством $C = \mathbb{F}_q^n$.

Пусть задан код $C \subset \mathbb{F}_q^n$. Для заданного вектора $x \in \mathbb{F}_q^n$ обозначим через $B_{x,i}$ число кодовых слов на расстоянии i от x, где $0 \leqslant i \leqslant n$. Назовем *матрицей внешних спектров* кода C матрицу B размера $q^n \times (n+1)$ с элементами

$$B_{x,i} = |\{v \in C \mid d(x,v) = i\}|.$$

Как следует из определения, строка B_x представляет собой весовой спектр сдвига кода C на вектор x, т.е. спектр кода $C+x$. Обозначим через $b+1$ число различных строк матрицы B.

Обозначим через $d(x,C) = \min\limits_{v \in C}\{d(x,v)\}$ расстояние между вектором x и кодом C, т.е. расстояние между x и ближайшим к нему кодовым словом. В этой терминологии радиус покрытия кода ρ_C равен максимальному значению $d(x,C)$, когда x пробегает все пространство. Определим множества

$$C(i) = \{x \in \mathbb{F}_q^n \mid d(x,C) = i\}.$$

Множества $C, C(1), \ldots, C(\rho)$ названы в [18] *подкомпонентами*, а некоторые другие авторы называют их *слоями*. Заметим, что $C(0) = C$ и что $C(t) \neq \varnothing$, если и только если $t \leqslant \rho$.

Скажем, что двоичный код C длины n *антиподален*, если для любого кодового слова $c \in C$ имеется кодовое слово $\bar{c}$, находящееся на расстоянии n от c, т.е. $\bar{c} = c + (1, 1, \ldots, 1)$. Очевидно, что если C представляет собой двоичный дистанционно инвариантный код и содержит кодовое слово веса n, то C антиподален. Если же $(1, \ldots, 1) \notin C$, то C неантиподален.

Определение 1 [4]. Код C с радиусом покрытия ρ называется *t-регулярным*, $0 \leqslant t \leqslant \rho$, если для всех $i = 0, \ldots, t$ величина $B_{x,i}$ зависит только от i и от расстояния $d(x, C)$ от вектора x до C для всех x, таких что $d(x, C) \leqslant t$.

Другими словами, код C является t-регулярным, если B_x зависит только от $d(x, C)$ для всех расстояний $d(x, C) \leqslant t$. По определению, если C t-регулярен, то он и j-регулярен для всех $j = 0, \ldots, t$. Интуитивно, код C t-регулярен, если мы "видим" одно и то же число кодовых слов на тех же самых расстояниях от любого вектора x, находящегося на расстоянии не более t от кода C. Например, 0-регулярный код в точности представляет собой дистанционно инвариантный код.

Имеется несколько эквивалентных определений полностью регулярного кода (ПР-кода).

Определение 2 [3]. Код C *полностью регулярен*, если он ρ-регулярен.

Очевидно, что следующие определения эквивалентны:

(i) Код C является ПР-кодом, если для всех $x \in \mathbb{F}_q^n$ величина $B_{x,i}$ зависит только от i и расстояния $d(x, C)$.

(ii) Код C является ПР-кодом, если для всех $x \in \mathbb{F}_q^n$ весовой спектр B_x зависит только от расстояния $d(x, C)$.

(iii) Если для кода C имеет место равенство $b = \rho$, то он является ПР-кодом.

Однако увидеть эквивалентность приведенных выше определений и следующего определения не столь просто. Два вектора x и y из $\mathbb{F}_q^n$ назовем *соседями*, если они находятся друг от друга на расстоянии $d(x, y) = 1$.

Определение 3 [18]. Код C *полностью регулярен*, если для всех $\ell \geqslant 0$ каждый вектор $x \in C(\ell)$ имеет одно и то же число c_ℓ соседей в $C(\ell - 1)$ и одно и то же число b_ℓ соседей в $C(\ell + 1)$, где полагаем $c_0 = b_\rho = 0$.

Очевидно, что множества $C, C(1), \ldots, C(\rho)$ индуцируют разбиение всего пространства $\mathbb{F}_q^n$ на подкомпоненты кода C. Такое разбиение называется *дистанционным разбиением*. Если условия определения 3 удовлетворяются, то такое разбиение называется *равнодистанционным*. Следовательно, C является ПР-кодом, если и только если его дистанционное разбиение равнодистанционно.

Об эквивалентности определений 2 и 3 см. [18, теорема 4.1] или [22]. Для $\ell \geqslant 0$ положим $a_\ell = n(q-1) - b_\ell - c_\ell$. Таким образом, a_ℓ – это число соседей в $C(\ell)$ для любого вектора из $C(\ell)$. Параметры a_ℓ, b_ℓ и c_ℓ называются *числами пересечений*, а последовательность $\mathrm{IA} = \{b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho\}$ – *массивом пересечений* кода C.

Приведем примеры ПР-кодов. Напомним, что код C является *совершенным*, если $\rho = e$, и *квазисовершенным*, если $\rho = e + 1$. Следующие коды являются тривиальными совершенными кодами:

1. Одно кодовое слово $C = \{x\}$, $x \in \mathbb{F}_q^n$;
2. Все пространство $C = \mathbb{F}_q^n$;
3. Двоичные коды нечетной длины с повторением, состоящие из двух слов длины n с расстоянием между ними $d = n$.

Нетривиальные совершенные коды существуют только для $e \leqslant 3$ [14, 15]. В $\mathbb{F}_q^n$ известны следующие совершенные коды:

1. Двоичный код Голея с параметрами $n = 23$, $k = 12$, $d = 7$;
2. Троичный код Голея с параметрами $n = 11$, $k = 6$, $d = 5$;
3. Совершенные коды с параметрами $n = (q^m - 1)/(q - 1)$, $M = q^{n-m}$, $d = 3$.

В последнем случае для каждой степени q простого числа и каждой длины $n = (q^m-1)/(q-1)$ имеется единственный линейный код, называемый кодом Хэмминга.

Интересным классом кодов, тесно связанных с ПР-кодами, являются *равномерно упакованные коды* (РУ-коды). Имеются три основных класса РУ-кодов, удовлетворяющие разным условиям. Отметим, что равномерно упакованные коды были введены в 1971 г. в [2].

Определение 4 [2]. Двоичный квазисовершенный код C с минимальным расстоянием $d = 2e + 1$ называется *равномерно упакованным в узком смысле*, если существует натуральное число μ, такое что $B_{x,e} + B_{x,e+1} = \mu$ для любого вектора $x \in C(e) \cup C(e + 1)$.

Подчеркнем, что все двоичные совершенные коды попадают в этот класс кодов с параметром $\mu = (n + 1)/(e + 1)$, названным в [2] *плотностью упаковки*; для всех других кодов μ меньше $(n + 1)/(e + 1)$. РУ-коды в узком смысле включают в себя коды, полученные укорочением двоичных совершенных кодов на одну позицию. В этот класс входят коды Препараты, двоичные примитивные коды БЧХ с расстоянием 5 длины $2^{2m+1} - 1$, код Адамара длины 11. В [2] было доказано в терминах определения 2 (iii), что все РУ-коды в узком смысле, а также коды, полученные их расширением (равномерно упакованные уже не в узком смысле, а в широком, см. определение 6 ниже), являются ПР-кодами.

РУ-коды в узком смысле являются подклассом РУ-кодов, введенных в 1975 г. Гёталсом и ван Тилборгом [4].

Определение 5 [4]. Квазисовершенный q-ичный код C, исправляющий e ошибок, называется *равномерно упакованным*, если существуют натуральные числа λ и μ, такие что для любого вектора x величина $B_{x,e+1}$ принимает два значения:

$$B_{x,e+1} = \begin{cases} \lambda, & \text{если } d(x, C) = e, \\ \mu, & \text{если } d(x, C) = e + 1. \end{cases}$$

Для случая $\mu = \lambda + 1$ любой такой двоичный код является РУ-кодом в узком смысле. Заметим, что двоичные расширенные совершенные коды входят в этот класс кодов для значений $\lambda = 0$ и $\mu = (n + 1)/(e + 1)$ [2]. Эти коды включают в себя также троичный код Голея, код, полученный его расширением, и код, полученный его укорочением (на одну позицию). Ван Тилборг [5] (см. также [2, 23]) показал, что для $e > 3$ никаких других кодов, кроме указанных, не существует.

Следующий результат обобщает результат работы [2] на РУ-коды.

Предложение 1 [4]. *Равномерно упакованный код полностью регулярен.*

Заметим, что расширение любого РУ-кода, не являющегося совершенным, вообще говоря, может уже не быть РУ-кодом. Это было одним из мотивирующих фактов для введения следующего класса РУ-кодов.

Определение 6 [24]. Код C с радиусом покрытия ρ называется *равномерно упакованным кодом в широком смысле*, если существуют рациональные числа $\beta_0, \ldots, \beta_\rho$, такие что для любого вектора $x \in \mathbb{F}_q^n$ имеет место следующее равенство:

$$\sum_{i=0}^{\rho} \beta_i B_{x,i} = 1.$$

Числа $\beta_0, \ldots, \beta_\rho$ называются *параметрами упаковки* (например, для совершенных кодов все эти числа равны: $\beta_i = 1$ для всех $i = 0, 1, \ldots, \rho = e$). Введенный

выше класс кодов намного шире, чем коды, введенные в определениях 4 и 5. Другими словами, код C представляет собой РУ-код в широком смысле, если столбец из всех единиц является линейной комбинацией первых ρ столбцов матрицы внешних спектров B. Далее будет видно, что любой ПР-код всегда равномерно упакован в широком смысле.

Прежде чем привести несколько простых примеров ПР-кодов, еще раз упомянем работу Гёталса и ван Тилборга [4], которые ввели также *равномерно упакованные коды порядка* j, представляющие собой промежуточный класс таких кодов между РУ-кодами и РУ-кодами в широком смысле. Примеры ПР-кодов:

1. Как уже отмечалось, любой совершенный код полностью регулярен [1];
2. Множество всех векторов четного веса представляет собой линейный ПР-код с $\rho = 1$ [2];
3. Двоичный расширенный совершенный код является квазисовершенным РУ-кодом, и поэтому полностью регулярен [2];
4. Для любого ПР-кода C его подкомпонента $C(\rho)$ также полностью регулярна, а ее массив пересечений получен инверсией массива кода C [18].

2.2. t-схемы и дистанционно регулярные графы. Две комбинаторные структуры, тесно связанные с ПР-кодами и представляющие особый интерес, это *t-схемы* и *дистанционно регулярные графы*.

Определение 7. Схема $T = T(v, k, t, \lambda)$ (называемая также t-(v, k, λ)-схемой) представляет собой инцидентную структуру $(X, \mathcal{B})$, где X – множество из v элементов (называемых также *точками*), а $\mathcal{B}$ – семейство k-подмножеств множества X (называемых *блоками*), такие что каждое t-подмножество множества X содержится ровно в λ блоках, где $0 \leqslant t \leqslant k \leqslant v$.

В терминах (двоичной) матрицы инцидентности схема $T(v, k, t, \lambda)$ представляет собой двоичный код C длины $n = v$ с кодовыми словами веса $w = k$, такими что любой двоичный вектор длины n и веса t покрыт в точности λ кодовыми словами. Схема $T(v, k, t, \lambda)$ называется *простой*, если она не содержит повторяющихся блоков (в этом случае соответствующий код C имеет расстояние 2 или более) и *нетривиальной*, если она не содержит все k-подмножества X. Схема $T(v, k, t, \lambda)$ с $\lambda = 1$ называется *системой Штейнера* и обозначается также через $S(v, k, t)$. Следующие свойства t-схем хорошо известны и могут быть найдены, например, в монографиях [25–27].

Предложение 2. *Для заданной схемы $T(v, k, t, \lambda)$ каждое i-подмножество элементов, $0 \leqslant i \leqslant t$, содержится ровно в λ_i блоках, где*

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}.$$

Следствие 1. *Пусть задана $T(v, k, t, \lambda)$-схема T. Тогда*

(i) *T является схемой $T(v, k, i, \lambda_i)$ для любого $i \leqslant t$;*
(ii) *$\lambda = \lambda_t$;*
(iii) *число блоков схемы T равно $b = \lambda_0$;*
(iv) *каждый элемент из X содержится в одном и том же числе блоков, а именно в $r = \lambda_1 = bk/v$ блоках (величина r называется* числом повторений*).*

Схемы с $t \leqslant 5$ известны давно – с 1938 г. (начиная со знаменитых схем Витта [28], т.е. с систем Штейнера $S(24, 8, 5)$ и $S(12, 6, 5)$). Первые нетривиальные схемы с $t = 6$ были построены в 1983 г. Магливерасом и Ливиттом [29]. В 1987 г. Терлинк [30] доказал существование нетривиальных простых t-схем для любого натурального числа t. Существует естественное обобщение t-схем на q-ичный случай (см. [1, 3, 4, 15, 31, 32]).

Пусть $E = \{0, 1, \ldots, q-1\}$. Семейство $\mathcal{B}$ векторов x длины v и веса k над E называется схемой $T(v, k, t, \lambda)_q$, если для каждого вектора y над E длины v и веса t имеется ровно λ векторов $x_{i_1}, \ldots, x_{i_\lambda}$ из $\mathcal{B}$, таких что $d(y, x_{i_j}) = k - t$ для всех $j = 1, \ldots, \lambda$. Если $\lambda = 1$, то получаем q-ичную систему Штейнера, обозначаемую через $S(v, k, t)_q$.

Для заданного кода C обозначим через C_w множество всех его кодовых слов веса w. Для вектора $x = (x_1, \ldots, x_n)$ из E^n обозначим через $\mathrm{supp}(x)$ его *носитель*, т.е. множество номеров его ненулевых позиций:

$$\mathrm{supp}(x) = \{i : \ x_i \neq 0\}.$$

Из регулярности кода C следует, что множества C_w являются t-схемами. Для РУ-кодов в узком смысле этот факт был указан в 1971 г. в [2].

Теорема 1 [4]. *Пусть C является e-регулярным кодом с минимальным расстоянием $d \geqslant 2e$, тогда носители его кодовых слов из любого непустого множества C_w представляют собой матрицу инцидентности e-схемы (индуцируют e-схему).*

Непосредственно из определения ПР-кода получаем следующий результат.

Теорема 2. *Пусть C – q-ичный ПР-код длины n с расстоянием d.*

(i) *Если $d = 2e + 1$, то любое непустое множество C_w является схемой $T(n, w, e, \lambda_w)_q$.*

(ii) *Если $d = 2e + 2$, то любое непустое множество C_w является схемой $T(n, w, e + 1, \lambda_w)_q$.*

(iii) *Если C – q-ичный совершенный код, то любое непустое множество C_w является схемой $T(n, w, e + 1, \lambda_w)_q$, а множество C_d – системой Штейнера $S(n, 2e + 1, e + 1)_q$.*

(iv) *Если C – расширенный двоичный совершенный код с расстоянием $d = 2e + 2$, то любое непустое множество C_w является схемой $T(n, w, e+2, \lambda_w)_q$, а множество C_d – системой Штейнера $S(n, 2e + 2, e + 2)_q$.*

Пусть Γ – конечный связанный простой граф (т.е. неориентированный граф без петель и кратных ребер). Пусть $d(\gamma, \delta)$ – расстояние между двумя вершинами γ и δ, т.е. число ребер в минимальном пути между γ и δ). *Диаметром* D графа Γ называется наибольшее расстояние между двумя вершинами графа. Две вершины γ и δ из Γ называются *соседями*, если $d(\gamma, \delta) = 1$ (т.е. если они связаны ребром). Обозначим

$$\Gamma_i(\gamma) = \{\delta \in \Gamma : \ d(\gamma, \delta) = i\}.$$

Автоморфизмом графа Γ называется перестановка π множества вершин Γ, такая что для всех $\gamma, \delta \in \Gamma$ условие $d(\gamma, \delta) = 1$ имеет место, если и только если $d(\pi(\gamma), \pi(\delta)) = 1$.

Определение 8 [10]. Простой связанный граф Γ называется *дистанционно регулярным*, если он регулярен с валентностью k и для любых двух вершин $\gamma, \delta \in \Gamma$, находящихся на расстоянии i друг от друга, имеется ровно c_i соседей вершины δ в множестве $\Gamma_{i-1}(\gamma)$ и b_i соседей δ в множестве $\Gamma_{i+1}(\gamma)$. Более того, этот граф называется *дистанционно транзитивным*, если для любой пары вершин γ, δ на расстоянии $d(\gamma, \delta)$ имеется автоморфизм π из его группы автоморфизмов $\mathrm{Aut}(\Gamma)$, переводящий эту пару (γ, δ) в любую другую пару вершин γ', δ', находящихся на том же расстоянии $d(\gamma, \delta) = d(\gamma', \delta')$ друг от друга.

Последовательность $\{b_0, b_1, \ldots, b_{D-1}; c_1, c_2, \ldots, c_D\}$, где D – диаметр графа Γ, называется (так же как и для ПР-кодов) *массивом пересечений* графа Γ. Положим $a_i = k - b_i - c_i$. Числа a_i, b_i и c_i называются *числами пересечений* этого графа. Очевидно, что $b_0 = k$, $b_D = c_0 = 0$ и $c_1 = 1$.

Пусть C – линейный ПР-код с радиусом покрытия ρ и массивом пересечений $\mathrm{IA} = \{b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho\}$. Пусть $\{A\}$ обозначает множество всех смежных классов кода C. Определим граф Γ_C, называемый *графом смежных классов* кода C, выбирая в качестве множества вершин графа все различные смежные классы $A = C + x$, где ребро соединяет пару вершин, если два соответствующих смежных класса содержат пару соседних векторов. Иначе говоря, две вершины $\gamma = \gamma(A)$ и $\gamma' = \gamma(A')$ соединены ребром (т.е. являются соседями), если и только если смежные классы A и A' содержат векторы $v \in A$ и $u \in A'$, такие что $d(v, u) = 1$.

2.3. Параметры и свойства ПР-кодов. Для кода C обозначим через $s + 1$ число ненулевых координатных позиций в векторе, дуальном к усредненному вектору спектра расстояний кода C, полученному преобразованием Мак-Вильямс [21]. Параметр s был назван Дельсартом [3] *внешним расстоянием*, и он равен числу ненулевых весов в коде $C^\perp$, если C – линейный код. Этот параметр является ключевым для ПР-кодов, в чем можно убедиться по их свойствам. Напомним, что матрица B представляет собой матрицу внешних спектров кода C, а величина $b+1$ равна числу различных строк в матрице B.

Теорема 3. *Имеют место следующие утверждения*:

(i) $\mathrm{rank}(B) = s + 1$ [3];
(ii) $b \geqslant s$ [6];
(iii) $\rho \leqslant s$ [3].

Следовательно, выполняются неравенства $e \leqslant \rho \leqslant s \leqslant b$. В этих терминах имеют место следующие характеризации рассматриваемых здесь кодов.

Теорема 4. *Имеют место следующие утверждения*:

(i) *Код C совершенен, если и только если $e = s$* [3];
(ii) *Код C равномерно упакован, если и только если $s = e + 1$* [2, 4];
(iii) *Если код C полностью регулярен, то $\rho = s$* [6];
(iv) *Код C равномерно упакован в широком смысле, если и только если $\rho = s$* [33].

Утверждение, обратное к (iii), вообще говоря, неверно. Дельсарт [3] привел пример расширенного квадратично-вычетного $[48, 24, 12]$-кода с параметрами $\rho = s = 8$ и $b = 14$. Однако то же самое условие является необходимым и достаточным для РУ-кодов в широком смысле. Следовательно, имеет место

Следствие 2. *Если код C полностью регулярен, то он равномерно упакован в широком смысле.*

В работах [34, 35] было построено много бесконечных семейств РУ-кодов в широком смысле, которые не полностью регулярны. Следующие свойства ПР-кодов получены Дельсартом [3].

Теорема 5 [3]. *Имеют место следующие утверждения*:

(i) *Если $t \geqslant d - s \geqslant 0$, то C – t-регулярный код*;
(ii) *Если C – t-регулярный код, причем $t \geqslant s - 1$ и $d \geqslant 2s - 1$, то C полностью регулярен.*

Условия этой теоремы можно усилить, если все слова кода C имеют четный вес (такой код называется *четным*).

Следствие 3. *Пусть C – четный код. Тогда*

(i) *Если $t \geqslant d - s + 1 \geqslant 0$, то C t-регулярен* [33];
(ii) *Если $d \geqslant 2s - 2$, то C полностью регулярен* [10].

Теорема 6. *Пусть C – неантиподальный ПР-код с радиусом покрытия ρ.*

(i) *Множество $C(\rho)$ представляет собой сдвиг кода C на вектор $(1, \ldots, 1)$* [19];
(ii) *Множество $C \cup C(\rho)$ является ПР-кодом* [36].

2.4. Необходимые условия существования ПР-кодов. Для заданного ПР-кода C с радиусом покрытия ρ и числами пересечений a_i, b_i, c_i определим следующую трехдиагональную матрицу A, называемую *матрицей пересечений*:

$$A = \begin{bmatrix} a_0 & b_0 & 0 & \dots & 0 & 0 \\ c_1 & a_1 & b_1 & \dots & 0 & 0 \\ 0 & c_2 & a_2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{\rho-1} & b_{\rho-1} \\ 0 & 0 & 0 & \dots & c_\rho & a_\rho \end{bmatrix}.$$

Следующее утверждение называется теоремой Ллойда для ПР-кодов. Напомним, что собственными значениями схемы Хэмминга $H(q,n)$ являются собственные значения матрицы пересечений этой схемы $H(q,n)$, которые равны $(q-1)n - qj$, $j = 0, 1, \dots, n$.

