ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.725

© 2022 г. **М. Вильянуэва[1], В.А. Зиновьев[2], Д.В. Зиновьев[2]**

ОБ ОДНОМ МЕТОДЕ ПОСТРОЕНИЯ МАТРИЦ АДАМАРА

Используя каскадную конструкцию q-ичных кодов, построены коды над $\mathbb{Z}_q$ в метрике Ли, которые после отображения в двоичный алфавит (которое в случае алфавита $\mathbb{Z}_4$ является отображением Грея) становятся кодами Адамара, в частности, матрицами Адамара. Наша конструкция позволяет увеличить ранг и размерность ядра получаемого таким образом кода Адамара. С помощью компьютера построены новые неэквивалентные матрицы Адамара порядка 32, 48 и 64 с разными фиксированными значениями их рангов и размерности ядер из диапазонов возможных значений. Оказалось, что в специальном случае наша конструкция совпадает с кронекеровской (или конструкцией Сильвестра) и может считаться вариантом известной в настоящее время [1] модифицированной конструкции Сильвестра, которая использует одну матрицу Адамара порядка m и m (не обязательно различных) матриц Адамара порядка k. Мы обобщаем здесь эту модифицированную конструкцию, предложив новую более общую конструкцию типа Сильвестра, основанную уже на двух семействах (не обязательно различных) матриц Адамара, а именно на k матрицах порядка m и m матрицах порядка k. Получающаяся матрица Адамара имеет порядок mk, как и в конструкции в [1].

Ключевые слова: матрица Адамара, код Адамара, обобщенная каскадная конструкция, код в метрике Ли, кронекеровское произведение, конструкция Сильвестра, ранг матрицы Адамара, размерность ядра матрицы Адамара, неэквивалентные матрицы Адамара.

DOI: 10.31857/S0555292322040039, **EDN:** EBOXEM

§ 1. Введение

Пусть $E_q = \{0, 1, \ldots, q-1\}$ – алфавит размера q. Произвольное подмножество $C \subseteq E_q^n$ называется q-ичным кодом и обозначается через $(n, N, d)_q$, где n – *длина* кода, N – число его кодовых слов (или *мощность*), и d – его *минимальное расстояние* (*Хэмминга*), т.е.

$$d = d(C) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y},\ \boldsymbol{x}, \boldsymbol{y} \in C\},$$

где для $\boldsymbol{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, \ldots, y_n)$ из множества E^n

$$d(\boldsymbol{x}, \boldsymbol{y}) = |\{j : x_j \neq y_j,\ j = 1, \ldots, n\}|.$$

[1] Работа выполнена при поддержке Национального гранта правительства Испании PID2019-104664GB-I00 (AEI, 10.13039/501100011033).

[2] Исследования были выполнены в ИППИ им. А.А. Харкевича РАН в рамках проводимых фундаментальных исследований по теме “Математические теории корректирующих кодов”, а также поддержаны грантом Национального научного фонда Болгарии (номер проекта 20-51-18002).

Для случая, когда q – степень простого числа, а E – конечное поле порядка q, обозначаемое через $\mathbb{F}_q$, q-ичный $(n, N = q^k, d)_q$-код C является линейным пространством размерности k над $\mathbb{F}_q$, и для него используется стандартное обозначение $[n, k, d]_q$.

Для двоичных кодов принято обозначение (n, N, d) и $[n, k, d]$ (т.е. q опускается).

Расстоянием Ли $d_L(i, j)$ между символами i и j из E называется минимальная разность между этими символами по модулю q:

$$d_L(i, j) = \min\big\{|j - i|, q - |j - i|\big\}.$$

Это расстояние симметрично, т.е. $d_L(i, j) = d_L(j, i)$, и продолжается на векторы $\boldsymbol{x}$ и $\boldsymbol{y}$ из E^n стандартным образом:

$$d_L(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} d_L(x_i, y_i).$$

Минимальное расстояние q-ичного кода $\mathcal{C}$ в метрике Ли определяется как

$$d_L = \min\{d_L(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x} \neq \boldsymbol{y},\ \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}\}.$$

В случае, когда E – кольцо $\mathbb{Z}_q$, назовем q-ичный код $\mathbb{Z}_q$-*аддитивным*, или $\mathbb{Z}_q$-*линейным*, если он при этом является подгруппой группы $E^n = \mathbb{Z}_q^n$. В противном случае будем называть его нелинейным $\mathbb{Z}_q$-кодом, либо просто $\mathbb{Z}_q$-кодом.

Заметим, что в случае, когда $q = 2$, $\mathbb{Z}_q$-аддитивный код является линейным двоичным кодом, а в случае $q = 4$ – линейным четверичным или линейным $\mathbb{Z}_4$-кодом. В этой статье мы рассматриваем алфавит $E = \mathbb{Z}_q$.

Произвольный, не обязательно линейный, $\mathbb{Z}_q$-код можно рассматривать как двоичный код, получаемый с помощью отображения Грея. В работе [2] отображение Грея из $\mathbb{Z}_4$ на $\mathbb{Z}_2^2$ определено как

$$\varphi(0) = (0, 0), \quad \varphi(1) = (0, 1), \quad \varphi(2) = (1, 1), \quad \varphi(3) = (1, 0).$$

Существуют различные обобщения отображения Грея, действующие из $\mathbb{Z}_{2^s}$ в пространство $\mathbb{Z}_2^{2^{s-1}}$ (см. [3–6]). В работе Карле [3] отображение

$$\varphi\colon \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$$

определено как

$$\varphi(u) = (u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-2})Y, \tag{1}$$

где $u \in \mathbb{Z}_{2^s}$, $[u_0, u_1, \ldots, u_{s-1}]_2$ – двоичное представление числа u, т.е.

$$u = \sum_{i=0}^{s-1} 2^i u_i, \quad u_i \in \{0, 1\},$$

а Y – матрица размера $(s-1) \times 2^{s-1}$, столбцами которой являются элементы $\mathbb{Z}_2^{s-1}$. Заметим, что $(u_{s-1}, \ldots, u_{s-1})$ и $(u_0, \ldots, u_{s-2})Y$ являются двоичными векторами длины 2^{s-1} и что строки матрицы Y вместе со строкой, состоящей из одних единиц, образуют базис кода Рида – Маллера первого порядка.

В работе [7] показано, что обобщение Карле является специальным случаем обобщения, рассмотренного в работе [6], для которого имеет место равенство

$$\sum_{i=0}^{s-1} \lambda_i \varphi(2^i) = \varphi\Big(\sum_{i=0}^{s-1} \lambda_i 2^i\Big), \quad \lambda_i \in \{0, 1\}.$$

Далее, доопределим отображение для векторов

$$\Phi\colon \mathbb{Z}_{2^s}^n \to \mathbb{Z}_2^{n2^{s-1}}$$

как покомпонентное отображение Грея φ. В этой статье мы используем новое отображение Грея, являющееся обобщением отображения Грея, рассмотренного в [6]. Новое отображение Грея определено на словах, являющихся строками матриц Адамара, для любого натурального числа q, такого что существует матрица Адамара порядка $q/2$.

Помимо фундаментальных кодовых параметров, двумя другими важными параметрами произвольных двоичных кодов являются *ранг* и *размерность ядра* кода. Рангом двоичного кода C является размерность его линейной оболочки $\langle C\rangle$. Ядро двоичного кода C длины n, введенное в [8] и обозначаемое через $\ker(C)$, образовано векторами, стабилизирующими код C:

$$\ker(C) = \{\boldsymbol{x} \in \mathbb{Z}_2^n : \boldsymbol{x} + C = C\}. \tag{2}$$

Если код C содержит нулевой вектор, т.е. вектор из одних нулей, то $\ker(C)$ является линейным подкодом C. Заметим, что если код C линейный, то $\ker(C) = C = \langle C\rangle$. Обозначим ранг двоичного кода C через $\mathrm{rank}(C)$, а размерность ядра – через $\dim(\ker(C))$.

Для кодов, содержащих нулевой вектор, ранг и размерность ядра могут быть использованы как достаточное условие неэквивалентности этих кодов, так как очевидно, что эквивалентные коды имеют одинаковый ранг и размерность ядра.

Матрица Адамара H порядка n – это квадратная матрица размера $n \times n$, состоящая из элементов $+1$ и -1, такая что выполнено условие $HH^T = nI$, где I – (двоичная) диагональная матрица размера $n \times n$, а H^T – транспонированная матрица H. Как известно [9], матрица Адамара H порядка n существует для n, равных 1, 2, либо кратных 4. Две матрицы Адамара эквивалентны, если одна переводится в другую перестановкой строк и/или столбцов и умножением строк и/или столбцов на строку/столбец, состоящий из одних элементов -1.

Поэтому всегда можно считать, что первая строка и первый столбец матрицы H состоят из элементов $+1$, получая таким образом эквивалентную матрицу, которую будем называть *нормализованной*. Если заменить $+1$ на 0, а -1 на 1, и добавить дополнительные строки (т.е. полученные заменой нулей на единицы и, наоборот, единиц на нули), то получим двоичный $(n, 2n, n/2)$-код, который будем называть (двоичным) кодом Адамара и обозначать через H_n (см. [9]). Мы всегда предполагаем, что матрица Адамара нормализована, и таким образом, соответствующий код Адамара содержит нулевое слово.

Пусть H – матрица Адамара порядка n. Обозначим через j_m столбец длины m, состоящий из одних единиц. Применяя перестановки строк и столбцов и умножая столбцы и строки матрицы H на -1, любые четыре столбца матрицы H можно (единственным образом) привести к следующему виду:

$$\begin{bmatrix}
j_a & j_a & j_a & j_a \\
j_a & j_a & -j_a & -j_a \\
j_a & -j_a & j_a & -j_a \\
j_a & -j_a & -j_a & j_a \\
j_b & j_b & j_b & -j_b \\
j_b & j_b & -j_b & j_b \\
j_b & -j_b & j_b & j_b \\
j_b & -j_b & -j_b & -j_b
\end{bmatrix}$$

Таблица 1

Число матриц Адамара различных типов порядка $n \leqslant 32$

Тип	Порядок							
	4	8	12	16	20	24	28	32
0	1	1	0	5	0	58	0	13680757
1	0	0	1	0	3	1	486	26369
2	0	0	0	0	0	1	1	2900
3	0	0	0	0	0	0	0	1

Таблица 2

Размерность ядра и ранг кода Адамара длины $n = 32$

$\dim(\ker(C))$	$\operatorname{rank}(C)$										
	6	7	8	9	10	11	12	13	14	15	16
6	$*$										
4		$*$									
3		$*$	$*$	$*$	$*$						
2			$\circ$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$	$\diamond$
1			$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$	$\circ$

для некоторых натуральных чисел a, b, таких что $a + b = n/4$ и $0 \leqslant b \leqslant \lfloor n/8 \rfloor$. Следуя [10], будем говорить, что произвольный набор из четырех столбцов, который может быть приведен к такому виду, имеет тип b. Очевидно, что перестановки и смены знака строк и столбцов подматрицы из четырех столбцов не меняют тип. Матрица Адамара имеет тип b (где $0 \leqslant b \leqslant \lfloor n/8 \rfloor$), если у нее имеется набор из четырех столбцов типа b и нет набора из четырех столбцов типа, меньшего чем b.

Все матрицы Адамара порядка $n \leqslant 32$ классифицированы согласно своему типу. В частности, пользуясь соответствующей таблицей работы [11] и результатами для $n = 32$ из работ [11, 12], получается классификация, приведенная в табл. 1.

Заметим, что линейные коды Адамара являются кодами Рида – Маллера первого порядка, или, что эквивалентно, кодами, дуальными к расширенным кодам Хэмминга.

