УДК 004.052.2 **DOI** 10.15622/SP.50.9

Ю.Н. Балонин, А.А. Востриков, А.М. Сергеев, И.С. Егорова

О ВЗАИМОСВЯЗЯХ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ, ПОСТРОЕННЫХ НА ИЗВЕСТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ЧИСЕЛ

Балонин Ю.Н., Востриков А.А., Сергеев А.М., Егорова И.С. **О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел.**

Аннотация. Цель работы: показать связь чисел, принадлежащих известным последовательностям, и квазиортогональных матриц, существующих на порядках, равных этим числам, а также взаимосвязь таких матриц через алгоритмы вычисления. Методы: анализ последовательностей квазиортогональных матриц абсолютного и локального максимумов детерминанта, выделение в матрицах структурных инвариантов, сопоставление алгоритмов вычисления таких матриц. Результаты: рассмотрены известные последовательности натуральных чисел, сформулировано определение матрицы, ассоциированной с натуральным числом. Приведены последовательности чисел, для которых доказано существование ассоциированных с ними квазиортогональных матриц. Высказано предположение, что ассоциированные матрицы существуют для всех натуральных чисел. Рассмотрены свойства типов таких матриц, их взаимосвязи через алгоритмы вычисления. Приведены модифицированные алгоритмы и основные цепочки матриц Эйлера и Мерсенна, последовательности порядков которых являются системообразующими. Практическая значимость: квазиортогональные матрицы абсолютного и локального максимумов детерминанта имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации. Их разнообразие позволяет разработчикам технических систем значительно облегчить выбор матрицы, оптимальной для конкретной задачи.

Ключевые слова: числовые последовательности, числа Мерсенна, числа Ферма, ортогональные матрицы, квазиортогональные матрицы, матрицы Адамара, матрицы Мерсенна, матрицы Эйлера, матрицы Ферма, цепочки матриц, алгоритмы вычисления квазиортогональных матриц.

1. Введение. Практический интерес к ортогональным (квазиортогональным) матрицам обусловлен основными свойствами таких матриц, обеспечивающими им широкое применение в цифровых системах обработки и преобразования информации [1]. Ортогональность матриц позволяет реализовывать конгруэнтные преобразования, а существующие ортогональные базисы, включая симметричные, циклические, двуциклические и другие конструкции значительно расширяют возможности выбора оптимальной матрицы для решения конкретной задачи преобразования информации.

В теории кодирования, например, столбцы ортогональных матриц Адамара используются для построения кодов с большим кодовым расстоянием [2]. Специальный порядок нумерации столбцов таких матриц в цифровой обработке сигналов, сжатии и маскировании изображений интерпретируется как двухуровневое представление широко используемых функций Уолша [3].

Первый алгоритм вычисления ортогональных по столбцам (квазиортогональных) матриц с элементами {1, –1} четных порядков $n=2^k$, где k — целое, был предложен Сильвестром (Sylvester) [4].

Адамар (Hadamard) сформулировал гипотезу о существовании таких матриц на порядках 1, 2 и 4t, где t — натуральное число, включающих порядки 2^k, заложив основы исследований [1, 5], во-первых, соответствия последовательностей целых чисел и квазиортогональных матриц на порядках, равных этим числам; во-вторых, вложенности числовых последовательностей при сохранении качества соответствия чисел и матриц.

С последовательностью $4t$ соседствуют известные последовательности нечетных чисел $4t+1$ и $4t-1$ ($4t+3$), на обособленные числовые свойства которых обратили внимание еще Ферма и Эйлер.

Последовательность нечетных чисел вида $4t-1$ включает последовательность чисел Мерсенна, задаваемую как $n=2^k-1$ и начинающуюся с чисел 1, 3, 7, 15, 31, … Последовательность чисел Ферма, определяемая формулой $n=2^{2^k}+1$, начинается с чисел 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, … и принадлежит последовательности чисел вида $4t+1$.

Отличительной особенностью матриц Адамара, поставленных в соответствие последовательности чисел Сильвестра $n=2^k$, является их оптимальность по детерминанту. В общем случае квазиортогональные матрицы могут иметь как глобальный, так и локальный максимум детерминанта [4, 6].

Определение 1. Субоптимальную (строго оптимальную) по детерминанту квазиортогональную (или соответствующую ей ортогональную) матрицу порядка, равного некоторому числу числовой последовательности, будем называть матрицей, ассоциированной с этим числом.

Цель настоящей статьи — показать, что последовательностям натуральных чисел соответствуют последовательности матриц, которые будем называть ассоциированными с ними. На четных порядках это могут быть оптимальные матрицы Адамара [5], Белевича [7] и тому подобное, на нечетных — субоптимальные матрицы, ассоциированные с последовательностями Мерсенна и Ферма. Указанное обстоятельство дает хорошую ориентацию в разнообразии базисов и позволяет разработчикам технических систем значительно облегчить выбор матрицы, оптимальной для конкретной задачи обработки или преобразования информации.