Теорема 7 [10,18]. *Пусть C – ПР-код длины n с матрицей пересечений A. Тогда A имеет ρ целых собственных значений, которые являются собственными значениями схемы $H(q,n)$.*

Так как любой ПР-код является РУ-кодом в широком смысле, то существует другой вариант этой теоремы, который в некоторых случаях может быть более полезным и который представляет собой естественное обобщение классической теоремы Ллойда для совершенных кодов (см. [21]). Обозначим через K_i мощность множества $C(i)$. Определим $\varkappa_i$, полагая $K_i = \varkappa_i |C|$. Легко видеть, что

$$\varkappa_i = \beta_i (q-1)^i \binom{n}{i},$$

где $\beta_0, \beta_1, \dots, \beta_\rho$ – параметры упаковки РУ-кода (см. определение 7).

Теорема 8 [24]. *Пусть код C длины n равномерно упакован в широком смысле с параметрами упаковки $\beta_0, \beta_1, \dots, \beta_\rho$. Тогда обобщенный многочлен Ллойда степени ρ от ξ*

$$L_\rho(n,\xi) = \sum_{r=0}^{\rho} \beta_r P_r(n,\xi), \tag{1}$$

где $P_r(n,\xi)$ – многочлен Кравчука

$$P_r(n,\xi) = \sum_{j=o}^{r} (-1)^{r-j} (q-1)^j \binom{n-\xi}{j} \binom{\xi}{r-j}$$

и для любого вещественного числа a

$$\binom{a}{i} = \frac{1}{i!}\, a(a-1)\dots(a-i+1),$$

имеет ρ различных целочисленных корней в диапазоне от 0 до n.

Следующая теорема обобщает классическое *условие сферической упаковки* для совершенных кодов на РУ-коды в широком смысле, и следовательно, на любой полностью регулярный код.

Теорема 9 [24]. *Пусть код C длины n равномерно упакован в широком смысле с параметрами упаковки $\beta_0, \beta_1, \ldots, \beta_\rho$. Тогда мощность кода имеет вид*

$$|C| = \frac{q^n}{\sum\limits_{i=0}^{\rho} \beta_i (q-1)^i \binom{n}{i}}. \tag{2}$$

Некоторые другие интересные свойства ПР-кодов (являющиеся также необходимыми условиями существования таких кодов) можно найти в [10, 18].

Рассмотрим два иллюстрирующих примера [24]. Коды Препараты P с параметрами ($n = 2^{2m}-1$, $M = 2^{n+1-4m}$, $d = 5$) для $m = 2, 3, \ldots$ имеют следующие параметры упаковки β_i и корни ξ_i обобщенного многочлена Ллойда $P_\rho(n, \xi)$:

$$\beta_0 = \beta_1 = 1, \quad \beta_2 = \beta_3 = \frac{3}{n},$$
$$\xi_1 = \frac{1}{2}(n+1-\sqrt{n+1}), \quad \xi_2 = \frac{(n+1)}{2}, \quad \xi_3 = \frac{1}{2}(n+1+\sqrt{n+1}).$$

Интересный факт, отмеченный в [2], состоит в том, что коды Препараты не только полностью регулярны в схеме Хэмминга $H(2, n)$, но также полностью регулярны в коде Хэмминга.

Двоичные примитивные коды БЧХ с параметрами [$n = 2^{2m+1}-1$, $k = n-4m-2$, $d = 5$] для $m = 2, 3, \ldots$ имеют следующие параметры упаковки β_i и корни ξ_i многочлена Ллойда:

$$\beta_0 = \beta_1 = 1, \quad \beta_2 = \beta_3 = \frac{6}{(n-1)},$$
$$\xi_1 = \frac{n+1}{2} - \sqrt{\frac{n+1}{2}}, \quad \xi_2 = \frac{n+1}{2}, \quad \xi_3 = \frac{n+1}{2} + \sqrt{\frac{n+1}{2}}.$$

2.5. Расширение полностью регулярных кодов. Напомним, что для двоичного кода C расширенный код C^* получается из C добавлением общей проверки на четность (или на нечетность) к каждому кодовому слову. Один из интересных открытых вопросов для ПР-кодов связан с расширением этих кодов и формулируется следующим образом: *при каких условиях расширение полностью регулярного (n, N, d)-кода C с нечетным расстоянием $d = 2e+1$ приводит к расширенному полностью регулярному $(n+1, N, d+1)$-коду C^*?* Здесь мы ограничимся только двоичными кодами, хотя кажется, что некоторые из приводимых ниже результатов могут быть обобщены и на недвоичный случай.

В [22] доказано, что удаление любой одной позиции в четном ПР-коде приводит к коду, также являющемуся ПР-кодом, что отвечает на ранее поставленный в [24] вопрос. Следовательно, если C^* представляет собой ПР-код, то выколотый код C также полностью регулярен. Однако обратное, вообще говоря, не верно. В работе [33] приводится пример ПР-кода C, такого что его расширение C^* уже не является ПР-кодом: это $[21, 12, 5]$-код C, полученный выкалыванием двух позиций из двоичного совершенного кода Голея. Но его расширение, т.е. $[22, 12, 6]$-код C^*, уже не полностью регулярно. Более того, для этого случая расширенный $[22, 12, 6]$-код C^* даже не равномерно упакован в широком смысле. Следовательно, расширение РУ-кода в широком смысле, вообще говоря, может не быть РУ-кодом в широком смысле. Для таких равномерно упакованных кодов этот вопрос был полностью решен в [33]. Необходимое и достаточное условие сохранения свойства равномерной упаковки при расширении дает следующая

Теорема 10 [33]. *Двоичный РУ-код C в широком смысле длины n с параметрами упаковки $\beta_0, \ldots, \beta_\rho$ остается при расширении РУ-кодом в широком смысле, если и только если имеет место следующая система равенств*:

$$\beta_{\rho-2i} = \beta_{\rho-2i-1} \quad \text{для всех } i,\ 0 \leqslant i \leqslant [(\rho-1)/2].$$

Более того, параметры упаковки $\gamma_0, \ldots, \gamma_\rho, \gamma_{\rho+1}$ расширенного кода C^* однозначно определяются следующими формулами:

$$\gamma_{\rho-2i} = \beta_{\rho-2i}, \quad \forall\, i = 0, 1, \ldots, \lfloor \rho/2 \rfloor,$$
$$\gamma_{\rho-2i+1} = \frac{1}{n+1}\big((\rho+1-2i)\beta_{\rho-2i} + (n-\rho+2i)\beta_{\rho-2i+2}\big), \quad \forall\, i = 0, \ldots, \left\lfloor \frac{\rho+1}{2} \right\rfloor.$$

Условия предыдущей теоремы очевидным образом являются необходимыми для того, чтобы ПР-код при расширении оставался ПР-кодом. Вопрос о том, является ли это достаточным условием, открыт для ПР-кодов.

Приведем еще одно также полезное необходимое условие для ПР-кодов. Как известно (теорема 2), множество C_d для двоичного РУ-кода C длины n с расстоянием $d = 2e+1$ индуцирует схему $T(n, d, e, \lambda)$.

Предложение 3 [33]. *Пусть C^* получен расширением двоичного РУ-кода C в широком смысле. Пусть C имеет длину n и минимальное расстояние $d = 2e+1$. Если C^* равномерно упакован, то множество C^*_{d+1} индуцирует схему $T(n+1, d+1, e+1, \lambda)$.*

В случае, когда коды C и C^* равномерно упакованы и C имеет радиус покрытия $\rho = e+1$, оба кода также полностью регулярны.

Предложение 4 [2,37]. *Пусть C – квазисовершенный РУ-код (следовательно, ПР-код). Если C^* равномерно упакован, то он также полностью регулярен.*

Другое необходимое условие существования выглядит так.

Предложение 5. *Пусть C – ПР-код четной длины, являющийся антиподальным. Тогда C^* не равномерно упакован в широком смысле, и следовательно, не полностью регулярен.*

Доказательство. Предположим, что код C^* равномерно упакован в широком смысле. Тогда внешнее расстояние равно $s^* = s+1$, откуда вытекает, что для каждого веса w в дуальном спектре число $n+1-w$ также является весом в дуальном спектре. Но w должно быть четным, так как C содержит вектор из всех единиц, и следовательно, число $n+1-w$ нечетно, что приводит к противоречию. ▲

Следующее свойство представляет собой усиление результата работы [38].

Предложение 6 [39]. *Пусть C – двоичный линейный ПР-код длины $n = 2^m - 1$ с минимальным расстоянием $d = 3$, радиусом покрытия $\rho = 3$ и массивом пересечений $\{n, b_1, 1; 1, c_2, n\}$. Пусть дуальный код $C^\perp$ имеет ненулевые веса w_1, w_2 и w_3. Тогда расширенный код C^* полностью регулярен с радиусом покрытия $\rho^* = 4$, если и только если $w_1 + w_3 = 2w_2 = n+1$. В этом случае массив пересечений кода C^* равен $\{n+1, n, b_1, 1; 1, c_2, n, n+1\}$.*

Следовательно, веса дуального кода (когда C – линейный код) играют важную роль. Другим важным критерием являются свойства различных выколотых кодов при удалении разных координат из расширенного кода C^*: результирующий i-выколотый код C должен быть почти одним и тем же независимо от выбора удаляемой позиции i.

Предложение 7 [6]. *Пусть C – двоичный ПР-код. Предположим, что i-выколотый код, полученный из C^*, совпадает с кодом C независимо от выбора пози-*

ции i. Пусть s^* – внешнее расстояние кода C^*. Если $s^* \leqslant s+1$, то C^* полностью регулярен.

Следствие 4 [6]. *Пусть C – двоичный линейный ПР-код, дуальный код $C^\perp$ которого имеет четные веса, симметричные относительно $(n+1)/2$. Если группа $\mathrm{Aut}(C^*)$ транзитивна, то C^* полностью регулярен.*

Рассмотрим двоичный примитивный код БЧХ C, имеющий параметры $[2^m-1, 2^m-1-2m, 5]$, где $m \geqslant 3$ нечетно. Веса дуального кода удовлетворяют условиям следствия 4, и C^* инвариантен относительно действия аффинной группы слева. Следовательно, C^* – ПР-код с радиусом покрытия $\rho^* = s^* = 4$ и (радиусом упаковки) $e^* = 2$. Этот результат можно получить из [24], где было показано, что рассматриваемые коды БЧХ равномерно упакованы в узком смысле с параметрами упаковки

$$\beta_0 = \beta_1 = 1, \quad \beta_2 = \beta_3 = \frac{6}{(n-1)}.$$

Согласно теореме 10 расширенные коды БЧХ равномерно упакованы, а в силу предложения 4 эти коды полностью регулярны.

Рассмотрим теперь коды, которые исследовались Кальдербэнком и Гёталсом в [40,41], а именно трехвесовые циклические подкоды выколотых кодов Рида – Маллера второго порядка. Обозначим через C код, дуальный к одному из таких кодов. Код C полностью регулярен, а C^* инвариантен относительно действия аффинной группы слева. Опять убеждаемся, что три ненулевых веса кода $C^\perp$ удовлетворяют условиям следствия 4. Следовательно, C^* – ПР-код с $\rho^* = s^* = 4$ и $e^* = 1$.

Следствие 4 можно обобщить на случай нелинейных кодов.

Следствие 5 [6]. *Пусть двоичный код C имеет четные дуальные расстояния, симметричные относительно $(n+1)/2$. Если C полностью регулярен и его группа автоморфизмов $\mathrm{Aut}(C^*)$ транзитивна, то C^* полностью регулярен.*

Из метода построения кодов Препараты, представленного в [42], вытекает, что группа автоморфизмов расширенного кода Препараты транзитивна. Его выколотый код, т.е. код Препараты длины $n = 2^{2m}-1$, $m = 2, 3, \ldots$, является ПР-кодом [2], а его дуальные расстояния – это расстояния кода Кердока [43], удовлетворяющие условиям следствия 5. Отсюда заключаем, что расширенный код Препараты является полностью регулярным [2] с $\rho^* = s^* = 4$ и $e^* = 2$.

Рассмотрим $(12, 24, 6)$-код Адамара C^*. Известно, что C равномерно упакован с дуальными расстояниями $4, 6, 8$ [4, 44]. Группа автоморфизмов $\mathrm{Aut}(C^*)$ изоморфна группе Матье M_{12}. Следовательно, C^* полностью регулярен с $\rho^* = s^* = 4$ и $e^* = 2$. В [37] было доказано следующее

Предложение 8 [37]. *Пусть C – двоичный полностью регулярный код с параметрами (n, d).*

(i) *Если $(n, d) = (12, 6)$, то C эквивалентен коду Адамара;*
(ii) *Если $(n, d) = (11, 5)$, то C эквивалентен выколотому коду Адамара.*

Результаты Соле [6] были несколько усилены Брауэром в [45].

Предложение 9 [45]. *Пусть C – двоичный ПР-код. Если матрицы внешних спектров всех выколотых кодов, полученных из C^*, имеют одно и то же множество строк, и в частности, если C^* инвариантен относительно группы, транзитивной на множестве координатных позиций, то C^* полностью регулярен.*

Следствие 6 [45]. *Код C^* полностью регулярен, если и только если все его выколотые коды являются ПР-кодами с одинаковым внешним спектром расстояний.*

Интересно, конечно, найти необходимые и достаточные условия на код C, при которых C^* был бы ПР-кодом. Из последнего следствия можно вывести некоторые необходимые условия на выколотые коды, полученные из C^*, в частности, на код C.

Для любого двоичного вектора $v = (v_1, \ldots, v_n)$ и для каждого $i = 1, \ldots, n$ определим вектор

$$\tau_i(v) = (v_1, \ldots, v_{i-1}, p(v), v_{i+1}, \ldots, v_n),$$

где $p(v)$ обозначает четность исходного вектора v, т.е.

$$p(v) \equiv \sum_{i=1}^{n} v_i \pmod 2.$$

Для каждой позиции $i = 1, \ldots, n$ определим код $C_{[i]} = \{\tau_i(x) \mid x \in C\}$.

Лемма 1. *Код C^* полностью регулярен, если и только если C и $C_{[i]}$ – ПР-коды для всех $i = 1, \ldots, n$.*

Доказательство. Для любого кода D обозначим через $D^{(i)}$ код, полученный i-выкалыванием кода D. Через $\sigma_{i,j}$ обозначим транспозицию координат i и j. Предположим, что при расширении добавляется $(n+1)$-я координата. Получаем, очевидно, что

$$C_{[i]} = (\sigma_{i,n+1}(C^*))^{(i)} \quad \text{и} \quad C = (C^*)^{(n+1)}.$$

Результат теперь вытекает из следствия 6. ▲

Предложение 10. *Если C^* является ПР-кодом, то для всех $i = 1, \ldots, n$*

(i) *Весовые спектры кодов C и $C_{[i]}$ совпадают*;
(ii) *Минимальные расстояния кодов C и $C_{[i]}$ совпадают и нечетны*;
(iii) *Внешние расстояния кодов C и $C_{[i]}$ совпадают*;
(iv) *Радиусы покрытия кодов C и $C_{[i]}$ совпадают.*

Доказательство. Утверждение (i) следует из того, что для каждого кодового слова x строка B_x должна быть одной и той же для всех кодов C и $C_{[i]}$. Утверждения (ii) и (iii) прямо вытекают из (i).

Если радиус покрытия кода C равен ρ, то радиус покрытия кода C^* равен $\rho^* = \rho + 1$. Отсюда, следовательно, получаем (iv). ▲

Теперь у нас есть следующее необходимое условие на код C (или $C_{[i]}$).

Следствие 7. *Если C^* – ПР-код длины $n+1$ с минимальным расстоянием $d^* = 2e + 2 \geqslant 4$, то для всех нечетных w имеет место равенство*

$$(n - w)A_w = (w + 1)A_{w+1}, \tag{3}$$

где A_w – число кодовых слов веса $w \geqslant 2e + 1$ в коде C (или $C_{[i]}$).

Доказательство. Обозначим через A^*_{w+1} число кодовых слов веса $w+1$ в коде C^*, где $w+1$ нечетно. Множество C^*_{w+1} всех слов веса $w+1$ образует согласно теореме 1 схему $T(n+1, w+1, 2, \lambda^*_2)$. Число кодовых слов C^*_{w+1} с ненулевым элементом в позиции $n+1$, т.е. число повторений схемы, равно r^*. Очевидно, что $r^* = A_w$. Следовательно,

$$A^*_{w+1}(w + 1) = (n + 1)r^*. \tag{4}$$

Объединяя (4) с очевидным равенством $A^*_{w+1} = A_{w+1} + A_w$, получаем результат. ▲

В частности, любой совершенный код должен удовлетворять соотношению (3). Для случая двоичных совершенных кодов с $d = 3$ это рекуррентное выражение

хорошо известно (см., например, [21]):

$$(n-i+1)A_{i-1} + A_i + (i+1)A_{i+1} = \binom{n}{i}. \tag{5}$$

Объединяя теперь (3) и (5), получаем

Следствие 8. *Для любого совершенного кода с $d = 3$, содержащего нулевое кодовое слово, число кодовых слов веса i равно*

$$A_i = \begin{cases} \binom{n}{i}\dfrac{1}{n-i+1} - A_{i-1}, & \text{если } i \text{ нечетно,} \\ \dfrac{n-i+1}{i}A_{i-1}, & \text{если } i \text{ четно.} \end{cases}$$

Из [19] мы знаем, что четная половина (двоичного) $[23, 12, 7]$-кода Голея, скажем, код C^*, является ПР-кодом. Выкалывая этот код по любой координате, получаем код C со следующим весовым спектром:

A_0	A_7	A_8	A_{11}	A_{12}	A_{15}	A_{16}
1	176	330	672	616	176	77

.

Код C, конечно, полностью регулярен [19], и следовательно, подтверждает равенство (3), в чем нетрудно убедиться.

§ 3. Полностью транзитивные коды

Полностью транзитивные коды (ПТ-коды) были впервые введены Соле в 1990 г. [6] как подкласс двоичных линейных ПР-кодов. Пусть C – двоичный линейный код. Рассмотрим действие его группы автоморфизмов $\mathrm{Aut}(C)$ на фактор-пространстве $\mathbb{F}_2^n/C$: для любого смежного класса $C + x$ и любого автоморфизма $\sigma \in \mathrm{Aut}(C)$ положим

$$\sigma(C + x) = \sigma(C) + \sigma(x) = C + \sigma(x).$$

Определение 9 [6]. Двоичный линейный код C с радиусом покрытия ρ называется *полностью транзитивным* (ПТ-кодом), если группа $\mathrm{Aut}(C)$ индуцирует $\rho + 1$ орбиту при действии на (множестве смежных классов) $\mathbb{F}_2^n/C$.

Так как два смежных класса из одной орбиты имеют одинаковые весовые спектры, то имеет место следующий факт.

Предложение 11 [6]. *Если C – двоичный линейный ПТ-код, то C полностью регулярен.*

Следующий факт представляет собой усиление теоремы 6.

Предложение 12 [36]. *Если C – неантиподальный двоичный линейный ПТ-код, то $C \cup C(\rho)$ также является ПТ-кодом.*

ПТ-коды и дистанционно регулярные графы тесно связаны. В частности, имеет место следующее

Предложение 13. *Пусть C – двоичный линейный ПР-код с радиусом покрытия ρ и массивом пересечений* IA $= \{b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho\}$, *и пусть Γ_C – граф, построенный на смежных классах кода C. Тогда*

(i) *Граф Γ_C дистанционно регулярен с диаметром $D = \rho$ и тем же самым массивом пересечений* IA [10];

(ii) *Если C полностью транзитивен, то Γ_C дистанционно транзитивен* [46].

Следовательно, согласно предложению 13 любой ПР- или ПТ-код индуцирует дистанционно регулярный или дистанционно транзитивный граф соответственно. В настоящей работе мы не касаемся соответствующих дистанционно регулярных и дистанционно транзитивных графов, существование которых вытекает из связанных с ними ПР- и ПТ-кодов соответственно. Об этих графах с такими же массивами пересечений, что и коды, см. в работах [10–12], где они подробно рассматриваются.

Для заданной группы перестановок G степени n (действующей на множестве из n элементов) скажем, что G является t-транзитивной (соответственно, t-однородной), если она переставляет любой (упорядоченный) t-набор (соответственно, t-множество) в любой другой t-набор (соответственно, t-множество). Группа G транзитивна, если она 1-транзитивна. Теорема Ливингстона и Вагнера [47] утверждает, что если G является i-однородной с $i \leqslant n/2$, то G также j-однородна для $j \leqslant i$. Из этого факта вытекает следующее

Предложение 14 [6]. *Пусть C – двоичный линейный код длины n с радиусом покрытия $\rho \leqslant n/2$. Если $\mathrm{Aut}(C)$ является ρ-однородной, то код C полностью транзитивен.*

Используя это свойство, получаем, что следующие коды полностью транзитивны:

(i) Все совершенные двоичные линейные коды (код с повторением, коды Хэмминга и двоичный код Голея);

(ii) Все расширенные двоичные линейные совершенные коды.

