

УДК 621.391:519.725

© 2024 г. Ж. Рифа¹, М. Вильянуэва¹, В.А. Зиновьев², Д.В. Зиновьев²О КРОНЕКЕРОВСКОЙ КОНСТРУКЦИИ РЕГУЛЯРНЫХ
МАТРИЦ АДАМАРА И БЕНТ-ФУНКЦИЙ

Классическая кронекеровская конструкция применяется для построения новых матриц Адамара с новыми значениями ранга и размерности ядра. В частности, по двум матрицам Адамара H_1 и H_2 порядка n наша новая конструкция дает матрицу Адамара H порядка n^2 . Если одна из исходных матриц Адамара линейна (т.е. строки матрицы, представленные в двоичном виде, замкнуты относительно их покомпонентного сложения), то получающаяся матрица Адамара H сводится к регулярной матрице, когда все строки имеют один и тот же вес, равный $n^2/2 - n/2$ (при двоичном $(0, 1)$ -представлении получившейся матрицы Адамара H). В частности, таким способом мы получаем бент-функции, т.е. строки полученной матрицы Адамара H являются бент-функциями. Построены матрицы Адамара, в которых каждая строка и каждый столбец являются бент-функцией.

Ключевые слова: матрица Адамара, конструкция Кронекера, размерность ядра, схема Менона, ранг, регулярная матрица Адамара, бент-функция.

DOI: 10.31857/S0555292324040016, EDN: LGMDZT

§ 1. Введение

Пусть $v > k > \lambda \geq 0$ – натуральные числа. Симметричная (v, k, λ) -схема – это структура инцидентности (X, B) , где $X = \{x_1, \dots, x_v\}$ – множество из v элементов, а $B = \{B_1, \dots, B_v\}$ – семейство k -подмножеств множества X (называемых блоками), таких что любые два различных элемента x_i, x_j встречаются вместе ровно в λ блоках из семейства B . Такую схему можно описать ее матрицей инцидентности, а именно двоичной матрицей $A = [a_{i,j}]$ порядка v , где $a_{i,j} = 1$ тогда и только тогда, когда $x_i \in B_j$.

Матрица Адамара H порядка n – это $(n \times n)$ -матрица из элементов $+1$ и -1 , такая что

$$HH^t = nI_n,$$

где I_n – двоичная диагональная матрица порядка n , а H^t – транспонированная матрица H . Хорошо известно, что порядок n матрицы Адамара H равен 1, 2 или $4m$ для любого натурального числа m [1]. Две матрицы Адамара эквивалентны, если одна может быть получена из другой перестановкой строк и/или столбцов и умножением строк и/или столбцов на -1 . Используя эти операции, матрицу Адамара

¹ Исследования выполнены при частичной поддержке Национального гранта правительства Испании PID2022-137924NB-I00 (AEI 10.13039/501100011033), а также гранта правительства Каталонии (SGR 2021-00643).

² Исследования выполнены в ИППИ им. А.А. Харкевича РАН в рамках проводимых фундаментальных исследований по теме “Математические основы теории корректирующих кодов”.

всегда можно представить в *нормализованном* виде, где первая строка и первый столбец содержат только единицы. Будем говорить, что матрица Адамара *нормализована по строкам*, если первая строка содержит только единицы, и *нормализована по столбцам*, если первый столбец содержит только единицы.

Для двух заданных матриц $A = [a_{r,s}]$ и $B = [b_{i,j}]$ над одним и тем же кольцом без делителей нуля определим новую матрицу H , являющуюся *кронекеровым* (или *прямым*) *произведением* $H = A \otimes B$, где H получена заменой любого элемента $a_{r,s}$ матрицы A на матрицу $a_{r,s}B$. Самое первое известное семейство матриц Адамара, полученное Сильвестром, состоит из матриц порядка 2^n , где $n \geq 1$. Эти матрицы, называемые *сильвестровыми матрицами Адамара*, строятся с помощью кронекеровского произведения $\otimes^n(S_1)$, т.е. итерацией тензорного произведения матрицы

$$S_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

на самую себя.

Если все элементы $+1$ матрицы H заменить элементом 0 , а элементы -1 заменить элементом 1 , то получим *двоичную* $(0, 1)$ -*матрицу Адамара*, которую будем обозначать через H_b . Так как любые две строки совпадают в $n/2$ позициях и различны в $n/2$ позициях, легко видеть, что эти две строки находятся на расстоянии Хэмминга $n/2$ друг от друга. Двоичный $(n, 2n, n/2)$ -код, состоящий из строк двоичной матрицы Адамара порядка n и дополнительных к ним строк, называется (*двоичным*) *кодом Адамара*. Если матрица Адамара линейна, то соответствующий двоичный код Адамара представляет собой хорошо известный код Рида–Маллера первого порядка $R(1, n)$ длины $n = 2^m$ и размерности $m + 1$.

Булева функция f – это отображение из двоичного пространства $\mathbb{Z}_2^m$ всех двоичных векторов длины m в кольцо $\mathbb{Z}_2$. Степень нелинейности булевой функции f определяется как минимальное расстояние Хэмминга между f и всеми аффинными функциями пространства $\mathbb{Z}_2^m$. Другими словами, это ее расстояние до кода Рида–Маллера первого порядка. Это расстояние ограничено сверху величиной

$$2^{m-1} - 2^{\frac{m}{2}-1},$$

причем в случае равенства (которое возможно только для четного m) функция называется *бент-функцией*. Одним из важных классов бент-функций является класс Майораны – Мак-Фарланда, введенный в [2] и представляющий собой булевы функции $f(x, y)$ от $2m$ переменных вида

$$f(x, y) = \langle x, \pi(y) \rangle + h(y) \quad \text{для любых } x, y \in \mathbb{Z}_2^m, \quad (1)$$

где π – произвольная перестановка на множестве $\mathbb{Z}_2^m$, а h – произвольная булева функция от m переменных.

Двумя важными параметрами двоичных кодов являются ранг и размерность ядра. *Ранг* двоичного кода C , обозначаемый $\text{rank}(C)$, представляет собой размерность линейной оболочки $\langle C \rangle$, образованной кодовыми словами кода C . *Ядро* $K(C)$ двоичного кода C длины n определяется как

$$K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}.$$

Если код C содержит нулевой вектор, то ядро $K(C)$ является линейным подкодом кода C . Легко видеть, что если C линейен, то ядро совпадает с кодом:

$$K(C) = C = \langle C \rangle.$$

Обозначим через $\ker(C)$ размерность ядра кода C . Два этих параметра могут быть использованы для выяснения эквивалентности различных матриц Адамара или соответствующих кодов (см., например, [3]).

Хорошо известно, что нормализованная двоичная матрица Адамара порядка $4m$ существует тогда и только тогда, когда существует симметричная $(4m - 1, 2m - 1, m - 1)$ -схема [4]. Однако в дальнейшем мы будем рассматривать другой тип (v, k, λ) -схем, также связанных с матрицами Адамара. Будем говорить, что матрица Адамара порядка n *регулярна по строкам* (соответственно, *регулярна по столбцам*), если сумма элементов каждой строки (соответственно, каждого столбца) одна и та же для всех строк (соответственно, всех столбцов). Кроме того, будем говорить, что матрица Адамара порядка n *регулярна*, если сумма элементов каждой строки и каждого столбца одна и та же для всех ее строк и столбцов [1].