2. Таблица квазиортогональных матриц. Для большей определенности в типах встречаемых квазиортогональных матриц мы приведем таблицу 1 матриц порядков $4t \pm k$, здесь $k \le 3$, классифицируемых по принадлежности их элементов заданным константам (как у матриц Адамара) или функциям уровня, зависящим от порядка *n*. Порядки $4t-3$ (или $4t+1$) сложнее прочих тем, что ортогональность столбцов матриц достижима при введении дополнительного уровня *d* для элементов диагонали (матрицы Зейделя) или каймы *s* (матрицы Ферма).

Таблица 1. Значения уровней семейств матриц

Символ	Порядок *n*	Матрица	Значения элементов
H	$4t$	Адамара	1, –1
C	$2t$, $4t$	Белевича	1, –1, 0
W	t, $2t$, $3t$, $4t$	Себерри (взвешенная)	1, –1, 0
M	$4t-1$	Мерсенна	1, $-b$, где $b=\dfrac{t}{t+\sqrt{t}}$
E	$4t-2$	Эйлера	1, $-b$, где $b=\dfrac{t}{t+\sqrt{2t}}$
S	$4t-3$	Зейделя	1, $-b$, d, где $b=1-2d$, $d=\dfrac{1}{1+\sqrt{n}}$
F	$4t+1$	Ферма	1, $-b$, s, где $q=n-1=4u^2$, $p=q+\sqrt{q}$, $b=\dfrac{2n-p}{p}=1-\dfrac{2u-1}{2u+1}\times\dfrac{1}{u}$, $s=\dfrac{\sqrt{nq-2\sqrt{q}}}{p}=\dfrac{\sqrt{nu-1}}{2u+1}\times\dfrac{1}{\sqrt{u}}$

3. Квазиортогональные матрицы Мерсенна. В работе [8] предложены квазиортогональные матрицы, существующие на нечетных порядках $n=2^k-1$, которые могут быть вложены в последовательность $4t-1$ при сохранении значения модулей элементов матрицы.

Определение 2. Матрица Мерсенна (**M**) — квадратная матрица порядка $n=4t-1$, состоящая из чисел $\{a=1,-b\}$, столбцы которой ортогональны $\mathbf{M}_n{}^{\mathrm{T}}\mathbf{M}_n=\mu\mathbf{I}$, $b=\dfrac{t}{t+\sqrt{t}}$, $\mu=\dfrac{p+qb^2}{2}$, $p=n-1$, $q=n+1$ (порядок матрицы Адамара).

4. Вычисление матриц Мерсенна. Для вычисления матриц Мерсенна повышенного порядка может использоваться *модифицированная последовательность Сильвестра* [8], представляемая в виде:

$$\mathbf{S}_{2n} = \begin{pmatrix} \mathbf{M}_n & \mathbf{M}_n \\ \mathbf{M}_n & \mathbf{M}_n^* \end{pmatrix}$$

и отличающаяся от классической тем, что матрица $\mathbf{M}_n^*$ образована перестановкой местами элементов a=1 и $-b$. У матриц Адамара это приводит к смене знака. Матрицы порядков, равных числам последовательности Мерсенна, образованы дополнением указанной основы строкой и столбцом в виде:

$$\mathbf{M}_{2n+1} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{S}_{2n} \end{pmatrix},$$

где $\lambda = -a$ — собственное число, а e — собственный вектор матрицы $\mathbf{S}_{2n}$.

5. Прикладная сторона, построение фильтров Мерсенна. В работе с участием авторов подробно раскрывается построение на основе матриц Мерсенна фильтров Мерсенна. К удобству читателя приведем краткую выдержку из этой работы, поясняющую ее суть. Элементарными преобразованиями (умножениями на –1, перестановками строк и столбцов) матрицы Мерсенна порядков $n = 2^k - 1$ переупорядочиваются к форме Мерсенна-Уолша (рисунок 1).

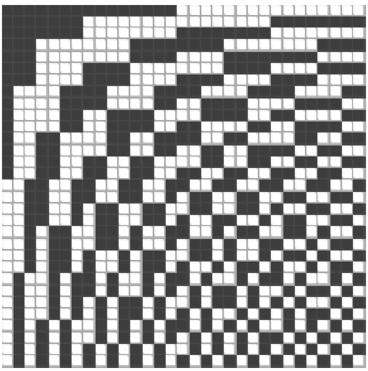

Рис. 1. Квазиортогональная матрица Мерсенна-Уолша $\mathbf{M}_{31}$

Фильтр Мерсенна оперирует двумерным спектром изображения **P**, который вычисляется по формуле $\mathbf{S} = \mathbf{M}^{\mathrm{T}}\mathbf{P}\mathbf{M}$ (столбцы М нормализованы до единичных норм). Высокочастотная часть спектра содержится в нижнем правом углу элементов **S**, которые в целях фильтрации либо обнуляются, либо умножаются на понижающие элементы. После передачи по каналу связи исходное изображение восстанавливается $\mathbf{P}=\mathbf{MSM}^{\mathrm{T}}$, не меняя обозначений для большей простоты. Восстановленные изображения будут отличаться от исходного на величину ошибки сжатия изображения, которая равна 0, если не вносить изменения. Напомним, что в задачах маскирования сжатие не производится или производится вынужденно с целью скрытия факта маскирования. Для маскирования большое значение играет не столько частота, сколько иррациональность уровней. В отличие от матриц Адамара перебор перестает играть роль ключа для скрытия изображения, нужно знать еще и уровень, а при иррациональном значении его не подобрать рациональными приближениями.