Предложение 14 дает достаточное (но не необходимое) условие для того, чтобы код был ПТ-кодом. Это можно увидеть из двоичного $[9, 5, 3]$-кода C, дуального коду, полученному кронекеровым произведением двух $[3, 2, 2]$-кодов с проверкой на четность. Код C равномерно упакован в узком смысле [2, 6] с $\rho = s = 2$ и $e = 1$. Более того, код C полностью транзитивен, однако группа $\mathrm{Aut}(C)$ транзитивна, но не 2-однородна.

Необходимое условие выглядит следующим образом.

Предложение 15 [6]. *Группа автоморфизмов $\mathrm{Aut}(C)$ полностью регулярного двоичного линейного кода C, исправляющего e ошибок, e-однородна.*

В качестве примера полностью регулярного кода, не являющегося полностью транзитивным, рассмотрим двоичный примитивный $[2^m - 1, 2^m - 2m - 1, 5; 3]$-код БЧХ, т.е. циклический код C с $m > 4$ и нечетным m. Этот код полностью регулярен [2,24,33] с массивом пересечений $\{n, n-1, (n+3)/2; 1, 2, (n-1)/2\}$, где $n = 2^m - 1$ (эти же коды с $\ell = 3$ принадлежат семейству из п. 5.13; см. также п. 2.4). Как следует из работы [48], группа автоморфизмов $\mathrm{Aut}(C)$ – это полулинейная группа $\Gamma\mathrm{L}(1, 2^m)$ поля $\mathbb{F}_{2^m}$ над $\mathbb{F}_{2^m}$ (напомним, что полулинейная группа, обозначаемая через $\Gamma\mathrm{L}(t, q)$, состоит из всех обратимых полулинейных преобразований $(\mathbb{F}_q)^t$ над $\mathbb{F}_q$). Если $q = p^r$, то хорошо известно, что $|\Gamma\mathrm{L}(t, q)| = r|\mathrm{GL}(t, q)|$, где через $\mathrm{GL}(t, q)$ обозначена общая линейная группа (см., например, в [25, с. 163]; в нашем случае $t = 1$). Следовательно, порядок группы $\mathrm{Aut}(C)$ равен $|\Gamma\mathrm{L}(1, 2^m)| = m|\mathrm{GL}(1, 2^m)| = m(2^m - 1)$. Так как C имеет радиус упаковки $e = 2$, то известно, что C имеет ровно $(2^m - 1)(2^{m-1} - 1)$ смежных классов веса 2. Так как число смежных классов больше, чем порядок группы $|\mathrm{Aut}(C)|$, то они не могут принадлежать одной и той же орбите, индуцируемой действием $\mathrm{Aut}(C)$. Значит, C не полностью транзитивен.

Аналогично совершенным и квазисовершенным РУ-кодам, несуществование ПТ-кодов также установлено для значений $e > 3$. В 2000 г. Боржес и Рифа [16] установили, что имеет место следующая

Теорема 11 [16]. *Если C – нетривиальный двоичный линейный ПТ-код, исправляющий e ошибок, то $e \leqslant 4$.*

Доказательство было основано на несуществовании высоко транзитивных групп и на некоторых оценках мощности кода. Используя затем границу Грайсмера и несу-

ществование некоторых схем, этот результат был улучшен. В 2001 г. Боржес, Рифа и Зиновьев [17] доказали следующий результат.

Теорема 12 [17]. *Если C – нетривиальный двоичный линейный ПТ-код, исправляющий e ошибок, то $e \leqslant 3$.*

Ясно, что определение 9 может быть расширено на недвоичные линейные коды. Джудичи и Прейгер [7, 8] исследовали этот более общий случай. Эти коды, включающие двоичные ПТ-коды, введенные Соле [6], они назвали *полностью транзитивными на смежных классах*. В предшествующем препринте Годсил и Прейгер обобщили понятие полностной транзитивности на случай нелинейных кодов. Работа [49] представляет собой обновленную версию этого препринта.

Определение 10 [49]. Код $C \subset \mathbb{F}_q^n$ является *G-полностью транзитивным*, или просто *полностью транзитивным*, если существует подгруппа G группы автоморфизмов $\mathrm{Aut}(\mathbb{F}_q^n)$, такая что каждая подкомпонента (слой) $C(i)$ дистанционного разбиения кода C является G-орбитой.

Предложение 16 [8]. *Если код $C \subset \mathbb{F}_q^n$ полностью транзитивен в смысле определения* 10, *то он полностью регулярен.*

Заметим, что в общем случае код, полностью транзитивный на смежных классах, не является $\mathrm{Aut}(C)$-полностью транзитивным в смысле определения 10. Это связано с тем, что группа $\mathrm{Aut}(C)$ часто даже не транзитивна на C, например, когда C имеет кодовые слова разного веса.

Для линейного кода $C \subset \mathbb{F}_q^n$ определим N_C как множество всех сдвигов пространства $\mathbb{F}_q^n$ векторами из кода C, т.е. $N_C = \{\tau_x \mid x \in C\}$, где $\tau_x(v) = v + x$ для каждого вектора $v \in \mathbb{F}_q^n$. Ясно, что N_C – подгруппа, так как C – линейный код. Пусть G получена полупрямым произведением N_C и $\mathrm{Aut}(C)$, т.е. $G = N_C \rtimes \mathrm{Aut}(C)$. Группа G стабилизирует C как множество, а N_C-орбиты представляют собой не что иное, как смежные классы кода C. В частности, C является G-орбитой [8]. Из такого рода соображений вытекает следующая

Теорема 13 [8]. *Пусть $C \subset \mathbb{F}_q^n$ – линейный код. Тогда C полностью транзитивен на смежных классах, если и только если C является $(N_C \rtimes \mathrm{Aut}(C))$-полностью транзитивным.*

Однако для $q \leqslant 3$ эти два понятия эквивалентны.

Теорема 14 [8]. *Пусть $C \subset \mathbb{F}_q^n$ – линейный код, причем $q \leqslant 3$. Тогда C полностью транзитивен на смежных классах, если и только если C полностью транзитивен.*

Пусть $q \geqslant 7$ – степень простого числа, $q \neq 8$, и пусть C – код с повторением в $\mathbb{F}_q^3$, т.е. $[3, 1, 3]_q$-код. Определим группу $G = S_q \rtimes S_3$. Прямая проверка показывает, что C является G-полностью транзитивным, однако C не полностью транзитивен на смежных классах [8].

Следует отметить, что полная транзитивность представляет собой довольно специальное свойство, которое, вообще говоря, не имеет отношения к оптимальности кодов. Например, наилучшие после совершенных кодов нелинейные оптимальные коды Препараты, имеющие максимально возможную плотность упаковки после совершенных кодов [2], не являются полностью транзитивными за исключением случая, когда они пересекаются с кодами Кердока, т.е. за исключением кода Нордстрома – Робинсона.

Теорема 15 [9]. *Код Препараты длины n и его расширение полностью транзитивны, если и только если $n = 15$.*

§ 4. Полностью регулярные коды в схемах Джонсона

Схема Джонсона $J(n, w)$ – это множество всех двоичных векторов длины n и веса w (т.е. векторов с w ненулевыми позициями). Произвольное подмножество C схемы $J(n, w)$ – это равновесный код, имеющий четыре параметра, а именно: длину n, постоянный вес слов w, минимальное расстояние (Хэмминга) $d = 2\delta$ и мощность (число кодовых слов) $N = |C|$. Если определить расстояние между двумя векторами x и y веса w как половину расстояния Хэмминга (в самом деле, расстояние Хэмминга между двумя словами одного веса всегда четно), то получим новое расстояние (также являющееся метрикой), которое называется *расстоянием Джонсона* и обозначается здесь через d_J. Два вектора x и y на расстоянии $d_J = 1$ друг от друга называются *соседями*.

Со схемой Джонсона естественным образом связывается *граф Джонсона*, часто обозначаемый таким же образом, как и схема (т.е. $J(n, w)$). Вершинами этого графа являются все двоичные векторы длины n и веса w, и две вершины связаны ребром, если соответствующие векторы являются соседями. Две вершины x и y находятся друг от друга на расстоянии Джонсона $d_J(x, y)$, если оно равно числу ребер в кратчайшем пути между x и y. Ясно, что два графа Джонсона $J(n, w)$ и $J(n, n - w)$ изоморфны друг другу, и поэтому мы рассматриваем только случай $w \leqslant n/2$.

Определение 11. Совершенной m-раскраской схемы Джонсона $J(n, w)$ называется раскраска векторов $J(n, w)$ в m цветов $\{1, \ldots, m\}$, такая что фиксированный вектор x цвета i имеет $a_{i,j}$ соседей y цвета j, причем $a_{i,j}$ не зависит от выбора x.

Очевидно, что такие m-раскраски графа Джонсона представляют собой не что иное, как дистанционно регулярные графы. Матрица $A = [a_{i,j}]$ называется *матрицей параметров совершенной раскраски*, или кратко *матрицей параметров. Совершенный код* в схеме Джонсона представляет собой классический пример полностью регулярного кода.

Определение 12. Равновесный код C длины n с весом слов w и минимальным расстоянием $d_J = 2e + 1$ является совершенным e-кодом в $J(n, w)$, если для любого вектора $x \in J(n, w)$ найдется в точности одно кодовое слово $c \in C$, такое что $d_J(x, c) \leqslant e$. Другими словами, все шары радиуса (Джонсона) e, проведенные вокруг каждого кодового слова кода C, не пересекаются друг с другом и заполняют все множество векторов схемы $J(n, w)$.

Обозначим через $\Phi_e(n, w)$ мощность шара в $J(n, w)$ радиуса e. Очевидно, что

$$\Phi_e(n, w) = \sum_{i=0}^{e} \binom{w}{i} \binom{n-w}{i}.$$

Тогда для совершенного e-кода C в $J(n, w)$ по условию сферической упаковки получаем следующее выражение для мощности кода C:

$$|C| = \frac{\binom{n}{w}}{\Phi_e(n, w)},$$

что означает, конечно, целочисленность полученного выражения в правой части. Известны следующие тривиальные примеры совершенных e-кодов в $J(n, w)$:

1. Схема Джонсона $J(n, w)$ с $e = 0$;
2. Любой вектор x из $J(n, w)$ с $e = w$;
3. Для случая $n = 4e + 2$ и $w = 2e + 1$ любая пара векторов x и y из $J(n, w)$ на расстоянии $d_J(x, y) = w$ образует совершенный e-код.

Заметим, что в специальном случае $n = 2w$ схема Джонсона $J(2w, w)$ полностью транзитивна, и следовательно, полностью регулярна в схеме Хэмминга $H(2, 2w)$ (см. п. 5.8).

Проблема существования нетривиальных совершенных кодов в схеме Джонсона была поставлена в 1973 г. Дельсартом [3] (который высказал гипотезу, что таких кодов не существует), и эта проблема до сих пор открыта. Баннаи [50] доказал несуществование совершенных e-кодов в схемах Джонсона $J(2w + 1, w)$ при $e \geqslant 2$. Хаммонд [51] улучшил этот результат, показав несуществование в $J(n, w)$ нетривиальных совершенных кодов для значений $n \in \{2w - 2,\ 2w - 1,\ 2w + 1,\ 2w + 2\}$. Отметим, что обобщение теоремы Ллойда (которая была основным инструментом для доказательства несуществования совершенных кодов в схемах Хэмминга; см. работы [14,15] и библиографию в них) на схемы Джонсона [3,50] не привело к каким-либо значительным результатам. Многие результаты о несуществовании были получены в работах Этциона и Шварца [52–54]. Используя условия делимости, вытекающие из существования совершенных кодов, а также из систем Штейнера, которые должны сосуществовать с совершенными кодами в $J(n, w)$, Этцион [52] получил следующие результаты:

Теорема 16 [52]. *Совершенных e-кодов не существует*

1) *в схемах $J(2w + e + 1, w)$;*
2) *в схемах $J(2w + p, w)$, p – простое;*
3) *в схемах $J(2w + 2p, w)$, p – простое, $p \neq 3$;*
4) *в схемах $J(2w + 3p, w)$, p – простое, $p \neq 2,\ 3,\ 5$.*

Симабукуро [55] добавил к этому списку схемы $J(2w + p^2, w)$ (в которых совершенных e-кодов нет). Этцион и Шварц [53] использовали другой подход для результатов несуществования. Они использовали *k-регулярность* совершенных кодов в схемах $J(n, w)$. К этому понятию мы вернемся при рассмотрении совершенных 2-раскрашиваний. Для случая небольших $e \leqslant 2$ Этцион и Шварц [53] получили следующий результат.

Теорема 17 [53]. *В схеме $J(n, w)$ не существует совершенных 1-кодов для $n \leqslant 50000$ и совершенных 2-кодов для $n \leqslant 40000$.*

Гордон [56] получил необходимые условия существования совершенных 1-кодов, рассматривая возможные простые делители числа $\Phi_e(w, a)$. При этом использовались два теоретико-числовых результата, которые мы напомним. Первый представляет собой следующую лемму Куммера.

Лемма 2 [57]. *Пусть p – простое число. Множитель p встречается в выражении $\binom{a}{b}$ столько раз, сколько переносов в следующий разряд появляется при сложении чисел b и $a - b$ по модулю p.*

Второй результат – это следующая лемма Локстона [58] (в доказательстве которой Бернштейн [59] устранил одну неточность).

Лемма 3 [58,59]. *Количество совершенных степеней (т.е. чисел вида a^m, где $a, m > 1$) в интервале $[w, w + \sqrt{w}\,]$ не превосходит*

$$\exp(40\sqrt{\log\log w \log\log\log w}).$$

Используя эти две леммы, Гордон [56] установил, что справедлива следующая

Теорема 18 [56]. *В схеме $J(n, w)$ не существует совершенных 1-кодов для длин $n \leqslant 2^{250}$.*

К настоящему времени получен целый ряд необходимых условий для существования совершенных кодов в схемах Джонсона, часть которых мы рассмотрим. Руз [60] (см. также [53] с более простым доказательством) ограничил длину n совершенного

e-кода в $J(n,w)$ сверху, а Мовсисян [61] снизу. Это приводит к следующему интервалу длин n для существования совершенных кодов.

Теорема 19 [60,61]. *Если C – совершенный e-код в схеме Джонсона $J(n,w)$, то его длина n ограничена следующими пределами*:

$$\frac{2e+1}{e+1}(w+1) \leqslant n \leqslant \frac{2e+1}{e}(w-1). \tag{6}$$

Из нижней оценки на длину совершенного e-кода получаем

Следствие 9 [61]. *Для любого фиксированного w число совершенных e-кодов в схеме $J(n,w)$ конечно.*

Пусть $C \in J(n,w)$ – совершенный e-код. Для любого вектора y из $J(n,w+1)$ обозначим через $R(y)$ число кодовых слов $x \in C$, таких что $d_J(x,y) = 2e+1$.

Следствие 10 [61]. *Если C – совершенный e-код в $J(n,w)$, то для каждого вектора $y \in J(n,w+1)$ множество $R(y)$ имеет мощность $(w+1)/(e+1)$, откуда следует, что $e+1$ делит $w+1$.*

Из теоремы 19 непосредственно следует, что вес w векторов совершенного e-кода ограничен снизу: $w \geqslant 2e+1$. Мовсисян [61] показал, что вес w должен расти с ростом e как квадратичная функция.

Предложение 17 [61]. *Для нетривиального совершенного e-кода в $J(n,w)$ величина w ограничена снизу следующим образом*:

$$w \geqslant e^2 + 3e + 1.$$

Ясно, что два замечательных комбинаторных объекта в схемах Джонсона – системы Штейнера $S(n,w,t)$ и совершенные e-коды – должны быть тесно связаны. Несколько результатов относительно такой взаимосвязи получено в [52,62].

Предложение 18 [62]. *Совершенный e-код в схеме $J(n,w)$ сосуществует с системой Штейнера $S(n,w,t)$, если и только если выполняются следующие равенства*:

$$n = 3w-3, \quad t = w-2 \quad и \quad e = 1. \tag{7}$$

Предложение 19 [52]. *Существование совершенного e-кода в схеме $J(n,w)$ влечет существование систем Штейнера $S(w,2e+1,e+1)$ и $S(n-w,2e+1,e+1)$.*

Предложение 20 [52]. *Единственными системами Штейнера, являющимися совершенными кодами в схеме Джонсона $J(n,w)$, являются тривиальные системы $S(2w,w,1)$ и $S(n,w,w)$.*

Существование совершенных равновесных кодов тесно связано с задачей *D-представления кодов* [63,64], которую мы сейчас обсудим. Пусть A – любое подмножество двоичного пространства $\mathbb{F}_2^n$ и φ – произвольная функция, определенная на множестве натуральных чисел. Для вектора x из A определим *область Дирихле* $D_x(\varphi)$ следующим образом:

$$D_x(\varphi) = \{y \in \mathbb{F}_2^n : \varphi(d_J(x,y)) \leqslant \varphi(d_J(z,y)),\ \forall z \in A\},$$

и будем обозначать ее просто D_x, когда φ – тождественная функция.

Определение 13. Множество A векторов из $\mathbb{F}_2^n$ называется *$D(\varphi)$-представимым кодом* (D-представимым, соответственно), если и только если области Дирихле $D_x(\varphi)$ (соответственно, D_x) всех векторов A попарно различны в $\mathbb{F}_2^n$ (т.е. не пересекаются).

Предложение 21 [63,64]. *Множество C – совершенный e-код в $J(n,w)$, если и только если этот код $D(\varphi)$–представим для любой строго монотонной функции φ.*

Рассмотрим теперь некоторые совершенные раскраски в схемах Джонсона. Начнем с простого наблюдения о том, что совершенный 1-код в $J(n,w)$ индуцирует совершенную 2-раскраску P схемы $J(n,w)$ со следующей матрицей A:

$$A = \begin{bmatrix} 0 & w(n-w) \\ 1 & w(n-w)-1 \end{bmatrix}.$$

Для этого надо покрасить все кодовые слова в один цвет (обычно белый), а все другие векторы из $J(n,w)$ – в другой (обычно черный) [65]. Начнем с понятия *k-регулярности*, введенного в [65] для совершенных 2-раскрасок и обобщающего соответствующее понятие для совершенных e-кодов [53]. Для двух двоичных векторов x и y длины n будем писать $x \preceq y$, если x покрыт y, т.е. если $x_i \leqslant y_i$ для всех $i \in \{1,\dots,n\}$. Для совершенной 2-раскраски P схемы $J(n,w)$ обозначим через W и B множества векторов этой схемы белого и черного цвета соответственно. Для двух векторов x и y, таких что $y \preceq x$ (т.е. x покрывает y), обозначим через Γ_x^y грань, индуцированную x и y, т.е. следующее множество двоичных векторов из $\mathbb{F}_2^n$:

$$\Gamma_x^y = \{z + y + x : \ z \in \mathbb{F}_2^n,\ x \preceq z\}$$

(т.е. Γ_x^y состоит из всех $2^{n-\mathrm{wt}(x)}$ векторов пространства $\mathbb{F}_2^n$, покрывающих y и совпадающих с y на носителе x).

Определение 14 [65]. Совершенная 2-раскраска P схемы Джонсона $J(n,w)$ называется k-регулярной, если существуют k^2 чисел γ_{ij}, таких что для каждых двоичных векторов x и y длины n, таких что $y \preceq x$, с весами $\mathrm{wt}(x) = i$ и $\mathrm{wt}(y) = j$, где $i \leqslant k \leqslant w$, имеет место следующее равенство:

$$|\Gamma_x^y \cap W| = \gamma_{ij}.$$

Достаточное условие k-регулярности совершенной 2-раскраски дает

Предложение 22 [65]. *Пусть P – совершенная 2-раскраска схемы Джонсона $J(n,w)$ с матрицей $A = [a_{ij}]$, $i,j \in \{1,2\}$. Тогда число k_1, где*

$$k_1 = \frac{1}{2}\left(n + 1 - \sqrt{(n-2w+1)^2 + 4(w + a_{11} - a_{21})}\right),$$

является натуральным, а раскраска P является (k_1-1)-регулярной.

Следствие 11 [65]. *Пусть P – совершенная 2-раскраска схемы Джонсона $J(n,w)$ с матрицей $A = [a_{ij}]$, $i,j = 1,2$. Тогда выражение*

$$\frac{a_{21}}{a_{12}+a_{21}}\binom{n-i}{w-i+j}$$

представляет собой целое число для любых i и j, таких что $0 \leqslant j \leqslant i \leqslant k_1 - 1$, где k_1 определено в предложении 22.

Используя эти результаты, в [66] было доказано несуществование некоторых совершенных 2-раскрасок для длин $n \leqslant 13$. В частности, это было сделано для следующих значений (n,w):

$$(n,w) \in \{(9,3),\ (10,5),\ (11,3),\ (12,4),\ (12,5),\ (12,6),\ (13,4)\}$$

с соответствующими матрицами параметров для каждой пары (n,w) из этого множества.