$\mathbb{Z}_{2^s}$-аддитивный код (т.е. код над $\mathbb{Z}_{2^s}$), образ которого под действием отображения Грея Φ является кодом Адамара, будем называть $\mathbb{Z}_{2^s}$-аддитивным кодом Адамара, а его образ под действием Φ будем называть $\mathbb{Z}_{2^s}$-линейным кодом Адамара. В работах [7, 13, 14] рассматривалось отображение Φ Карле [3] и изучались ранг, размерность ядра и эквивалентность $\mathbb{Z}_{2^s}$-линейных кодов Адамара. В работах [15, 16] приведены оценки на возможные значения ранга и размерности ядра кодов Адамара. Кроме того, приведены конструкции кодов Адамара для различных рангов и размерностей ядер. В частности, в работе [15] показано, что в дополнение к линейным кодам Адамара существует код Адамара длины $n = 2^t$, $t > 4$, с размерностью ядра k и рангом r для всех значений r, таких что

$$\begin{cases} t + 2 \leqslant r \leqslant 2^{t+1-k} + k - 1, & \text{если } 3 \leqslant k \leqslant t - 1, \\ t + 3 \leqslant r \leqslant 2^{t-1}, & \text{если } 1 \leqslant k \leqslant 2. \end{cases} \tag{3}$$

Например, в табл. 2 и 3 приведены все возможные значения этих параметров r и k (помеченные символами $*$, $\diamond$ и $\circ$, значение которых объясняется в § 4) для случаев $t = 5$ и $t = 6$ соответственно. В случае $t = 4$ существуют ровно пять неэквивалентных кодов Адамара [9, с. 266]. Один из них – линейный код Адамара с рангом и размерностью ядра, равными 5, и по одному коду Адамара для каждого из значений параметров $(r, k) \in \{(6, 3), (7, 2), (8, 2), (8, 1)\}$.

Таблица 3

Размерность ядра и ранг кода Адамара длины $n = 64$

$\dim(\ker(C))$	$\operatorname{rank}(C)$													
	7	8	9	10	11	12	13	...	17	18	19	20	...	32
7	*													
5		*												
4		*	*	*	○									
3		○	*	*	*	*	*	...	*	○				
2			◇	◇	◇	◇	◇	...	◇	◇	◇	◇	...	◇
1			◇	◇	◇	◇	◇	...	◇	◇	◇	◇	...	◇

Таблица 4

Размерность ядра и ранг кода Адамара длины $n = 48$

$\dim(\ker(C))$	$\operatorname{rank}(C)$					
	13	14	15	16	...	24
3	*	○				
2	◇	◇	◇	◇	...	◇
1	*	*	○	○	...	○

В [16] доказано существование кодов Адамара длины $n = 2^t \cdot s$ ($s \neq 1$ нечетное) ранга r и размерности ядра k для всех $r \in \{4s + t - 3, \ldots, n/2\}$ и $k \in \{1, \ldots, t - 1\}$ при условии существования кода Адамара длины $4s$. Кроме того, там же доказано, что существование кода Адамара длины $4s$, где $s \neq 1$ – нечетное число, влечет существование кода Адамара длины $n = 2^t s$ ($t \geqslant 3$) с размерностью ядра k и рангом r для всех значений r, таких что

$$4s + t - 3 \leqslant r \leqslant \begin{cases} 2^{t+1-k}s + k - 1, & \text{если } 3 \leqslant k \leqslant t - 1, \\ 2^{t-1}s, & \text{если } 1 \leqslant k \leqslant 2. \end{cases} \tag{4}$$

Например, для длины $n = 48$ в табл. 4 приведены все возможные значения для ранга и размерности ядра (помеченные символами $*$, $\diamond$ и $\circ$, значение которых объясняется в § 4). Нахождение точной нижней границы для ранга является открытой проблемой. Однако для случая, когда размерность ядра равна $t-1$ или $t-2$, точная нижняя оценка равна $4s + t - 3$. В работе [16] установлено, что для того чтобы доказать точность этой нижней границы, достаточно показать несуществование кодов Адамара с $k = 1$ и $r < 4s + t - 3$. Наименьшая длина, для которой это неизвестно, – это $n = 48$, где $k = 1$ и $r < 13$.

Цель настоящей статьи – описать новую общую конструкцию двоичных кодов (или матриц) Адамара, которые могут быть представлены как $\mathbb{Z}_q$-коды. Построение основано на обобщенной каскадной конструкции и на результатах и идеях работ [17–19]. Для случая $q = 4$ наша конструкция дает $\mathbb{Z}_4$-коды произвольной длины n (при условии существования матрицы Адамара порядка n) с минимальным расстоянием Ли, равным n, которые после применения известного отображения Грея дают двоичные коды Адамара длины $2n$. Для кодов Адамара длины 16, 32, 48 и 64 мы приводим примеры конструкции кодов Адамара почти для всех возможных значений ранга и размерности ядра, а также приводим новые нижние оценки числа таких неэквивалентных кодов с фиксированным рангом и размерностью ядра. Оказалось, что в специальном случае наша конструкция совпадает с кронекеровской (или конструкцией Сильвестра), и может считаться вариантом известной в настоящее время [1] модифицированной конструкции Сильвестра, которая использует одну матрицу Адамара порядка m, а также m (не обязательно различных) матриц Адамара порядка k.

Здесь мы обобщаем эту модифицированную конструкцию, предложив новую более общую конструкцию типа Сильвестра, основанную уже на двух семействах (не обязательно различных) матриц Адамара, а именно на k матрицах порядка m и m матрицах порядка k. Результирующая матрица Адамара имеет порядок mk, как и в конструкции из [1].

§ 2. Построение $\mathbb{Z}_q$-кодов в метрике Ли

Для независимости изложения вкратце повторим конструкцию q-ичных кодов в метрике Ли, введенную в [20, 21]. Пусть имеется алфавит $E = \{0, 1, \ldots, q-1\}$ размера q. Пронумеруем элементы алфавита: $E = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Предположим, что q можно представить в виде произведения $q = q_1 q_2 \ldots q_s$, где все q_i – произвольные натуральные числа, упорядоченные произвольным образом. Это разложение на множители мы используем для нумерации элементов алфавита E. Определим числа

$$Q_j = \frac{q}{q_1 q_2 \ldots q_j}, \quad j = 1, \ldots, s.$$

Сначала разобьем E на q_1 подмножеств E_i размера Q_1:

$$E = E_0 \cup \ldots \cup E_{q_1-1}, \quad E_i = \{i + j \cdot q_1 : \ j = 0, \ldots, Q_1 - 1\}.$$

Затем сделаем то же самое для каждого множества E_i:

$$E_i = E_{i,0} \cup E_{i,1} \cup \ldots \cup E_{i,q_2-1},$$

где

$$E_{i,j} = \{i + j \cdot q_1 + k \cdot q_1 q_2 : \ k = 0, \ldots, Q_2 - 1\},$$

и так далее. Эта процедура повторяется s шагов, в результате которых получаем подмножества $E_{i_1,\ldots,i_{s-1}}$ размера $Q_{s-1} = q_s$, такие что

$$E = \bigcup_{i_1=0}^{q_1-1} \ldots \bigcup_{i_{s-1}=0}^{q_{s-1}-1} E_{i_1,\ldots,i_{s-1}}, \tag{5}$$

где каждое множество $E_{i_1,\ldots,i_{s-1}}$ содержит q_s элементов. Каждому элементу a из алфавита E размера q с разложением $q = q_1 q_2 \ldots q_s$ приписывается номер, а именно его вектор индексов $L(a) = (i_1, i_2, \ldots, i_{s-1}, i_s)$, если элемент a принадлежит подмножеству $E_{i_1,\ldots,i_{s-1}}$ и имеет индекс i_s в множестве $E_{i_1,\ldots,i_{s-1}}$, где элементы $E_{i_1,\ldots,i_{s-1}}$ упорядочены по возрастанию.

Таким образом, каждому элементу из E ставится в соответствие его номер, представляющий собой целочисленный вектор $L(a) = (i_1, \ldots, i_s)$ длины s, удовлетворяющий следующему свойству: *j-й индекс i_j принадлежит множеству* $\{0, 1, \ldots, q_j - 1\}$. Определим обратное отображение:

$$L^{-1}(i_1, i_2, \ldots, i_s) = a.$$

Легко видеть, что вектор $L(a)$ является $(q_1, \ldots, q_s)$-разложением числа a, а именно

$$L(a) = (i_1, i_2, \ldots, i_s), \quad a = L^{-1}(i_1, i_2, \ldots, i_s),$$

где

$$a = \sum_{j=1}^{s} i_j \cdot q_1 \ldots q_{j-1} \quad \text{и} \quad q_0 = 1.$$

Конструкция. Пусть задано множество $E = \{0, 1, \ldots, q-1\}$ размера q, где q представимо в виде произведения s натуральных чисел $q = q_1 q_2 \ldots q_s$. Предположим, что имеется s кодов A_j (одной и той же длины), $j = 1, \ldots, j$, где код A_j над алфавитом $E_{q_j} = \{0, 1, \ldots, q_j - 1\}$ размера q_j имеет параметры $(n, N_j, d_j)_{q_j}$. Из каждого кода A_j, $j = 1, \ldots, s$, выберем по произвольному кодовому слову $\boldsymbol{a}^{(j)} = (a_1^{(j)}, \ldots, a_n^{(j)})$. Для каждого i, $i = 1, \ldots, n$, построим вектор $\boldsymbol{b}_i = (a_i^{(1)}, \ldots, a_i^{(s)})$ из i-х координат s векторов $\boldsymbol{a}^{(j)}$, $j = 1, \ldots, s$. Очевидно, что элемент j-й позиции этого вектора $\boldsymbol{b}_i$ принадлежит алфавиту размера q_j, поскольку это как раз алфавит кода A_j. Отсюда следует, что любой такой вектор является вектором индексов $L(a)$ некоторого элемента a_i из множества E, который имеет такой номер, т.е. $L(a_i) = (a_i^{(1)}, \ldots, a_i^{(s)})$. Зададим кодовое слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ над E нового результирующего кода $\mathcal{C}$, заменяя каждый i-й вектор $\boldsymbol{b}_i$ элементом $c_i = L^{-1}(\boldsymbol{b}_i)$, индексный вектор которого $L(c_i)$ совпадает с вектором $\boldsymbol{b}_i$, т.е. $L(c_i) = \boldsymbol{b}_i$. Это означает, что на i-й позиции кодового слова $\boldsymbol{c} = (c_1, \ldots, c_n)$ стоит элемент c_i, т.е. что $c_i = L^{-1}(\boldsymbol{b}_i)$. Когда все кодовые слова $\boldsymbol{a}^{(j)}$ пробегают все внешние коды A_j для всех $j = 1, \ldots, s$, соответствующие кодовые слова $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(s)})$ пробегают весь код $\mathcal{C}$.

Теорема 1 [20, 21]. *Пусть задано множество $E = \{0, 1, \ldots, q-1\}$ размера q, где q представимо в виде произведения s натуральных чисел $q = q_1 q_2 \ldots q_s$. Предположим, что имеются s внешних q_j-ичных кодов A_j, $j = 1, \ldots, s$, с параметрами $(n, N_j, d_j)_{q_j}$. Тогда описанная выше конструкция приводит к q-ичному коду C над алфавитом E с параметрами*

$$n, \quad N = \prod_{j=1}^{s} N_j, \quad d_L = \min\{d_1, q_1 d_2, q_1 q_2 d_3, \ldots, q_1 q_2 \ldots q_{s-1} d_s\}.$$

В следующем параграфе мы представим общую конструкцию кодов в метрике Ли над алфавитом $\mathbb{Z}_q$, которые под действием отображения Грея становятся двоичными $(n, 2n, n/2)$-кодами Адамара.

§ 3. Построение $\mathbb{Z}_q$-кодов Адамара

В работах [20,21] было замечено, что при существовании двоичного кода Адамара длины n теорема 1 порождает q-ичный код Адамара той же длины n в метрике Ли над алфавитом $\mathbb{Z}_4$, из которого под действием отображения Грея получается двоичный код Адамара (в метрике Хэмминга) длины $2n$. Объясним этот результат как начальный шаг к пояснению более общей конструкции.