Система ортогональных функций, порождаемых упорядоченными по частоте столбцами матриц Мерсенна, принимает значения $\{1, -b\}$. Перечислим ее отличительные особенности и назовем причины, по которым такой базис сигналов может быть интересным. Система функций Мерсенна — Уолша — двухуровневая, она такая же, как и классическая система функций Уолша. Она отличается от функций Уолша пониженным по амплитуде нижним значением $-b$, которое с ростом размерности системы стремится к -1. В этом смысле она отличается от системы функций Уолша, но является достаточно близкой аппроксимацией ее на нечетных значениях порядка. Систему функций Мерсенна — Уолша отличает также пониженное на единицу количество порождающих ее элементов, она более проста для вычисления.

Любой базис отличает предпочтительная область его применения. Система функций Мерсенна — Уолша более высокочастотная, чем система функций Уолша, в ее составе нет функции нулевой частоты (константы). Таким образом, она более удобна для построения полосовых фильтров изображений. Первые единичные столбец и строка нормализованных матриц Адамара представляют собой ненужную составляющую, которая у полосовых фильтров никакой нагрузки не несет, поскольку отвечает частоте, которую они фильтруют, соответственно, она означает лишние затраты процессорного времени. Однако заметим, что простое удаление канвы матрицы Адамара отбрасыванием ее первых строки и столбца нарушает ортогональность столбцов усеченной матрицы.

6. Взаимосвязи квазиортогональных матриц. В работе [9] раскрывается гипотеза о существовании аналогичных матриц на всех нечетных порядках $n=4t-1$. Она имеет для матриц Мерсенна системное значение и отвечает гипотезе Адамара, расширяющей трактовку матриц порядков Сильвестра на порядки $n=4t$. Покажем, каким образом можно находить дополнительные к основной последовательности матрицы Мерсенна. Согласно работе [8], ассоциированные с числами последовательностей Сильвестра и Мерсенна матрицы встречаются чаще, чем относительно более редкие матрицы, ассоциированные с числами последовательности Ферма [10]. Причем матрицы Адамара порядков $4t$ можно получить на основе матриц Мерсенна порядков $4t-1$, и наоборот. Последовательности чисел Сильвестра и Мерсенна связаны между собой однозначно, столь же однозначно связаны между собой и ассоциированные с ними матрицы.

Взаимосвязь 1. Матрица $\mathbf{H}_{4t}$ вычисляется путем окаймления округленной до целых матрицы Мерсенна в виде:

$$\mathbf{H}_{4t} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{M}_{4t-1} \end{pmatrix},$$

с заменой элементов $-b$ образующей ее матрицы на -1. Здесь λ, e — собственное число и собственный вектор округленной целочисленной матрицы $\mathbf{M}_{4t-1}$ соответственно.

Возможен и обратный ход этого алгоритма, когда усечением нормированной матрицы Адамара (с изменением по знаку) и изменением отрицательных значений ее элементов до расчетного значения уровня $-b$, вычисляемого по формулам, приведенным в определении 2, формируется матрица Мерсенна. Такая взаимосвязь показывает, что с точностью до знака округленная матрица Мерсенна является ядром (core) нормализованной матрицы Адамара.

В качестве примера матриц, отличных от матриц основной последовательности, на рисунке 2 и на рисунке 3 приведены портреты матриц Адамара $\mathbf{H}_{12}$ с инвертированным по знаку, чтобы обеспечить должное значение $-\lambda$, ядром и матрицы Мерсенна $\mathbf{M}_{11}$ соответственно.

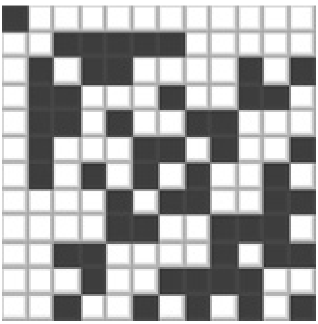

Рис. 2. Портрет матрицы $\mathbf{H}_{12}$

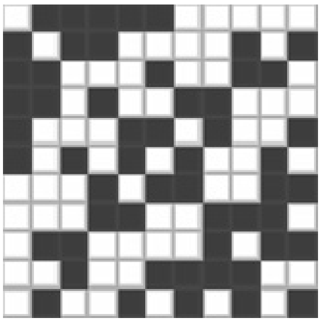

Рис. 3. Портрет матрицы $\mathbf{M}_{11}$

Следовательно, матрица Мерсенна, включая порядки, отличные от чисел Мерсенна, может быть найдена посредством матрицы Адамара, и наоборот. Более того, каждая из таких матриц Мерсенна является исходной для получения ветви матриц применением описанного выше и модифицированного для нечетных порядков алгоритма Сильвестра.