Хорошо известно, что регулярная двоичная матрица Адамара порядка v является матрицей инцидентности симметричной $(v^2, v^2/2 - v/2, v^2/4 - v/2)$ -схемы, обычно называемой *схемой Менона* [5]. И наоборот, матрица инцидентности симметричной $(v^2, v^2/2 - v/2, v^2/4 - v/2)$ -схемы представляет собой двоичную регулярную матрицу Адамара порядка v^2 . Нетрудно видеть (и также хорошо известно), что матрица инцидентности симметричной (v, k, λ) -схемы при условии ортогональности $v = 4(k - \lambda)$ является двоичной регулярной матрицей Адамара порядка v , где v представляет собой полный квадрат.

Следующие две леммы относятся к регулярным матрицам Адамара. Первая из них представляет собой вариант хорошо известного результата Райзера [6], связанного с симметричными блок-схемами. Вторая лемма представляет собой важный результат о величине ядра любой двоичной регулярной матрицы Адамара.

Лемма 1. *Матрица Адамара, регулярная по строкам, регулярна, и ее порядок равен v^2 , где v – сумма элементов строки или столбца.*

Доказательство. Пусть H – регулярная по строкам матрица Адамара порядка n , и предположим, что сумма каждой строки равна v . Следовательно, $H\mathbf{u} = v\mathbf{u}$, где $\mathbf{u}$ – вектор из всех единиц. Тогда получаем

$$H^t H \mathbf{u} = v H^t \mathbf{u},$$

и так как H – матрица Адамара, то $n\mathbf{u} = v H^t \mathbf{u}$. Поэтому получаем

$$H^t \mathbf{u} = \frac{n}{v} \mathbf{u}.$$

Следовательно, все столбцы имеют одну и ту же сумму, равную $\frac{n}{v}$. Так как общая сумма всех элементов матрицы H совпадает с аналогичной суммой для матрицы H^t , получаем, что $n \frac{n}{v} = nv$, или $\frac{n}{v} = v$ (т.е. $n = v^2$). Это доказывает, что суммы по столбцам равны суммам по строкам, и поэтому матрица H регулярна. Мы также получили, что эта постоянная сумма v удовлетворяет условию $v^2 = n$. ▲

Лемма 2. *Ядро двоичной регулярной матрицы Адамара порядка v^2 содержит только нулевой вектор.*

Доказательство. Пусть H – двоичная регулярная матрица Адамара порядка n . Предположим, что $\mathbf{x}$ – ненулевая строка матрицы H , т.е. двоичный вектор длины $v^2 = n$, такой что $H + \mathbf{x} = H$. Это означает, что для любого вектора-строки матрицы H , скажем, $\mathbf{r}_1$, имеем $\mathbf{r}_1 + \mathbf{x} = \mathbf{r}_2$, где $\mathbf{r}_2$ – также вектор-строка матрицы H . Векторы $\mathbf{r}_1$ и $\mathbf{r}_2$ отличаются в $n/2$ позициях, следовательно, вес вектора $\mathbf{x}$ равен $n/2$. Зафиксируем любую ненулевую позицию вектора $\mathbf{x}$. Если прибавить $\mathbf{x}$ ко всем строкам матрицы H , мы получим в этой фиксированной позиции (где $\mathbf{x}$

имеет ненулевую позицию) столбец $\mathbf{h}$ матрицы $H + \mathbf{x}$ одного из двух весов:

$$n/2 + \sqrt{n}/2 \quad \text{или} \quad n/2 - \sqrt{n}/2.$$

Так как $\text{wt}(\mathbf{h}) \neq n - \text{wt}(\mathbf{h})$, эта операция меняет число единиц матрицы H в этом столбце. Прибавление же нулевых позиций вектора $\mathbf{x}$ не меняет числа единиц в соответствующем столбце. Так как $\text{wt}(\mathbf{x}) = n/2$, заключаем, что число единиц в матрицах H и $H + \mathbf{x}$ различно, откуда следует, что $\mathbf{x}$ – нулевой вектор. $\blacktriangle$

В 1962 г. Менон [5] построил класс симметричных блок схем с параметрами

$$(2^{2m}, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1})$$

с помощью разностных множеств в абелевых группах, что непосредственно приводит к бент-функциям. В работе [7] эта конструкция была изучена в терминах полностью регулярных кодов, причем в ней был построен еще один класс таких функций. Затем идеи этой конструкции были перенесены на бент-функции в [8], где было получено очень простое описание всех симметричных квадратичных бент-функций. Симметричные ортогональные схемы (или регулярные матрицы Адамара) являются предметом активных исследований в течение более 50 лет (см. работу [1] и библиографию в ней).

Мейснер [9] предложил весьма общую конструкцию регулярных матриц Адамара, основанную на кронекеровском произведении. В качестве исходных матриц он использовал a^2 матриц Адамара порядка v и $2a$ матриц Адамара порядка a . При некоторых условиях на исходные матрицы получаемая матрица оказывается регулярной матрицей Адамара порядка a^2v . В частности, его конструкция дает симметричные и кососимметричные регулярные матрицы Адамара.

Цель настоящей статьи – описать общую конструкцию регулярных матриц Адамара и бент-функций. Наша конструкция представляет собой вариант конструкции Кронекера. В отличие от конструкции Мейснера в [9], наша конструкция фактически основана на четырех различных исходных матрицах порядка ν и ν^2 , а именно на двух произвольных матрицах Адамара одинакового порядка ν , специальной двоичной перестановочной матрице порядка ν^2 и произвольном векторе длины ν^2 с элементами ± 1 . Получаемая матрица L всегда является матрицей Адамара порядка ν^2 (теорема 1). Если одна из исходных матриц линейна, то получаемая матрица L является регулярной, а в случае, когда эта исходная матрица является силвестровой матрицей Адамара, в получаемой матрице L каждая строка или каждый столбец (в зависимости от использования исходных матриц Адамара, т.е. от того, какая из этих матриц линейна) является бент-функцией (теорема 2).

В случае, когда обе начальные матрицы Адамара линейны и нормализованы, можно получить верхнюю границу на ранг получаемой двоичной матрицы Адамара L_b и гарантировать существование бент-функций максимальной алгебраической степени (теорема 3). В § 3 даны две явные конструкции, для которых почти во всех случаях мы знаем алгебраическую степень бент-функций и ранг получаемой матрицы Адамара. Используя конструкцию, приведенную в п. 3.2, мы получаем регулярные матрицы Адамара, в которых каждая строка и каждый столбец является бент-функцией (теорема 4).

§ 2. Матрицы Адамара порядка ν^2

Начнем с рассмотрения перестановок, имеющих некоторые специфические свойства, позволяющие нам получать бент-функции в каждой строке матрицы Адамара, задаваемой формулой (8).

Пусть $L = [\ell_{i,j}]$ – квадратная матрица порядка ν^2 . Перенумеруем ее строки и столбцы парами чисел из алфавита $\{1, \dots, \nu\}$. В этих обозначениях произвольный

элемент L имеет номер

$$\ell_{(a-1)\nu+x, (b-1)\nu+y} = \ell_{(a,x), (b,y)}, \quad 1 \leq a, x, b, y \leq \nu. \quad (2)$$

Назовем *блоком* с номером (a, b) подматрицу матрицы L , образованную элементами вида (2), где числа a и b фиксированы. Элемент $\ell_{(a,x), (b,y)}$ матрицы L называется элементом (x, y) блока (a, b) .