Пусть $E = \{0, 1, 2, 3\}$, т.е. $q = 4 = 2 \cdot 2$, а значит, $q_1 = q_2 = 2$. Произвольному элементу a из E поставим в соответствие вектор индексов $L(a) = (i_1, i_2)$, являющийся двоичным представлением числа a, т.е. $a = i_1 + 2\, i_2$, где $i_1, i_2 \in \mathbb{Z}_2$. Пусть n – некоторое натуральное число, такое что существует двоичный $(n, 2n, n/2)$-код Адамара H_n, и пусть A_1 – тривиальный $(n, 2, n)$-код, состоящий из пары дополнительных векторов длины n. Пусть $\boldsymbol{h} = (h_1, \ldots, h_n)$ – произвольное кодовое слово кода H_n, а $\boldsymbol{a} = (a_1, \ldots, a_n)$ – одно из двух кодовых слов кода A_1. Для такой пары выбранных слов поставим в соответствие слово $\boldsymbol{c} = \boldsymbol{c}(\boldsymbol{a}, \boldsymbol{h}) = (c_1, c_2, \ldots, c_n)$ нового кода, где $c_i = L^{-1}(a_i, h_i)$ – элемент из $\mathbb{Z}_4$. Таким образом мы получаем новый код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ с параметрами $(n, 4n, d_L = n)_4$, где d_L – расстояние Ли, а значит, отображение Грея порождает двоичный $(2n, 4n, n)$-код Адамара H_{2n} [20, 21].

Теорема 2 [20,21]. *Пусть H_n – двоичный $(n, 2n, n/2)$-код Адамара. Тогда конструкция, приведенная в теореме* 1, *дает код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ с параметрами $(n, 4n, d_L = n)_4$, который под действием отображения Грея индуцирует двоичный $(2n, 4n, n)$-код Адамара H_{2n}.*

Новый код $\mathcal{C}$ над алфавитом $\mathbb{Z}_4$ сохраняет ряд свойств изначального кода Адамара H_n. Необходимо отметить, что в работе [22] были классифицированы все линейные $\mathbb{Z}_2\mathbb{Z}_4$-коды Адамара. Цель настоящей статьи – показать, какие коды могут быть получены общей конструкцией, приведенной в теореме 1 для произвольного $q > 4$. В частности, главной целью является изучение значений q, для которых существуют $\mathbb{Z}_q$-коды Адамара. Однако поясним сначала, что подразумевается под $\mathbb{Z}_q$-кодом Адамара, или, что эквивалентно, кодом Адамара над $\mathbb{Z}_q$.

Поскольку отображение Грея существует только для случая $q = 4$, нам придется для случаев $q > 4$ использовать другие отображения множества E в двоичные векторы. Как мы уже упоминали ранее, одно из таких возможных отображений было предложено Карле [3]. В частности, для $q = 2^s$ элементы алфавита E отображаются в кодовые слова линейного $[q/2, q, q/4]$-кода Адамара $H_{q/2}$, и таким образом, конструкцию можно рассматривать как каскадный код второго порядка с кодом Адамара в качестве внутреннего кода [17]. В работе [6] Кротов слегка обобщил отображение Грея – Карле, предложив использовать в качестве внутреннего кода произвольный код Адамара. Мы модифицируем оба отображения, используя идеи обобщенной каскадной конструкции [17, 19].

Пусть q – целое число, такое что существует двоичный код Адамара $H_{q/2}$. Предположим, что элементы $\mathbb{Z}_q$ пронумерованы в соответствии с разложением числа q, а именно пусть $q = q_1 \cdot q_2$, где $q_1 = q/2$ и $q_2 = 2$. Таким образом, произвольному $a \in \mathbb{Z}_q$ ставим в соответствие вектор индексов $L(a) = (i_1, i_2)$, где $i_1 \in \mathbb{Z}_{q/2}$ и $i_2 \in \mathbb{Z}_2$, причем

$$\{0, 1\} = \mathbb{Z}_2 \subset \mathbb{Z}_{q/2} \subset \mathbb{Z}_q = \{0, 1, \ldots, q-1\}.$$

Предположим, что $H_{q/2}$ – двоичный $(q/2, q, q/4)$-код Адамара, кодовые слова которого $\boldsymbol{h}_i$, $i = 0, 1, \ldots, q-1$, пронумерованы таким образом, что для произвольного $i = 0, 1, \ldots, q/2 - 1$ имеет место следующее равенство:

$$d_H(\boldsymbol{h}_i, \boldsymbol{h}_{i+q/2}) = q/2. \tag{6}$$

Для произвольного элемента $a \in \mathbb{Z}_q$ с вектором индексов $L(a) = (i_1, i_2)$ определим следующее отображение $\Phi(a, H_{q/2})$ (являющееся переформулировкой отображений из [3, 6]) в множество кодовых слов кода Адамара $H_{q/2}$:

$$\boldsymbol{h}_a = \Phi(a, H_{q/2}) = \boldsymbol{h}_{i_1 + i_2 q/2} = \boldsymbol{h}_{i_1} + i_2(1, 1, \ldots, 1). \tag{7}$$

Это отображение может быть естественным образом продолжено на векторы $\boldsymbol{u} = (u_1, \ldots, u_m)$ над $\mathbb{Z}_q$, отображающиеся в двоичные векторы длины $qm/2$:

$$\boldsymbol{c} = \Phi(\boldsymbol{u}, H_{q/2}) = (\boldsymbol{h}_{u_1}, \ldots, \boldsymbol{h}_{u_m}), \tag{8}$$

а также для множеств U векторов над алфавитом $\mathbb{Z}_q$:

$$\Phi(U, H_{q/2}) = \{\Phi(\boldsymbol{u}, H_{q/2}) : \boldsymbol{u} \in U\}. \tag{9}$$

Определение 1. Будем называть $\mathbb{Z}_q$-код $\mathcal{C}$ длины m и мощности $N = qm$ *$\mathbb{Z}_q$-кодом Адамара*, если его образ $C = \Phi(\mathcal{C}, H_{q/2})$ является двоичным $(qm/2, qm, qm/4)$-кодом Адамара $H_{qm/2}$.

Теорема 3. *Пусть q и m – натуральные числа, такие что существуют матрицы Адамара $H_{q/2}$ и H_m порядков $q/2$ и m. Тогда конструкция, заданная в теореме* 1, *дает $\mathbb{Z}_q$-код Адамара $\mathcal{C}$ длины m, такой что его образ $C = \Phi(\mathcal{C}, H_{q/2})$, заданный отображениями* (7)–(9), *представляет собой двоичный $(qm/2, qm, qm/4)$-код Адамара $H_{qm/2}$.*

Доказательство. В качестве кода $A_1 = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{q/2-1}\}$ возьмем тривиальный $(m, q/2, m)_{q/2}$-код U, состоящий из $q/2$ кодовых слов $\boldsymbol{a}_i$ над алфавитом $\mathbb{Z}_{q/2}$. В качестве кода A_2 возьмем $(m, 2m, m/2)$-код Адамара $H_m = \{\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{2m-1}\}$. По построению, приведенному в теореме 1, получаем $\mathbb{Z}_q$-код $\mathcal{C}$ длины m и мощности qm с минимальным расстоянием Ли

$$d_L = \min\{m, 2 \cdot m/2\} = m.$$

Мы утверждаем, что $\mathcal{C}$ является $\mathbb{Z}_q$-кодом Адамара. Чтобы убедиться в этом, возьмем произвольный двоичный $(q/2, q, q/4)$-код Адамара $H_{q/2}$ с кодовыми словами $\{\boldsymbol{h}_0, \boldsymbol{h}_1, \ldots, \boldsymbol{h}_{q-1}\}$, пронумерованными так, что для произвольного i, $i = 0, 1, \ldots, q/2-1$, кодовые слова $\boldsymbol{h}_i$ и $\boldsymbol{h}_{i+q/2}$ находятся на расстоянии Хэмминга $q/2$. Рассмотрим двоичный код $C = \Phi(\mathcal{C}, H_{q/2})$. Ясно, что длина кода C равна $n = qm/2$, а его мощность $N = qm$. Необходимо проверить, что минимальное расстояние (Хэмминга) составляет $qm/4$. Рассмотрим два кодовых слова $\boldsymbol{c}_1 = \Phi(\boldsymbol{v}_1, H_{q/2})$ и $\boldsymbol{c}_2 = \Phi(\boldsymbol{v}_2, H_{q/2})$ кода C. Предположим, что $\boldsymbol{v}_1$ получено из кодовых слов $\boldsymbol{a}_{i_1} \in A_1$ и $\boldsymbol{b}_{j_1} \in H_m$, а $\boldsymbol{v}_2$ – из кодовых слов $\boldsymbol{a}_{i_2} \in A_1$ и $\boldsymbol{b}_{j_2} \in H_m$. В соответствии с конструкцией векторы $\boldsymbol{v}_1 = (v_{1,1}, \ldots, v_{1,m})$ и $\boldsymbol{v}_2 = (v_{2,1}, \ldots, v_{2,m})$ представляются в виде

$$\boldsymbol{v}_1 = \boldsymbol{a}_{i_1} + \frac{q}{2}\boldsymbol{b}_{j_1}, \quad \boldsymbol{v}_2 = \boldsymbol{a}_{i_2} + \frac{q}{2}\boldsymbol{b}_{j_2}, \tag{10}$$

где покомпонентное сложение производится в кольце $\mathbb{Z}_q$ и при этом мы полагаем, что $\mathbb{Z}_{q/2} \subset \mathbb{Z}_q$. Необходимо рассмотреть два случая: (i) $\boldsymbol{a}_{i_1} = \boldsymbol{a}_{i_2}$ и (ii) $\boldsymbol{a}_{i_1} \neq \boldsymbol{a}_{i_1}$.

Сначала предположим, что $\boldsymbol{a}_{i_1} = \boldsymbol{a}_{i_2}$. Из этого следует, что $\boldsymbol{b}_{j_1} \neq \boldsymbol{b}_{j_2}$. Значит, эти слова различаются в $m/2$ позициях, из чего, в свою очередь, следует, что слова $\boldsymbol{v}_1$ и $\boldsymbol{v}_2$ находятся на расстоянии $d_H(\boldsymbol{v}_1, \boldsymbol{v}_2) = m/2$. Однако для каждой s-й позиции, в которой они различны (т.е. когда $v_{1,s} \neq v_{2,s}$), в соответствии с (10) имеет место равенство

$$d_L(v_{1,s}, v_{2,s}) = |v_{1,s} - v_{2,s}| = q/2,$$

из чего опять вытекает, что под действием отображения $\Phi(\mathcal{C}, H_{q/2})$ согласно условию (6) каждая такая позиция увеличивает расстояние Хэмминга ровно на $q/2$ (а не на $q/4$). Следовательно, общий вклад в расстояние Хэмминга будет $m/2 \cdot q/2$, из чего следует, что в этом случае $d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) = qm/4$.

Теперь предположим, что $\boldsymbol{a}_{i_1} \neq \boldsymbol{a}_{i_2}$. Из этого следует, что $d_H(\boldsymbol{a}_{i_1}, \boldsymbol{a}_{i_2}) = m$. Поскольку для любой пары кодовых слов $\boldsymbol{b}_i, \boldsymbol{b}_j \in H_{q/2}$ выполнено условие $d_H(\boldsymbol{b}_i, \boldsymbol{b}_j) \geqslant$ $\geqslant q/4$, из этого также следует, что $d_H(\boldsymbol{c}_1, \boldsymbol{c}_2) = qm/4$. Таким образом, получаем, что результирующий код $C = \Phi(\mathcal{C}, H_{q/2})$ имеет минимальное расстояние Хэмминга $d_H(C) = qm/4$, откуда (учитывая его длину $m\,q/2$ и мощность $m\,q$) заключаем, что результирующий код C – это двоичный код Адамара $H_{qm/2}$. ▲

Определение 2. Для заданных натуральных чисел $q \geqslant 2$ и $m \geqslant 4$, двоичного вектора $\boldsymbol{a} = (a_1, \ldots, a_m)$ и вектора $\boldsymbol{v} = (v_1, \ldots, v_m)$ длины m над алфавитом $\mathbb{Z}_{q/2}$ обозначим через $\Psi(\boldsymbol{v}, \boldsymbol{a})$ следующее отображение этой пары векторов в вектор $\boldsymbol{u}$ длины m над алфавитом $\mathbb{Z}_q$:

$$\boldsymbol{u} = \Psi(\boldsymbol{v}, \boldsymbol{a}) = \Big(v_1 + a_1\frac{q}{2},\ v_2 + a_2\frac{q}{2},\ \ldots,\ v_m + a_m\frac{q}{2}\Big),$$

где покомпонентное сложение производится в кольце $\mathbb{Z}_q$ и мы предполагаем, что $\mathbb{Z}_{q/2} \subset \mathbb{Z}_q$. Пусть теперь $\boldsymbol{v}$ пробегает некоторое множество V, а $\boldsymbol{a}$ – некоторое множество A, тогда определим соответствующее множество результирующих векторов над алфавитом $\mathbb{Z}_q$:

$$\mathcal{C} = \Psi(V, A) = \{\Psi(\boldsymbol{v}, \boldsymbol{a}) :\ \boldsymbol{v} \in V,\ \boldsymbol{a} \in A\}. \tag{11}$$

Теперь опишем обобщенную конструкцию $\mathbb{Z}_q$-кодов Адамара. Рассмотрим множество

$$S_H(q/2) = \{H_{q/2}(i) : \ i = 1, \ldots, s_{q/2}\},$$

состоящее из $s_{q/2}$ различных двоичных $(q/2, q, q/4)$-кодов Адамара $H_{q/2}(i)$. Предположим, что кодовые слова каждого из кодов $H_{q/2}(i)$ пронумерованы:

$$H_{q/2}(i) = \{\boldsymbol{h}_0^{(i)}, \boldsymbol{h}_1^{(i)}, \ldots, \boldsymbol{h}_{q-1}^{(i)}\},$$

причем таким образом, что для произвольного i и произвольного $j = 0, 1, \ldots, q/2-1$ кодовые слова $\boldsymbol{h}_j^{(i)}$ и $\boldsymbol{h}_{j+q/2}^{(i)}$ находятся на расстоянии $q/2$ друг от друга, т.е. выполнено условие (6). Обобщим отображение, заданное формулой (8).