В работах [8, 10] матрицы Мерсенна и Ферма представлены самостоятельно, отдельно друг от друга. Однако существуют некоторые общие структуры квазиортогональных матриц четного и нечетного порядков.

Взаимосвязь 2. Матрица Ферма $\mathbf{F}_{4u^2+1}$, где u — целое число, может быть получена путем окаймления *регулярной* матрицы Адамара в виде:

$$\mathbf{F}_{4u^2+1}=\begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{H}_{4u^2} \end{pmatrix},$$

где λ, e — собственное число и собственный вектор *регулярной* матрицы Адамара $\mathbf{H}_{4u^2}$ (суммы строк и столбцов одинаковы), у которой отрицательные элементы заменены значениями, характерными для матриц Ферма.

Элемент –1 матрицы Адамара следует принять равным значению $-b$, $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u}$, элементы $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}$ собственного вектора являются элементами ($a<s\leq b$) каймы матриц Ферма, $q=n-1=4u^2$ (порядок регулярной матрицы Адамара), $p=q+\sqrt{q}$ [10].

Возможен обратный ход алгоритма вычисления вложенной матрицы Адамара по матрице Ферма. Отличие матриц Ферма от матриц Мерсенна состоит в том, что первые существуют только для значений порядков, равных числам Ферма, а также расширенных порядков, равных числам вида $n=4u^2+1$, где u — натуральное число, имеем: 3, 5, 17, 37, 65, 101, 145, 197, 257, ….

Матрица Адамара после нормализации (операции, при которой знаки элементов ее первого столбца и строки совпадают) дальнейшим усечением ее с пересчетом уровня переводится сначала в матрицу Мерсенна, а потом усечением — в матрицу Эйлера [6] четного порядка с модулем уровня $b=\frac{q-\sqrt{8q}}{q-8}$, $q=n+2$, $n=4t-2$.

Матрицы Эйлера сходны с матрицами Адамара в том, что они четных порядков, для них справедливо следующее разложение на квадратные блоки:

$$\mathbf{E}_{2n}=\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix},$$

верхние блоки образуются из матриц Мерсенна $\mathbf{A}=\mathbf{B}=\mathbf{M}_n$. Расширение этого простого частного случая на матрицы с не совпадающими блоками даст весь набор порядков $n=4t-2$ матриц с указанными уровнями.

Матрицы Мерсенна есть для всех значений $n=4t-1$ без исключения. Матрицы Эйлера удобны для технических приложений тем, что они существуют, соответственно, для всех $n=4t-2$. Они удачным образом заполняют известные пробелы порядков 22, 34, 58 и т. п. среди квазиортогональных матриц Белевича [7]. Объясняется это тем, что матрицы Эйлера могут быть иррациональны, тогда как целочисленные матрицы Белевича даны только для порядков, на которых n–1 разложимо в сумму квадратов целых чисел.

7. Другие взаимосвязи квазиортогональных матриц. В работе [4] вводится определение, согласно которому порядок матриц Эйлера четен и равен $n=4t-2$, где t — натуральное число.

На основе матриц Мерсенна порядков $n=4t-1$, принимающих значения 3, 7, 11, 15…, вычисляются матрицы Эйлера порядков 6, 14, 30…. Так как каждая матрица Эйлера расширением ее каймой дает матрицу Мерсенна, серия матриц складывается в *основную* цепочку $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$.

Рассмотрим алгоритмы построения квазиортогональных матриц заданных порядков, а также произведем оценку сложности таких процедур. Заметим, что в итерационных алгоритмах вычисления матриц Мерсенна (см. раздел 4 настоящей статьи) нет необходимости вычислять собственные числа и собственные векторы $\mathbf{S}_{2n}$.

Для уменьшения трудоемкости решение этой задачи, служащее источником определения уровней, ищется аналитически [8]: половину элементов собственного вектора e матрицы $\mathbf{S}_{2n}$ составляют элементы $-b$, остальную — элементы a, что дает возможность быстрого вычисления матриц требуемых базисов в виде:

$$\mathbf{M}_{2n+1} = \begin{pmatrix} 1 & e^{\mathrm{T}} \\ e & \mathbf{S}_{2n} \end{pmatrix}.$$

Для большего понимания материала приведем числовой пример. Итерации вычисления матриц Мерсенна основной последовательности $n=2^k-1$ начинаются с матрицы:

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix}, \text{ причем } \mathbf{M}_3^* = \begin{pmatrix} -b & a & -b \\ a & -b & -b \\ -b & -b & a \end{pmatrix},$$

где $a=1$, модуль второго элемента $b=\dfrac{t}{t+\sqrt{t}}$ принимает значение 0,5 при $t=1$ (порядок $n=4t-1=3$) и растет до $b=2-\sqrt{2}=0{,}5858...$ при t=1 (порядок $n=7$). Учитывая выписанное выше выражение, расчетная матрица Мерсенна $\mathbf{M}_7=\begin{pmatrix}1 & e^{\mathrm{T}}\\ e & \mathbf{S}_6\end{pmatrix}$ при $e=(-b,-b,-b,1,1,1)^{\mathrm{T}}$ также квазиортогональна, итерации можно продолжить до бесконечности.