Определение 1. Назовем c -перестановкой (блоковой перестановкой) перестановочную матрицу $P^{(c)}$ порядка ν^2 , содержащую в каждом блоке ровно один ненулевой элемент 1.

Латинским квадратом порядка ν называется $(\nu \times \nu)$ -матрица P , элементами которой являются ν разных чисел $1, 2, \dots, \nu$, так что каждое число встречается по одному разу в каждой строке и в каждом столбце этой матрицы. Два латинских квадрата $P = [p_{ij}]$ и $Q = [q_{ij}]$ порядка ν ортогональны, если упорядоченная пара чисел (p_{ij}, q_{ij}) встречается ровно один раз, когда i, j пробегает все значения из множества $\{1, \dots, \nu\}$.

Чтобы работать с блоковыми перестановками, удобно использовать двоичные квадратные матрицы порядка ν только с одним ненулевым элементом. Обозначим через $Z_{i,j}$ такую матрицу с одним ненулевым элементом 1 в позиции (i, j) . Обозначим через σ произвольное отображение множества $\{Z_{i,j}\}$ в себя. В этих обозначениях c -перестановку $P^{(c)}$ можно представить в следующем виде:

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}).$$

Определение 2. Назовем lc -перестановкой (латинско-блоковой перестановкой) блоковую перестановочную матрицу $P^{(c)}$ порядка ν^2 следующего вида:

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}), \quad (3)$$

где σ – отображение множества $\{Z_{i,j}\}$ в себя, такое что для каждого индекса $i \in \{1, \dots, \nu\}$ матрица $\sum_{j=1}^{\nu} \sigma(Z_{i,j})$ является перестановочной.

Перед тем как рассматривать дальнейшие результаты, напомним некоторые известные факты о кронекеровском произведении. Пусть A, B, C, D – матрицы над одним и тем же кольцом без делителей нуля, такие что имеют смысл произведения матриц (AB) и (CD) . Тогда имеют место следующие равенства:

$$(AB) \otimes (CD) = (A \otimes C)(B \otimes D). \quad (4)$$

Если A и B – квадратные матрицы порядка ν , то имеет место следующее равенство:

$$A \otimes B = K_{\nu^2}(B \otimes A)K_{\nu^2}, \quad (5)$$

где K_{ν^2} – перестановочная матрица, обычно называемая *коммутационной матрицей* порядка ν^2 [10] и определяемая как

$$K_{\nu^2} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes Z_{i,j}^t. \quad (6)$$

Лемма 3. Пусть

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j})$$

– lc -перестановочная матрица порядка ν^2 , σ – соответствующее отображение из множества $\{Z_{i,j}\}$ в себя, а K_{ν^2} – коммутационная матрица порядка ν^2 , где $\nu \geq 4$. Тогда матрица $P^{(c)}K_{\nu^2}$ является lc -перестановочной.

Доказательство. Из соотношений (3)–(6) следует, что

$$\begin{aligned} P^{(c)}K_{\nu^2} &= \left(\sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}) \right) \left(\sum_{k,s=1}^{\nu} Z_{k,s} \otimes Z_{k,s}^t \right) = \\ &= \sum_{i,j,k,s=1}^{\nu} Z_{i,j} Z_{k,s} \otimes \sigma(Z_{i,j}) Z_{k,s}^t. \end{aligned}$$

Матрица $Z_{i,j}Z_{k,s}$ всегда нулевая, кроме случая, когда $k = j$. Следовательно,

$$Z_{i,j}Z_{k,s} = \delta_{kj}Z_{i,s},$$

где $\delta_{kj} = 1$, если $k = j$, и $\delta_{kj} = 0$ в остальных случаях. Таким образом,

$$P^{(c)}K_{\nu^2} = \sum_{i,j,s=1}^{\nu} Z_{i,s} \otimes \sigma(Z_{i,j})Z_{j,s}^t = \sum_{i,s=1}^{\nu} Z_{i,s} \otimes \left(\sum_{j=1}^{\nu} \sigma(Z_{i,j})Z_{j,s} \right).$$

Так как $P^{(c)}$ является lc -перестановочной матрицей, то для любого индекса $i \in \{1, \dots, \nu\}$ матрица $\sum_{j=1}^{\nu} \sigma(Z_{i,j})$ является перестановочной. Заметим, что $\sum_{j=1}^{\nu} \sigma(Z_{i,j})$ будет перестановочной матрицей, если и только если $\sigma(Z_{i,j}) = Z_{\alpha_j, \beta_j}$, где оба элемента α_j и β_j покрывают весь диапазон $\{1, \dots, \nu\}$, когда $j \in \{1, \dots, \nu\}$.

Для $j \in \{1, \dots, \nu\}$ произведение $\sigma(Z_{i,j})Z_{j,s}$ всегда равно нулю, кроме случая, когда индекс $\sigma(Z_{i,j})$ имеет вид $Z_{x,s}$ для некоторого индекса x , который всегда существует, так как по определению lc -перестановки сумма $\sum_{j=1}^{\nu} \sigma(Z_{i,j})$ является перестановочной матрицей. Это означает, что существует некоторое значение индекса j , скажем, y , такое что

$$\sum_{j=1}^{\nu} \sigma(Z_{i,j})Z_{j,s} = Z_{x,y}.$$

Тем самым, можно определить отображение

$$\sigma'(Z_{i,s}) = Z_{x,y}.$$

Таким образом, получаем, что

$$P^{(c)}K_{\nu^2} = \sum_{i,s=1}^{\nu} Z_{i,s} \otimes \sigma'(Z_{i,s}).$$

В силу определения 2, чтобы доказать, что $P^{(c)}K_{\nu^2}$ является lc -перестановочной, нужно проверить, что для любого индекса $i \in \{1, \dots, \nu\}$ матрица $\sum_{s=1}^{\nu} \sigma'(Z_{i,s})$

представляет собой перестановочную матрицу. Еще раз перепишем

$$\sum_{s=1}^{\nu} \sigma'(Z_{i,s}) = \sum_{s,j=1}^{\nu} \sigma(Z_{i,j}) Z_{s,j} = \sum_{j=1}^{\nu} \left(\sigma(Z_{i,j}) \left(\sum_{s=1}^{\nu} Z_{s,j} \right) \right) = \sum_{j=1}^{\nu} \sigma(Z_{i,j}) M_j,$$

где M_j – матрица, имеющая единицы только в j -м столбце и нули в остальных.

Следовательно, справедливо равенство

$$\sum_{s=1}^{\nu} \sigma'(Z_{i,s}) = \sum_{j=1}^{\nu} (Z_{\alpha_j, \beta_j} M_j) = \sum_{j=1}^{\nu} Z_{\alpha_j, j}.$$

Теперь ясно, что оба индекса α_j и j покрывают весь диапазон $\{1, \dots, \nu\}$, когда $j \in \{1, \dots, \nu\}$. $\blacktriangle$

Пусть $\mathbf{c} = (c_1, c_2, \dots, c_{\nu^2})$ – вектор длины ν^2 с элементами ± 1 . Этот вектор $\mathbf{c}$ можно представить в блоковом виде $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_{\nu})$, где каждый блок $\mathbf{c}_k$, $k = 1, \dots, \nu$, имеет длину ν . Назовем такой вектор $\mathbf{c}$ *блочно-постоянным*, если он имеет постоянное значение на всех позициях каждого блока $\mathbf{c}_i$, т.е. блок $\mathbf{c}_i$ имеет вид $\mathbf{c}_i = c_i(11 \dots 11)$, где $c_i \in \{\pm 1\}$. Следующее утверждение тривиально.