Согласно [67] наименьший открытый случай для существования совершенной 2-раскраски в схеме Джонсона $J(n,w)$ – это совершенная 2-раскраска в схеме $J(9,3)$ со следующей матрицей параметров:

$$A = \begin{bmatrix} 10 & 8 \\ 8 & 10 \end{bmatrix}.$$

Очевидно, что система Штейнера $S(n,w,t)$, будучи совершенным комбинаторным объектом, является хорошим кандидатом для индуцирования совершенных раскрасок. Действительно, это так для случаев $w = t+1$, $w = t+2$ [68, 69] и некоторых других случаев, как, например, для *полностью регулярных схем*, введенных Мартином [68, 69]. Любая простая схема $T = T(n,w,t,\lambda)$ (т.е. множество различных векторов схемы Джонсона $J(n,w)$) определяет естественным образом (как и любой код в схеме Хэмминга) разбиение всех векторов схемы $J(n,w)$ согласно их расстоянию от T. Для натурального числа i положим

$$T(i) := \Big\{ x \in J(n,w) : \min_{b \in T} d_J(x,b) = i \Big\}.$$

Наибольшее число i, для которого множество $T(i)$ не пусто, обозначим через ρ и назовем это число *радиусом покрытия схемы* T. Разбиение

$$P = \{T = T(0), T(1), \ldots, T(\rho)\},$$

состоящее из непустых множеств $T(i)$, называется *дистанционным разбиением*.

Определение 15 [68, 70]. Простая схема $T = T(n,w,t,\lambda)$ называется полностью регулярной (ПР-схемой) в $J(n,w)$, если для каждого числа $i \in \{0,1,\ldots,\rho\}$ каждый вектор из $T(i)$ имеет γ_i соседей в $T(i-1)$, α_i соседей в $T(i)$ и β_i соседей в $T(i+1)$.

Согласно Мееровичу [70], если T полностью регулярна в $J(n,w)$ и имеет силу ноль ($t = 0$), т.е. представляет собой схему $T(n,w,0,\lambda)$, то существует подмножество V схемы $J(n,w)$, такое что либо

$$T = \{B : |B| = w,\ B \subseteq V\}, \quad \text{либо} \quad T = \{B : |B| = w,\ V \subseteq B\}.$$

Мартин [68] классифицировал ПР-схемы, имеющие силу 1, т.е. схемы $T(n,w,1,\lambda)$. Чтобы сформулировать этот результат, определим так называемые *полные схемы группового типа*. Рассмотрим схему Джонсона $J(n,w)$ с $n = h\ell$ и $w = u\ell$, где $\ell \geqslant 2$ и $h \geqslant 2u$. Пусть $\{X_1, X_2, \ldots, X_h\}$ – разбиение координатного множества $\{1,2,\ldots,n\}$ на h групп размера ℓ каждая. Блоками B схемы T будут все $\binom{h}{u}$ подмножеств вида

$$B = \bigcup_{i \in I} X_i,$$

где I – любое u-подмножество множества $\{1,2,\ldots,h\}$. Так как $\ell \geqslant 2$ и $h > u$, такая схема имеет силу один (т.е. $t = 1$). Ясно также, что эта схема (по построению) имеет минимальное расстояние (Джонсона) ℓ. Такая схема была названа Мартином [68] полной схемой группового типа.

Предложение 23 [68]. *Пусть T – полная схема группового типа в $J(n,w)$. Тогда T полностью регулярна, если и только если выполняется одно из следующих условий*:

1) $\ell = w$ *и* $n = 2w$, *а схема* T – *антиподальная пара* (*т.е. два непересекающихся вектора*);
2) $\ell = 2$;
3) $\ell = 3$ *и* $u = 1$.

Имеются и другие ПР-схемы силы один (см. работу [68] и библиографию в ней). Следующий результат объясняет роль полных схем группового типа.

Теорема 20 [68]. *Пусть T – простая ПР-схема силы один в $J(n,w)$. Тогда T – полная схема группового типа.*

Пусть T – схема $T(n,w,t,\lambda)$. Определим *степень* схемы T как число $s=s(T)$ различных значений пересечений между блоками схемы (или как число разных расстояний между двумя различными блоками схемы T):

$$s(T) := |\{d_J(b,b') : b,b' \in T,\ b \neq b'\}.$$

Аналогично схеме Хэмминга для схемы T в схеме Джонсона $J(n,w)$ можно определить *дуальную степень* (см. [3]), обозначаемую $s^*=s^*(T)$. Пусть $d_J(T)$ обозначает минимальное расстояние (Джонсона) между различными векторами схемы T.

Предложение 24 [3]. *Любая схема с дуальной степенью s^* и минимальным расстоянием $d_J(T)$, такими что $d_J(T) \geqslant 2s^*-1$, полностью регулярна.*

Большая схема Витта, т.е. система Штейнера $S(24,8,5)$, полностью регулярна в $J(24,8)$. Она имеет дуальную степень $s^*=2$ и минимальное расстояние (Джонсона) 4. Следовательно, согласно предложению 24 эта система Штейнера $S(24,8,5)$ полностью регулярна (что было отмечено еще Дельсартом [3]). Так как вычисление величины s^* довольно затруднительно, обычно используется несколько более слабое достаточное условие [69]:

Предложение 25 [3,68]. *Любая простая схема T силы t с минимальным расстоянием $d_J(T) \geqslant 2(w-t)-1$ полностью регулярна.*

Откуда немедленно вытекает

Теорема 21 [69]. *Имеют место следующие утверждения*:

1. *Любая схема $T(n,w,t,\lambda)$ с $w=t+1$ полностью регулярна*;
2. *Система Штейнера $S(n,w,t)$ с $w=t+2$ полностью регулярна.*

Мы немедленно заключаем, что маленькие схемы Витта, т.е. системы Штейнера $S(12,6,5)$ и $S(11,5,4)$, полностью регулярны [69].

Чтобы проверить полную регулярность второй большой схемы Витта (системы Штейнера $S(23,7,4)$), необходимо для всех $i \in \{0,\ldots,\rho\}$ вычислить числовые константы $(\alpha_i,\beta_i,\gamma_i)$ [69]. Так как первая большая схема Витта $S(24,8,5)$ имеет радиус покрытия 2, то вторая большая схема Витта $S(23,7,4)$ (получаемая 1-укорочением из $S(24,8,5)$) имеет радиус покрытия $\rho=3$. Поэтому надо вычислить константы $(\alpha_i,\beta_i,\gamma_i)$ для $i \in \{0,1,2,3\}$. Для этой схемы имеем [69]

$$\begin{array}{lll} \alpha_0=0, & \beta_0=112, & \gamma_0=0, \\ \alpha_1=21, & \beta_1=90, & \gamma_1=1, \\ \alpha_2=108, & \beta_2=2, & \gamma_2=12, \\ \alpha_3=7, & \beta_3=0, & \gamma_3=105. \end{array}$$

Отсюда мы заключаем, что система Штейнера $S(23,7,4)$ полностью регулярна. Третья большая схема Витта, т.е. система Штейнера $S(22,6,3)$, уже не полностью регулярна [69]. Тот же отрицательный результат имеет место для следующей системы Штейнера $S(21,5,2)$, т.е. для проективной плоскости $PG(2,4)$ порядка 4 [69].

Следующая простая идея позволяет получить новые ПР-схемы из систем Штейнера. Это специальный случай более общей известной конструкции новых схем из уже существующих (см., например, [2]). Определим *k-тень* схемы $T(n,w,t,\lambda)$ как семейство всех k-множеств, содержащихся в некотором блоке схемы T. Полученная новая схема уже находится в $J(n,k)$. Годсил [71] заметил следующий факт.

Предложение 26 [69]. *Для любой системы Штейнера $S(n, w, t)$ ее $(t+2)$-тень полностью регулярна с радиусом покрытия $\rho = 2$.*

Необходимое условие для существования ПР-схемы дает следующее

Предложение 27 [69]. *Если T является ПР-схемой в $J(n, w)$ с минимальным расстоянием $d_J(T) < w$, то*

$$d_J(T) \leqslant \frac{1}{3}(2w+1).$$

Отсюда получаем

Следствие 12 [69]. *Если система Штейнера $S(n, w, t)$ полностью регулярна, то $w \leqslant 3t-2$.*

Следующий замечательный результат [69] классифицирует все возможные симметричные ПР-схемы $T(n, w, 2, \lambda)$ (т.е. схемы T, для которых $n = |T|$).

Теорема 22 [69]. *Если T – симметричная ПР-схема $T(n, w, 2, \lambda)$, то T – проективная плоскость (т.е. $\lambda = 1$) порядка 2 или 3 (т.е. одна из двух систем Штейнера $S(7, 3, 2)$ или $S(13, 4, 2)$).*

Напомним, что схема $T(n, w, t, \lambda)$ с $t \geqslant 2$ называется *квазисимметричной*, если ее степень равна $s = 2$ (т.е. любые два различных блока схемы находятся друг от друга на одном из двух расстояний). Для несимметричных схем Мартин [69] получил следующие необходимые условия.

Следствие 13 [69]. *Имеют место следующие утверждения*:

1. *Если ПР-схема $T(n, w, 2, \lambda)$ имеет минимальное расстояние $d_J(T) \geqslant 4$, то $\lambda \geqslant n - w$.*
2. *В квазисимметричной ПР-схеме T в $J(n, w)$ расстояние $d_J(T) \leqslant 7$.*

Для заданной системы Штейнера $S(n, w, w-1)$ (полностью регулярной согласно теореме 21) Мартин [69] заметил, что раскраска $J(n, w)$ в соответствии с расстоянием от S является совершенной с матрицей параметров

$$A = \begin{bmatrix} 0 & w(n-w) \\ w & w(n-w-1) \end{bmatrix}.$$

Этот результат был усилен в [72] с использованием так называемой *индуцированной совершенной раскраски*, идея которой была заложена в более ранних работах [73] (*дистанционно бирегулярные графы*) и [74] (*индуцированные собственные функции*).

Предложение 28 [72]. *Система Штейнера $S(n, w, w-1)$ индуцирует совершенную 2-раскраску схемы $J(n, w+1)$ с матрицей параметров*

$$A = \begin{bmatrix} (w+1)(n-2w-1) & (w+1)w \\ w(n-2w) & w^2-2w-1+n \end{bmatrix}.$$

Так как имеются бесконечные семейства троек и четверок Штейнера – $S(n, 3, 2)$ и $S(n+1, 4, 3)$ (которые существуют для любого $n \equiv 1, 3 \pmod 6$), то получаем

Предложение 29 [72]. *Имеют место следующие утверждения*:

1. *Для каждого $n \equiv 1, 3 \pmod 6$ существует совершенная 2-раскраска $J(n, 4)$ с матрицей параметров*

$$A = \begin{bmatrix} 4(n-7) & 12 \\ 3(n-8) & n+2 \end{bmatrix}.$$

2. *Для каждого* $n \equiv 2, 4 \pmod 6$ *существует совершенная* 2*-раскраска* $J(n, 5)$ *с матрицей параметров*

$$A = \begin{bmatrix} 5(n-5) & 20 \\ 4(n-8) & n+7 \end{bmatrix}.$$

Наконец, сформулируем еще один результат из [72] о раскраске, индуцированной совершенным 1-кодом.

Предложение 30 [72]. *Пусть* C *– совершенный* 1*-код в* $J(n, w)$*. Тогда существует совершенная* 2*-раскраска схемы* $J(n, w+1)$ *с матрицей параметров*

$$A = \begin{bmatrix} (w+1)(n-w-2) & w+1 \\ w(n-w-1) & n-w-1 \end{bmatrix}.$$

Аналогично ПР-кодам в схеме Хэмминга, содержащим большой подкласс ПТ-кодов, подобное понятие существует и в схеме Джонсона. Схема $T(n, w, t, \lambda)$, чье дистанционное разбиение представляет собой разбиение орбит (т.е. для любого $i = 0, 1, \ldots, \rho$ множество $T(i)$ является орбитой) под действием некоторой группы автоморфизмов схемы $J(n, w)$, называется *полностью транзитивной схемой* (см. [49] для этого интересного подкласса ПР-схем).

О других результатах по совершенным e-кодам, ПР-схемам и совершенным раскраскам $J(n, w)$, а также о примерах таких схем небольшой длины см. работы [53, 54, 65–69, 72, 75].

§ 5. Существование и методы построения ПР-кодов

В этом параграфе приводятся бесконечные семейства (занумерованные в виде (F.i)) и отдельные спорадические примеры (занумерованные в виде (S.i)) известных нам ПР-кодов. Для всех кодов даются их массивы пересечений IA (см. определение в п. 2.1). Напомним, что далее используется терминология, введенная в п. 2.1, и q – степень простого числа.

5.1. ПР- и ПТ-коды из совершенных кодов. В работах [1–3] описаны следующие хорошо известные семейства ПР-кодов. Мы указываем также случаи, когда они являются ПТ-кодами.

(F.1) Любой q-ичный совершенный $(n, q^n/(1+n(q-1)), 3; 1)_q$-код является ПР- и ПТ-кодом с

$$\mathrm{IA} = \{(q-1)n; 1\}, \quad \text{где} \quad q \geqslant 2,\ n \geqslant 3.$$

(F.2) Любой q-ичный расширенный совершенный $(n+1, q^n/(1+n(q-1)), 4; 2)_q$-код является ПР-кодом (и ПТ-кодом в двоичном случае) с

$$\mathrm{IA} = \{(q-1)(n+1), (q-1)n; 1, 4\}, \quad \text{где} \quad q \geqslant 2,\ n \geqslant 4.$$

Код также полностью транзитивен для случая, когда $q = 4$ и $m = 2$.

(F.3) Любой q-ичный выколотый $(n-1, q^n/(1+n(q-1)), 2; 1)$-код любого совершенного $(n, q^n/(1+n(q-1)), 3; 1)$-кода является ПР- и ПТ-кодом с

$$\mathrm{IA} = \{(q-1)(n-1); q)\}, \quad \text{где} \quad q, n \geqslant 3.$$

Пусть B – любой q-ичный совершенный $(n, N, 3)_q$-код (n нечетно), и пусть C – любой его $(n, N/q, 4)$-подкод со следующим свойством: при любом выборе нулевого кодового слова в B множество слов C_4 представляет собой q-ичную схему $T(n, 4, 2, \lambda)_q$, где $\lambda = (n-3)/2$. Тогда из [32, 39] получаем следующее:

(F.4) Для $q \geqslant 2$ и $n \geqslant 4$ код C – ПР-код с

$$\text{IA} = \{n(q-1), (n-1)(q-1), 1; 1, (n-1), n(q-1)\}.$$

(F.5) В частности, для любой степени простого числа $q = 2^u$, где $u \in \{2, 3, \ldots\}$, существует $[q+1, q-2, 4; 3]_q$-ПР-код, являющийся подкодом совершенного $[q+1, q-1, 3]_q$-кода, с

$$\text{IA} = \{q^2 - 1, q(q-1), 1; 1, q, q^2 - 1\}.$$

(F.6) Любой q-ичный $(n, N, 3; 2)_q$-код, полученный укорочением совершенного $(n+1, qN, 3; 1)_q$-кода C, представляет собой ПР- и ПТ-код с

$$\text{IA} = \{(q-1)n, q-1; 1, (q-1)n\}.$$

Приведем теперь несколько разных подкодов, являющихся различными половинами двоичного совершенного кода, дающих ПР-коды с разными массивами пересечений. Пусть C – двоичный совершенный $(n, N, 3)$-код. Из [19] известно, что четная или нечетная половина кода C представляет собой ПР-код (входящий в семейство (F.4)). Из [19] также следует, что выколотый код четной половины (совершенного) кода C – это ПР-код (включенный в семейство (F.6)).

Другие половины двоичных кодов Хэмминга можно получить с помощью следующей конструкции. Пусть H_m обозначает проверочную матрицу двоичного кода Хэмминга длины $n = 2^m - 1$. Для заданного четного $m \geqslant 4$ и целых $i_1, i_2 \in \{0, 1, 2, 3\}$, таких что $i_1 \neq i_2$, обозначим через $\boldsymbol{v}_{i_1,i_2}$ двоичный вектор длины n, в котором i-я позиция v_i является следующей функцией значения веса i-го столбца $\boldsymbol{h}_i$ матрицы H_m:

$$v_i = \begin{cases} 1, & \text{если } \operatorname{wt}(\boldsymbol{h}_i) \equiv i_1 \text{ или } i_2 \pmod 4, \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть C_{i_1,i_2} – двоичный линейный $[n = 2^m - 1, k = n - m - 1, 3]$-код, где m четно, заданный проверочной матрицей $H_m(\boldsymbol{v}_{i_1,i_2})$, полученной из проверочной матрицы H_m (совершенного кода C той же длины) добавлением еще одной проверочной строки $\boldsymbol{v}_{i_1,i_2}$. Тогда для результирующего кода C_{i_1,i_2} имеем [38] следующее:

(F.7) Если $\{i_1, i_2\} = \{1, 2\}$ или $\{i_1, i_2\} = \{2, 3\}$, то C_{i_1,i_2} – антиподальная половина кода Хэмминга, являющаяся $[n, n-m-1, 3; 3]$-ПР- и ПТ-кодом с

$$\text{IA} = \{n, (n+1)/2, 1; 1, (n+1)/2, n\}.$$

(F.8) Если $\{i_1, i_2\} = \{0, 1\}$ или $\{i_1, i_2\} = \{0, 3\}$, то C_{i_1,i_2} – неантиподальная половина кода Хэмминга, являющаяся $[n, n-m-1, 3; 3]$-ПР- и ПТ-кодом с

$$\text{IA} = \{n, (n-3)/2, 1; 1, (n-3)/2, n\}.$$

Как можно увидеть из [38], если $\{i_1, i_2\} = \{0, 2\}$, то C_{i_1,i_2} – четная половина кода Хэмминга, которая, следовательно, входит в семейство (F.4). Если же $\{i_1, i_2\} = \{1, 3\}$, то C_{i_1,i_2} – $[n, n-m, 3]$-код Хэмминга.

Расширения кодов (F.7) также полностью регулярны [38]:

(F.9) Расширение кода (F.7) является антиподальным $[n+1, n-m, 4; 4]$-ПР- и ПТ-кодом с

$$\text{IA} = \{n+1, n, (n+1)/2, 1; 1, (n+1)/2, n, n+1\}.$$

Из [32, 76] имеем несколько семейств, полученных укорочением двоичных совершенных кодов или расширенных совершенных кодов. Пусть C^* – произвольный двоичный расширенный совершенный $(n^*, N^*, 4)$-код длины $n^* = 2^m \geqslant 8$.

(F.10) Пусть C – $(n = n^* - 2, N = N^*/2, 2; 3)$-код, полученный $\{(00), (11)\}$-укорочением кода C^*. Тогда C – ПР- и ПТ-код с

$$\text{IA} = \{n, n-2, 2; 2, n-2, n\}, \text{ где } n = 2^m - 2 \geqslant 6.$$

(F.11) Пусть C – двоичный $(n = n^* - 3, N^*/4, 1; 2)$-код, полученный $\{(000), (111)\}$-укорочением кода C^*. Тогда C – ПР- и ПТ-код с

$$\text{IA} = \{n-1, 3; 1, n-1\}, \text{ где } n = 2^m - 3 \geqslant 5.$$

(F.12) Пусть B – произвольный двоичный совершенный $(n, N, 3)$-код длины $n = 2^m - 1 \geqslant 7$. Пусть C представляет собой $(n-2, N/2, 1; 2)$-код, полученный $\{(00), (11)\}$-укорочением кода B. Тогда C – ПР- и ПТ-код с

$$\text{IA} = \{n-3, 2; 2, n-3\}.$$

Из работ [32, 76] получаем также семейство кодов, полученных укорочением q-ичных расширенных совершенных кодов:

(F.13) Пусть C^* – произвольный q-ичный расширенный совершенный $[n^*, k^*, 4; 2]_q$-код, такой что $q = 2^m \geqslant 4$, $n^* = q+2$ и $k^* = q-1$. Пусть C – $[n = q, k = q-2, 2; 2]_q$-код, полученный S-укорочением кода C^*, с множеством $S = \{(\alpha, \alpha) : \alpha \in \mathbb{F}_q\}$. Тогда C – ПР-код с

$$\text{IA} = \{q(q-1), (q-1)(q-2); 2, q\}, \quad \text{где} \quad q = 2^m \geqslant 4.$$

Перейдем теперь к отдельным примерам ПР-кодов, полученных из совершенных кодов Голея [19, 76]. Полная регулярность и полная транзитивность кодов (S.5) и (S.6) были указаны в [19].