На рисунке 4 изображены первые три матрицы этого бесконечного семейства $\mathbf{M}_3$, $\mathbf{M}_7$, $\mathbf{M}_{15}$.

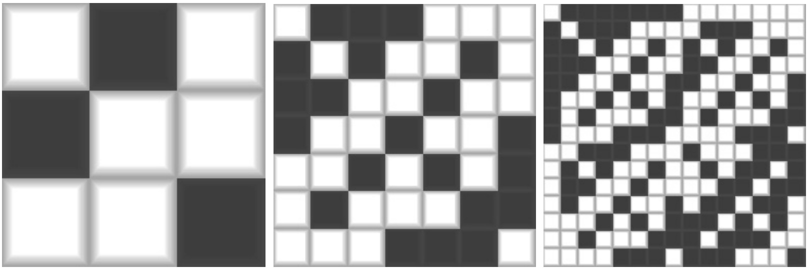

Рис. 4. Квазиортогональные матрицы Мерсенна $\mathbf{M}_3$, $\mathbf{M}_7$, $\mathbf{M}_{15}$

Приведенные выше формулы, как видно, несложно компьютеризировать, получая цепочки ортогональных по столбцам матриц Мерсенна *нечетных порядков* 2^k-1 — столь же легко, как и цепочки матриц Адамара *четных порядков* 2^k, содержащих элементы 1, –1.

Число уровней матриц Мерсенна ровно такое же, причем с ростом порядка значение модуля уровня второго элемента $b=\dfrac{t}{t+\sqrt{t}}$ стремится к 1, то есть эти две цепочки матриц сближаются между собой по значениям их элементов.

Алгоритм вычисления матриц Эйлера четных порядков использует алгоритм вычисления матриц Мерсенна, то есть не превосходит его по трудоемкости:

$$\mathbf{E}_{2n}=\begin{pmatrix}\mathbf{M}_n & \mathbf{M}_n\\ \mathbf{M}_n^{\mathrm{T}} & -\mathbf{M}_n^{\mathrm{T}}\end{pmatrix}.$$

В работе [11] показано, что цепочка последовательно вычисляемых матриц может начинаться непосредственно с матрицы Эйлера, если соответствующей ей по порядку матрицы Белевича нет.

Эти матрицы обладают сходными свойствами, вместе они образуют расширенное семейство матриц типа Адамара, и могут использоваться в прикладных алгоритмах, расширяя их возможности.

8. Рекомендации по вычислению цепочек матриц. Дополнительный анализ [6] показывает, что вместо стартовых матриц Мерсенна (когда их нет) можно использовать отличающиеся от них диагональными элементами матрицы Зейделя $\mathbf{S}_n$, в таком случае цепочка обретает другой предиктор: $\mathbf{S}_5 - \mathbf{E}_{10} - \mathbf{M}_{11} - \mathbf{E}_{22} - \mathbf{M}_{23} - \ldots$ или $\mathbf{S}_9 - \mathbf{E}_{18}$ $-\mathbf{M}_{19} - \mathbf{E}_{38} - \mathbf{M}_{39} - \ldots$ и т.п. Случай подробно рассмотрен с участием соавтора этой статьи в [11] и не комментируется подробно для полезной краткости. В работе [12] также показывается, что помимо универсальных матриц Эйлера существует сходная с ней частная структура, связанная с *золотым сечением*, а пропуск в последовательности матриц Белевича на порядке 22 [13] восполняется не только матрицей Эйлера $\mathbf{E}_{22}$, но и квазиортогональными матрицами с тремя [14] или шестью значениями элементов [15].

Тем не менее благодаря отмеченным взаимосвязям основное множество квазиортогональных матриц может быть вычислено на основе бициклических матриц Эйлера, когда блоки **A**, **B** — циклические.

Для квазиортогональных матриц произведение $\mathbf{A}^{\mathrm{T}}\mathbf{B}+\mathbf{B}^{\mathrm{T}}\mathbf{B}$ диагонально по определению. Несложно показать, что округление элементов матрицы Эйлера до 1 и –1 не сказывается на преобладании диагонали, причем в силу сохранения структуры блоков внедиагональные элементы хотя и теряют свое нулевое значение, но не перестают быть равными друг другу. Общее число элементов на диагонали и вне ее пропорционально квадрату размера блока, то есть растет очень быстро, что ограничивает грубый поиск матриц Эйлера тривиальным перебором $n!$ бинарных последовательностей блоков.

Тем не менее для матриц значений порядков до 100 и выше случайный поиск вполне возможен, если принять во внимание два существенных обстоятельства.