Лемма 4. Пусть $\mathbf{c}$ – блочно-постоянный ± 1 -вектор длины ν^2 , а M – матрица порядка $\nu \geq 4$. Тогда

$$\text{diag}(\mathbf{c}) (I_{\nu} \otimes M) = (I_{\nu} \otimes M) \text{diag}(\mathbf{c}),$$

где $\text{diag}(\mathbf{c})$ означает квадратную двоичную диагональную матрицу, содержащую вектор $\mathbf{c}$ на диагонали и нули во всех других позициях.

Лемма 5. Пусть $P^{(c)}$ является c -перестановочной матрицей порядка ν^2 , σ – соответствующее отображение множества $\{Z_{i,j}\}$ в себя, а $\mathbf{c} = (c_1, c_2, \dots, c_{\nu^2})$ – произвольный вектор длины ν^2 с элементами ± 1 , где $\nu \geq 4$. Тогда

$$P^{(c)} \text{diag}(\mathbf{c}) = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \varepsilon_{ij} \sigma(Z_{i,j}),$$

где $\sigma(Z_{i,j}) = Z_{k,s}$ и $\varepsilon_{ij} = c_{s+(j-1)\nu}$.

Доказательство. Вектор $\mathbf{c} = (c_1, c_2, \dots, c_{\nu^2})$ можно представить в блоковом виде следующим образом: $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_{\nu})$, где каждый блок $\mathbf{c}_t$ имеет вид

$$\mathbf{c}_t = (c_{1+(t-1)\nu}, c_{2+(t-1)\nu}, \dots, c_{\nu+(t-1)\nu}).$$

Следовательно, $\mathbf{c} = (c_{r+(t-1)\nu})$, где $r, t \in \{1, \dots, \nu\}$.

Поэтому можно записать

$$\text{diag}(\mathbf{c}) = \sum_{r,t=1}^{\nu} c_{r+(t-1)\nu} (Z_{t,t} \otimes Z_{r,r}). \quad (7)$$

Таким образом,

$$\begin{aligned} P^{(c)} \text{diag}(\mathbf{c}) &= \left(\sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}) \right) \text{diag}(\mathbf{c}) = \\ &= \left(\sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}) \right) \left(\sum_{r,t=1}^{\nu} c_{r+(t-1)\nu} (Z_{t,t} \otimes Z_{r,r}) \right). \end{aligned}$$

Используя (4) и тот факт, что для любых $a, b, c, d \in \{1, \dots, \nu\}$ справедливо равенство $Z_{a,b}Z_{c,d} = \delta_{bc}Z_{a,d}$, где $\delta_{bc} = 1$, если $b = c$, и $\delta_{bc} = 0$ в противном случае, получаем

$$P^{(c)} \text{diag}(\mathbf{c}) = \sum_{i,j,r,t=1}^{\nu} c_{r+(t-1)\nu} \delta_{jt} Z_{i,t} \otimes \delta_{sr} Z_{k,r},$$

где $\sigma(Z_{i,j}) = Z_{k,s}$. Следовательно,

$$P^{(c)} \text{diag}(\mathbf{c}) = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes c_{r+(j-1)\nu} \sigma(Z_{i,j}) = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \varepsilon_{ij} \sigma(Z_{i,j}),$$

где $\varepsilon_{ij} = c_{s+(j-1)\nu}$. ▲

Лемма 6. Пусть $\mathbf{c}$ – произвольный вектор длины ν^2 с элементами ± 1 , а K_{ν^2} – коммутационная матрица порядка ν^2 , где $\nu \geq 4$. Тогда существует вектор $\mathbf{d}$ длины ν^2 с элементами ± 1 , такой что

$$\text{diag}(\mathbf{c})K_{\nu^2} = K_{\nu^2} \text{diag}(\mathbf{d}).$$

Доказательство. Так как K_{ν^2} является перестановочной матрицей, в качестве вектора $\mathbf{d}$ с элементами ± 1 можно выбрать вектор $\mathbf{d}$, такой что

$$\text{diag}(\mathbf{d}) = K_{\nu^2}^{-1} \text{diag}(\mathbf{c})K_{\nu^2}. \quad \blacktriangle$$

Заметим, что вектор $\mathbf{d}$ из элементов ± 1 длины ν^2 задается выражением

$$d_{t+(r-1)\nu} = c_{r+(t-1)\nu}.$$

Следующая теорема приведена в [11, 12].

Теорема 1. Пусть ν – произвольное натуральное число, такое что существует матрица Адамара порядка ν . Пусть $P^{(c)}$ – c -перестановочная матрица порядка ν^2 , а $\mathbf{c}$ – произвольный ± 1 -вектор длины ν^2 , и пусть H_1 и H_2 – любые матрицы Адамара порядка ν . Пусть L – матрица следующего вида:

$$L = (I_{\nu} \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (I_{\nu} \otimes H_2). \quad (8)$$

Тогда L является матрицей Адамара порядка ν^2 .

Доказательство этой теоремы можно найти в [13].

Одним из основных результатов данной статьи является следующий.

Теорема 2. Пусть $P^{(c)}$ – lc -перестановочная матрица порядка ν^2 , $\mathbf{c}$ – произвольный вектор длины ν^2 с элементами ± 1 , H_1 – произвольная матрица Адамара порядка ν , и H_2 – симметричная матрица Адамара порядка $\nu \geq 4$.

Пусть

$$L = (I_{\nu} \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (I_{\nu} \otimes H_2).$$

Тогда

- (i) Матрица L представляет собой матрицу Адамара с двумя возможными значениями $\pm \nu$ весов (т.е. суммы элементов) ее строк, и меняя знаки строк (умножением строк на -1), меняя тем самым сумму $-\nu$ на сумму ν , мы получаем регулярную матрицу Адамара L^* с суммой элементов каждой строки и каждого столбца, равной ν ;
- (ii) Каждая строка двоичной матрицы L_b (т.е. матрицы L_b^* , полученной из L^*) является бент-функцией типа Майораны – Мак-Фарланда.

Доказательство. Так как $P^{(c)}$ является lc -перестановочной матрицей и, следовательно, c -перестановочной, из теоремы 1 мы получаем, что L является матрицей Адамара. Теперь вычислим скалярное произведение любой строки матрицы L с любой строкой симвестровой матрицы Адамара порядка ν^2 , которую можно представить в виде $H \otimes H$, где H – симвестрова матрица Адамара порядка ν . Возьмем также в качестве H_2 симвестрову матрицу Адамара H . Тогда получаем

$$\begin{aligned} L(H \otimes H)^t &= (I_\nu \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (I_\nu \otimes H) (H^t \otimes H^t) = \\ &= (I_\nu \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (H^t \otimes \nu I_\nu) = \\ &= \nu (I_\nu \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) K_{\nu^2} (I_\nu \otimes H^t) K_{\nu^2} = \\ &= \nu (I_\nu \otimes H_1) P^{(c)} K_{\nu^2} \text{diag}(\mathbf{d}) (I_\nu \otimes H^t) K_{\nu^2}, \end{aligned} \quad (9)$$

где K_{ν^2} – коммутационная матрица (см. (6)), а $\mathbf{d}$ – вектор длины ν^2 с элементами ± 1 , указанный в лемме 6. Из леммы 3 получаем, что $P^{(c)} K_{\nu^2}$ – lc -перестановочная матрица, и так как K_{ν^2} – перестановочная матрица, мы заключаем, что матрица

$$\frac{1}{\nu} L(H \otimes H)^t$$

является матрицей Адамара. Элементами матрицы $L(H \otimes H)^t$ являются $\pm \nu$. Следовательно, так как скалярное произведение любой строки L с любой строкой симвестровой матрицы Адамара соответствует элементам матрицы $L(H \otimes H)^t$, мы получаем, что скалярные произведения равны $\pm \nu$. Так как первая строка симвестровой матрицы Адамара $H \otimes H$ – это вектор из всех единиц, мы заключаем, что сумма элементов каждой строки матрицы L принимает два значения $\pm \nu$. Меняя знаки элементов строк с суммой $-\nu$ на противоположные (умножением этих строк на -1), мы получаем матрицу L^* с постоянной суммой элементов всех строк, равной ν , что означает регулярность по строкам матрицы L^* , а значит, по лемме 1, и регулярность с суммой элементов каждой строки и каждого столбца, равной ν , что доказывает утверждение (i).