(S.1) *Двоичный код Голея.* Это совершенный $[23, 12, 7; 3]$-ПР- и ПТ-код с

$$\text{IA} = \{23, 22, 21; 1, 2, 3\}.$$

(S.2) *Двоичный выколотый код Голея.* Это $[22, 12, 6; 3]$-ПР- и ПТ-код с

$$\text{IA} = \{22, 21, 20; 1, 2, 6\}.$$

(S.3) *Двоичный расширенный код Голея.* Это $[24, 12, 8; 4]$-ПР- и ПТ-код с

$$\text{IA} = \{24, 23, 22, 21; 1, 2, 3, 24\}.$$

(S.4) *Двоичный дважды выколотый код Голея.* Это $[21, 12, 5; 3]$-ПР- и ПТ-код с

$$\text{IA} = \{21, 20, 16; 1, 2, 12\}.$$

(S.5) *Половина двоичного кода Голея.* Это $[23, 11, 8; 7]$-ПР- и ПТ-код с

$$\text{IA} = \{23, 22, 21, 20, 3, 2, 1; 1, 2, 3, 20, 21, 22, 23\}.$$

(S.6) *Выколотая половина двоичного кода Голея.* Это $[22, 11, 7; 6]$-ПР- и ПТ-код с

$$\text{IA} = \{22, 21, 20, 3, 2, 1; 1, 2, 3, 20, 21, 22\}.$$

(S.7) $\{(00, 11)\}$*-укороченный двоичный расширенный код Голея.* Это $[22, 11, 6; 7]$-ПР- и ПТ-код с

$$\text{IA} = \{22, 21, 20, 16, 6, 2, 1; 1, 2, 6, 16, 20, 21, 22\}.$$

(S.8) $\{(000, 111)\}$*-укороченный двоичный расширенный код Голея.* Это $[21, 10, 5; 6]$-ПР- и ПТ-код с

$$\text{IA} = \{21, 20, 16, 9, 2, 1; 1, 2, 3, 16, 20, 21\}.$$

(S.9) $\{(00,11)\}$-*укороченный двоичный код Голея.* Это $[21,11,5;6]$-ПР- и ПТ-код с

$$\mathrm{IA} = \{21,20,16,6,2,1;1,2,6,16,20,21\}.$$

Обозначим через G троичный совершенный $[11,6,5]_3$-код Голея, а через $G^{(0)}$ – подкод кода G, состоящий из всех слов кода G с общей проверкой на четность 0. Легко видеть, что $G^{(0)}$ – это $[11,5,6]_3$-код, состоящий из всех кодовых слов веса 0, 6 и 9. Назовем этот код одной третьей частью троичного кода Голея.

(S.10) *Троичный код Голея.* Это совершенный $[11,6,5;2]_3$-ПР- и ПТ-код с

$$\mathrm{IA} = \{22,20;1,2\}.$$

(S.11) *Троичный выколотый код Голея.* Это $[10,6,4;2]_3$-ПР- и ПТ-код с

$$\mathrm{IA} = (20,18;1,6).$$

(S.12) *Троичный расширенный код Голея.* Это $[12,6,6;3]_3$-ПР- и ПТ-код с

$$\mathrm{IA} = \{24,22,20;1,2,12\}.$$

(S.13) *Третья часть троичного Кода Голея.* Это троичный $[11,5,6;5]_3$-ПР- и ПТ-код $G^{(0)}$ с

$$\mathrm{IA} = \{22,20,18,2,1;1,2,9,20,22\}.$$

(S.14) *Выколотая третья часть троичного кода Голея.* Это троичный $[10,5,5;4]_3$-ПР- и ПТ-код с

$$\mathrm{IA} = \{20,18,4,1;1,2,18,20\}.$$

Отметим, что многие из приводимых ниже кодов также тем или иным образом основаны на совершенных кодах (см. пп. 5.2, 5.4, 5.9, 5.10 и 5.12).

5.2. Вложенные семейства ПР-кодов. Обозначим через $\mathcal{H}_m$ двоичный код Хэмминга длины $n = 2^m - 1$. Пусть $m = 2u,\ q = 2^u,\ r = 2^u + 1$ и $\bar{r} = 2^u - 1$. Проверочную матрицу H_m кода $\mathcal{H}_m$ можно представить в виде двоичной записи упорядоченных элементов поля $[\alpha^0, \alpha^1, \ldots, \alpha^{n-1}]$, где $\alpha \in \mathbb{F}_{2^m}$ – примитивный элемент этого поля. Представим теперь элементы поля $\mathbb{F}_{2^m}$ как элементы квадратичного расширения подполя $\mathbb{F}_{2^u}$. Пусть $\beta = \alpha^r$ – примитивный элемент $\mathbb{F}_{2^u}$, и пусть $\mathbb{F}_{2^m} = \mathbb{F}_{2^u}[\alpha]$. Обозначим через E_m двоичное представление матрицы со столбцами $[\alpha^0, \alpha^r, \ldots, \alpha^{(n-1)r}]$. Определим матрицу P_m как вертикальное объединение матриц H_m и E_m:

$$P_m = \begin{bmatrix} H_m \\ E_m \end{bmatrix}.$$

Хорошо известно [40], что код $C^{(u)}$ с проверочной матрицей P_m представляет собой двоичный циклический ПР-код с радиусом покрытия $\rho = 3$, минимальным расстоянием $d = 3$ и размерностью $n - (m + u)$.

Как можно увидеть из [39], число смежных классов $C^{(u)} + v$ веса 3 равно $\bar{r}$. Действительно, их синдромы $S(v)$ представляют собой ненулевые элементы поля $\mathbb{F}_{2^u}$. Для каждого $i \in \{0, \ldots, u\}$ выберем $u - i$ смежных классов $C^{(u)} + v^{(1)}, \ldots, C^{(u)} + v^{(u-i)}$, синдромы которых $S(v^{(1)}), \ldots, S(v^{(u-i)})$ линейно независимы (т.е. их соответствующие двоичные представления линейно независимы как двоичные векторы в пространстве $\mathbb{F}_2^u$). Используя выбранные синдромы, построим линейный двоичный код $C^{(i)}$ как следующее линейное замыкание:

$$C^{(i)} = \langle C^{(u)}, v^{(1)}, \ldots, v^{(u-i)} \rangle.$$

Обозначим через A_{u-i} линейное подпространство $\mathbb{F}_2^u$, порожденное синдромами $S(v^{(1)}), \ldots, S(v^{(u-i)})$.

Размерность кода $C^{(i)}$ равна $\dim(C^{(i)}) = u - i + \dim(C^{(u)})$, где $\dim(C^{(u)}) = n - m - u$. Заметим, что максимальное число независимых синдромов, которое можно выбрать, равно u, т.е. наибольший код, который можно построить, имеет размерность $u + \dim(C^{(u)}) = n - m$, что представляет собой код Хэмминга $C^{(0)} = \mathcal{H}_m$. Все построенные коды содержат код $C^{(u)}$, и в то же самое время все они содержатся в коде Хэмминга $C^{(0)}$.

Число различных кодов $C^{(u-i)}$ равно числу подпространств размерности i, которые можно выбрать в $\mathbb{F}_2^u$, т.е. равно гауссовскому биномиальному коэффициенту

$$|\{C^{(u-i)}\}| = \begin{bmatrix} u \\ i \end{bmatrix}_2 = \frac{(2^u-1)(2^u-2)\ldots(2^u-2^{i-1})}{(2^i-1)(2^i-2)\ldots(2^i-2^{i-1})}.$$

Отсюда получаем, что число различных вложенных семейств кодов, которые можно построить между кодами $C^{(u)}$ и $C^{(0)} = \mathcal{H}_m$, равно

$$\prod_{i=0}^{u-1}(2^{u-i}-1).$$

Следующий факт был доказан в [40] для кодов $C^{(u)}$, но его можно распространить на все коды $C^{(i)}$, $i \in \{1, \ldots, u\}$.

Предложение 31. *Для любого $i \in \{1, \ldots, u\}$ смежные классы веса 3 кода $C^{(i)}$ находятся на расстоянии 3 друг от друга, и множество $C^{(i)} \cup C^{(i)}(3)$ является кодом Хэмминга.*

Напомним, что $C^{(i)*}$ получен из $C^{(i)}$ расширением и что из свойства ПТ вытекает свойство ПР.

Теорема 23 [39]. *Имеют место следующие утверждения*:

(i) $C^{(1)}$ – *ПТ-код с радиусом покрытия* 3;

(ii) $C^{(u)}$ – *ПТ-код с радиусом покрытия* 3;

(iii) *Если $C^{(i)}$ полностью транзитивен, то $C^{(i)*}$ также полностью транзитивен для любого $i \in \{0, \ldots, u\}$*;

(iv) *Для любого $i \in \{1, \ldots, u\}$ код $C^{(i)}$ является подкодом $C^{(i-1)}$, а код $C^{(i)*}$ – подкодом $C^{(i-1)*}$.*

(F.14) *Для любого $i \in \{0, \ldots, u\}$ код $C^{(i)}$ полностью регулярен с*

$$\text{IA} = \{2^m - 1, 2^m - 2^{m-i}, 1; 1, 2^{m-i}, 2^m - 1\};$$

(F.15) *Для любого $i \in \{0, \ldots, u\}$ расширенный код $C^{(i)*}$ полностью регулярен с*

$$\text{IA} = \{2^m, 2^m - 1, 2^m - 2^{m-i}, 1; 1, 2^{m-i}, 2^m - 1, 2^m\}.$$

Заметим, что для значений $i \in \{0, 1, u\}$ коды $C^{(i)}$ и $C^{(i)*}$ являются полностью транзитивными. Кроме того, для случая $m = 6$ вычисления показали, что все коды $C^{(i)}$ и $C^{(i)*}$ полностью транзитивны. В работе [77] было доказано, что дистанционно регулярные графы смежных классов, которые строятся на основе рассматриваемых кодов, дистанционно транзитивны при выполнении одного из следующих условий делимости: 2^m должно быть степенью 2^i, либо $2^m = 2^i$, либо $2^i - 1$ делит $2m$. Мы предполагаем, следовательно, что когда одно из этих условий делимости выполнено, то расширенный код $C^{(i)*}$ также является ПТ-кодом. Более того, для таких случаев

мы предполагаем, что $C^{(i)}$ также является ПТ-кодом. Однако вопрос о полной транзитивности кодов $C^{(i)}$ и $C^{(i)*}$ для случаев $i \notin \{0, 1, u\}$ открыт и требует большего внимания.

5.3. Коды типа Препараты и коды БЧХ. Из работ [2, 24] получаем следующие ПР-коды.

(F.16) Любой (двоичный) код типа Препараты, т.е. любой код с параметрами ($n = 2^{2m}-1, M = 2^{n+1-4m}, 5$), где $m \geqslant 2$, полностью регулярен с радиусом покрытия $\rho = 3$ [2] и

$$\mathrm{IA} = \{n, n-1, 1; 1, 2, 3\}.$$

(F.17) Расширенный код типа Препараты, т.е. любой код с параметрами ($n+1 = 2^{2m}, M = 2^{n+1-4m}, 6$) полностью регулярен с радиусом покрытия $\rho = 4$ [2] и

$$\mathrm{IA} = \{n+1, n, n-1, 1; 1, 2, 3, n+1\}.$$

(F.18) Двоичный примитивный код БЧХ с параметрами ($n = 2^{2m+1}-1, N = 2^{n-4m}$, $5; 3$), где $m \geqslant 2$, полностью регулярен с

$$\mathrm{IA} = \{n, n-1, (n+3)/2; 1, 2, (n-1)/2\}.$$

(F.19) Расширенный двоичный примитивный код БЧХ с параметрами ($n+1 = 2^{2m+1}, N = 2^{n-4m}, 6; 4$) полностью регулярен с

$$\mathrm{IA} = \{n+1, n, n-1, (n+3)/2; 1, 2, (n-1)/2, n+1\}.$$

5.4. Поднятие алфавитов кодов Хэмминга. ПР-коды можно получить поднятием алфавитов кодов Хэмминга. Обозначим через H_m^q проверочную матрицу кода Хэмминга $C = C(H_m^q)$ длины $n = (q^m-1)/(q-1)$ над $\mathbb{F}_q$. Определим новый линейный код, который мы обозначим через $C_r(H_m^q)$, той же длины n, но над полем $\mathbb{F}_{q^r}$, где $r \geqslant 2$, с той же проверочной матрицей H_m^q.

Теорема 24 [35]. *Имеет место следующее утверждение*:

(F.20) *Код $C_r(H_m^q)$ имеет параметры $[n, n-m, 3; \rho]_{q^r}$ и полностью регулярен с $\rho = \min\{r, m\}$ и числами пересечений*

$$b_i = \frac{(q^r - q^i)(q^m - q^i)}{(q-1)}, \quad i = 0, \ldots, \rho-1; \quad c_i = q^{i-1}\frac{q^i - 1}{q-1}, \quad i = 1, \ldots, \rho.$$

Если $r \neq m$, то коды $C_r(H_m^q)$ и $C_m(H_r^q)$ не эквивалентны, но имеют одинаковые массивы пересечений.

Заметим, что коды Хэмминга – это единственные коды, поднятие алфавитов которых приводит к ПР-кодам.

Теорема 25 [35]. *Пусть $C(H^q)$ – нетривиальный код длины n над полем $\mathbb{F}_q$ с минимальным расстоянием $d \geqslant 3$ и радиусом покрытия $\rho \geqslant 1$, и пусть $C_r(H^q)$ – поднятие кода $C(H^q)$ над полем $\mathbb{F}_{q^r}$. Тогда новый код $C_r(H^q)$ полностью регулярен, если и только если исходный код $C(H^q)$ является кодом Хэмминга.*

Согласно теореме 25 коды, полученные поднятием расширенных совершенных кодов, никогда не являются ПР-кодами. Однако все эти коды равномерно упакованы в широком смысле [35].

Следующее утверждение обобщает результаты работ [24, 33] на недвоичный случай.

Предложение 32 [35]. *Пусть C – q-ичный $[n, n-m, 3]$-код Хэмминга длины $n = (q^m-1)/(q-1)$, и пусть C^* – расширение этого кода. Тогда код C^* равномерно*

упакован, если и только если он имеет минимальное расстояние 4. *Другими словами,* C^* *равномерно упакован, если и только если* $q = 2$ *и* $m \geqslant 2$ *или* $q = 2^u \geqslant 4$ *и* $m = 2$.

Теорема 26 [35]. *Пусть* C – q-*ичный* $[n, n-m, 3]$-*код Хэмминга длины* $n = (q^m - 1)/(q-1)$, *и пусть* C^* – *расширение этого кода. Поднятый код* C_r^* *равномерно упакован, если и только если код* C^* *равномерно упакован. Следовательно, поднятый код* C_r^* *равномерно упакован, если и только если* $q = 2$ *и* $m \geqslant 2$ *или* $q = 2^u \geqslant 4$ *и* $m = 2$.

5.5. ПР-коды по кронекеровым произведениям. Построение ПР-кодов с помощью кронекерова произведения матриц над одним и тем же алфавитом было рассмотрено в [34]. Позднее эта конструкция была обобщена в [78] на случай разных алфавитов исходных компонентных кодов. Новая общая конструкция оказалась связанной с поднятием кодов, что было рассмотрено в предыдущем пункте. Отметим следующий интересный факт. Новая конструкция дает растущее число ПР-кодов с различными параметрами (и над различными алфавитами), но с одним и тем же массивом пересечений (т.е. все результирующие дистанционно регулярные графы смежных классов изоморфны, но строятся из разных ПР-кодов с разными параметрами).

Напомним, что кронекерово произведение двух матриц $A = [a_{r,s}]$ над $\mathbb{F}_{q^u}$ и B над $\mathbb{F}_q$ (где $\mathbb{F}_q$ – подполе $\mathbb{F}_{q^u}$) – это новая матрица $H = A \otimes B$, полученная заменой каждого элемента $a_{r,s}$ в A матрицей $a_{r,s}B$.

Теорема 27 [34, 78]. *Пусть коды Хэмминга* $C(H^{q^u}_{m_a})$ *и* $C(H^q_{m_b})$ *имеют параметры* $[n_a, n_a - m_a, 3]_{q^u}$ *и* $[n_b, n_b - m_b, 3]_q$ *соответственно, где* q – *степень простого числа,* $n_a = (q^{um_a} - 1)/(q^u - 1)$, $n_b = (q^{m_b} - 1)/(q-1)$, $m_a, m_b \geqslant 2$ *и* $u \geqslant 1$.

(F.21) *Код* $C = C(H)$ *с проверочной матрицей* $H = H^{q^u}_{m_a} \otimes H^q_{m_b}$, *представляющей собой кронекерово произведение матриц* $H^{q^u}_{m_a}$ *и* $H^q_{m_b}$, *полностью транзитивен и поэтому полностью регулярен с параметрами* $[n, k, d; \rho]_{q^u}$, *где*

$$n = n_a\, n_b, \quad k = n - m_a\, m_b, \quad d = 3, \quad \rho = \min\{u\, m_a,\ m_b\}, \tag{8}$$

и с числами пересечений

$$b_\ell = \frac{(q^{u\, m_a} - q^\ell)(q^{m_b} - q^\ell)}{(q-1)}, \quad \ell = 0, 1, \ldots, \rho - 1,$$

$$c_\ell = q^{\ell-1}\frac{q^\ell - 1}{q-1}, \quad \ell = 1, 2, \ldots, \rho.$$

Поднятый код $C_{m_b}(H^q_{um_a})$ *полностью регулярен с тем же самым массивом пересечений, что и код* C.

Заметим, что в теореме 27 нельзя выбрать код $C_{m_b}(H^{q^u}_{m_a})$ вместо $C_{m_b}(H^q_{um_a})$, что кажется вполне естественным. Подчеркнем здесь, что коды $C_{m_b}(H^q_{um_a})$ и $C_{m_b}(H^{q^u}_{m_a})$ не только являются различными ПР-кодами, но и индуцируют различные дистанционно регулярные графы смежных классов с разными массивами пересечений. Поэтому код $C_{m_b}(H^q_{um_a})$ подходит к кодам из семейства (F.21) в том смысле, что он имеет тот же самый массив пересечений. Например, код $C_2(H_3^{2^2})$ индуцирует дистанционно регулярный граф с массивом пересечений $\{315, 240; 1, 20\}$, а код $C_2(H_6^2)$ – дистанционно регулярный граф с массивом $\{189, 124; 1, 6\}$. Отметим, что для получения всех этих результатов в обоих случаях используется одна и та же теорема 24.

Заметим, что предыдущая теорема 27 не может быть обобщена на более общий случай, когда алфавиты $\mathbb{F}_{q^a}$ и $\mathbb{F}_{q^b}$ компонентных кодов C_A и C_B, соответственно, являются полями произвольных порядков одной и той же характеристики. Проиллюстрируем этот факт минимальным нетривиальным примером. Возьмем два кода

Хэмминга – $[5,3,3]$-код C_A над $\mathbb{F}_{2^2}$ с проверочной матрицей $H_2^{2^2}$ и $[9,7,3]$-код C_B над $\mathbb{F}_{2^3}$ с проверочной матрицей $H_2^{2^3}$. Тогда результирующий $[45,41,3]$-код $C = C(H_2^{2^2} \otimes H_2^{2^3})$ над $\mathbb{F}_{2^6}$ даже не является равномерно упакованным кодом в широком смысле, так как он имеет радиус покрытия $\rho = 3$, а внешнее расстояние $s = 7$, что легко проверяется по проверочной матрице кода C.

Теорема 28 [78]. *Пусть q – любая степень простого числа, и пусть a, b, u – любые натуральные числа. Тогда существуют следующие ПР-коды с различными параметрами $[n,k,d;\rho]_{q'}$, где q' – степень q, расстояние $d = 3$, а радиус покрытия $\rho = \min\{ua, b\}$:*

(F.22) $C_{ua}(H_b^q)$ *над* $\mathbb{F}_{q^{ua}}$ *длины* $n = \dfrac{q^b-1}{q-1}$, $k = n - b$;

(F.23) $C_b(H_{ua}^q)$ *над* $\mathbb{F}_{q^b}$ *длины* $n = \dfrac{q^{ua}-1}{q-1}$, $k = n - ua$;

(F.24) $C(H_b^q \otimes H_{ua}^q)$ *над* $\mathbb{F}_q$ *длины* $n = \dfrac{q^b-1}{q-1}\dfrac{q^{ua}-1}{q-1}$, $k = n - bua$;

(F.25) $C(H_b^q \otimes H_u^{q^a})$ *над* $\mathbb{F}_{q^a}$ *длины* $n = \dfrac{q^b-1}{q-1}\dfrac{q^{ua}-1}{q^a-1}$, $k = n - bu$;

(F.26) $C(H_b^q \otimes H_a^{q^u})$ *над* $\mathbb{F}_{q^u}$ *длины* $n = \dfrac{q^b-1}{q-1}\dfrac{q^{ua}-1}{q^u-1}$, $k = n - ba$;

Все вышеприведенные коды имеют следующие одинаковые числа пересечений:

$$b_\ell = \frac{(q^b - q^\ell)(q^{ua} - q^\ell)}{(q-1)}, \quad \ell = 0, \dots, \rho - 1; \quad c_\ell = q^{\ell-1}\frac{q^\ell - 1}{q-1}, \quad \ell = 1, \dots, \rho.$$

Все вышеприведенные коды, построенные по кронекеровым произведениям (т.е. семейства (F.24)–(F.26)*), являются полностью транзитивными.*

Обозначим через $\tau(n)$ число различных делителей натурального числа n.

Следствие 14 [78]. *Для заданной степени простого числа q выберем два произвольных натуральных числа $a, b > 1$. Тогда можно построить $\tau(a)+\tau(b)$ следующих различных ПР-кодов с одинаковым массивом пересечений и радиусом покрытия $\rho = \min\{a, b\}$:*

(i) *ПТ-коды $C(H_r^{q^{r^*}} \otimes H_b^q)$ над $\mathbb{F}_{q^{r^*}}$ для любого собственного делителя r числа a, такого что $rr^* = a$;*

(ii) *ПТ-коды $C(H_a^q \otimes H_r^{q^{r^*}})$ над $\mathbb{F}_{q^{r^*}}$ для любого собственного делителя r числа b, такого что $rr^* = b$;*

(iii) *ПР-коды $C_a(H_b^q)$ над $\mathbb{F}_{q^a}$ и ПР-коды $C_b(H_a^q)$ над $\mathbb{F}_{q^b}$.*

Эта конструкция дает также РУ-коды в широком смысле, не являющиеся полностью регулярными. Пусть $R_t = [I_{t-1} \mid \mathbf{1}]$, где I_{t-1} – двоичная диагональная матрица порядка $t-1$, а $\mathbf{1}$ – столбец из всех единиц.