Определение 3. Пусть $S_H(q/2)$ – множество, состоящее из $s_{q/2}$ различных кодов Адамара

$$H_{q/2}(i) = \{\boldsymbol{h}_0^{(i)}, \boldsymbol{h}_1^{(i)}, \ldots, \boldsymbol{h}_{q-1}^{(i)}\}, \quad i = 1, \ldots, s_{q/2},$$

с нумерацией кодовых слов, удовлетворяющих условию (6). Пусть $\boldsymbol{f} = (f_1, \ldots, f_m)$ – произвольный вектор длины m над алфавитом $\{1, 2, \ldots, s_{q/2}\}$, а $\boldsymbol{u} = (u_1, \ldots, u_m)$ – произвольный вектор длины m над алфавитом $\mathbb{Z}_q$. Определим следующее отображение $\Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2))$ из векторов $\boldsymbol{f}$ и $\boldsymbol{u}$ в двоичный вектор $\boldsymbol{c}$ длины $n = qm/2$:

$$\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2)) = \left(\boldsymbol{h}_{u_1}^{(f_1)}, \boldsymbol{h}_{u_2}^{(f_2)}, \ldots, \boldsymbol{h}_{u_m}^{(f_m)}\right). \tag{12}$$

Соответственно, обозначим через $\Phi(U, \boldsymbol{f}, S_H(q/2))$ отображение из множества U таких векторов $\boldsymbol{u}$ длины m над алфавитом $\mathbb{Z}_q$ в множество C двоичных векторов $\boldsymbol{c}$:

$$C = \Phi(U, \boldsymbol{f}, S_H(q/2)) = \{\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2)) : \ \boldsymbol{u} \in U\}. \tag{13}$$

Следующее утверждение является обобщением теоремы 3.

Теорема 4. *Пусть $q \geqslant 4$ и $m \geqslant 2$ – произвольные натуральные числа, для которых существуют матрицы Адамара порядков $q/2$ и m. Пусть $S_H(q/2)$ – множество, состоящее из $s_{q/2}$ различных кодов Адамара $H_{q/2}(i)$, $i = 1, \ldots, s_{q/2}$. Тогда для произвольного $(m, 2m, m/2)$-кода Адамара H_m, тривиального $(m, q/2, m)_{q/2}$-кода V и произвольного вектора $\boldsymbol{f} = (f_1, \ldots, f_m)$ длины m над алфавитом $\{1, 2, \ldots, s_{q/2}\}$ результирующий двоичный код*

$$C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(q/2)), \quad \textit{где } \mathcal{C} = \Psi(V, H_m), \tag{14}$$

является двоичным $(qm/2, qm, qm/4)$-кодом Адамара $H_{qm/2}$.

Доказательство. В соответствии с определением отображения Φ кодовые слова $\boldsymbol{c} = \Phi(\boldsymbol{u}, \boldsymbol{f}, S_H(q/2))$ кода C имеет следующую блоковую структуру: $\boldsymbol{c} = (\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_m)$, где $\boldsymbol{c}_i$ – подвектор длины $q/2$, являющийся некоторым кодовым словом $\boldsymbol{h}_j^{(f_i)}$ кода Адамара $H_{q/2}(f_i)$, где f_i – элемент, стоящей на i-й позиции вектора $\boldsymbol{f}$. Таким образом, произвольное кодовое слово $\boldsymbol{c}$ кода C имеет в качестве i-го блока некоторое слово кода $H_{q/2}(f_i)$. Поскольку все коды $H_{q/2}(i)$ имеют одинаковое минимальное расстояние, а нумерация их кодовых слов удовлетворяет условию (6), то вклад в расстояние (Хэмминга) между различными кодовыми словами $\boldsymbol{c}$ и $\boldsymbol{c}'$ не зависит от индекса f_i. Таким образом, утверждение теоремы вытекает из предыдущей теоремы 3. ▲

§ 4. Примеры построения кодов Адамара

Для заданного множества $S_H(n) = \{H_n(i) : i = 1, \ldots, s_n\}$ двоичных $(n, 2n, n/2)$-кодов Адамара обозначим через $r_n(i)$ двоичный ранг кода $H_n(i)$, а через $k_n(i)$ – размерность ядра кода $H_n(i)$. Представляет интерес следующий вопрос: *знаем ли мы ранг и размерность ядра кодов Адамара, построенных конструкцией, введенной в теореме* 4? Ясно, что для того чтобы ранг был как можно больше, необходимо выбрать коды V_i с попарно различными столбцами, а в качестве векторов f_i – векторы с различными компонентами. Для того чтобы размерность ядра была большой, необходимо уменьшить число различных столбцов в кодах V_i и число различных компонент в векторах f_i. Примеры, приведенные в данном параграфе для случаев $n = 16$, 32, 48, 64, демонстрируют сложность данного вопроса.

Пример 1. Пусть $q = 8$ и $m = 4$. Пусть множество

$$S_H(4) = \{H_4(1), H_4(2), H_4(3)\}$$

состоит, например, из трех (т.е. $s_4 = 3$) различных кодов Адамара длины 4, где каждый код $H_4(i)$ задается множеством слов, образующих матрицу Адамара порядка 4, в объединении с множеством их дополнительных слов, которое обозначается через $\bar{H}$:

$$H_4(1) = \{(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1)\} \cup \bar{H},$$
$$H_4(2) = \{(0,0,0,0), (0,1,1,0), (0,1,0,1), (0,0,1,1)\} \cup \bar{H},$$
$$H_4(3) = \{(0,0,0,0), (1,1,0,0), (0,1,1,0), (0,1,0,1)\} \cup \bar{H}.$$

Пусть V_i – следующие тривиальные $(4,4,4)_4$-коды над алфавитом $\mathbb{Z}_4$, $i = 0, \ldots, 4$:

$$V_0 = \{(k,k,k,k) : k \in \{0,1,2,3\}\},$$
$$V_1 = \{(0,0,0,0), (1,1,1,2), (3,2,2,1), (2,3,3,3)\},$$
$$V_2 = \{(0,0,0,0), (1,3,2,1), (3,2,1,2), (2,1,3,3)\},$$
$$V_3 = \{(0,0,0,0), (1,1,1,1), (3,2,2,3), (2,3,3,2)\},$$
$$V_4 = \{(0,0,0,0), (1,2,2,3), (2,3,1,2), (3,1,3,1)\}.$$

В качестве вектора $\boldsymbol{f}$ можно взять один из $3^4 = 81$ векторов длины 4 над алфавитом $\{1,2,3\}$. В качестве кода Адамара H_4 длины $m = 4$ выберем, например, $H_4 = H_4(2)$. Тогда можно построить $\mathbb{Z}_8$-код Адамара $\mathcal{C}$ длины 4 с $|H_4| \cdot |V_i| = 8 \cdot 4 = 32$ кодовыми словами, полагая $\mathcal{C} = \Psi(V_i, H_4)$, что дает $(16, 32, 8)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$. С помощью системы компьютерной алгебры Magma [23] мы проверили, что все такие коды Адамара длины 16 являются либо линейными (с рангом и размерностью ядра, равными 5), либо нелинейными с рангом 6 и размерностью ядра 3. Кроме того, для длины 16 известно, что с точностью до эквивалентности существует ровно один код для каждого такого параметра. Следовательно, возможными значениями для параметров (r,k) являются $\{(5,5), (6,3)\}$, и не существует кодов с размерностью ядра 2 или 1. Другими словами, мы можем получить коды Адамара для всех возможных пар значений (r,k), таких что $k \geqslant 3$. Интересный факт был получен из результатов компьютерных вычислений. Было замечено, что для любого кода V_i, $i = 0, \ldots, 4$, получающийся $(16, 32, 8)$-код Адамара является линейным, если и только если используемый вектор $\boldsymbol{f} = (f_1, f_2, f_3, f_4)$ удовлетворяет следующему условию:

$$f_1 + f_2 + f_3 + f_4 \equiv 0 \pmod 2,$$

и соответственно является нелинейным в противном случае. Более того, если теперь вместо $H_4 = H_4(2)$ выбрать другую матрицу – $H_4 = H_4(1)$ либо $H_4 = H_4(3)$, то результат не меняется.

Таблица 5

Число неэквивалентных $(32, 64, 16)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$ относительно общего числа

k	r										
	6	7	8	9	10	11	12	13	14	15	16
6	1/3										
4		1/38									
3		1/40	1/23	5/120	3/32						

Пример 2. Пусть $q = 16$ и $m = 4$. В качестве кода Адамара H_4 длины 4 возьмем код из примера 1. Пусть V – следующий тривиальный $(4, 8, 4)_8$-код над алфавитом $\mathbb{Z}_8$:

$$V = \{(0,0,0,0), (1,2,3,4), (2,3,4,5), (3,4,5,6), (4,5,6,7), (5,6,7,1), (6,7,1,2), (7,1,2,3)\}.$$

На основе этих кодов с помощью нашей конструкции можно построить $\mathbb{Z}_{16}$-код Адамара $\mathcal{C} = \Psi(V, H_4)$ длины 4 и мощности $|H_4| \cdot |V| = 8 \cdot 8 = 64$. В качестве различных кодов Адамара длины 8 выберем следующие четыре кода Адамара

$$S_H(8) = \{H_8(1), H_8(2), H_8(3), H_8(4)\}$$

(т.е. $s_8 = 4$), которые мы задаем половиной кодовых слов (так как вторая, обозначенная через $\bar{H}$, однозначно определяется первой):

$$H_8(1) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (0,0,0,0,1,1,1,1) \\ (0,0,1,1,0,0,1,1) \\ (0,0,1,1,1,1,0,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,0,1,0,1,0,1) \\ (0,1,0,1,1,0,1,0) \\ (0,1,1,0,0,1,1,0) \\ (0,1,1,0,1,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(2) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (1,1,1,0,1,0,0,0) \\ (1,0,1,1,0,1,0,0) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (1,0,0,0,1,1,0,1) \\ (1,1,0,0,0,1,1,0) \\ (1,0,1,0,0,0,1,1) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(3) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (1,1,1,0,1,0,0,0) \\ (0,1,0,0,1,0,1,1) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,1,1,0,0,1,0) \\ (1,1,0,0,0,1,1,0) \\ (0,1,0,1,1,1,0,0) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H},$$

$$H_8(4) = \begin{Bmatrix} (0,0,0,0,0,0,0,0) \\ (0,0,0,1,0,1,1,1) \\ (0,1,0,0,1,0,1,1) \\ (1,0,0,1,1,0,1,0) \end{Bmatrix} \cup \begin{Bmatrix} (0,1,1,1,0,0,1,0) \\ (0,0,1,1,1,0,0,1) \\ (1,0,1,0,0,0,1,1) \\ (1,1,0,1,0,0,0,1) \end{Bmatrix} \cup \bar{H}.$$

Используя все возможные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4\}$, получаем 256 различных $(32, 64, 16)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$. Все эти коды имеют тип 0. Можно получить коды Адамара для всех возможных значений параметров (r, k) при условии, что $k \geqslant 3$, т.е. всех пар параметров с символом $*$ в табл. 2. С помощью системы компьютерной алгебры Magma [23] мы получили коды Адамара длины 32, параметры (r, k) которых приведены в табл. 5. В таблице указано число неэквивалентных кодов Адамара относительно общего числа различных кодов для всех возможных пар (r, k). Кроме того, табл. 6 показывает значения $\boldsymbol{f}$ для соответствующих неэквивалентных кодов.