Для доказательства утверждения (ii) необходимо проверить расстояние Хэмминга от любой строки L_b до симвестровой матрицы Адамара $(H \otimes H)_b$. Из предыдущих рассуждений известно, что значения скалярного произведения строк матрицы L со строками матрицы $H \otimes H$ равны $\pm \nu$. Это означает, что расстояние Хэмминга между строками L_b и строками $(H \otimes H)_b$ равно $\frac{\nu^2 \pm \nu}{2}$, и поэтому минимальное расстояние между строками этих двух матриц равно $\frac{\nu^2 - \nu}{2}$. Отсюда вытекает, что любая строка матрицы L_b дает бент-функцию. Тот факт, что полученные бент-функции являются функциями типа Майораны – Мак-Фарланда, доказан в [13]. $\blacktriangle$

Теперь мы переходим к рассмотрению алгебраической степени построенных регулярных матриц Адамара. Напомним, что преобразование Мёбиуса булевой функции связывает таблицу истинности функции с ее алгебраической нормальной формой (АНФ). Здесь мы следуем работе [14].

В начале перечислим все векторы пространства $\mathbb{Z}_2^m$ в виде

$$\alpha_0 = (0, \dots, 0), \quad \alpha_1 = (0, \dots, 1), \quad \dots, \quad \alpha_{2^m-1} = (1, \dots, 1),$$

где α_i – двоичное представление целого числа i . Таблица истинности булевой функции f на $\mathbb{Z}_2^m$ представляет собой двоичную последовательность, определяемую следующим образом:

$$(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^m-1})).$$

Функцию f можно единственным образом представить в виде АНФ как

$$f(x_1, \dots, x_m) = \bigoplus_{(a_1, \dots, a_m)} g(a_1, \dots, a_m) x_1^{a_1} \dots x_m^{a_m}, \quad (10)$$

где $(a_1, \dots, a_m) \in \mathbb{Z}_2^m$, а g – функция на $\mathbb{Z}_2^m$, которая называется *преобразованием Мёбиуса* функции f и обозначается через $g = \mu(f)$.

Для булевой функции f число переменных в самом длинном мономе ее АНФ называется ее *алгебраической степенью* и обозначается $\deg(f)$. Хорошо известно (см., например, [15]), что для любой бент-функции f с $2m$ переменными справедливо неравенство

$$\deg(f) \leq m.$$

Если $\deg(f) = m$, то f называется бент-функцией с *максимальной алгебраической степенью*.

Преобразование Мёбиуса задается двоичной $(2^m \times 2^m)$ -матрицей T_m , i -я строка которой представляет собой таблицу истинности монома $x_1^{a_1} \dots x_m^{a_m}$, где $(a_1, \dots, a_m)$ – двоичное представление целого числа i . Матрицу T_m можно рекуррентно представить в следующем виде:

$$T_s = \begin{pmatrix} T_{s-1} & T_{s-1} \\ 0_{s-1} & T_{s-1} \end{pmatrix},$$

где 0_{s-1} – нулевая матрица размера $2^{s-1} \times 2^{s-1}$, матрица T_1 имеет вид

$$T_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

а $s \geq 2$ – любое целое число. Более того, матрица T_m обладает следующим свойством:

$$T_m^{-1} = T_m,$$

и для заданной булевой функции f имеем

$$(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^m-1})) T_m = (g(\alpha_1), \dots, g(\alpha_{2^m-1})). \quad (11)$$

Алгебраическая степень бент-функции, заданной строками матрицы L_b в теореме 2, почти всегда максимальна, т.е. достигает максимума для бент-функции. Это максимальное значение равно m , где $\nu = 2^m$. Следующая теорема, в которой добавлены некоторые ограничения на условия теоремы 2, показывает, что при изменении вектора $\mathbf{c}$ по крайней мере одна строка в матрице L_b даст бент-функцию с максимальной алгебраической степенью. Кроме того, мы получаем верхнюю границу на ранг полученной регулярной матрицы Адамара L_b^* , ассоциированной с матрицей L_b .

Теорема 3. Пусть $P^{(c)}$ является $1c$ -перестановочной матрицей порядка ν^2 , где $\nu = 2^m \geq 4$. Пусть $\mathbf{c}$ – произвольный вектор длины ν^2 с элементами ± 1 , и пусть H_1, H_2 – сильвестровы матрицы Адамара порядка ν .

Пусть

$$L = (I_\nu \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (I_\nu \otimes H_2),$$

и пусть L^* – регулярная матрица Адамара, ассоциированная с L (т.е. полученная умножением соответствующих строк на -1). Пусть L_b и L_b^* – двоичные матрицы, отвечающие матрицам L и L^* соответственно. Наконец, пусть i – любое число в диапазоне $i \in \{1, \dots, \nu^2\}$. Тогда

- (i) $\text{rank}(L_b^*) \leq 2\nu - 2$, если $\mathbf{c}$ – постоянный блочный вектор, и $\text{rank}(L_b^*) \leq 2\nu - 1$ в противном случае;
- (ii) $\ker(L_b^*) = (0, 0, \dots, 0)$;
- (iii) для заданного $i \in \{1, \dots, \nu^2\}$ существует вектор $\mathbf{c}$, такой что i -я строка матрицы L_b^* является бент-функцией с максимальной алгебраической степенью m .

Доказательство. Для доказательства первого утверждения заметим, что

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}),$$

где $\sigma(Z_{i,j}) = Z_{k,s}$, так что в множестве пар $\{(k, s)\}$, индуцированных при фиксации индекса i , имеются все значения $k, s \in \{1, \dots, \nu\}$.