Теорема 29 [78]. *Пусть заданы q^u-ичный $[n,k,3]_{q^u}$-код Хэмминга $C(H_m^{q^u})$ длины $n_a = (q^{um}-1)/(q^u-1)$ и q-ичный $[n_b, 1, n_b]_q$-код с повторением $C(R_{n_b})$ длины n_b, где $4 \leqslant n_b \leqslant (q^u-1)n_a + 1$, q – степень простого числа, $u \geqslant 1$ и $m \geqslant 2$.*

(i) *Код $C = C(H_m^{q^u} \otimes R_{n_b})$ – это q^u-ичный РУ-код в широком смысле с радиусом покрытия $\rho = n_b - 1$ и параметрами*

$$n = n_a n_b, \quad k = n - m(n_b - 1), \quad d = 3. \tag{9}$$

(ii) *Код C не полностью регулярен.*

5.6. Биномиальные ПР-коды. Обозначим через $H^{(m,\ell)}$ двоичную матрицу размера $m \times \binom{m}{\ell}$, столбцами которой являются все различные векторы длины m и веса ℓ.

Определим двоичный линейный код $C^{(m,\ell)}$ с проверочной матрицей $H^{(m,\ell)}$, который будем называть биномиальным.

Теорема 30 [79]. *Пусть m и ℓ – два натуральных числа, такие что $2 \leqslant \ell \leqslant m-2$. Код $C^{(m,\ell)}$ полностью транзитивен (и следовательно, полностью регулярен) в точности в следующих четырех случаях*:

(F.27) *Для любого $m \geqslant 4$ код $C^{(m,2)}$ представляет собой $[n,k,d;\rho]$-код с параметрами*

$$n = \binom{m}{2}, \quad k = n - m + 1, \quad d = 3, \quad \rho = \lfloor m/2 \rfloor$$

и числами пересечений для $i = 0, \ldots, \rho$

$$a_i = 2i(m-2i), \quad b_i = \binom{m-2i}{2}, \quad c_i = \binom{2i}{2};$$

(S.15) *Код $C^{(5,3)}$ является $[10,5,4;3]$-кодом с*

$$\mathrm{IA} = \{10, 9, 4; 1, 6, 10\};$$

(S.16) *Код $C^{(6,4)}$ является $[15,10,3;3]$-кодом с*

$$\mathrm{IA} = \{15, 8, 1; 1, 8, 15\};$$

(S.17) *Код $C^{(7,4)}$ является $[35,29,3;2]$-кодом с*

$$\mathrm{IA} = \{35, 16; 1, 20\}.$$

Из кодов с $\ell = 2$ можно построить новые полностью регулярные коды. Сначала разделим все эти коды на два семейства [79]. Обозначим $C^{(m)} = C^{(m,2)}$.

Теорема 31 [36,79]. *Пусть m – натуральное число, $m \geqslant 3$. Код $C^{(m)}$ антиподален, если m нечетно, и неантиподален, если m четно.*

Так как для четного m код $C^{(m)}$ неантиподален, его покрывающее множество $C^{(m)}(\rho)$ представляет собой сдвиг кода $C^{(m)}$ (теорема 6) на вектор $(1,1,\ldots,1)$. Рассмотрим новый (линейный) код $C^{[m]} = C^{(m)} \cup C^{(m)}(\rho)$. Его порождающая матрица $G^{[m]}$ имеет следующую симметричную структуру:

$$G^{[m]} = \left[\begin{array}{c|c} I_{k-1} & H^t_{m-1} \\ \hline 0\ldots0 & 1\ldots1 \end{array}\right],$$

где H^t_{m-1} – это транспонированная матрица $H^{(m-1,2)}$. Используя тот факт, что $C^{(m)}(\rho) = C^{(m)} + (1,1,\ldots,1)$ (теорема 6), заключаем, что справедлива следующая

Теорема 32 [36]. *Пусть m четно, $m \geqslant 6$.*

(F.28) *Код $C^{[m]}$ полностью транзитивен (и поэтому полностью регулярен) с параметрами*

$$n = m(m-1)/2, \quad k = n - m + 2, \quad d = 3, \quad \rho = \lfloor m/4 \rfloor$$

и следующими числами пересечений: для $m \equiv 0 \pmod 4$ и $\rho = m/4$

$$b_i = \binom{m-2i}{2}, \quad c_i = \binom{2i}{2}, \quad i = 0, 1, \ldots, \rho-1, \quad c_\rho = 2\binom{2\rho}{2},$$

а для $m \equiv 2 \pmod 4$ *и* $\rho = (m-2)/4$

$$b_i = \binom{m-2i}{2}, \quad c_i = \binom{2i}{2}, \quad i = 0, 1, \ldots, \rho.$$

5.7. ПР-коды, построенные с помощью прямой суммы. Пусть C_1 и C_2 – два кода, не обязательно линейные, одной и той же длины n. Прямая сумма кодов C_1 и C_2 – это код, полученный следующим образом:

$$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1,\ c_2 \in C_2\}.$$

Теорема 33 [6, 24]. *Пусть* r *– произвольное натуральное число, и пусть* C_i, $i = 1, 2, \ldots, r$, *– q-ичные* $(n, N, d; 1)_q$*-ПР-коды, имеющие одинаковый массив пересечений* $(b_0; c_1)$.

(F.29) *Тогда для любого* $r \geqslant 1$ *прямая сумма*

$$C = C_1 \oplus \ldots \oplus C_r$$

представляет собой $(nr, N^r, d; r)_q$*-ПР-код с числами пересечений*

$$a(r)_i = n(q-1) - (r-i)b_0 - ic_1, \quad b(r)_i = (r-i)b_0, \quad c(r)_i = ic_1,$$

где $i = 0, 1, \ldots, r$. *Более того, если все* C_i *– ПТ-коды,* (*перестановочно*) *эквивалентные друг другу, то код* C *также полностью транзитивен.*

Заметим, что конструкция, описанная в теореме 33, была рассмотрена в [6] для частного случая, когда все C_i – двоичные совершенные коды.

5.8. ПР-коды из комбинаторных конфигураций. Имеются следующие конструкции.

(F.30) *Коды на основе одного латинского квадрата.* Для любого алфавита F размера $q \geqslant 2$ существует q-ичный $(3, q^2, 2; 1)_q$-МДР-код над F, являющийся ПР-кодом с

$$\mathrm{IA} = \{3(q-1); 3\}.$$

В этом случае множество $C(\rho)$ представляет собой все остальные векторы из $\mathbb{F}^3$, т.е. $C(\rho) = F^3 \setminus C$.

(F.31) *Коды на основе двух латинских квадратов.* Для любого алфавита F размера $q \geqslant 3$, где $q \neq 6$, существует q-ичный $(4, q^2, 3; 2)_q$-МДР-код над F, являющийся ПР-кодом с

$$\mathrm{IA} = \{4(q-1), 3(q-3); 1, 12\}.$$

(S.18) *Код на основе трех латинских квадратов.* Три взаимно ортогональных латинских квадрата порядка 4 образуют эквидистантный (т.е. любые два кодовых слова находятся на расстоянии d) $[5, 2, 4; 3]_4$-код C. Этот код полностью регулярен с

$$\mathrm{IA} = \{15, 12, 3; 1, 4, 15\}.$$

Выколотый $[4, 2, 3]_4$-код $C^{(i)}$, полученный из этого кода, также полностью регулярен и принадлежит семейству (F.31).

(S.19) *Код на основе четырех латинских квадратов.* Четыре взаимно ортогональных латинских квадрата порядка 5 образуют эквидистантный $[6, 2, 5; 3]_5$-код C. Это ПР-код с

$$\mathrm{IA} = \{24, 20, 13; 1, 2, 6\}.$$

Выколотый $[5,2,4]_5$-код $C^{(i)}$, полученный из кода C, уже не полностью регулярен, так как множество $(C^{(p)})_4$ не является 2-схемой. Но дважды выколотый $[4,2,3;2]_5$-код полностью регулярен и принадлежит семейству (F.31).

(S.20) *Код Адамара.* Единственная (с точностью до эквивалентности) матрица Адамара порядка 12 индуцирует двоичный $(11,24,5;3)$-код H. В [4] было показано, что H полностью регулярен с

$$\mathrm{IA} = \{11,10,3;1,2,9\},$$

а в [37] установлено, что H полностью транзитивен, а также доказана единственность такого кода в классе ПР-кодов с $(n,d) = (11,5)$ (см. предложение 8).

(S.21) *Расширенный код Адамара.* Расширенный код H, рассмотренный выше, представляет собой $(12,24,6;4)$-код H^*. Согласно [33] код H^* равномерно упакован и поэтому является ПР-кодом с

$$\mathrm{IA} = \{12,11,10,3;1,2,9,12\}.$$

В [37] было установлено, что H^* полностью транзитивен, а также доказана единственность этого кода в классе ПР-кодов с $(n,d) = (12,6)$ (см. предложение 8).

(F.32) *Схема Джонсона в схеме Хэмминга.* Для любого натурального $w \geqslant 1$ тривиальный равновесный $(n,N,d;\rho)$-код (или схема Джонсона $J(n,w)$) с параметрами

$$n = 2w, \quad N = \binom{2w}{w}, \quad d = 2, \quad \rho = w$$

полностью регулярен с

$$\mathrm{IA} = \{2w, 2w-1, 2w-2, \ldots, 1; w+1, w+2, \ldots, 2w\}.$$

Ясно также, что этот код полностью транзитивен, так как его группой автоморфизмов является полная симметрическая группа. В § 4 рассматриваются ПР-коды в схемах Джонсона. Таким образом, схема Джонсона $J(2w,w)$ является полностью регулярной и полностью транзитивной в схеме Хэмминга $H(2,2w)$.

5.9. ПР-коды, полученные каскадными конструкциями. В этом пункте обсудим некоторые результаты из работы [80], в которой рассматривались ПР-коды, построенные каскадированием кодов Хэмминга.

Пусть H – циклическая проверочная матрица q-ичного кода Хэмминга длины $n = (q^m-1)/(q-1)$, т.е. мы предполагаем, что $\mathrm{НОД}(n, q-1) = 1$. Поэтому симплексный код, порожденный матрицей H, также циклический. Для любого $c \in \{1,2,\ldots,n\}$ рассмотрим код C с проверочной матрицей

$$\begin{bmatrix} H & H & \ldots & H \\ H_1 & H_2 & \ldots & H_c \end{bmatrix}, \tag{10}$$

где H_i – матрица, полученная из H циклическим сдвигом всех ее столбцов на i позиций вправо.

(F.33) Код C с проверочной матрицей (10) полностью регулярен с параметрами $[nc, nc-2m, 3; 2]_q$ и массивом пересечений

$$\mathrm{IA} = \{(q-1)nc, ((q-1)n-c+2)(c-1); 1, c(c-1)\}.$$

Почти все коды семейства (F.33) не полностью транзитивны. Однако в двоичном случае и для любого числа m, т.е. для любой длины $n = 2^m-1$, код C полностью транзитивен для значений $c \in \{2,3,n-1,n\}$. В q-ичном случае код C полностью транзитивен для случая $c = 2$.

Расширение кодов из семейства (F.33) не приводит к ПР-кодам, за исключением двоичного случая, когда $c = 2^{m-1}+1$. В этом случае результирующий расширенный код с параметрами $[n(2^{m-1}+1)+1, n(2^{m-1}+1)-2m, 4; 3]$ совпадает с кодами из семейства (F.35), описанного ниже.

Определим теперь код $A^{(c)}$ длины $n(c+3)$ с проверочной матрицей

$$H_a(c) = \begin{bmatrix} H & 0 & H & H & \dots & H \\ 0 & H & H & H_1 & \dots & H_c \end{bmatrix}, \tag{11}$$

где 0 обозначает нулевую матрицу того же размера, что и H. В [80] было доказано, что все коды $A^{(c)}$ полностью регулярны.

(F.34) Для $c \leqslant n-1$ код $A^{(c)}$ с проверочной матрицей (11) представляет собой ПР-код с параметрами $[(c+3)n, (c+3)n-2m, 3; 2]_q$ и массивом пересечений

$$\text{IA} = \{(c+3)(q-1)n, (c+2)((q-1)n-1-c); 1, (c+2)(c+3)\}.$$

В двоичном случае, когда $c = n-1$, код $A^{(n-1)}$ совпадает с $[2^{2m}-1, 2^{2m}-1-2m, 3; 1]$-кодом Хэмминга.

Из всех кодов семейства (F.34) полностью транзитивными являются двоичные коды $A^{(c)}$ с $m > 2$ для значений $c \in \{2^m-5, 2^m-4, 2^m-3\}$.

Расширение кодов $A^{(c)}$ из семейства (F.34) приводит к новым ПР-кодам только в двоичном случае для двух значений $c \in \{2^{m-1}-2, 2^m-2\}$.

(F.35) Пусть $A^{(c)}$ – код с проверочной матрицей $H_a(c)$, и пусть $A^{(c)*}$ получен его расширением. Для $c = 2^{m-1}-2$ код $A^{(c)*}$ с параметрами $[(c+3)n+1, (c+3)n-2m, 4; 3]$ полностью регулярен с

$$\text{IA} = \{(c+3)n+1, (c+3)n, 2^{2m-2}; 1, (c+2)(c+3), (c+3)n+1\}.$$

Для $c = 2^m-2$ код $A^{(c)*}$ с параметрами $[(c+3)n+1, (c+3)n-2m, 4; 2]$ совпадает с расширенным кодом Хэмминга длины 2^{2m}. Для $c \notin \{2^{m-1}-2, 2^m-2\}$ код $A^{(c)*}$ не полностью регулярен.

Пусть m и c – натуральные числа, такие что $1 \leqslant c \leqslant n-1 = 2^m-2$. Пусть $C = A^{(n-2)}$, и пусть H_c – его проверочная матрица. Код C – это код Хэмминга длины $2^{2m}-1$. Пусть $B^{(n-1-c)}$ – код, заданный матрицей (10) после удаления из этой матрицы столбцов, имеющихся в матрице $H_a(c)$. Пусть $H_b(n-1-c)$ – проверочная матрица кода $B^{(n-1-c)}$. Три введенных кода $A^{(c)}$, $B^{(n-1-c)}$ и C имеют длины $n_a = (c+3)(2^m-1)$, $n_b = (n-1-c)(2^m-1)$ и $n_c = n_a + n_b = 2^{2m}-1$ соответственно. Следовательно, матрица H_c представляется в виде

$$H_c = [H_a(c) \mid H_b(n-1-c)].$$

Код $B^{(n-1-c)}$ эквивалентен коду, заданному условием (10), при выборе значения c, равного $n-1-c$, в этой формуле. Следовательно, $A^{(n-1-c)}$ и $B^{(c)}$ полностью регулярны. Кроме того, коды $A^{(n-1-c)}$ и $B^{(c)}$ являются или не являются полностью транзитивными одновременно.

Пусть $\mathrm{Aut}(B)$ – группа автоморфизмов кода $B^{(c)}$, а $\mathrm{Aut}(A)$ – группа автоморфизмов кода $A^{(n-1-c)}$ для $1 \leqslant c \leqslant n-1$. Тогда группы $\mathrm{Aut}(A)$ и $\mathrm{Aut}(B)$ изоморфны [81].

Обозначим через $\mathcal{C}_t$ циклическую группу порядка t, и пусть $\mathrm{GL}(m, 2)$ – двоичная общая линейная группа. Напомним, что $\mathcal{S}_3$ – симметрическая группа. В [81] авторы установили, что

- $\mathrm{Aut}(B) = \mathrm{GL}(m, 2) \times \mathrm{GL}(m, 2) \times \mathcal{C}_2$ *для* $c = 2$;
- $\mathrm{Aut}(B) = \mathrm{GL}(m, 2) \times \mathcal{S}_3$ *для* $c = 3$;

- *Коды* $A^{(c)}$ *и* $B^{(n-1-c)}$ *полностью транзитивны, если и только если* $n-1-c \in \in \{1,2,3\}$.

Заметим, что в случае $c = n-2 = 2^m-3$ код $B^{(c)}$ является кодом Хэмминга длины 2^m-1.

Перейдем теперь к спорадическим примерам кодов, полученных каскадными методами.

(S.22) Пусть $H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ – проверочная матрица двоичного кода Хэмминга длины 3, и пусть H_1 (соответственно, H_2) – матрицы, полученные одним циклическим сдвигом столбцов $H = H_0$ (соответственно, двумя циклическими сдвигами). Двоичный $[15, 9, 3; 3]$-код C с проверочной матрицей

$$\begin{bmatrix} H & 0 & 0 & H & H \\ 0 & H & 0 & H & H_1 \\ 0 & 0 & H & H & H_2 \end{bmatrix}$$

полностью регулярен с

$$\mathrm{IA} = \{15, 12, 1; 1, 4, 15\}.$$

(S.23) Двоичный $[16, 9, 4; 4]$ код, полученный расширением $[15, 9, 3; 3]$-кода, описанного выше, также полностью регулярен с

$$\mathrm{IA} = \{16, 15, 12, 1; 1, 4, 15, 16\}.$$

Обозначим через $D(u, q)$ разностную матрицу (см. [25]), т.е. квадратную матрицу порядка qu над аддитивной группой порядка q, такую что покомпонентная разность любых двух различных строк содержит каждый элемент группы ровно u раз. Возьмем разностную матрицу $D = D(2, 3)$, имеющую вид

$$D = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}.$$

(S.24) Пусть H – матрица размера 12×18, полученная из D заменой каждого элемента i на матрицу H_i (определенную в (S.22)). Тогда $[18, 12, 3; 2]$-код с проверочной матрицей H полностью регулярен с $\mathrm{IA} = \{18, 15; 1, 6\}$.

(S.25) Используем ту же конструкцию, что и в (S.24), для матрицы D^*, полученной из разностной матрицы $D(2, 3)$ удалением тривиального столбца. Полученный таким образом $[15, 9, 3; 3]$-код представляет собой ПР-код с $\mathrm{IA} = \{15, 12, 1; 1, 4, 15\}$. Этот код совпадает с кодом, построенным в (S.22).

5.10. Линейные q-ичные ПР-коды с $\rho = 1$. Линейные q-ичные ПР-коды с $\rho = 1$ полностью классифицированы в [82] с помощью следующих двух простых конструкций.

Конструкция $I(u)$. Пусть C – $[n, k, d]_q$-код с проверочной матрицей H. Определим новый код C^{+u} с параметрами $[n+u, k+u, 1]_q$ как код с проверочной матрицей H^{+u}, полученной из H добавлением к ней $u > 0$ нулевых столбцов.

Теорема 34 [82]. *Коды* C *и* C^{+u} *имеют одинаковые радиусы покрытия. Более того, код* C^{+u} *полностью регулярен, если и только если* C *полностью регулярен. В этом случае оба кода имеют одни и те же числа пересечений* $b_i = b'_i$ *и* $c_i = c'_i$, *так что*

$$a'_i = a_i + (q-1)u, \quad b'_i = b_i, \quad c'_i = c_i, \quad i = 0, 1, \ldots, \rho$$

(*здесь* a_i, b_i, c_i *– числа пересечений кода* C).

Конструкция $\Pi(\ell)$. Пусть C – $[n,k,d]_q$-код с проверочной матрицей H. Пусть $C^{\times\ell}$ – код с параметрами $[n\ell, k+(\ell-1)n, 2]_q$, чья проверочная матрица $H^{\times\ell}$ получена ℓ-кратным повторением матрицы H (или матриц, эквивалентных матрице H), т.е.

$$H^{\times\ell} = \left[H^{(1)} \,|\, H^{(2)} \,|\, \ldots \,|\, H^{(\ell)}\right],$$

где для всех $i = 1, \ldots, \ell$ матрица $H^{(i)}$ – это проверочная матрица кода, эквивалентного коду C.

Теорема 35 [82]. *Новый* $[n,k,d]_q$*-код* $C^{\times\ell}$ *является ПР-кодом с радиусом покрытия* $\rho = 1$, *если и только если* C *– ПР-код с радиусом покрытия* $\rho' = 1$.

Итак, для линейных ПР-кодов с $\rho = 1$ имеет место следующая

Теорема 36 [82]. *Пусть* $C = C(H)$ *– нетривиальный* $[n,k,d]_q$*-код с радиусом покрытия* $\rho = 1$ *и проверочной матрицей* H.

(F.36) *Тогда код* C *полностью транзитивен* (*следовательно, полностью регулярен*) *с параметрами* $[n, n-m, d; 1]_q$, *где* $n = n_m\,\ell + u$ *и* $n_m = (q^m-1)/(q-1)$, *если и только если матрица* H *имеет* (*с точностью до эквивалентности*) *следующий вид*:

$$H = \left((H_m^q)^{\times\ell}\right)^{+u},$$

где H_m^q *– проверочная матрица кода Хэмминга длины* $n_m = (q^m-1)/(q-1)$ *над* $\mathbb{F}_q$.

Более того,

$d = 3$, *если и только если* $u = 0$, $\ell = 1$, $n = n_m$, *а* C *– код Хэмминга*; *в этом случае эти коды включены в семейство* (F.1);

(F.37) $d = 2$, *если и только если* $u = 0$, $\ell \geqslant 2$, $n = n_m\ell$;

(F.38) $d = 1$, *если и только если* $u > 0$, $\ell \geqslant 1$.