Таблица 6

Значения векторов $\boldsymbol{f}$ для неэквивалентных $(32, 64, 16)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$

r	k	$\boldsymbol{f}$
6	6	$(2,2,2,2)$
7	4	$(4,2,2,2)$
7	3	$(3,2,2,2)$
8	3	$(3,2,2,1)$
9	3	$(1,1,1,1)$, $(2,2,1,1)$, $(1,3,1,1)$, $(2,2,2,1)$, $(4,3,2,1)$
10	3	$(2,1,1,1)$, $(1,2,1,1)$, $(3,2,1,1)$

Пример 3. Пусть $q = 8$ и $m = 8$. Пусть H_8 – код Адамара $H_8(1)$, заданный в примере 2, а $S_H(4)$ – множество из трех кодов, заданных в примере 1. Рассматривая тривиальный код

$$V = \{(0,0,0,0,0,0,0,0), (1,3,3,2,1,3,1,2), (3,1,2,1,3,2,2,1), (2,2,1,3,2,1,3,3)\},$$

можно построить $3^8 = 6561$ различных $(32, 64, 16)$-кодов Адамара: один линейный (при выборе $\boldsymbol{f} = (1,1,1,1,1,1,1,1)$) и два неэквивалентных (например, когда $\boldsymbol{f} = (1,1,1,1,1,1,1,2)$ и $\boldsymbol{f} = (1,1,1,1,1,1,2,2)$) кода типа 0 ранга 7 с ядром размерности 4. Таким образом, мы строим коды для всех возможных пар (r, k), таких что $k \geqslant 4$. Кроме того, мы получаем коды, не эквивалентные кодам из примера 2.

Пример 4. Пусть $q = 32$ и $m = 4$. Пусть H_4 будет тем же кодом Адамара, что и в примере 1, а V_i, $i \in \{1, 2\}$, – следующие тривиальные $(4, 16, 4)_{16}$-коды над алфавитом $\mathbb{Z}_{16}$:

$$V_1 = \{(k,k,k,k) : \ k \in \{0, \ldots, 15\}\}$$

и

$$V_2 = \{(k,k,k,k) : \ k \in \{0, \ldots, 7, 10, \ldots 15\}\} \cup \{(8,9,8,9), (9,8,9,8)\}.$$

С этими исходными кодами мы можем построить $\mathbb{Z}_{32}$-коды $\mathcal{C}$ длины 4 мощности $|H_4| \cdot |V_i| = 8 \cdot 16 = 128$, полагая $\mathcal{C} = \Psi(V_i, H_4)$, $i \in \{1, 2\}$. Пусть

$$S_H(16) = \{H_{16}(1), H_{16}(2), H_{16}(3), H_{16}(4), H_{16}(5)\}$$

– множество из пяти попарно неэквивалентных кода Адамара длины 16, приведенных в [23], которые были описаны в 1933 г. в работе [24] (см. также [25, 26]). Рассматривая различные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4, 5\}$, получаем 625 различных $(64, 128, 32)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$. В табл. 7 для данных тривиальных кодов V_1 и V_2 приводится число неэквивалентных кодов Адамара в зависимости от ранга и размерности ядра. Заметим, что можно получить коды Адамара для всех возможных пар (r, k), таких что $k \geqslant 3$, за исключением случаев $(11, 4)$, $(8, 3)$, и $(18, 3)$ (т.е. для пар (r, k), обозначенных символом $*$ в табл. 3). Выбирая максимальное значение для каждой пары (r, k), мы получаем по крайней мере 137 неэквивалентных кодов. И наконец, в табл. 8 приведены значения векторов $\boldsymbol{f}$, для которых мы можем построить коды Адамара для каждой из возможных пар параметров (r, k), используя коды V_1 и V_2.

Пример 5. Пусть $q = 8$ и $m = 12$. Пусть $S_H(4)$ – такое же множество, как в примере 1, с $s_4 = 3$ различными кодами Адамара длины 4. Пусть V_0 – тривиальный $(12, 4, 12)_4$-код над алфавитом $\mathbb{Z}_4$:

$$V_0 = \{(k,k,k,k,k,k,k,k,k,k,k,k) : \ k \in \{0,1,2,3\}\}.$$

Таблица 7

Неэквивалентные $(64, 128, 32)$-коды $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с использованием кодов V_1 и V_2

k	r													
	7	8	9	10	11	12	13	14	15	16	17	18	...	32
7	1-0													
5		1-0												
4		0-1	1-0	1-0	0-0									
3		0-0	0-1	4-1	0-6	6-2	6-13	9-12	12-6	6-29	23-49	0-0		

Таблица 8

Значения векторов $\boldsymbol{f}$ для некоторых неэквивалентных $(64, 128, 32)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с использованием кодов V_1 и V_2

r	k	$\boldsymbol{f}$ с использ. V_1	$\boldsymbol{f}$ с использ. V_2
7	7	$(1,1,1,1)$	
8	5	$(4,4,4,4)$	
8	4		$(1,1,1,1)$
8	3		
9	4	$(5,5,5,5)$	
9	3		$(4,4,4,4)$
10	4	$(3,3,3,3)$	
10	3	$(2,1,1,1)$	$(5,5,5,5)$

r	k	$\boldsymbol{f}$ с использ. V_1	$\boldsymbol{f}$ с использ. V_2
11	4		
11	3		$(2,1,1,1)$
12	3	$(4,1,1,1)$	$(4,1,4,1)$
13	3	$(5,1,1,1)$	$(4,1,1,1)$
14	3	$(3,1,1,1)$	$(5,2,1,1)$
15	3	$(4,2,1,1)$	$(3,1,1,1)$
16	3	$(4,3,1,1)$	$(4,2,1,1)$
17	3	$(3,2,1,1)$	$(3,2,1,1)$

В качестве кода Адамара H_{12} длины $m = 12$ выбираем следующий код:

$$H_{12} = \left\{ \begin{array}{l} (0,0,0,0,0,0,0,0,0,0,0,0) \\ (0,0,0,0,0,0,1,1,1,1,1,1) \\ (0,0,0,1,1,1,0,0,0,1,1,1) \\ (0,0,1,0,1,1,0,1,1,0,0,1) \\ (0,0,1,1,0,1,1,0,1,0,1,0) \\ (0,0,1,1,1,0,1,1,0,1,0,0) \\ (0,1,1,1,0,0,0,0,1,1,0,1) \\ (0,1,0,0,1,1,1,0,1,1,0,0) \\ (0,1,0,1,1,0,0,1,1,0,1,0) \\ (0,1,1,0,1,0,1,0,0,0,1,1) \\ (0,1,1,0,0,1,0,1,0,1,1,0) \\ (0,1,0,1,0,1,1,1,0,0,0,1) \end{array} \right\} \cup \bar{H},$$

который получен из строк двоичной матрицы Адамара порядка 12 и ее дополнения, обозначенного через $\bar{H}$. Теперь можно построить $\mathbb{Z}_8$-коды Адамара $\mathcal{C}$ длины 12 мощности $|H_{12}| \cdot |V_0| = 24 \cdot 4 = 96$, полагая $\mathcal{C} = \Psi(V_0, H_{12})$. Рассматривая различные векторы $\boldsymbol{f}$ длины 12 над алфавитом $\{1, 2, 3\}$, мы получаем $3^{12} = 531441$ различных $(48, 96, 24)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$.

В табл. 9 приведено число таких кодов в зависимости от ранга и размерности ядра, а также все различные векторы $\boldsymbol{f}$, для которых получаются неэквивалентные коды с этими параметрами. Заметим, что мы можем построить коды Адамара только для параметров $(13, 3)$, $(13, 1)$ и $(14, 1)$, т.е. для пар, обозначенных символом $*$ в табл. 4. Такие же результаты получаются при других выборах тривиальных $(12, 4, 12)_4$-кодов V_i над алфавитом $\mathbb{Z}_4$.

Пример 6. Пусть $q = 24$ и $m = 4$. Пусть H_4 – код Адамара $H_4(1)$ из примера 1, а V – следующий тривиальный $(4, 12, 4)_{12}$-код над алфавитом $\mathbb{Z}_{12}$:

$$V = \{(0,0,0,0), (1,2,3,4), (2,3,4,5), (3,4,5,6), (4,5,6,7), (5,6,7,8),$$
$$(6,7,8,9), (7,8,9,10), (8,9,10,11), (9,10,11,1), (10,11,1,2), (11,1,2,3)\}.$$

Таблица 9

Векторы $\boldsymbol{f}$ для неэквивалентных $(48, 96, 24)$-кодов $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(4))$

r	k	$\boldsymbol{f}$	Число кодов
13	3	$(1,1,1,1,1,1,1,1,1,1,1,1,1)$	4097
13	1	$(2,2,1,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,2,2,1,1,1,1,1,1,1)$ $(2,2,2,2,2,1,2,1,1,1,1,1,1)$	261624
14	1	$(2,1,1,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,1,1,1,1,1,1,1,1,1,1)$ $(2,2,2,2,2,1,1,1,1,1,1,1,1)$	265720

Для этих значений q и m можно построить $\mathbb{Z}_{24}$-коды $\mathcal{C}$ длины 4 мощности $|H_4|\cdot|V| = 8 \cdot 12 = 96$, полагая $\mathcal{C} = \Psi(V, H_4)$. Пусть

$$S_H(12) = \{H_{12}, \pi_1(H_{12}), \ldots, \pi_4(H_{12})\}$$

– множество из пяти различных кодов Адамара длины 12, полученных из кода H_{12}, приведенного в примере 5, и следующих четырех случайных перестановок множества $\{0, 1, \ldots, 11\}$:

$$\pi_1 = (2, 9, 8, 4, 3),$$
$$\pi_2 = (2, 11, 8, 10, 9, 7, 6, 5, 4, 3),$$
$$\pi_3 = (1, 3)(5, 6)(9, 11, 10),$$
$$\pi_4 = (1, 2, 3, 4)(5, 10, 9, 8, 7, 6).$$

Выбирая различные векторы $\boldsymbol{f}$ длины 4 над алфавитом $\{1, 2, 3, 4, 5\}$, получаем $5^4 = 625$ различных $(48, 96, 24)$-кодов Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(12))$. Все такие коды имеют ранг 13 и размерность ядра 3. Кроме того, все эти $(48, 96, 24)$-коды Адамара попарно не эквивалентны.

§ 5. Случай $m = 2$

В предыдущих примерах в случаях, когда m равно степени двойки, мы всегда получали коды с размерностью ядра $k \geqslant \log_2 m + 1$. В данном параграфе мы рассмотрим случай $m = 2$ и покажем, что для этого случая можно получить коды с меньшим ядром, вплоть до размерности 2. Заметим, что коды с размерностью ядра 1 получить невозможно. Кроме того, мы покажем, что если исходные коды Адамара из множества $S_H(q/2)$ не эквивалентны, то и результирующие коды Адамара не эквивалентны.