Выберем симметрические матрицы Адамара $H_1 = H_2 = H$. Возьмем также в качестве $\mathbf{c}$ постоянный вектор из всех единиц (в противном случае применим лемму 4). Тогда получаем

$$\begin{aligned} L &= (I_\nu \otimes H_1) P^{(c)} (I_\nu \otimes H_2) = \\ &= \sum_{i,j=1}^{\nu} (I_\nu \otimes H) (Z_{i,j} \otimes Z_{k,s}) (I_\nu \otimes H) = \sum_{i,j=1}^{\nu} (Z_{i,j} \otimes H Z_{k,s} H). \end{aligned}$$

Матрицу L можно рассматривать как матрицу, состоящую из блоков размера $\nu \times \nu$. Каждый блок матрицы L соответствует разным значениям индексов i, j (т.е. каждый из ν^2 блоков задан одной упорядоченной парой индексов (i, j)),

$$L = \sum_{i,j=1}^{\nu} (Z_{i,j} \otimes H Z_{k,s} H).$$

Пусть H_b и L_b – двоичные матрицы, отвечающие матрицам H и L соответственно. Заметим, что элемент с координатами (a, b) в блоке с координатной парой (i, j) матрицы $H Z_{k,s} H$ равен $h_{a,k} h_{s,b}$, где h_{xy} обозначает элемент (x, y) матрицы H . Для удобства обозначим через $\bar{h}_{a,b}$ двоичное значение элемента $h_{a,b}$, т.е. $\bar{h}_{a,b} = 0$, когда $h_{a,b} = 1$, и $\bar{h}_{a,b} = 1$, когда $h_{a,b} = -1$. Следовательно, элементом с координатами (a, b) матрицы $(H Z_{k,s} H)_b$ (т.е. блока (i, j)) является следующая сумма двух элементов:

$$\bar{h}_{a,k} + \bar{h}_{s,b}. \quad (12)$$

Рассмотрим теперь две строки матрицы L_b внутри одного и того же строчного блока. Величина $\bar{h}_{x,y}$ равна 0 или 1 в матрице H_b . Каждую строку можно разбить на ν последовательных столбцовых блоков, и можно убедиться, что элементы первого столбца этих двух строк равны $(\bar{h}_{a,k} + \bar{h}_{s,b})$ и $(\bar{h}_{a',k} + \bar{h}_{s,b})$ соответственно, где индексы k, s, a, a' фиксированы и $b \in \{1, \dots, \nu\}$. Складывая эти две строки матрицы L_b , мы получим вектор, такой что все элементы в координатах первого столбцового блока равны $\bar{h}_{a,k} + \bar{h}_{a',k}$. Для всех других элементов столбцовых блоков имеем такое же выражение, но с другим k . Так как величина $\bar{h}_{a,k} + \bar{h}_{a',k}$ не зависит от b , то это означает, что полученный вектор имеет постоянное значение 0 или 1 в каждом блоке. Если мы отождествим все координаты одного столбцового блока в одну координату (а это можно сделать, так как все эти координаты имеют одно и то же значение), мы получим сумму двух строк с индексами a и a' матрицы H_b после перестановки столбцов в соответствии с σ .

Применяя теперь это же рассуждение ко всем ν строчным блокам в матрице L_b , мы каждый раз будем получать сумму тех же самых двух строк в матрице H_b с ин-

дексами a и a' после некоторой перестановки столбцов. Следовательно, множество S всех двоичных векторов, получаемых как сумма двух строк матрицы L_b в одном и том же строчном блоке, эквивалентны с точки зрения линейной зависимости множеству S' всех двоичных векторов, полученных как сумма двух строк матрицы H_b после некоторой перестановки столбцов. Следовательно, ранг S не выше $\nu - 2$. Чтобы получить L^* из L , нужно добавить вектор из всех единиц. Следовательно, прибавляя вектор из всех единиц к строкам множества S' , мы получим множество векторов длины ν четного веса, откуда

$$\text{rank}(S^*) \leq \nu - 1,$$

где через S^* обозначено множество строк S с добавлением вектора из всех единиц.

Чтобы вычислить $\text{rank}(L_b)$, рассмотрим вышеуказанное множество векторов S^* , а также все строки из V , где V – подмножество строк матрицы L_b , не содержащее двух строк из одного и того же строчного блока. Например, можно взять все строки в матрице H_b с координатами

$$(\bar{h}_{1,k} + \bar{h}_{s,1}, \bar{h}_{1,k} + \bar{h}_{s,2}, \dots),$$

где $k, s \in \{1, \dots, \nu\}$. Каждый вектор из множества V представляет собой последовательное повторение ν блоков, где каждый блок – это строка матрицы H_b . Полное число векторов в множестве V равно ν , но при этом сложение всех векторов из V дает нулевой вектор. Следовательно, $\text{rank}(V) \leq \nu - 1$, и поэтому

$$\text{rank}(L_b^*) \leq \nu - 1 + \nu - 1 = 2\nu - 2.$$

Если теперь c является блочно-постоянным вектором, но не вектором из всех единиц, то используя лемму 4 и приведенные выше рассуждения, легко убедиться, что ранг матрицы L_b^* удовлетворяет той же самой верхней границе.

Пусть теперь c является не блочно-постоянным вектором, а произвольным вектором с элементами ± 1 . В этом случае используем лемму 5. При этом выражение (12) принимает вид

$$\bar{h}_{a,k} + \bar{h}_{s,b} + \delta_{ks},$$

где δ_{ks} принимает двоичные значения 0 или 1 в зависимости от значения $+1$ или -1 величины ε_{ij} в лемме 5 соответственно.

Теперь с помощью тех же рассуждений, которые использовались в случае, когда c является вектором из всех единиц, $\text{rank}(S^*)$ вычисляется точно так же, без каких-либо изменений, но при построении множества V мы не можем гарантировать, что сложение всех векторов множества V дает нулевой вектор. Следовательно, мы можем лишь заключить, что $\text{rank}(V) \leq \nu$, и поэтому

$$\text{rank}(L_b^*) \leq 2\nu - 1.$$

На этом заканчивается доказательство первого утверждения теоремы.

Второе утверждение теоремы вытекает непосредственно из леммы 2.

Для доказательства третьего утверждения, следуя формуле (11), вычислим $g = fT_m$, где $\nu = 2^m$, f – любая строка матрицы L_b , а g задает АНФ-представление бент-функции, соответствующей строке f .

Рассмотрим $T_m^{(a)}$, т.е. a -й столбец матрицы T_m , где

$$a = 2 + 2^m(2^{m-1} - 1).$$

Вес Хэмминга двоичного представления числа a равен m . Это означает, что когда $fT_m^{(a)} = 1$, в выражении $g = fT_m$ заведомо имеется моном алгебраической степени m .

Следовательно, для доказательства утверждения (iii) нужно вычислить $fT_m^{(a)}$ для строк f матрицы L_b и проверить, что результат вычисления равен 1.

Выберем строку в матрице L_b , например, i -ю строку блока, для которого матрицы $Z_{k,s}$ имеют индексы $\{(k_1, s_1), \dots, (k_\nu, s_\nu)\}$. Заметим, что в столбце $T_m^{(a)}$ всюду стоят нули, кроме следующих ν координатных позиций:

$$1, 2, \nu + 1, \nu + 2, 2\nu + 1, 2\nu + 2, \dots, \left(\frac{\nu}{2} - 1\right)\nu + 1, \left(\frac{\nu}{2} - 1\right)\nu + 2.$$

Элементами выбранной строки являются $\bar{h}_{i,k} + \bar{h}_{s,j}$, где индекс i фиксирован, а $j \in \{1, \dots, \nu\}$. Пара индексов (k, s) пробегает значения $\{(k_1, s_1), \dots, (k_\nu, s_\nu)\}$. Вычисляя $fT_m^{(a)}$, получаем

$$\begin{aligned} fT_m^{(a)} = & \bar{h}_{i,k_1} + \bar{h}_{s_1,1} + \bar{h}_{i,k_1} + \bar{h}_{s_1,2} + \bar{h}_{i,k_2} + \bar{h}_{s_2,1} + \bar{h}_{i,k_2} + \bar{h}_{s_2,2} + \dots + \\ & + \bar{h}_{i,k_\mu} + \bar{h}_{s_\mu,1} + \bar{h}_{i,k_\mu} + \bar{h}_{s_\mu,2} = \bar{h}_{s_1,1} + \bar{h}_{s_1,2} + \bar{h}_{s_2,1} + \bar{h}_{s_2,2} + \dots + \bar{h}_{s_\mu,1} + \bar{h}_{s_\mu,2}, \end{aligned}$$