Во всех случаях код C *имеет*

$$\mathrm{IA} = \{(q-1)\ell\, n_{n-k}; \ell\}$$

Отметим, что аналогичный результат был получен в [13] в терминах арифметических кодов.

5.11. Нелинейные q-ичные ПР-коды с $\rho = 1$. Смежный класс линейного ПР-кода с $\rho = 1$, очевидным образом, является нелинейным ПР-кодом с тем же самым $\rho = 1$. Кроме этих тривиальных кодов, мало что известно для этого случая. Имеются интересные результаты Фон-Дер-Флааса [83–85], к которым мы сейчас перейдем. Эквивалентный термин для построения ПР-кодов с заданным ρ – так называемая *совершенная* $(\rho+1)$*-раскраска гиперкуба*. Особенно просто совершенная раскраска определяется для случая $\rho = 1$, т.е. для 2-раскраски. Пусть $H(2,n)$ – двоичный гиперкуб размерности n (или двоичная схема Хэмминга). Вершинами его являются все двоичные векторы длины n, и две вершины соединены ребром (или являются соседями), если соответствующие векторы находятся друг от друга на расстоянии 1. Раскраска вершин гиперкуба (обычно) белым и черным цветами называется совершенной 2-раскраской с матрицей пересечений

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

если каждая черная вершина имеет в качестве соседей a черных и b белых вершин, а каждая белая вершина – c черных и d белых вершин. Так как в двоичном случае

любая вершина имеет n соседей, то получаем, очевидно, что $a + b = c + d = n$. В терминах чисел пересечения

$$a_0 = a, \quad b_0 = b, \quad c_1 = c, \quad a_1 = d,$$

и следовательно, совершенная 2-раскраска – это нелинейный ПР-код с массивом пересечений $\mathrm{IA} = \{b; c\}$. Нижнюю оценку на величину $a = n - b$ (представляющую собой наилучшую известную оценку на *корреляционную иммунность* (см. работу [83] и библиографию в ней) дает

Теорема 37 [83]. *Пусть C – двоичный ПР-код длины n с радиусом покрытия $\rho = 1$ и массивом пересечений $\mathrm{IA} = \{b; c\}$. Если $b \neq c$, то*

$$c - a \leqslant \frac{n}{3}. \tag{12}$$

Другое необходимое условие обеспечивает [84] следующая

Теорема 38 [84]. *Пусть C – двоичный ПР-код длины n с $\rho = 1$ и массивом пересечений $(b; c)$. Тогда $b \neq 0 \neq c$, и*

$$\frac{b + c}{\mathrm{НОД}(b, c)} \text{ – степень числа } 2, \tag{13}$$

где $\mathrm{НОД}(b, c)$ *– наибольший общий делитель.*

Обе конструкции для линейных кодов с $\rho = 1$, рассмотренные в предыдущем пункте, можно использовать также и для нелинейных кодов. Следующее утверждение обобщает соответствующие результаты [82] на нелинейные коды и результаты [84] на недвоичный случай.

Предложение 33. *Имеют место следующие утверждения*:

(i) *Для каждого $n = (q^m - 1)/(q - 1)$, $m \geqslant 2$, и любого k, $1 \leqslant k \leqslant (q - 1)n$, существует q-ичный ПР-код C с $\rho = 1$ и $\mathrm{IA} = \{(q-1)n - k + 1; k\}$, образованный k произвольными сдвигами q-ичного совершенного кода длины n с минимальным расстоянием $d = 3$;*

(ii) *Существование q-ичного ПР-кода C длины n с $\mathrm{IA} = \{b; c\}$ влечет для любого $k \geqslant 1$ существование ПР-кода C^{+k} с $\mathrm{IA} = \{b + k(q-1); c + k(q-1)\}$, образованного заменой каждого кодового слова $c \in C$ множеством из q^k кодовых слов вида $(c \,|\, x)$, где x пробегает $\mathbb{F}_q^n$;*

(iii) *Существование ПР-кода C длины n с $\mathrm{IA} = \{b; c\}$ влечет для любого $k \geqslant 1$ существование ПР-кода $C^{\times k}$ с $\mathrm{IA} = \{kb; kc\}$. Каждое кодовое слово $v = (v_1, \ldots, v_n)$ кода C заменяется на все векторы вида*

$$(v_{1,1}, v_{1,2}, \ldots, v_{1,k}, \ldots, v_{1,1}, v_{1,2}, \ldots, v_{1,k}) \in \mathbb{F}_q^{kn},$$

для которых

$$\sum_{j=1}^{k} v_{i,j} = v_i.$$

Наиболее интересны, конечно, коды, достигающие оценки (12). Такие коды длины $n = 3u$ должны иметь массив пересечений $\mathrm{IA} = \{3u - a; a + u\}$, где $a \geqslant 0$. Известны два бесконечных семейства кодов, имеющие следующие два массива пересечений (см. работы [83,85] и библиографию в них): $\{3k; k\}$ и $\{5k; 3k\}$. Эти семейства получены из начальных кодов с массивами пересечений $\{3; 1\}$ и $\{5; 3\}$ применением предложения 33. Первый начальный код – это тривиальный двоичный совершенный код длины 3, а второй – код длины 6, построенный Таранниковым в [86]. Второй код можно построить из первого, используя следующие две леммы Фон-Дер-Флааса [84].

Лемма 4 [84]. *Пусть задан ПР-код C с $\rho = 1$ и матрицей пересечений*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Предположим, что C можно представить в виде объединения непересекающихся k-граней, где $0 \leqslant k \leqslant a$. Тогда существует ПР-код с $\rho = 2$ и матрицей пересечений

$$\begin{bmatrix} a-k & a+k & 2b \\ a+k & a-k & 2b \\ c & c & 2d \end{bmatrix}.$$

Лемма 5 [84]. *Существование ПР-кода с $\rho = 2$ и матрицей пересечений*

$$\begin{bmatrix} a-k & a+k & 2b \\ a+k & a-k & 2b \\ c & c & 2d \end{bmatrix},$$

где $c \geqslant a+k$, влечет существование ПР-кода с $\rho = 1$ и матрицей пересечений

$$\begin{bmatrix} a-k & 2b+c \\ c & 2d+2c-a-k \end{bmatrix}.$$

В связи с условием делимости (13) возникает естественный вопрос [84]: *найти для всех пар b, c значение $a^*(b,c)$, удовлетворяющее условию* (13). Под величиной $a^*(b,c)$ понимается минимальное число a, для которого существует ПР-код с массивом пересечений $\mathrm{IA} = \{b; c\}$, если и только если $a \geqslant a^*(b,c)$. На эту величину $a^*(b,c)$ имеются нижние и верхние оценки (см. работу [84] и библиографию в ней). Наилучшие известные такие оценки приведены в следующих утверждениях.

Теорема 39 [84]. *Имеют место следующие утверждения*:

(i) *Если $c < b < 2c$, то*

$$a^*(b,c) \geqslant \frac{1}{2} + \sqrt{c(b-c) + \frac{1}{4}} - (b-c);$$

(ii) *Если $2c < b < 2c + \sqrt{3c-2}$, то $a^*(b,c) \geqslant 1$.*

Для заданных натуральных чисел x, y, таких что $x+y = 2^k - 1$, одно из этих чисел нечетно и содержит в своем двоичном разложении ℓ единиц подряд, где $1 \leqslant \ell < k$. Определим функцию $z(x,y) = k-1$.

Теорема 40 [84]. *Имеют место следующие утверждения*:

(i) $a^*(2b+c, c) \leqslant \max(0, a^*(b,c) - 1)$;

(ii) *Пусть b и c удовлетворяют условию* (13). *Тогда*

$$a^*(c,b) = a^*(b,c) + b - c;$$

(iii) *Пусть b и c удовлетворяют условию* (13) *и $b \geqslant c$. Пусть $m = (b,c)$, $b = m(2b'+1)$ и $c = m(2c'+1)$. Если $c' = 0$, то $a^*(b,c) = 0$. В противном случае*

$$a^*(b,c) \leqslant \max(0, c - m(z(b',c') + 1)).$$

Оптимальный двоичный ПР-код длины $n = 12$ с массивом пересечений $\mathrm{IA} = \{9; 7\}$, удовлетворяющий границе (12), был построен в [85]. Там же было доказано, что предполагаемый ПР-код длины $n = 12$ с массивом пересечений $\mathrm{IA} = \{11; 5\}$ не существует.

5.12. Линейные q-ичные ПР-коды с $\rho = 2$. Код, дуальный любому линейному коду, в котором веса ненулевых кодовых слов принимают два значения, должен быть ПР-кодом с $\rho = 2$ согласно результату Дельсарта [3] о том, что $\rho \leqslant s$ (см. теорему 3). Имеется большое число различных бесконечных семейств таких кодов, и их классификация далека от завершения (подробный обзор по этим кодам см. в [87]).

Классификация линейных ПР-кодов с радиусом покрытия $\rho = 1$ дает возможность описать структуру линейных ПР-кодов с $\rho = 2$, дуальные коды которых антиподальны.

Теорема 41 [82]. *Пусть $C = C(H)$ – нетривиальный $[n, k, d]_q$-код. Тогда C полностью регулярен с радиусом покрытия $\rho = 2$ и дуальным антиподальным кодом $C^\perp$, если и только если его проверочная матрица H имеет следующий вид с точностью до эквивалентности*:

$$H = \begin{bmatrix} 1 & \dots & 1 \\ & M & \end{bmatrix},$$

где матрица M порождает эквидистантный код E с минимальным расстоянием d', обладающий следующим дополнительным свойством: *для любого ненулевого кодового слова $v \in E$ каждый символ $\alpha \in \mathbb{F}_q$, встречающийся в его координатной позиции, встречается в этом слове ровно $n - d'$ раз. Более того, с точностью до эквивалентности код C получен расширением ПР-кода C' с радиусом покрытия $\rho' = 1$.*

Перечислим теперь известные нам ПР-коды с радиусом покрытия $\rho = 2$, дуальные коды которых антиподальны [82]. Пусть C_1 и C_2 – линейные q-ичные коды одинаковой мощности с порождающими матрицами G_1 и G_2, где q – произвольная степень простого числа. Будем говорить, что C_1 и C_2 – *дополнительные коды*, если матрица $G = [G_1 \mid G_2]$ (с точностью до перестановки строк матрицы G_2) порождает *симплексный код*, т.е. общеизвестный код с параметрами

$$n = (q^m - 1)/(q - 1), \quad k = m, \quad d = q^{m-1}$$

(дуальный коду Хэмминга $\mathcal{H}_m$).

Следствие 15 [82]. *Следующие коды, дуальные коды которых антиподальны, полностью регулярны с радиусом покрытия $\rho = 2$*:

(F.39) *Двоичный расширенный совершенный $[n, k, 4; 2]_2$-код $\mathcal{H}^*_m$ длины $n = 2^m$, где $k = n - m - 1$ и $m \geqslant 2$, с*

$$\mathrm{IA} = \{n, n-1; 1, n\};$$

(F.40) *Расширенный q-ичный совершенный $[n, k, 4; 2]_q$-код $\mathcal{H}^*_m$ длины $n = q + 2$ с $k = q - 1$, где $q = 2^r \geqslant 4$, и $m = 2$ [88, 89] (семейство* TF1 *в обзоре* [87]) *с*

$$\mathrm{IA} = \{(q+2)(q-1), q^2 - 1; 1, q+2\};$$

(F.41) *$[n, k, 3; 2]_q$-код, дуальный коду, порожденному разностной матрицей $D_m = D(n/q, q)$ (см. определение после кода* (S.23)), *с*

$$\mathrm{IA} = \{n(q-1), n-1; 1, n(q-1)\}.$$

Этот код имеет длину $n = q^m$, размерность $k = n - (m + 1)$ и проверочную матрицу D_m, где $m \geqslant 1$, а $q \geqslant 3$ – любая степень простого числа (все коды такого типа, порожденные матрицей D_m, были построены в работе [90]). *Дополнительным к приведенному коду является код Хэмминга $\mathcal{H}_m$*;

(F.42) $[n, n-2, 3; 2]_q$-*код, дуальный МДР-коду с* $k = 2$ *длины* n, *где* $3 \leqslant n \leqslant q$, $q \geqslant 3$ – *любая степень простого числа, с массивом пересечений* [89]

$$\mathrm{IA} = \{n(q-1), (q-n+1)(n-1); 1, n(n-1)\};$$

(F.43) $[n = q(q-1)/2,\ k = n-3,\ 4;\ 2]_q$-*код над алфавитом размера* $q = 2^r \geqslant 4$ [89] *с*

$$\mathrm{IA} = \{(q-1)n, (q-2)(q+1)(q+2)/4; 1, q(q-1)(q-2)/4\}.$$

Код, дополнительный к этому коду, принадлежит семейству $\mathrm{TF1}^d$, *т.е. это проективный дуальный код из семейства* TF1 *в* [87];

(F.44) $[n = 1 + (q+1)(h-1), k = n-3, 4]_q$-*код, где* $1 < h < q$ *и* h *делит* q *для* $q = 2^r \geqslant 4$ (*семейство* TF2 *в* [87]), *с*

$$\mathrm{IA} = \{(q-1)n, (q+1)(h-1)(q-h+1); 1, (h-1)n\};$$

(F.45) $[n = q(q-h+1)/h, k = n-3, 4]_q$-*код, где* $1 < h < q$ *и* h *делит* q *для* $q = 2^r \geqslant 4$, *с*

$$\mathrm{IA} = \{(q-1)n, (q+1)(q-h)(q(h-1)+h)/h^2; 1, q(q-h)(q-h+1)/h^2\}.$$

Дополнительный код принадлежит семейству $\mathrm{TF2}^d$ *в* [87].

Некоторые из этих кодов самодуальны [82].

Теорема 42 [82]. *Пусть код* $C' \subset \mathbb{F}_{q^r}^n$ *получен поднятием алфавита совершенного* $[n, n-m, 3]_q$-*кода Хэмминга. Тогда*

(F.46) *Для любого* r *код* C' *полностью регулярен. Более того,* C' *самодуален, если и только если* $\mathcal{H}_m$ – *троичный* $[4, 2, 3]_3$-*код Хэмминга.*

Теорема 43 [82]. *Пусть* $\{0, 1, \xi_2, \ldots, \xi_{q-1}\}$ – *элементы поля* $\mathbb{F}_q$, *где* $q \geqslant 4$ – *любая степень простого числа. Пусть*

$$D_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \xi_i & \xi_j \end{bmatrix}$$

представляет собой проверочную матрицу для кода C *и порождающую матрицу для дуального кода* $C^\perp$, *где* $\xi_i, \xi_j \in \mathbb{F}_q^*$ – *два разных элемента поля, таких что* $\xi_i + \xi_j + 1 = 0$. *Тогда*

(F.47) *Код* C, *так же как и код* $C^\perp$, *представляет собой линейный антиподальный полностью регулярный* $[4, 2, 3; 2]_q$-*код с*

$$\mathrm{IA} = \{4\,(q-1), 3\,(q-3); 1, 12\};$$

(F.48) *В случае* $q = 2^r \geqslant 4$ *эти два эквивалентных кода совпадают:* $C = C^\perp$, *т.е.* C *самодуален.*

Приведем еще одно семейство кодов, дуальные к которым – хорошо известные коды, имеющиеся в [87]. Пусть H_m – проверочная матрица q-ичного кода Хэмминга $\mathcal{H}_m$ длины $n = (q^m-1)/(q-1)$. Для заданной степени простого q и натуральных чисел m и $u < m$ определим код $C_{u,m}$, проверочная матрица которого получена из матрицы H_m выкидыванием всех $(q^u-1)/(q-1)$ столбцов проверочной матрицы H_u. Код $C_{u,m}$ имеет параметры

$$[n = (q^m - q^u)/(q-1), k = (q^m - q^u)/(q-1) - m, d; 2]_q,$$

где

$$d = \begin{cases} 4, & \text{если } u = m-1,\ q = 2, \\ 3 & \text{в противном случае.} \end{cases}$$

Теорема 44. *Имеет место следующее утверждение*:

(F.49) *Для любой степени простого q и любых натуральных $m > 3$ и $u < m$ код $C_{u,m}$ полностью транзитивен и полностью регулярен с радиусом покрытия $\rho = 2$ и*

$$\mathrm{IA} = \{q^m - q^u, q^u - 1; 1, q^m - q^u\}.$$

5.13. Двоичные линейные ПР-коды с $\rho = 3$ и $\rho = 4$ из булевых бент- и почти бент-функций. Пусть F – любая функция из $\mathbb{F}_2^m$ в $\mathbb{F}_2^m$. Для любых элементов $(a, b) \in (\mathbb{F}_2^m)^2$ определим преобразование Фурье функции F:

$$\mu_F(a, b) \;=\; \sum_{\boldsymbol{x} \in \mathbb{F}_2^m} (-1)^{\langle b \cdot F(x) \rangle + \langle a \cdot x \rangle}, \tag{14}$$

где $\langle \cdot \rangle$ обозначает обычное внутреннее произведение на $\mathbb{F}_2^m$.

Для четных m функция F на $\mathbb{F}_2^m$ называется *бент-функцией*, если для всех $a, b \in \mathbb{F}_2^m$ (где $b \neq 0$) ее преобразование Фурье равно $\mu_F(a, b) = \pm 2^{m/2}$. Для нечетных m функция F на $\mathbb{F}_2^m$ называется *почти бент-функцией* (АВ-функцией), если для всех $a, b \in \mathbb{F}_2^m$ (где $b \neq 0$) ее преобразование Фурье равно $\mu_F(a, b) = \pm 2^{(m-1)/2}$.

Пусть F – любая функция из $\mathbb{F}_q$ в $\mathbb{F}_q$, где $q = 2^m$, такая что $F(0) = 0$. Определим множество

$$\Omega_m = \begin{cases} \{2^{m-1}, 2^{m-1} \pm 2^{m/2}\}, & \text{если } m \text{ четно}, \\ \{2^{m-1}, 2^{m-1} \pm 2^{(m-1)/2}\}, & \text{если } m \text{ нечетно}. \end{cases}$$

Для двоичного линейного кода C определим числовое множество W_C, состоящее из всех значений весов ненулевых кодовых слов:

$$W_C = \{\mathrm{wt}(c) : \; c \in C, \; c \neq \mathbf{0}\}.$$

Для произвольной функции F определим матрицу

$$H_F = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{n-1}) \end{bmatrix}. \tag{15}$$

Следующие утверждения можно найти в работе [91].

Теорема 45 [91]. *Для заданной функции F пусть $C = C_F$ представляет собой $[n = 2^m - 1, k, d]$-код, заданный проверочной матрицей H_F вида* (15).

(i) *Если m нечетно, то F является АВ-функцией, если и только если $W_{C^\perp} = \Omega_m$;*
(ii) *Если m четно, то F является бент-функцией, если и только если $W_{C^\perp} = \Omega_m$;*
(iii) *Код C_F равномерно упакован в широком смысле, если и только если $|W_{C^\perp}| = 3$;*

(F.50) *Для четного m код C_F полностью регулярен, если F – бент-функция;*

(F.51) *Для нечетного m код C_F полностью регулярен, если F – АВ-функция.*

Используя соответствующие результаты работ [38, 39], получаем следующее

Предложение 34. *Пусть код $C = C_F$ длины $n = 2^m - 1$, где m нечетно, задан проверочной матрицей* (15)*, и пусть $C^\perp$ – дуальный к нему код с множеством значений весов $W_{C^\perp}$. Тогда*

(i) *Код C^* равномерно упакован, если и только если C равномерно упакован и $W_{C^\perp} = \Omega_m$.*
(ii) *Код C^* полностью регулярен, если и только если C полностью регулярен с минимальным расстоянием $d \in \{3, 5\}$ и код C^* равномерно упакован.*

Доказательство. Первое утверждение непосредственно следует из [33]. Для второго утверждения случай $d = 3$ известен [39]. Рассмотрим случай $d = 5$. Так как C – ПР-код, его радиус покрытия $\rho = 3$. Следовательно, C – квазисовершенный код. Теперь результат следует из предложения 4. ▲

(F.52) Выбирая теперь степенные функции F в (15) для нечетного m, получаем двоичные циклические примитивные $[n = 2^m - 1, n - 2m, d; \rho]$-коды с порождающими многочленами вида $g(x) = m_1(x)m_\ell$. Для случая $d = 5$ все такие коды полностью регулярны [90] с $\rho = 3$ и с массивом пересечений

$$\text{IA} = \{n, n-1, (n+3)/2; 1, 2, (n-1)/2\}.$$

В литературных источниках мы нашли следующие случаи:

(i) Коды БЧХ с $d = 5$ длины $n = 2^{2m+1} - 1$ [24] (см. п. 5.3), $\ell = 3$;

(ii) Коды Голда [92], $\ell = 2^t + 1$, НОД$(t, m) = 1$;

(iii) Коды Касами [93], $\ell = 2^{2t} - 2^t + 1$, НОД$(t, m) = 1$;

(iv) Коды Велча [94] (см. также [95, 96]), $\ell = 2^{\frac{m-1}{2}} + 3$;

(v) Коды Нихо [97]:

$$\ell = \begin{cases} 2^t + 2^{t/2} - 1, & \text{если } t \text{ четно}, \\ 2^t + 2^{(3t+1)/2} - 1, & \text{если } t \text{ нечетно}; \end{cases}$$

(vi) Инверсные коды [98], $\ell = 2^{2t} - 1$, $m = 2t + 1$;

(vii) Коды Доббертина [99], $\ell = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$, $m = 5t$.