Первое из них состоит в том, что если блоки **A**, **B** — циклические матрицы, то их произведение и сумма $\mathbf{A}^{\mathrm{T}}\mathbf{B}+\mathbf{B}^{\mathrm{T}}\mathbf{B}$ (матричная невязка) тоже циклическая. То есть для них имеет место не квадратичный, а линейный рост сложности задачи. Элементы первой строки матрицы невязок для округленных матриц Эйлера, за исключением первого элемента диагонали, равны –2. Из них можно контролировать половину, поскольку вторая половина строки зависима.

Второе обстоятельство состоит в ассоциативной связи матриц Эйлера с числами. Размер первой матрицы Эйлера равен 6, из двух блоков один может быть симметричным, второй – кососимметричным (с точностью до элементов диагонали). Соответственно, все матрицы размеров $q\times6$, q — простое нечетное число, сохраняют это качество. Учет симметрии позволяет экономить при генерации случайных последовательностей ресурсы процессора. Изучение семейств матриц Эйлера по признакам их симметрии резко упрощает матричные генераторы. С точки зрения теории сигналов, контролируемая квадратичная невязка называется спектральной плотностью сигнальной последовательности PSD (power spectral density) [16].

На рисунке 5 в качестве примера приведена найденная перебором симметричная матрица Эйлера $\mathbf{E}_{66}$ размера $n=11\times6=66$, а на рисунке 6 матрица квадратичной невязки половинного размера 33 ее PSD-теста, причем для полного контроля ортогональности хватает вычисления и проверки на значение –2 половины (без диагонального элемента) ее верхней строки.

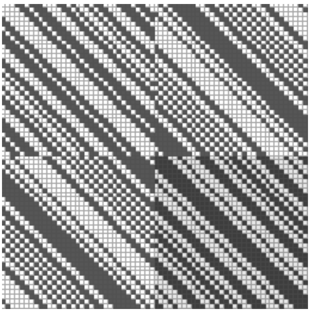

Рис. 5. Портрет матрицы $\mathbf{E}_{66}$

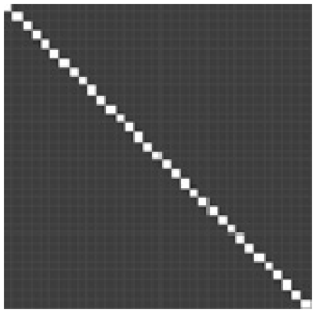

Рис. 6. Портрет PSD-теста для $\mathbf{E}_{66}$

Если генератор случайной последовательности распараллелен и работает быстрее технического устройства, на которое возложена проверка ортогональности (чаще всего это компьютер), можно контролировать не все, а несколько выборочно взятых значений квадратичной невязки. Это составляет основу так называемых PSD-тестов, фильтрующих миллионы ненужных для синтеза матриц Эйлера последовательностей.

9. Заключение. Ассоциация чисел с матрицами позволяет навести порядок среди множества матриц разнообразных базисов и свести проблему их поиска к нахождению бициклических матриц Эйлера. Как показано выше, сложности с их вычислением обходимы учетом специфики их структуры и присущих матрицам Эйлера симметрий. Выделение различных типов симметричных семейств значительно облегчает конструирование бинарных последовательностей для построения этих универсальных матриц и представляет непосредственный практический интерес для постановки как научных, так и учебных заданий в рамках целевых соревнований среди студентов в системе высшего образования по количеству и качеству находимых матриц (programming contests).

В процессе поиска квазиортогональных матриц четных и нечетных порядков, близких по своим свойствам к матрицам Адамара, удалось выделить классы матриц Мерсенна, Эйлера, Ферма. Матрицы Мерсенна порядков $4t-1$ регламентируют структуру матриц слева и справа от них, включая матрицы Адамара и Эйлера четных порядков $4t$ и $4t-2$ для t равных натуральным числам, а также матриц Ферма нечетных порядков $4t+1$ для t равных квадратам натуральных чисел u^2 (квадратичная ветвь квазиортогональных матриц). При отсутствии пропусков среди матриц Ферма, элементарным наращиванием каймы и пересчетом отрицательных элементов, периодически равных –1 и $-b$, можно было бы получить все квазиортогональные матрицы вдоль всей числовой оси, начиная со стартовой матрицы $\mathbf{H}_1 = 1$.

Пропуски матриц Ферма усложняют эту картину, лишая цепочки надстраиваемых матриц преемственности, что связано с разнообразием ассоциируемой числовой системы. Вместе с тем, появляются специфические матрицы-артефакты, наиболее полно отражающие особенность числа. Например, среди модификаций матриц Эйлера можно отметить, например, матрицу $\mathbf{G}_{10}$ со значениями элементов b, равными золотому сечению $b = \frac{\sqrt{5}-1}{2} \approx 0{,}618$.