где $\mu = \nu/2$. Это значение соответствует сложению всех элементов координатных позиций обоих столбцов, 1-го и 2-го, всех $\nu/2$ строк матрицы H_b с номерами $s_1, s_2, \dots, s_\mu$. Так как H_b – нормализованная двоичная матрица Адамара, все элементы первого столбца являются нулями, и поэтому величина fT_m равна сумме всех координат второго столбца матрицы H_b , соответствующих $\nu/2$ разным строкам с номерами $s_1, s_2, \dots, s_\mu$. Эта сумма не обязательно равна 1, однако мы можем изменить символ в координате s_1 , сохраняя остальные значения в координатах $s_2, \dots, s_\mu$ без изменения. Возьмем в качестве $\mathbf{c}$ вектор, все элементы которого равны 1, за исключением одного элемента -1 в позиции $c_{s_1+(j-1)\nu}$, где $\sigma(Z_{i,j}) = Z_{k_1,s_1}$. Теперь утверждение (iii) следует из леммы 5. ▲

Из теоремы 2 мы видим, что из lc -перестановочной матрицы порядка ν^2 мы получаем матрицу Адамара

$$L = (I_\nu \otimes H_1) P^{(c)} \text{diag}(\mathbf{c}) (I_\nu \otimes H_2),$$

строками которой являются бент-функции. Однако столбцы L_b не обязательно дают бент-функции. Это происходит из-за того, что определение lc -перестановочной матрицы не “симметрично”. Пусть $P^{(c)}$ – c -перестановочная матрица порядка ν^2 . Чтобы эта матрица $P^{(c)}$ была lc -перестановочной, необходимо, чтобы выполнялось равенство

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}),$$

где σ – отображение множества матриц $\{Z_{i,j}\}$ в себя, такое что для каждого индекса i сумма таких матриц по j

$$\sum_{j=1}^{\nu} \sigma(Z_{i,j})$$

представляет собой перестановочную матрицу (напомним, что двоичная матрица Z_{ij} размера $\nu \times \nu$ имеет только один ненулевой элемент в позиции (i, j)). Чтобы получить матрицу Адамара L , в которой каждая строка и каждый столбец матрицы L_b является бент-функцией, мы должны гарантировать, что для каждого индекса j сумма таких матриц по индексу i дает перестановочную матрицу, т.е. для каждого

индекса j матрица

$$\sum_{i=1}^{\nu} \sigma(Z_{i,j})$$

является перестановочной. Достаточным условием для этого является наличие матрицы G с парой (k, s) в i -й строке и j -м столбце, такой что $\sigma(Z_{i,j}) = Z_{k,s}$. Такую матрицу можно задать с помощью двух латинских квадратов. Это приводит к следующему определению.

Определение 3. Пусть G и D – два взаимно ортогональных латинских квадрата порядка ν . Определим биективное отображение

$$\sigma(Z_{i,j}) = Z_{k,s},$$

где $G_{ij} = k$ и $D_{ij} = s$. Определим olc -перестановочную матрицу $P^{(c)}$ порядка ν^2 следующим образом:

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}). \quad (13)$$

Теперь непосредственным образом получаем следующий результат.

Теорема 4. Пусть G и D – два произвольных взаимно ортогональных латинских квадрата порядка ν . Зададим биективное отображение $\sigma(Z_{i,j}) = Z_{k,s}$, где $G_{ij} = k$ и $D_{ij} = s$, и соответствующую olc -перестановочную матрицу

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j})$$

согласно определению 3. Пусть H – симметрическая матрица Адамара порядка ν . Тогда двоичная матрица Адамара L_b вида

$$L = (I_{\nu} \otimes H) P^{(c)} (I_{\nu} \otimes H)$$

такова, что каждая ее строка и каждый ее столбец представляет собой бент-функцию.

Доказательство. Этот результат следует из теоремы 2, если принять во внимание, что обе суммы

$$\sum_{i=1}^{\nu} \sigma(Z_{i,j}) \quad \text{и} \quad \sum_{j=1}^{\nu} \sigma(Z_{i,j})$$

являются перестановочными матрицами для всех индексов $i, j \in \{1, \dots, \nu\}$. В этом случае обе матрицы $P^{(c)}$ и $P^{(c)t}$ являются lc -перестановочными. ▲

Далее в § 3 мы построим два бесконечных семейства lc -перестановочных матриц $P^{(c)}$ порядка ν^2 для $\nu = 2^m$, где $m \geq 2$ – натуральное число (но четное для первой конструкции). С помощью первой конструкции полученные lc -перестановки индуцируют двоичные матрицы Адамара L_b , в которых все их строки являются бент-функциями согласно теореме 2. В некоторых случаях эти бент-функции имеют максимальную алгебраическую степень в соответствии с теоремой 3. Размерность ядра равна нулю, а значения ранга матрицы L_b для небольших значений ν были вычислены, и эти результаты мы приводим ниже. Все матрицы L_b из семейства,

построенного второй конструкцией в п. 3.2, имеют то дополнительное свойство, что каждый столбец их матрицы L_b также является бент-функцией.

§ 3. Построение lc -перестановочных и olc -перестановочных матриц

Чтобы говорить об lc -перестановках согласно определению 2, нам нужно, чтобы сумма блочковых матриц $\sigma(Z_{i,j})$ для любого i давала перестановочную матрицу, скажем, $P_i^{(c)}$. Идея состоит в том, чтобы вернуться назад и из c -перестановок $P_i^{(c)}$ построить блочковые матрицы $\sigma(Z_{i,j})$ для матрицы $P^{(c)}$. На этой идее основаны следующие две конструкции (более подробно эти конструкции описаны в [13]).

3.1. Семейство lc -перестановок. Для каждого четного положительного натурального числа $m \geq 2$ предположим, что нам известны $\nu = 2^m$ c -перестановок порядка ν , которые обозначим через $P_1^{(c)}, \dots, P_\nu^{(c)}$. Наша цель – представить $P_k^{(c)}$ в виде суммы блочковых матриц типа $Z_{i,j}$. Проблема, с которой мы сталкиваемся при разложении каждой матрицы $P_k^{(c)}$ на блочковые матрицы типа $Z_{i,j}$, состоит в том, что, например, две матрицы $Z_{i,a}$ и $Z_{i,b}$ появляются с разными значениями $a \neq b$, но с одним и тем же индексом i . В этом случае матрица $P^{(c)}$, которую мы хотим найти, не будет c -перестановочной порядка ν^2 . Чтобы справиться с этой проблемой, помимо перестановок $P_k^{(c)}$ для $k \in \{1, \dots, \nu\}$ мы будем строить перестановочную матрицу $P^{(c)}$, используя латинский квадрат Q порядка ν .