Пример 7. Пусть $q = 16$ и $m = 2$. Пусть $H_2 = \{(0\,0), (0\,1), (1\,0), (1\,1)\}$, и пусть $V_1 = \{(0\,0), (1\,2), (2\,3), \ldots, (6\,7), (7\,1)\}$ – тривиальный код над алфавитом $\mathbb{Z}_8$. Пусть $S_H(8)$ – множество из трех (эквивалентных) кодов Адамара длины 8. При этих параметрах исходных кодов можно построить $\mathbb{Z}_{16}$-коды Адамара $\mathcal{C}$ длины 2, что дает результирующие $(16, 32, 8)$-коды Адамара вида $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(8))$ со следующими параметрами (r, k):

$$(r, k) \in \{(5, 5), (6, 3), (7, 2), (8, 2)\},$$

т.е. все возможные неэквивалентные коды с ядрами размерности $k \geqslant 2$. Заметим, что в примере 1 мы получаем все неэквивалентные $(16, 32, 8)$-коды Адамара с ядрами размерности $k \geqslant 3$.

Напомним несколько простых свойств ядра (см. (2)) двоичного кода H. Если код H содержит нулевое слово и $\boldsymbol{x} \in \ker(H)$, то очевидно, что

$$\ker(H + \boldsymbol{x}) = \ker(H) \quad \text{и} \quad \ker(\pi(H)) = \pi(\ker(H)), \tag{15}$$

где π – некоторая перестановка координат. Напомним, что два двоичных кода H и H' длины n эквивалентны, если существуют некоторая перестановка координат π и кодовое слово $\boldsymbol{h} \in H'$, такие что

$$\pi(H) = H' + \boldsymbol{h}. \tag{16}$$

Определим стабилизатор ядра как

$$\mathrm{PAut}(H) = \{\pi : \ \pi(H) = H\}.$$

Тогда справедлива следующая

Лемма 1. *Предположим, что два двоичных кода H и H', содержащие нулевой вектор, эквивалентны, т.е. выполняется равенство* (16) *для некоторых π и $\boldsymbol{h} \in H'$. Если в дополнении к этому имеет место условие* $\ker(H) = \ker(H')$, *то тогда* $\pi \in \mathrm{PAut}(\ker(H))$.

Доказательство. Действительно, рассматривая ядра обеих сторон равенства (16) и принимая во внимание первое равенство в (15), получаем, что

$$\ker(\pi(H)) = \ker(H' + \boldsymbol{h}) = \ker(H').$$

Из второго равенства в (15) получаем, что $\pi(\ker(H)) = \ker(H')$. По предположению $\ker(H) = \ker(H')$, откуда и вытекает утверждение леммы. ▲

Рассмотрим теперь для случая $m = 2$ конструкцию, описанную в теореме 4. Тривиальный $(2, q/2, 2)_{q/2}$-код V можно задать перестановкой τ на множестве $\{0, 1, \ldots, q/2 - 1\}$ с помощью выражения

$$V = \{(i, \tau(i)) : \ i = 0, 1, \ldots, q/2 - 1\}.$$

При этом рассматриваются только те перестановки, для которых $\tau(0) = 0$. Предположим, что H_1 и H_1' – две двоичные матрицы Адамара с нулевым вектором и нулевым столбцом, такие что $H_1 \cup \bar{H}_1$ и $H_1' \cup \bar{H}_1'$ являются $(q/2, q, q/4)$-кодами Адамара. Пусть $P = P(\tau)$ – перестановочная матрица, индуцированная перестановкой τ. Тогда результирующий код Адамара $C = C(H_1, H_1', \tau)$ длины q представляется в следующем виде:

$$C = \begin{bmatrix} H_1 & PH_1' \\ H_1 & P\bar{H}_1' \\ \bar{H}_1 & PH_1' \\ \bar{H}_1 & P\bar{H}_1' \end{bmatrix}. \tag{17}$$

Из построения кода следует, что $\ker(C)$ содержит вектор из всех единиц $(1, \ldots, 1)$, а также вектор $(0, \ldots, 0, 1, \ldots, 1)$ веса $q/2$. Предположим, что $\ker(C)$ содержит эти два вектора, т.е. размерность ядра не меньше двух. Для двух пар матриц $\{H_1, H_1'\}$ и $\{H_2, H_2'\}$ скажем, что они эквивалентны, и обозначим это через $\{H_1, H_1'\} \approx \{H_2, H_2'\}$, если имеет место одно из следующих двух условий:

(i) матрица H_1 эквивалентна H_2, а матрица H_1' эквивалентна H_2', либо

(ii) H_1' эквивалентна H_2, а H_1 эквивалентна H_2'.

Лемма 2. *Предположим, что коды $C_1 = C_1(H_1, H_1', \tau_1)$ и $C_2 = C_1(H_2, H_2', \tau_2)$ построены конструкцией, заданной в теореме* 4, *и имеют вид* (17). *Предположим,*

что $\ker(C_1) = \ker(C_2)$ *и эти ядра имеют размерность* 2. *Тогда, если две пары матриц* $\{H_1, H_1'\}$ *и* $\{H_2, H_2'\}$ *не эквивалентны, то соответствующие результирующие коды* C_1 *и* C_2 (*с размерностью ядра* 2) *также не эквивалентны.*

Доказательство. Поскольку размерность $\ker(C_1)$ равна 2, то очевидно, что

$$\ker(C_1) = \ker(C_2) = \{(\mathbf{0},\mathbf{0}), (\mathbf{0},\mathbf{1}), (\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{1})\},$$

где $\mathbf{0} = (0,\ldots,0)$, и $\mathbf{1} = (1,\ldots,1)$ – векторы длины $q/2$. Предположим, что коды C_1 и C_2 эквивалентны, тогда существуют перестановка π и кодовое слово $\boldsymbol{c} \in C_2$, такие что $\pi(C_1) = C_2 + \boldsymbol{c}$. Без ограничения общности можно предположить, что $\boldsymbol{c} = (\boldsymbol{c}_2, \boldsymbol{c}_2')$, где $\boldsymbol{c}_2 \in H_2$ и $\boldsymbol{c}_2' \in H_2'$ (в противном случае можно добавить соответствующий вектор из $\ker(C_2)$). По лемме 1

$$\pi \in \mathrm{PAut}(\{(\mathbf{0},\mathbf{0}), (\mathbf{0},\mathbf{1}), (\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{1})\}),$$

откуда следует, что $\pi = \xi * (\pi_1 \times \pi_2)$, где перестановки π_1, π_2 переставляют $q/2$ координатных позиций исходных кодов, а ξ меняет местами первые $q/2$ координатных позиций со вторыми. Таким образом, имеем

$$\pi(C_1) = \begin{bmatrix} \pi_1(H_1) & \pi_2(P_1H_1') \\ \pi_1(H_1) & \pi_2(P_1\bar{H}_1') \\ \pi_1(\bar{H}_1) & \pi_2(P_1H_1') \\ \pi_1(\bar{H}_1) & \pi_2(P_1\bar{H}_1') \end{bmatrix} \quad \text{или} \quad \pi(C_1) = \begin{bmatrix} \pi_2(P_1H_1') & \pi_1(H_1) \\ \pi_2(P_1\bar{H}_1') & \pi_1(H_1) \\ \pi_2(P_1H_1') & \pi_1(\bar{H}_1) \\ \pi_2(P_1\bar{H}_1') & \pi_1(\bar{H}_1) \end{bmatrix} \tag{18}$$

и

$$C_2 + (\boldsymbol{c}_2, \boldsymbol{c}_2') = \begin{bmatrix} H_2 + \boldsymbol{c}_2 & P_2H_2' + \boldsymbol{c}_2' \\ H_2 + \boldsymbol{c}_2 & P_2\bar{H}_2' + \boldsymbol{c}_2' \\ \bar{H}_2 + \boldsymbol{c}_2 & P_2H_2' + \boldsymbol{c}_2' \\ \bar{H}_2 + \boldsymbol{c}_2 & P_2\bar{H}_2' + \boldsymbol{c}_2' \end{bmatrix} = \begin{bmatrix} H_2 + \boldsymbol{c}_2 & P_2(H_2' + \boldsymbol{c}_2') \\ \overline{H_2 + \boldsymbol{c}_2} & P_2(\overline{H_2' + \boldsymbol{c}_2'}) \\ \overline{H_2 + \boldsymbol{c}_2} & P_2(H_2' + \boldsymbol{c}_2') \\ H_2 + \boldsymbol{c}_2 & P_2(\overline{H_2' + \boldsymbol{c}_2'}) \end{bmatrix}. \tag{19}$$

Сравнивая матрицы (18) с (19), заключаем, что либо матрица H_1 эквивалентна H_2, а H_1' эквивалентна H_2', либо H_1' эквивалентна H_2, а H_1 эквивалентна H_2'. ▲

Пример 8. Пусть $q = 48$ и $m = 2$. Определим две перестановки

$$\tau_1 = (1,2,3,\ldots,23),$$
$$\tau_2 = (1,5)(2,10)(3,15)\ldots(19,23),$$

действующие на множестве $\{0,1,\ldots,23\}$, где $\tau_2(i) = 5i \pmod{24}$ для $i = 0,1,\ldots,23$. Пусть H_2 – код Адамара, рассмотренный в примере 7, а $V_1 = V(\tau_1)$ и $V_2 = V(\tau_2)$ – $(2,24,2)_{24}$-коды над алфавитом $\mathbb{Z}_{24}$, где

$$V_i = V(\tau_i) = \{(0,0), (1,\tau_i(1)), \ldots, (23,\tau_i(23))\}$$

для $i = 1,2$. Пусть $S_H(24)$ – множество из всех 60 попарно неэквивалентных кодов Адамара длины 24, указанных в работе [27] (см. также [28]). По лемме 2 получаем $60^2 = 3600$ попарно неэквивалентных матриц Адамара. Число таких матриц в зависимости от значений ранга и размерности ядра указано в табл. 10. Выбирая максимальные значения для каждого из рангов, получаем не менее 3932 неэквивалентных кодов. Все полученные матрицы имеют тип 0 и размерность ядра 2. Учитывая теперь результаты, приведенные в примерах 5, 6 и 8, получаем не менее $7 + 625 + 3931 = 4563$ неэквивалентных кодов Адамара длины 48.

Пример 9. Пусть $q = 32$ и $m = 2$. Пусть H_2 – код из примера 7, а V – код, соответствующий перестановке $\tau = (1,2,\ldots,15)$. Пусть $S_H(16)$ – множество из пяти неэквивалентных кодов Адамара длины 16. По лемме 2 получаем $5^2 = 25$ неэквивалентных матриц Адамара порядка 32. Если добавить к множеству $S_H(16)$ еще

Таблица 10

Неэквивалентные $(48, 96, 24)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(24))$, полученные с помощью кодов V_1 и V_2

r	k	Число неэквивалентных кодов с использованием V_1	Число неэквивалентных кодов с использованием V_2
13	2	1	1 ($k = 3$)
14	2	0	2
15	2	1	7
16	2	2	14
17	2	7	49
18	2	16	68
19	2	72	245
20	2	208	246
21	2	687	693
22	2	1043	964
23	2	1232	1005
24	2	331	306

Таблица 11

Неэквивалентные $(32, 64, 16)$-коды Адамара $C = \Phi(\mathcal{C}, \boldsymbol{f}, S_H(16))$ с размерностью ядра 2

k	r							
	9	10	11	12	13	14	15	16
2	1	3	7	14	19	23	10	3

четыре нелинейных кода Адамара, к которым применена случайная перестановка $\pi = (2, 9, 8, 4, 3)(12, 14)(13, 15)$, то получим 80 неэквивалентных матриц Адамара. В табл. 11 показано число таких неэквивалентных матриц Адамара с заданными рангом и размерностью ядра. Таким образом получаем коды с параметрами (r, k), помеченными в табл. 2 символом $\diamond$. Поскольку все они имеют размерность ядра 2, они не эквивалентны кодам, рассмотренным в примерах 2 и 3.

§ 6. Связь с модифицированной конструкцией Сильвестра матриц Адамара

Цель данного параграфа – показать связь нашей конструкции с известной в настоящее время модифицированной конструкцией Сильвестра [1], а затем обобщить эту модифицированную конструкцию. Существует очевидное сходство нашей конструкции и кронекеровского произведения (в частности, обе они имеют блочный тип), которое (для построения матриц Адамара) также называется конструкцией Сильвестра, известной уже с 1867 г. Следующее утверждение устанавливает связь нашей конструкции, введенной в теореме 3, с классической конструкцией Сильвестра. Сначала напомним, что под конструкцией Сильвестра для матриц Адамара из исходных матриц Адамара $H_n = [h_{i,j}]$ и H_m мы подразумеваем матрицу вида $H_{mn} = H_n \otimes H_m$, полученную заменой каждого элемента $h_{i,j}$ на матрицу $h_{i,j}H_m$ (очевидно, что в этом случае $h_{i,j} \in \{\pm 1\}$).