Литература

1. Algebraic Design Theory and Hadamard Matricess / Edited by C.J. Colbourn // Springer Proceedings in Mathematics & Statistics. 2014. vol. 133. 260 p.
2. *Shalom E.* La conjecture de Hadamard (I) – Images des Mathématiques, CNRS. 2012. URL: http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (дата обращения: 15.03.2016).
3. *Балонин Н.А., Балонин Ю.Н., Востриков А.А., Сергеев М.Б.* Вычисление матриц Мерсенна-Уолша // Вестник компьютерных и информационных технологий. 2014. № 11. С. 51–55.
4. *Sylvester J.J.* Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers // Philosophical Magazine. 1867. vol. 34. no. 232. pp. 461–475.
5. *Hadamard J.* Résolution d'une question relative aux determinants // Bulletin des Sciences Mathématiques. 1893. vol. 17. pp. 240–246.
6. *Balonin N.A., Sergeev M.B.* Quasi-Orthogonal Local Maximum Determinant Matrices // Applied Mathematical Sciences. 2015. vol. 9. no. 6. pp. 285–293.
7. *Belevitch V.* Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. vol. 26. pp. 231–244.
8. *Балонин Н.А., Сергеев М.Б., Мироновский Л.А.* Вычисление матриц Адамара-Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92–94.

9. *Sergeev A.* Generalized Mersenne Matrices and Balonin's Conjecture // Automatic Control and Computer Sciences. 2014. vol. 4. pp. 35–43.
10. *Балонин Н.А., Сергеев М.Б., Мироновский Л.А.* Вычисление матриц Адамара-Ферма // Информационно-управляющие системы. 2012. № 6. С. 90–93.
11. *Balonin N.A., Vostrikov A.A., and Sergeev M.B.* On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices // Automatic Control and Computer Sciences. 2015. vol. 49. no. 3. pp. 153–158.
12. *Balonin N.A., Sergeev M.B*. Quasi-Orthogonal Matrices with Level Based on Ratio of Fibonacci Numbers // Applied Mathematical Sciences. 2015. vol. 9. no. 86. pp. 4261–4268.
13. *Balonin N.A., Seberry J.* A Review and New Symmetric Conference Matrices // Информационно-управляющие системы. 2014. № 4(71). pp. 2–7.
14. *Балонин Н.А., Сергеев М.Б.* Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационно-управляющие системы. 2013. № 5. С. 97–98.
15. *Балонин Ю.Н., Сергеев М.Б.* М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
16. *Djokovic D.Z., Kotsireas I. S.* Compression of periodic complementary sequences and applications // Des. Codes Cryptogr. 2015. vol. 74. pp. 365–377.

Балонин Юрий Николаевич — инженер кафедры вычислительных систем и сетей, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: вычислительные методы, теория чисел, компьютерное моделирование. Число научных публикаций — 13. yuraball@mail.ru; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +7(812)355-17-07.

Востриков Антон Александрович — к-т техн. наук, доцент, доцент кафедры вычислительных систем и сетей, Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП). Область научных интересов: обработка видеоинформации, IP-сети, распределенные информационно-управляющие системы, встраиваемые системы управления, системы обеспечения безопасности. Число научных публикаций — 38. vostricov@mail.ru; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +79219430422.

Сергеев Александр Михайлович — старший преподаватель кафедры вычислительных систем и сетей, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: обработка изображений, вычислительная математика. Число научных публикаций — 7. mbse@mail.ru; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +7(812) 494-70-44.

Егорова Ирина Сергеевна — аспирант кафедры вычислительных систем и сетей, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: специализированные системы обработки информации, проектирование цифровых устройств на базе ПЛИС, автоматизация проектирования вычислительных систем. Число научных публикаций — 4. irina.egorova@ask-lab.com; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +7(921)090-55-32

DOI 10.15622/SP.50.9

Ju.N. Balonin, A.A. Vostrikov, A.M. Sergeev, I.S. Egorova

ON RELATIONSHIPS AMONG QUASI-ORTHOGONAL MATRICES CONSTRUCTED ON THE KNOWN SEQUENCES OF PRIME NUMBERS

Balonin Ju.N., Vostrikov A.A., Sergeev A.M., Egorova I.S. **On Relationships among Quasi-orthogonal Matrices Constructed on the Known Sequences of Prime Numbers.**

Abstract. The objective of the paper is to show the relationship among numbers, belonging to known sequences of prime numbers, and quasi-orthogonal matrices, existing for orders equal to these numbers, and the relationship among such matrices based on calculating algorithms. Methods: analysis of the sequences of quasi-orthogonal matrices with absolute and local maximum of its determinant, detecting of the structural invariants in the matrices, matching algorithms for calculating these matrices. Results: known sequences of natural numbers are considered, the definition of a matrix, associated with a natural number, is formulated. Sequences of numbers with proved existence of quasi-orthogonal matrices associated with them are presented. It is suggested that associated matrices exist for all positive natural numbers. Properties of these types of matrices, their relationships based on calculating algorithms are considered. There are modified algorithms and general key chains of Euler and Mersenne matrices presented, a sequence of orders of which are systemically important. Practical value: quasi-orthogonal matrices of absolute and local maximum of determinant have immediate practical value for error-correcting coding tasks, video compression and masking. Their diversity allows developers of technical systems greatly facilitate a matrix selection, optimal one for a particular task.