Существование всех указанных выше кодов вытекает из существования известных AB-функций. Некоторые новые AB-функции (которые также приводят к новым ПР-кодам), не являющиеся степенными функциями, могут быть найдены, например, в работах [100–102]. Вопрос о полной транзитивности указанных кодов требует дополнительного внимания.

(F.53) Коды, полученные расширением всех выше указанных двоичных кодов, также являются полностью регулярными кодами с радиусом покрытия $\rho = 4$ и массивом пересечений

$$\text{IA} = \{n+1, n, n-1, (n+3)/2; 1, 2, (n-1)/2, n+1\}.$$

5.14. Новые РУ-код длины 11 и ПР-код длины 33. В [24] в результате компьютерного поиска РУ-кодов были найдены следующие параметры возможного семейства 4-ичных РУ-кодов:

$$q = 4, \quad n = \frac{2^{2m+1}+1}{3}, \quad k = n - 2m - 1, \quad d = 5, \quad \mu = \lambda + 1 = \frac{2^{2m}-1}{3},$$
$$m = 2, 3, \ldots$$

Линейные коды над $\mathbb{F}_4$ с такими параметрами (которые оказались не равномерно упакованными) были построены в [103]. Позднее был построен нелинейный аддитивный 4-ичный код над $\mathbb{F}_4$ с параметрами $(12, 4^6, 6)_4$, называемый *додекакодом* (см. ссылку в [104]). Удаление любой позиции этого кода дает $(11, 4^6, 5)_4$-код, который оказался равномерно упакованным, что отвечает на вопрос, поставленный еще в [24]. Следуя [104], опишем конструкцию этого кода:

(S.26) Удалим одну позицию додекакода. Пусть G – порождающая матрица результирующего кода длины 11, и пусть α – примитивный элемент $\mathbb{F}_4$. Из матрицы G построим теперь двоичную матрицу H, заменяя каждый элемент поля $\mathbb{F}_4$ одним

из двух двоичных векторов длины 3 следующим образом:

$$\begin{aligned} 0 &\to 000 \text{ или } 111,\\ 1 &\to 100 \text{ или } 011,\\ \alpha &\to 001 \text{ или } 110,\\ \alpha^2 &\to 010 \text{ или } 101. \end{aligned}$$

Это означает, что из каждой строки матрицы G мы получаем 2^{11} слов в матрице H. Таким образом, H порождает двоичный линейный $[33, 23, 3; 3]$-код, являющийся полностью регулярным (но не полностью транзитивным) с

$$\mathrm{IA} := \{33, 30, 15; 1, 2, 15\}.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Shapiro H.S., Slotnick D.L.* On the Mathematical Theory of Error Correcting Codes // IBM J. Res. Dev. 1959. V. 3. № 1. P. 25–34.
2. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Равномерно упакованные коды // Пробл. передачи информ. 1971. Т. 7. № 1. С. 38–50.
3. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory // Philips Res. Rep. Suppl. 1973. № 10.
4. *Goethals J.-M., van Tilborg H.C.A.* Uniformly Packed Codes // Philips Res. Rep. 1975. V. 30. P. 9–36.
5. *van Tilborg H. C. A.* Uniformly Packed Codes. PhD Thesis. Technische Hogeschool Eindhoven, Nederland, 1976.
6. *Solé P.* Completely Regular Codes and Completely Transitive Codes // Discrete Math. 1990. V. 81. № 2. P. 193–201.
7. *Giudici M.* Completely Transitive Codes in Hamming Graphs. PhD Thesis. Univ. of Western Australia, Perth, Australia, 1998.
8. *Giudici M., Praeger C.E.* Completely Transitive Codes in Hamming Graphs // European J. Combin. 1999. V. 20. № 7. P. 647–662.
9. *Gillespie N.I., Praeger C.E.* New Characterisations of the Nordstrom–Robinson Codes // Bull. London Math. Soc. 2017. V. 49. № 2. P. 320–330.
10. *Brouwer A.E., Cohen A.M., Neumaier A.* Distance-Regular Graphs. Berlin: Springer-Verlag, 1989.
11. *van Dam E.R., Koolen J.H., Tanaka H.* Distance-Regular Graphs // Electron. J. Combin. 2016. DS22, Dynamic Survey, 156 pp.
12. *Koolen J., Krotov D., Martin B.* Completely Regular Codes. 2016. Available at `https://sites.google.com/site/completelyregularcodes`.
13. *Koolen J.H., Lee W.S., Martin W.J., Tanaka H.* Arithmetic Completely Regular Codes // Discrete Math. Theor. Comput. Sci. 2016. V. 17. № 3. P. 59–76.
14. *Tietäväinen A.* On the Nonexistence of Perfect Codes over Finite Fields // SIAM J. Appl. Math. 1973. V. 24. № 1. P. 88–96.
15. *Зиновьев В.А., Леонтьев В.К.* Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Вып. 2. С. 123–132.
16. *Borges J., Rifà J.* On the Nonexistence of Completely Transitive Codes // IEEE Trans. Inform. Theory. 2000. V. 46. № 1. P. 279–280.
17. *Borges J., Rifà J., Zinoviev V.* Nonexistence of Completely Transitive Codes with Error-Correcting Capability $e > 3$ // IEEE Trans. Inform. Theory. 2001. V. 47. № 4. P. 1619–1621.
18. *Neumaier A.* Completely Regular Codes // Discrete Math. 1992. V. 106/107. P. 353–360.
19. *Borges J., Rifà J., Zinoviev V.A.* On Non-antipodal Binary Completely Regular Codes // Discrete Math. 2008. V. 308. № 16. P. 3508–3525.
20. *Avgustinovich S.V., Krotov D.S., Vasil'eva A.Yu.* Completely Regular Codes in the Infinite Hexagonal Grid // Сиб. электрон. матем. изв. 2016. Т. 13. С. 987–1016.

21. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
22. *Brouwer A.E.* A Note on Completely Regular Codes // Discrete Math. 1990. V. 83. № 1. P. 115–117.
23. *Lindström K.* All Nearly Perfect Codes Are Known // Inform. Control. 1977. V. 35. № 1. P. 40–47.
24. *Бассалыго Л.А., Зайцев Г.В., Зиновьев В.А.* О равномерно упакованных кодах // Пробл. передачи информ. 1974. Т. 10. № 1. С. 9–14.
25. *Beth T., Jungnickel D., Lenz H.*, Design Theory. Cambridge: Cambridge Univ. Press, 1999.
26. *Blake I.F., Mullin R.C.* The Mathematical Theory of Coding. New York: Academic Press, 1975.
27. *Hughes D.R., Piper F.C.* Design Theory. Cabmridge: Cambridge Univ. Press, 1985.
28. Handbook of Combinatorial Designs. Boca Raton: Chapman & Hall, 2007.
29. *Magliveras S.S., Leavitt D.W.* Simple Six Designs Exist // Congr. Numer. 1983. V. 40. P. 195–205.
30. *Teirlinck L.* Non-trivial t-Designs without Repeated Blocks Exist for All t // Discrete Math. 1987. V. 65. № 3. P. 301–311.
31. *Assmus E.F., Jr., Goethals J.-M., Mattson H.F., Jr.* Generalized t-Designs and Majority Decoding of Linear Codes // Inform. Control. 1976. V. 32. № 1. P. 43–60.
32. *Зиновьев В.А., Рифа Д.* О новых полностью регулярных q-ичных кодах // Пробл. передачи информ. 2007. Т. 43. № 2. С. 34–51.
33. *Бассалыго Л.А., Зиновьев В.А.* Замечание о равномерно упакованных кодах // Пробл. передачи информ. 1977. Т. 13. № 3. С. 22–25.
34. *Rifà J., Zinoviev V.A.* New Completely Regular q-ary Codes Based on Kronecker Products // IEEE Trans. Inform. Theory. 2011. V. 56. № 1. P. 266–272.
35. *Rifà J., Zinoviev V.A.* On Lifting Perfect Codes // IEEE Trans. Inform. Theory. 2011. V. 57. № 9. P. 5918–5925.
36. *Rifà J., Zinoviev V.A.* On a Family of Binary Completely Transitive Codes with Growing Covering Radius // Discrete Math. 2014. V. 318. P. 48–52.
37. *Gillespie N.I., Praeger C.E.* Uniqueness of Certain Completely Regular Hadamard Codes // J. Combin. Theory Ser. A. 2013. V. 120. № 7. P. 1394–1400.
38. *Borges J., Rifà J., Zinoviev V.A.* New Families of Completely Regular Codes and Their Corresponding Distance Regular Coset Graphs // Des. Codes Cryptogr. 2014. V. 70. № 1–2. P. 139–148.
39. *Borges J., Rifà J., Zinoviev V.A.* Families of Nested Completely Regular Codes and Distance-Regular Graphs // Adv. Math. Commun. 2015. V. 9. № 2. P. 233–246.
40. *Calderbank A.R., Goethals J.-M.* Three-Weight Codes and Association Schemes // Philips J. Res. 1984. V. 39. № 4–5. P. 143–152.
41. *Calderbank A.R., Goethals J.-M.* On a Pair of Dual Subschemes of the Hamming Scheme $H_n(q)$ // European J. Combin. 1985. V. 6. № 2. P. 133–147.
42. *Baker R.D., van Lint J.H., Wilson R.M.* On the Preparata and Goethals Codes // IEEE Trans. Inform. Theory. 1983. V. 29. № 3. P. 342–345.
43. *Зайцев Г.В., Зиновьев В.А., Семаков Н.В.* О двойственности нелинейных кодов Препараты и Кердока // Тр. V конф. по теории кодирования и передачи информации. Ч. 2. Тез. докл. Москва–Горький, 1972. С. 55–58.
44. *Camion P., Courteau B., Delsarte P.* On r-Partition Designs in Hamming Spaces // Appl. Algebra Engrg. Commun. Comput. 1992. V. 2. № 3. P. 147–162.
45. *Brouwer A.E.* On Complete Regularity of Extended Codes // Discrete Math. 1993. V. 117. № 1–3. P. 271–273.
46. *Rifà J., Pujol J.* Completely Transitive Codes and Distance Transitive Graphs // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Proc. 9th Int. Sympos. AAECC-9. New Orleans, LA, USA. October 7–11, 1991). Lect. Notes Comp. Sci. V. 539. Berlin: Springer, 1991. P. 360–367.

47. *Livingstone D., Wagner A.* Transitivity of Finite Permutation Groups on Unordered Sets // Math. Z. 1965. V. 90. № 5. P. 393–403.
48. *Berger T.P.* The Automorphism Group of Double-Error-Correcting BCH Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 538–542.
49. *Godsil C.D., Praeger C.E.* Completely Transitive Designs // `arXiv:1405.2176 [math.CO]`, 2014.
50. *Bannai E.* Codes in Bipartite Distance-Regular Graphs // J. London Math. Soc. (2). 1977. V. 16. № 2. P. 197–202.
51. *Hammond P.* On the Non-existence of Perfect and Nearly Perfect Codes // Discrete Math. 1982. V. 39. № 1. P. 105–109.
52. *Etzion T.* On the Nonexistence of Perfect Codes in the Johnson Scheme // SIAM J. Discrete Math. 1996. V. 9. № 2. P. 201–209.
53. *Etzion T., Schwarz M.* Perfect Constant-Weight Codes // IEEE Trans. Inform. Theory. 2004. V. 50. № 9. P. 2156–2165.
54. *Etzion T.* Configuration Distribution and Designs of Codes in the Johnson Scheme // J. Combin. Des. 2007. V. 15. № 1. P. 15–34.
55. *Shimabukuro O.* On the Nonexistence of Perfect Codes in $J(2w + p^2, w)$ // Ars Combin. 2005. V. 75. P. 129–134.
56. *Gordon D.M.* Perfect Single Error-Correcting Codes in the Johnson Scheme // IEEE Trans. Inform. Theory. 2006. V. 52. № 10. P. 4670–4672.
57. *Kummer E.E.* Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen // J. Reine Angew. Math. 1852. V. 44. P. 93–146.
58. *Loxton J.H.* Some Problems Involving Powers of Integers // Acta Arith. 1986. V. 46. № 2. P. 113–123.
59. *Bernstein D.J.* Detecting Perfect Powers in Essentially Linear Time // Math. Comp. 1998. V. 67. № 223. P. 1253–1283.
60. *Roos C.* A Note on the Existence of Perfect Constant Weight Codes // Discrete Math. 1983. V. 47. № 1. P. 121–123.
61. *Мовсисян Г.Л.* Совершенные коды в схемах Джонсона // Вестн. Моск. ун-та. Сер. 15. Вычисл. Матем. Киберн. 1982. № 1. С. 64–69.
62. *Мовсисян Г.Л.* Совершенные равновесные коды и системы Штейнера // Пробл. передачи информ. 1983. Т. 19. № 2. С. 109–112.
63. *Movsisian G.L., Margarian Zh.G.* D-Representing Code Problem Solution // Fundamentals of Computation Theory (Proc. Int. Conf. FCT'87. Kazan, USSR. June 22–26, 1987). Lect. Notes Comp. Sci. V. 278. Berlin: Springer, 1987. P. 328–331.
64. *Leont'ev V.K., Movsisyan G.L., Margaryan Zh.G.* Constant Weight Perfect and D-Representable Codes // Уч. записки ЕГУ. Сер. Физика и Математика. 2012. № 1. С. 16–19.
65. *Могильных И.Ю.* О регулярности совершенных раскрасок графов Джонсона в два цвета // Пробл. передачи информ. 2007. Т. 43. № 4. С. 37–44.
66. *Могильных И.Ю.* О несуществовании некоторых совершенных 2-раскрасок графов Джонсона // Дискретн. анализ и исслед. опер. 2009. Т. 16. № 5. С. 52–68.
67. *Августинович С.В., Могильных И.Ю.* Совершенные раскраски графов Джонсона $J(8, 3)$ и $J(8, 4)$ в два цвета // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 2. С. 3–19.
68. *Martin W.J.* Completely Regular Designs of Strength One // J. Algebraic Combin. 1994. V. 3. № 2. P. 177–185.
69. *Martin W.J.* Completely Regular Designs // J. Combin. Des. 1998. V. 6. № 4. P. 261–273.
70. *Meyerowitz A. D.* Cycle-Balance Conditions for Distance-Regular Graphs // Discrete Math. 2003. V. 264. № 1–3. P. 149–165.
71. *Godsil C.* Частное сообщение У.Дж. Мартину [69].
72. *Avgustinovich S.V., Mogilnykh I.Yu.* Induced Perfect Colorings // Сиб. электрон. матем. изв. 2011. Т. 8. С. 310–316.

73. *Delorme C.* Régularité métrique forte // Rapport de Recherche № 156, Univ. Paris Sud. Orsay, France, 1983.
74. *Godsil C.* Association Schemes. Univ. of Waterloo, Canada, 2005. Available at `https://www.math.uwaterloo.ca/~cgodsil/pdfs/assoc2.pdf`.
75. *Godsil C.D.* Equitable Partitions // Combinatorics, Paul Erdős is Eighty. V. 1. Budapest: János Bolyai Math. Soc., 1993. P. 173–192.
76. *Rifà J., Zinoviev V.A.* On Completely Regular Codes from Perfect Codes // Proc. 10th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-10). Zvenigorod, Russia. September 3–9, 2006. P. 225–229.
77. *Ivanov A.A., Liebler R.A., Penttila T., Praeger C.E.* Antipodal Distance-Transitive Covers of Complete Bipartite Graphs // European J. Combin. 1997. V. 18. № 1. P. 11–33.
78. *Rifà J., Zinoviev V.A.* Completely Regular Codes with Different Parameters Giving the Same Distance-Regular Coset Graphs // Discrete Math. 2017. V. 340. № 7. P. 1649–1656.
79. *Rifà J., Zinoviev V.A.* On a Class of Binary Linear Completely Transitive Codes with Arbitrary Covering Radius // Discrete Math. 2009. V. 309. № 16. P. 5011–5016.
80. *Borges J., Rifà J., Zinoviev V.* Completely Regular Codes by Concatenating Hamming Codes // Adv. Math. Commun. 2018. V. 12. № 2. P. 337–349.
81. *Borges J., Rifà J., Zinoviev V.* On New Infinite Families of Completely Regular and Completely Transitive Binary Codes // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-16). Svetlogorsk, Russia. September 2–9, 2018. P. 7–8.
82. *Borges J., Rifà J., Zinoviev V.A.* On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal Dual // Adv. Math. Commun. 2010. V. 4. № 4. P. 567–578.
83. *Fon-Der-Flaass D.G.* A Bound on Correlation Immunity // Сиб. электрон. матем. изв. 2007. Т. 4. С. 133–135.
84. *Фон-Дер-Флаас Д.Г.* Совершенные 2-раскраски гиперкуба // Сиб. матем. журн. 2007. Т. 48. № 4. С. 923–930.
85. *Фон-Дер-Флаас Д.Г.* Совершенные 2-раскраски 12-мерного гиперкуба, достигающие границы корреляционной иммунности // Сиб. электрон. матем. изв. 2007. Т. 4. С. 292–295.
86. *Tarannikov Y.V.* On Resilient Boolean Functions with Maximal Possible Nonlinearity // Progress in Cryptology – INDOCRYPT 2000 (Proc. 1st Int. Conf. in Cryptology in India. Calcutta, India. December 10–13, 2000). Lect. Notes Comp. Sci. V. 1977. Berlin: Springer-Verlag, 2000. P. 19–30.
87. *Calderbank R., Kantor W.M.* The Geometry of Two-Weight Codes // Bull. London Math. Soc. 1986. V. 18. № 2. P. 97–122.
88. *Bush K.A.* Orthogonal Arrays of Index Unity // Ann. Math. Statist. 1952. V. 23. № 3. P. 426–434.
89. *Delsarte P.* Two-Weight Linear Codes and Strongly Regular Graphs // MBLE Research Lab. Report R160. Brussels, Belgium, 1971.
90. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87.
91. *Carlet C., Charpin P., Zinoviev V.* Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems // Des. Codes Cryptogr. 1998. V. 15. № 2. P. 125–156.
92. *Gold R.* Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions // IEEE Trans. Inform. Theory. 1968. V. 14. № 1. P. 154–156.
93. *Kasami T.* The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed–Muller Codes // Inform. Control. 1971. V. 18. № 4. P. 369–394.
94. *Welch L.R.* Trace Mappings in Finite Fields and Shift Register Cross-Correlation Properties // Dept. Electrical Engineering Report. Univ. of Southern California, Los Angeles, 1969.
95. *Canteaut A., Charpin P., Dobbertin H.* Binary m-Sequences with Three-Valued Crosscorrelation: A Proof of Welch's Conjecture // IEEE Trans. Inform. Theory. 2000. V. 46. № 1. P. 4–8.

96. *Hollmann H.D.L., Xiang Q.* A Proof of the Welch and Niho Conjectures on Cross-Correlations of Binary m-Sequences // Finite Fields Appl. 2001. V. 7. № 2. P. 253–286.
97. *Dobbertin H.* Almost Perfect Nonlinear Power Functions over GF(2^n): The Niho Case // Inform. and Comput. 1999. V. 151. № 1–2. P. 57–72.
98. *Beth T., Ding C.* On Almost Perfect Nonlinear Permutations // Advances in Cryptology – EUROCRYPT'93 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Lofthus, Norway. May 23–27, 1993). Lect. Notes Comp. Sci. V. 765. Berlin: Springer-Verlag, 1994. P. 65–76.
99. *Dobbertin H.* Almost Perfect Nonlinear Power Functions on GF(2^n): A New Case for n Divisible by 5 // Finite Fields and Applications. Berlin: Springer, 2001. P. 113–121.
100. *Budaghyan L., Carlet C., Pott A.* New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials // IEEE Trans. Inform. Theory. 2006. V. 52. № 3. P. 1141–1152.
101. *Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy Y.* On Almost Perfect Nonlinear Functions over $\boldsymbol{F}_2^n$ // IEEE Trans. Inform. Theory. 2006. V. 52. № 9. P. 4160–4170.
102. *Carlet C.* Boolean Functions for Cryptography and Error-Correcting Codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge Univ. Press, 2010. Ch. 8. P. 257–397.
103. *Думер И.И., Зиновьев В.А.* Некоторые новые максимальные коды над полем Галуа $GF(4)$ // Пробл. передачи информ. 1978. Т. 14. № 3. С. 24–34.
104. *Shi M., Krotov D.S., Solé P.* A New Distance-Regular Graph of Diameter 3 on 1024 Vertices // `arXiv:1806.07069v3 [math.CO]`, 2018.

Боржес Жуаким
Рифа Жузеп
Школа инженерии, отделение информационной
и телекоммуникационной инженерии,
Независимый университет Барселоны, Испания
`joaquim.borges@uab.cat`
`josep.rifa@uab.cat`
Зиновьев Виктор Александрович
Институт проблем передачи информации
им. А.А. Харкевича РАН
`zinov@iitp.ru`

Поступила в редакцию
22.12.2018
После доработки
06.02.2019
Принята к публикации
11.02.2019