Предложение 1. *Предположим, что выполнены условия теоремы* 3. *Если код A_1 состоит из тривиальных векторов вида $(i, \ldots, i)$, где $i \in \{0, 1, \ldots, q/2 - 1\}$, то получаемая матрица $H_{qm/2}$ совпадает с классической конструкцией Сильвестра при использовании матриц $H_{q/2}$ и H_m.*

Доказательство. Обозначим i-ю строку матрицы Адамара $H_{q/2}$ через $\boldsymbol{r}^{(i)}$, а через $H^{(i)}(A_1)$ – подматрицу, образованную $q/2$ строками результирующей матри-

цы Адамара порядка $qm/2$, полученную нашей конструкцией, когда мы выбираем все N_1 кодовых слов кода A_1 при фиксированном кодовом слове кода A_2, а именно i-й строки $\boldsymbol{r}^{(i)}$ кода $H_{q/2}$. Поскольку $\boldsymbol{r}^{(i)} = (h_{i,1}, h_{i,2}, \ldots, h_{i,q/2})$, то соответствующая подматрица $H^{(i)}(A_1)$ имеет следующий вид:

$$H^{(i)}(A_1) = \boldsymbol{r}^{(i)} \otimes H_m = \begin{bmatrix} h_{i,1}H_m & h_{i,2}H_m & \ldots & h_{i,q/2}H_m \end{bmatrix}$$

(действительно, используемый нами код A_1 не меняет порядок строк матрицы H_m). Выпишем подматрицы $H^{(i)}(A_1)$ друг под другом для всех значений $i = 1, 2, 3, 4$:

$$H = \begin{bmatrix} H^{(1)}(A_1) \\ H^{(2)}(A_1) \\ \vdots \\ H^{(q/2)}(A_1) \end{bmatrix}.$$

В результате мы в точности получаем матрицу Адамара H порядка $mq/2$, полученную, как легко заметить, классической конструкцией Сильвестра из матриц $H_{q/2}$ и H_m. ▲

В работе [1] предложен модифицированный метод Сильвестра построения матриц Адамара. Приведем этот результат. Положим для краткости, что под суммой $a + B$ элемента $a \in \{0, 1\}$ и двоичной матрицы $B = [b_{i,j}]$ понимается двоичная матрица $a + B = [b_{i,j} + a]$.

Теорема 5 [1]. *Пусть заданы m матриц Адамара $B_1, B_2, \ldots, B_m$ порядка k (не обязательно попарно различных) и матрица Адамара $C = [c_{i,j}]$ порядка m, где все матрицы определены над $\{0, 1\}$. Тогда матрица*

$$H = \begin{bmatrix} c_{1,1} + B_1 & c_{1,2} + B_2 & \ldots & c_{1,m} + B_m \\ c_{2,1} + B_1 & c_{2,2} + B_2 & \ldots & c_{2,m} + B_m \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ c_{m,1} + B_1 & c_{m,2} + B_2 & \ldots & c_{m,m} + B_m \end{bmatrix}$$

является матрицей Адамара порядка mk.

Следующий иллюстративный пример нашей конструкции показывает, что конструкция теоремы 4 является модифицированной конструкцией Сильвестра, и для случая $s_{q/2} \leqslant m$ совпадает с конструкцией, предложенной в работе [1], представленной в теореме 5.

Пример 10. Пример конструкции для случая $n = 16$, где $q/2 = m = 4$. Пусть $S_H(4) = \{H_4(i) : i = 1, \ldots, 4\}$, где

$$H_4(1) = \{(0,0,0,0), (0,1,0,1), (0,0,1,1), (0,1,1,0)\},$$
$$H_4(2) = \{(0,0,0,0), (1,0,0,1), (1,0,1,0), (0,0,1,1)\},$$
$$H_4(3) = \{(0,0,0,0), (1,1,0,0), (0,1,0,1), (1,0,0,1)\},$$
$$H_4(4) = \{(0,0,0,0), (1,0,1,0), (0,1,1,0), (1,1,0,0)\}.$$

Выберем $\boldsymbol{f} = (1, 2, 3, 4)$, матрицу Адамара H_4 и тривиальный $(4, 4, 4)_4$-код V над алфавитом $\mathbb{Z}_4$:

$$H_4 = \{(0,0,0,0), (0,0,1,1), (0,1,1,0), (0,1,0,1)\},$$
$$V \ = \{(0,0,0,0), (1,1,3,3), (3,2,2,2), (2,3,1,1)\}.$$

Сначала построим $(4,16,4)_8$-код $\mathcal{C}=\Psi(V,H_4)$ над алфавитом $\mathbb{Z}_8$:

$$\mathcal{C}=\begin{Bmatrix}(0,0,0,0), & (1,1,3,3), & (3,2,2,2), & (2,3,1,1),\\ (0,0,4,4), & (1,1,7,7), & (3,2,6,6), & (2,3,5,5),\\ (0,4,4,0), & (1,5,7,3), & (3,6,6,2), & (2,7,5,1),\\ (0,4,0,4), & (1,5,3,7), & (3,6,2,6), & (2,7,1,5)\end{Bmatrix}.$$

Далее получаем следующую результирующую матрицу $H=\Phi(\mathcal{C},S_H(4))$:

```
0000  0000  0000  0000
0101  1001  1001  1100
0110  1010  0101  0110
0011  0011  1100  1010

0000  0000  1111  1111
0101  1001  0110  0011
0110  1010  1010  1001
0011  0011  0011  0101

0000  1111  1111  0000
0101  0110  0110  1100
0110  0101  1010  0110
0011  1100  0011  1010

0000  1111  0000  1111
0101  0110  1001  0011
0110  0101  0101  1001
0011  1100  1100  0101
```

Легко видеть, что эта матрица может быть построена модифицированной конструкцией Сильвестра при выборе в теореме 5 матриц $B_i=H_4(i)$, $i=1,2,3,4$, и матрицы $C=H_4$.

§ 7. Обобщение модифицированной конструкции Сильвестра матриц Адамара

Теперь наша цель – обобщить модифицированную конструкцию Сильвестра, предложенную в [1] и сформулированную выше в теореме 5. Конструкцию, приведенную в теоремах 4 и 5, можно обобщить, вовлекая в такую конструкцию большее число исходных матриц Адамара. Идея такого усиления основана на том, что в обобщенной каскадной конструкции для каждого кодового слова $\boldsymbol{a}^{(i)}$ кода A_i мощности N_i, $i=1,\ldots,s$, можно выбирать кодовые слова $\boldsymbol{b}$ из N_i различных кодов $A_{i+1}(\boldsymbol{a}^{(i)})$, соответствующему кодовому слову $\boldsymbol{a}^{(i)}$, т.е. каждому слову соответствует свой код (см., например, [19] для кодов в метрике Хэмминга). Для случая $s=2$ и метрики Ли получаем следующее утверждение (где для удобства обозначений полагаем $A_i=H_q(i)$, $B_j=H_m(j)$ и $k=q/2$):

Теорема 6. *Пусть заданы два натуральных числа k и m, такие что существуют матрицы Адамара порядка k и m. Пусть заданы два множества (не обязательно различных) матриц Адамара A_i, $i=1,\ldots,m$, и B_j, $j=1,\ldots,k$, порядков k и m соответственно. Тогда для произвольного тривиального $(m,k,m)_k$-кода V и произвольного вектора $\boldsymbol{f}=(f_1,\ldots,f_m)$ длины m над алфавитом $\{1,2,\ldots,m\}$ матрица C, где*

$$C=\Phi(\mathcal{C},\boldsymbol{f},A_1,\ldots,A_m),\quad \mathcal{C}=\Psi(V,B_1,\ldots,B_k), \tag{20}$$

является матрицей Адамара H_{km} порядка km.

Эту теорему мы не будем доказывать, учитывая, что аналогичный результат для метрики Хэмминга известен [19], а докажем соответствующий результат, сформулированный в терминах модифицированной конструкции Сильвестра. т.е. в терминах теоремы 5 из работы [1].

Для произвольного двоичного вектора $\boldsymbol{a}$ и $e \in \{0,1\}$ для краткости будем обозначать

$$\boldsymbol{a} + e = \boldsymbol{a} + e(1,1,\ldots,1).$$

Новая общая конструкция Сильвестра, которая обобщает известную в настоящее время модифицированную конструкцию Сильвестра [1], представлена в следующей теореме.

Теорема 7. *Пусть задано m (не обязательно различных) матриц Адамара $A_1, A_2, \ldots, A_m$ порядка k и k (не обязательно различных) матриц Адамара $B_1, B_2, \ldots, B_k$ порядка m, где все матрицы определены над алфавитом $\{0,1\}$. Пусть $\boldsymbol{a}_i^{(j)}$, $j = 1,2,\ldots,m$, $i = 1,2,\ldots,k$, обозначает строку с номером i матрицы A_j, пусть*

$$B_u = \left[b_{r,s}^{(u)}\right], \quad u = 1,2,\ldots,k, \quad r,s = 1,2,\ldots,m,$$

и пусть $\boldsymbol{b}_r^{(u)}$ обозначает строку с номером r матрицы B_u. Тогда матрица H

$$H = \left[\begin{array}{cccc}
\boldsymbol{a}_1^{(1)} + b_{1,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{1,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{1,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{1,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{1,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{1,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{1,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{1,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{1,m}^{(k)} \\
\hline
\boldsymbol{a}_1^{(1)} + b_{2,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{2,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{2,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{2,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{2,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{2,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{2,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{2,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{2,m}^{(k)} \\
\hline
\ldots & \ldots & \ldots & \ldots \\
\hline
\boldsymbol{a}_1^{(1)} + b_{m,1}^{(1)} & \boldsymbol{a}_1^{(2)} + b_{m,2}^{(1)} & \ldots & \boldsymbol{a}_1^{(m)} + b_{m,m}^{(1)} \\
\boldsymbol{a}_2^{(1)} + b_{m,1}^{(2)} & \boldsymbol{a}_2^{(2)} + b_{m,2}^{(2)} & \ldots & \boldsymbol{a}_2^{(m)} + b_{m,m}^{(2)} \\
\ldots & \ldots & \ldots & \ldots \\
\boldsymbol{a}_k^{(1)} + b_{m,1}^{(k)} & \boldsymbol{a}_k^{(2)} + b_{m,2}^{(k)} & \ldots & \boldsymbol{a}_k^{(m)} + b_{m,m}^{(k)}
\end{array}\right]$$

является матрицей Адамара порядка mk.

Приведем независимое доказательство этого результата в обозначениях теоремы 7.

Доказательство. Пусть $\boldsymbol{h}_{i_1}$ и $\boldsymbol{h}_{i_2}$ – две различные строки матрицы H. Следует рассмотреть три различных случая.

(i) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{h}_{i_2}$ принадлежат одной и той же i-й полосе матрицы H, образованной векторами $\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}$ и $\boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}$, где $j, j' = 1,2,\ldots,k$ и $i, u = 1,2,\ldots,m$, т.е. $i = i'$ и $j \neq j'$. Так как

$$d(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}) = d(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}),$$

для любых (т.е. равных или неравных) элементов $b_{i,u}^{(j)}$ и $b_{i,u}^{(j')}$, то получаем для этого случая

$$d(\boldsymbol{h}_{i_1}\boldsymbol{h}_{i_2}) = \sum_{u=1}^{m} d(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i,u}^{(j')}) = m \times \sum_{u=1}^{m} d(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}) =$$
$$= m \times \frac{k}{2} = \frac{mk}{2},$$

поскольку $j \neq j'$.