Keywords: numerical sequences, Mersenne numbers, Fermat numbers, orthogonal sequences, quasiorthogonal matrices, Hadamard matrices, Mersenne matrices, Euler matrices, Fermat Matrices, matrix chains, quasiorthogonal matrix algorithms.

References

1. Algebraic Design Theory and Hadamard Matricess. Edited by C.J. Colbourn. Springer Proceedings in Mathematics & Statistics. 2014. vol. 133. 260 p.
2. Shalom E. La conjecture de Hadamard (I) – *Images des Mathématiques*, *CNRS*. 2012. http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (accessed: 15.03.2016).
3. Balonin N.A., Balonin Yu.N., Vostrikov A.A., Sergeev M.B. [Computation of Mersenne-Walsh Matrices]. *Vestnik komp'iuternykh i informatsionnykh tekhnologii – Herald of computer and information technologies*. 2014. vol. 11. pp. 51–55. (In Russ.).
4. Sylvester J.J. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Philosophical Magazine*. 1867. vol. 34. no. 232. pp. 461–475.
5. Hadamard J. Résolution d'une question relative aux determinants. *Bulletin des Sciences Mathématiques*. 1893. vol. 17. pp. 240–246.
6. Balonin N.A., Sergeev M.B. Quasi-Orthogonal Local Maximum Determinant Matrices. *Applied Mathematical Sciences*. 2015. vol. 9. no. 6. pp. 285–293.
7. Belevitch, V. Theorem of 2n-terminal networks with application to conference telephony, *Electr. Commun*. 1950. vol. 26. pp. 231–244.
8. Balonin N.A., Sergeev M.B., Mironovsky L.A. [Calculation of Hadamard-Mersenne Matrices]. *Informatsionno-upravliaiushchie sistemy – Information and Control Systems*. 2012. vol. 5(60). pp. 92–94 (In Russ.).

9. Sergeev A. Generalized Mersenne Matrices and Balonin's Conjecture, *Automatic Control and Computer Sciences*. 2014. no. 4. pp. 35–43.
10. Balonin N.A., Sergeev M.B. Mironovsky L.A. [Calculation of Hadamard-Fermat Matrices]. *Informatsionno-upravliaiushchie sistemy – Information and Control Systems.* 2012. vol. 6(61). pp. 90–93 (In Russ.).
11. Balonin N.A., Vostrikov A.A., Sergeev M.B. On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices. *Automatic Control and Computer Sciences*. 2015. vol. 49. no. 3. pp. 153–158.
12. Balonin N.A., Sergeev M.B. Quasi-Orthogonal Matrices with Level Based on Ratio of Fibonacci Numbers. *Applied Mathematical Sciences*. 2015. vol. 9. no. 86. pp. 4261–4268.
13. Balonin N.A., Seberry, Jennifer. A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie sistemy – Information and Control Systems*. 2014. no. 4 (71). pp. 2–7. (In English).
14. Balonin N.A., Sergeev M.B. [Weighted Conference Matrix Generalizing Belevich Matrix at the 22nd Order]. *Informatsionno-upravliaiushchie sistemy – Information and Control Systems*. 2013. vol. 5(66). pp. 97–98 (In Russ.).
15. Balonin Yu.N., Sergeev M.B. [M-matrix of 22nd order]. *Informatsionno-upravliaiushchie sistemy – Information and Control Systems*. 2011. vol. 5(54). pp. 87–90 (In Russ.).
16. Djokovic D.Z., Kotsireas I. S. Compression of periodic complementary sequences and applications. *Des. Codes Cryptogr*. 2015. vol. 74. pp. 365–377.

Balonin Yuriy Nikolaevich — engineer of computer systems and networks department, Saint Petersburg State University of Aerospace Instrumentation (SUAI). Research interests: numerical methods, number theory, computer simulation. The number of publications — 13. yuraball@mail.ru; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +7(812)355-17-07.

Vostrikov Anton Aleksandrovich — Ph.D., associate professor, associate professor of computer systems and networks department, Saint Petersburg State University of Aerospace Instrumentation (SUAI). Research interests: videoimage compression, IP-nets, distributed information and control, board control systems, safety systems. The number of publications — 38. vostricov@mail.ru; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +79219430422.

Sergeev Alexander Mikhailovich — senior lecturer of computer systems and networks department, Saint Petersburg State University of Aerospace Instrumentation (SUAI). Research interests: videoimage compression, numerical methods. The number of publications — 7. mbse@mail.ru; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +7(812) 494-70-44.

Egorova Irina Sergeevna — Ph.D. student of computer systems and networks department, Saint Petersburg State University of Aerospace Instrumentation (SUAI). Research interests: special information systems, PLIS digital system design, numerical system automatic design. The number of publications — 4. irina.egorova@ask-lab.com; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +7(921)090-55-32.