Конструкция 1. Пусть $m \geq 2$ – четное натуральное число, и пусть $\nu = 2^m$. Построение lc -перестановочной матрицы $P^{(c)}$ порядка ν^2 из ν c -перестановок $P_1^{(c)}, P_2^{(c)}, \dots, P_\nu^{(c)}$ порядка ν и латинского квадрата $Q = [q_{i,j}]$ порядка ν состоит в следующем. Для каждой матрицы $P_k^{(c)}$ рассмотрим отдельно каждую ее строку, например, строку j , и найдем в этой строке позицию, где стоит элемент 1. Пусть, например, этот элемент стоит в i -й позиции. Далее мы вычисляем *индикатор* $\tau = q_{k,i}$. Строка с номером j матрицы $P_k^{(c)}$ записывается в качестве строки с номером j блока (k, τ) матрицы $P^{(c)}$, которую мы строим. Таким образом мы гарантируем, что построенная матрица $P^{(c)}$ будет lc -перестановочной.

3.2. Семейство olc -перестановок. Теперь опишем другую конструкцию.

Конструкция 2. Возьмем пару ортогональных латинских квадратов $G = [g_{i,j}]$ и $D = [d_{i,j}]$ порядка ν и построим olc -перестановочную матрицу $P^{(c)}$ следующим образом:

$$P^{(c)} = \sum_{i,j=1}^{\nu} Z_{i,j} \otimes \sigma(Z_{i,j}),$$

где $\sigma(Z_{i,j}) = Z_{k,s}$, число k – элемент латинского квадрата G с координатами (i, j) , т.е. $g_{i,j} = k$, а число s – элемент латинского квадрата D с координатами (i, j) , т.е. $s = d_{i,j}$.

В табл. 1 для небольших значений ν приведены полученные значения ранга $\text{rank}(L_b^*)$ для постоянного или произвольного вектора c с элементами ± 1 для матриц L_b^* , построенных конструкцией 2. Кроме того, приведена верхняя граница (ВГ), заданная теоремой 3.

Матрицы L^* , построенные с помощью конструкции 2, имеют такие же свойства, как и приведенные в теоремах 1 и 2, лемме 2 и теореме 3 для случая lc -перестановочных матриц. Однако имеются некоторые исключения, такие как, например, тот факт, что не только строки, но и столбцы соответствующей двоичной матрицы L_b^*

Таблица 1

Ранги кодов из конструкции 2 и верхние границы

ν	Постоянный c		Произвольный c	
	Полученные ранги	ВГ	Полученные ранги	ВГ
2^2	6	6	6, 7	7
2^3	$[10, \dots, 14]$	14	$[10, \dots, 15]$	15
2^4	$[22, \dots, 30]$	30	$[22, \dots, 31]$	31
2^5	$[56, \dots, 61]$	62	$[58, \dots, 62]$	63
2^6	$[118, \dots, 125]$	126	$[122, \dots, 126]$	127

являются бент-функциями. Более того, результаты вычислений для небольших значений m показывают, что величина $\text{rank}(L_b^*)$ почти всегда удовлетворяет верхней границе, указанной в теореме 3. В табл. 1 приведены некоторые результаты вычислений, полученных с помощью системы компьютерной алгебры MAGMA [16].

СПИСОК ЛИТЕРАТУРЫ

1. Beth T., Jungnickel D., Lenz B. Design Theory. Cambridge, UK: Cambridge Univ. Press, 1986.
2. McFarland R.L. A Family of Difference Sets in Non-cyclic Groups // J. Combin. Theory Ser. A. 1973. V. 15. № 1. P. 1–10. [https://doi.org/10.1016/0097-3165\(73\)90031-9](https://doi.org/10.1016/0097-3165(73)90031-9)
3. 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>
4. Bose R.C., Shrikhande S.S. A Note on a Result in the Theory of Code Construction // Inform. Control. 1959. V. 2. № 2. P. 183–194. [https://doi.org/10.1016/S0019-9958\(59\)90376-6](https://doi.org/10.1016/S0019-9958(59)90376-6)
5. Kesava Menon P. On Difference Sets Whose Parameters Satisfy a Certain Relation // Proc. Amer. Math. Soc. 1962. V. 13. № 5. P. 739–745. <https://doi.org/10.1090/S0002-9939-1962-0142471-0>
6. Ryser H.J. A Note on a Combinatorial Problem // Proc. Amer. Math. Soc. 1950. V. 1. № 4. P. 422–424. <https://doi.org/10.1090/S0002-9939-1950-0036732-5>
7. Borges J., Rifà J., Zinoviev V. New Families of Completely Regular Codes and Their Corresponding Distance Regular Coset Graphs // Des. Codes Cryptogr. 2014. V. 70. № 1–2. P. 139–148. <https://doi.org/10.1007/s10623-012-9713-3>
8. Rifà J., Zinoviev V.A. On Binary Quadratic Symmetric Bent and Semi-Bent Functions // Mosc. Math. J. 2023. V. 23. № 1. P. 121–128. <https://doi.org/10.17323/1609-4514-2023-23-1-121-128>
9. Meisner D.B. On a Construction of Regular Hadamard Matrices // Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei Matem. Appl. Ser. 9. 1992. V. 3. № 4. P. 233–240.
10. Magnus J.R., Neudecker H. The Commutation Matrix: Some Properties and Applications // Ann. Statist. 1979. V. 7. № 2. P. 381–394. <https://doi.org/10.1214/aos/1176344621>
11. Семаков Н.В., Зайцев Г.В., Зиновьев В.А. Корреляционное декодирование блочных кодов методом быстрого преобразования Фурье–Адамара // Тр. 4-го Симпоз. по проблеме избыточности в информационных системах. Ч. 2. Тез. докл. Ленинград, 1970. С. 545–550.
12. Зайцев Г.В., Зиновьев В.А., Семаков Н.В. Быстрое корреляционное декодирование блочных кодов // Кодирование и передача дискретных сообщений в системах связи. М.: Наука, 1976. С. 76–85.
13. Rifà J., Villanueva M., Zinoviev D.V., Zinoviev V.A. On Constructions of Regular Hadamard Matrices and Bent Functions // Probl. Inf. Transm. 2024. V. 60. № 4 (to appear). <https://doi.org/10.1134/S003294602404001X>

14. *Pieprzyk J., Wang H., Zhang X.-M.* Möbius Transforms, Coincident Boolean Functions and Non-coincidence Property of Boolean Functions // Int. J. Comput. Math. 2011. V. 88. № 7. P. 1398–1416. <https://doi.org/10.1080/00207160.2010.509428>
15. *Rothaus O.S.* On “Bent” Functions // J. Combin. Theory Ser. A. 1976. V. 20. № 3. P. 300–305. [https://doi.org/10.1016/0097-3165\(76\)90024-8](https://doi.org/10.1016/0097-3165(76)90024-8)
16. *Bosma W., Cannon J., Playoust C.* The Magma Algebra System. I: The User Language // J. Symbolic Comput. 1997. V. 24. № 3–4. P. 235–265. <https://doi.org/10.1006/jSCO.1996.0125>

Рифа Жузен (Rifà, Josep)

Вильянуэва Мерсе (Villanueva, Mercè)

Факультет информационно-коммуникационных технологий,

Независимый университет Барселоны,

Серданыола-дель-Вальес, Каталония, Испания

josep.rifa@uab.cat

merce.villanueva@uab.cat

Зиновьев Виктор Александрович

Зиновьев Дмитрий Викторович

Институт проблем передачи информации

им. А.А. Харкевича РАН, Москва

vazinov@iitp.ru

dzinov@gmail.com

Поступила в редакцию

10.07.2024

После доработки

21.11.2024

Принята к публикации

18.12.2024