(ii) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{b}_{i_2}$ принадлежат разным i-й и i'-й полосам, соответственно, матрицы H, но имеют одинаковые номера строк $\boldsymbol{a}_j^{(u)}$ и $\boldsymbol{a}_{j'}^{(u)}$ внутри этих полос, т.е. $i \neq i'$ и $j = j'$. Принимая во внимание, что $\boldsymbol{a}_j^{(u)} = \boldsymbol{a}_{j'}^{(u)}$, получаем в этом случае

$$d(\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}) = \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_j^{(u)} + b_{i',u}^{(j)}\big) = k \times \sum_{u=1}^{m} d\big(b_{i,u}^{(j)}, b_{i',u}^{(j)}\big) =$$
$$= k \times d\big(\boldsymbol{b}_i^{(j)}, \boldsymbol{b}_{i'}^{(j)}\big) = k \times \frac{m}{2} = \frac{km}{2}.$$

(iii) Обе строки $\boldsymbol{h}_{i_1}$ и $\boldsymbol{b}_{i_2}$ принадлежат разным i-й и i'-й полосам, соответственно, матрицы H, и имеют разные номера строк $\boldsymbol{a}_j^{(u)}$ и $\boldsymbol{a}_{j'}^{(u)}$ внутри этих полос, т.е. $i \neq i'$ и $j \neq j'$. Тогда

$$d(\boldsymbol{h}_{i_1}, \boldsymbol{b}_{i_2}) = \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i',u}^{(j')}\big) = m \times \sum_{u=1}^{m} d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big) =$$
$$= m \times \frac{k}{2} = \frac{mk}{2}.$$

Действительно, второе равенство имеет место, поскольку для произвольных различных j и j' выполнено равенство

$$d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)} + (1, 1, \ldots, 1)\big) = d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big),$$

из которого следует, что

$$d\big(\boldsymbol{a}_j^{(u)} + b_{i,u}^{(j)}, \boldsymbol{a}_{j'}^{(u)} + b_{i',u}^{(j')}\big) = d\big(\boldsymbol{a}_j^{(u)}, \boldsymbol{a}_{j'}^{(u)}\big). \quad \blacktriangle$$

Проиллюстрируем новую конструкцию минимальным нетривиальным примером. Приведенное выше в примере 10 построение матрицы Адамара порядка 16 модифицированной конструкцией Сильвестра может быть обобщено следующим образом.

Пример 11. Пусть $q = m = 4$, и пусть $A_i = H_4(i)$ (как в примере 10), $i = 1, 2, 3, 4$. Пусть задан тривиальный код

$$V = \{(0,0,0,0), (1,1,1,1), (2,2,2,2), (3,3,3,3)\} \tag{21}$$

(отличный от кода в примере 10), и выберем следующие матрицы B_j, $j = 1, 2, 3, 4$:

$B_1 = \{(0,0,0,0), (0,0,1,1), (0,1,1,0), (0,1,0,1)\}$,
$B_2 = \{(0,0,0,0), (1,0,1,0), (1,0,0,1), (0,0,1,1)\}$,
$B_3 = \{(0,0,0,0), (1,1,0,0), (1,0,0,1), (0,1,0,1)\}$,
$B_4 = \{(0,0,0,0), (1,0,1,0), (1,1,0,0), (0,1,1,0)\}$.

Используя код V и матрицы B_1, B_2, B_3, B_4, сначала построим $(4, 16, 4)_8$-код $\mathcal{C} = \Psi(V, B_1, B_2, B_3, B_4)$ над алфавитом $\mathbb{Z}_8$:

$$\mathcal{C} = \begin{Bmatrix} (0,0,0,0), & (1,1,1,1), & (2,2,2,2), & (3,3,1,1), \\ (0,0,4,4), & (5,1,5,1), & (6,6,2,2), & (7,3,7,3), \\ (0,4,4,0), & (5,1,1,5), & (6,2,2,6), & (7,7,3,3), \\ (0,4,0,4), & (1,1,5,5), & (6,2,2,6), & (3,7,7,3) \end{Bmatrix}.$$

Пользуясь нашим отображением (для j-го столбца матрицы $\mathcal{C}$ мы используем код A_j), из кода $\mathcal{C}$ получаем результирующую матрицу Адамара H_{16}. Заметим, что поскольку у всех матриц B_i первая строка нулевая, первая полоса из k строк H_{16} состоит из m матриц $A_1, \ldots, A_m$. Таким образом, матрица H_{16} имеет следующий вид:

```
0000  0000  0000  0000
0101  1001  1100  1010
0011  1010  0101  0110
0110  0011  1001  1100

0000  0000  1111  1111
1010  1001  0011  1010
1100  0101  0101  0110
1001  0011  0110  1100

0000  1111  1111  0000
1010  1001  1100  0101
1100  1010  0101  1001
1001  1100  1001  1100

0000  1111  0000  1111
0101  1001  0011  0101
0011  0101  0101  1001
0110  1100  0110  1100
```

Результирующая матрица Адамара H_{16} нелинейна, хотя соответствующий код Адамара линеен. Легко убедится, что построенная матрица Адамара не может быть получена конструкцией, представленной в теореме 4 при использовании тривиального кода V, заданного в (21).

В заключение мы хотим отметить, что наша конструкция дает два независимых результата: (i) конструкцию q-ичных кодов в метрике Ли (дающие двоичные матрицы Адамара после применения отображения Грея) (ii) построение матриц Адамара с различными рангами и размерностью ядер.

Авторы выражают глубокую благодарность рецензенту, указавшему им на связь с обобщенной конструкцией Сильвестра и на соответствующую работу [1], в которой приведено такое обобщение.

СПИСОК ЛИТЕРАТУРЫ

1. *No J.-S., Song H.-Y.* Generalized Sylvester-Type Hadamard Matrices // Proc. 2000 IEEE Int. Symp. on Information Theory (ISIT'2000). Sorrento, Italy. June 25–30, 2000. P. 472. https://doi.org/10.1109/ISIT.2000.866770
2. *Hammons A.R., Jr., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319. https://doi.org/10.1109/18.312154
3. *Carlet C.* $\mathbb{Z}_{2^k}$-Linear Codes // IEEE Trans. Inform. Theory. 1998. V. 44. № 4. P. 1543–1547. https://doi.org/10.1109/18.681328

4. *Fernández C., Rifà J., Borges J.* Every $\mathbb{Z}_{2k}$-Code is a Binary Propelinear Code // Electron. Notes Discrete Math. 2001. V. 10. P. 100–102. https://doi.org/10.1016/S1571-0653(04)00370-1
5. *Dougherty S.T., Fernández-Córdoba C.* Codes over $\mathbb{Z}_{2^k}$, Gray Map and Self-Dual Codes // Adv. Math. Commun. 2011. V. 5. № 4. P. 571–588. https://doi.org/10.3934/amc.2011.5.571
6. *Krotov D.S.* On $\mathbb{Z}_{2^k}$-Dual Binary Codes // IEEE Trans. Inform. Theory. 2007. V. 53. № 4. P. 1532–1537. https://doi.org/10.1109/TIT.2007.892787
7. *Fernández-Córdoba C., Vela C., Villanueva M.* On $\mathbb{Z}_{2^s}$-Linear Hadamard Codes: Kernel and Partial Classification // Des. Codes Cryptogr. 2019. V. 87. № 2–3. P. 417–435. https://doi.org/10.1007/s10623-018-0546-6
8. *Bauer H., Ganter B., Hergert F.* Algebraic Techniques for Nonlinear Codes // Combinatorica. 1983. V. 3. № 1. P. 21–33. https://doi.org/10.1007/BF02579339
9. *Assmus E.F., Jr., Key J.D.* Designs and Their Codes. Cambridge, UK: Cambridge Univ. Press, 1992.
10. *Kimura H.* Classfication of Hadamard Matrices of Order 28 // Discrete Math. 1994. V. 133. № 1–3. P. 171–180. https://doi.org/10.1016/0012-365X(94)90024-8
11. *Kharaghani H., Tayfeh-Rezaie B.* On the Classification of Hadamard Matrices of Order 32 // J. Combin. Des. 2010. V. 18. № 5. P. 328–336. https://doi.org/10.1002/jcd.20245
12. *Kharaghani H., Tayfeh-Rezaie B.* Hadamard Matrices of Order 32 // J. Combin. Des. 2013. V. 21. № 5. P. 212–221. https://doi.org/10.1002/jcd.21323
13. *Fernández-Córdoba C., Vela C., Villanueva M.* On $\mathbb{Z}_8$-Linear Hadamard Codes: Rank and Classification // IEEE Trans. Inform. Theory. 2020. V. 66. № 2. P. 970–982. https://doi.org/10.1109/TIT.2019.2952599
14. *Fernández-Córdoba C., Vela C., Villanueva M.* Equivalences among $\mathbb{Z}_{2^s}$-Linear Hadamard Codes // Discrete Math. 2020. V. 343. № 3. Art. 111721 (13 pp.). https://doi.org/10.1016/j.disc.2019.111721
15. *Phelps K.T., Rifà J., Villanueva M.* Rank and Kernel of Binary Hadamard Codes // IEEE Trans. Inform. Theory. 2005. V. 51. № 11. P. 3931–3937. https://doi.org/10.1109/TIT.2005.856940
16. *Phelps K.T., Rifà J., Villanueva M.* Hadamard Codes of Length $2^t s$ (s Odd). Rank and Kernel // Proc. 16th Int. Symp. on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-16). Las Vegas, NV, USA. Feb. 20–24, 2006. Lect. Notes Comput. Sci. V. 3857. Berlin: Springer, 2006. P. 328–337. https://doi.org/10.1007/11617983_32
17. *Зиновьев В.А.* Обобщенные каскадные коды // Пробл. передачи информ. 1976. Т. 12. № 1. С. 5–15. http://mi.mathnet.ru/ppi1670
18. *Ericson T., Zinoviev V.* Spherical Codes Generated by Binary Partitions of Symmetric Pointsets // IEEE Trans. Inform. Theory. 1995. V. 41. № 1. P. 107–129. https://doi.org/10.1109/18.370114
19. *Зиновьев В.А., Зиновьев Д.В.* Структура систем троек Штейнера $S(2^m-1,3,2)$ ранга 2^m-m+2 над $\mathbb{F}_2$ // Пробл. передачи информ. 2013. Т. 49. № 3. С. 40–56. http://mi.mathnet.ru/ppi2115
20. *Zinoviev D.V., Zinoviev V.A.* On Generalized Concatenated Construction of Codes in Metrics Lee L and L_1 // Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2018). Svetlogorsk, Kaliningrad region, Russia. Sept. 2–8, 2018. P. 62–65. Available at https://www.dropbox.com/s/h7u89lh8vyirww9.
21. *Зиновьев В.А., Зиновьев Д.В.* Об обобщенной каскадной конструкции кодов в модульной метрике и метрике Ли // Пробл. передачи информ. 2021. Т. 57. № 1. С. 81–95. https://doi.org/10.31857/S0555292321010046
22. *Krotov D.S., Villanueva M.* Classification of the $\mathbb{Z}_2\mathbb{Z}_4$-Linear Hadamard Codes and Their Automorphism Groups // IEEE Trans. Inform. Theory. 2015. V. 61. № 2. P. 887–894. https://doi.org/10.1109/TIT.2014.2379644
23. Handbook of Magma Functions / Bosma W., Cannon J.J., Fieker C., Steel A. (Eds.) Edition 2.26-4, 2021. Available at http://magma.maths.usyd.edu.au/magma/handbook/

24. *Todd J.A.* A Combinatorial Problem // J. Math. Phys. Camb. 1933. V. 12. № 1–4. P. 321–333. https://doi.org/10.1002/sapm1933121321
25. *Hall M., Jr.* Hadamard Matrices of Order 16 // JPL Research Summary № 36-10.1. 1961. P. 21–26.
26. *Hall M., Jr.* Hadamard Matrices of Order 20 // JPL Tech. Rep. № 32-761. 1965.
27. *Kimura H.* New Hadamard Matrix of Order 24 // Graphs Combin. 1989. V. 5. P. 235–242. https://doi.org/10.1007/BF01788676
28. A Library of Hadamard Matrices (online library; maintained by Sloane N.J.A.). http://neilsloane.com/hadamard/

Вильянуэва Мерсе (Villanueva, Mercè)
Независимый университет Барселоны, Беллатерра, Испания
merce.villanueva@uab.cat
Зиновьев Виктор Александрович
Зиновьев Дмитрий Викторович
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
vazinov@iitp.ru
dzinov@iitp.ru

Поступила в редакцию
07.04.2022
После доработки
18.10.2022
Принята к публикации
18.10.2022