УДК 519.614

А. М. Сергеев
Санкт-Петербургский государственный университет аэрокосмического приборостроения

О взаимосвязи одного вида квазиортогональных матриц, построенных на порядках последовательностей $4k$ и $4k - 1$

Показана связь чисел, принадлежащих последовательностям 4k и 4k – 1, с симметричными квазиортогональными матрицами, существующими на порядках, равных этим числам. Показана взаимосвязь таких матриц через простейшие преобразования. В результате рассмотрены последовательности натуральных чисел вида 4k и 4k – 1, показано, что матрицы Мерсенна с округленными до целых значениями коэффициентов являются «ядром» матриц Адамара. Матрицы Адамара различных порядков и видов симметрии «портретов» имеют большое практическое значение при решении задач обработки информации в медицинской диагностической технике, в задачах сжатия и преобразования видеоинформации. Найти матрицу Адамара через матрицу Мерсенна просто, что позволяет быстро вычислять оптимальную для конкретной задачи матрицу.

Медицинская техника, обработка информации, преобразование изображений, числовые последовательности, числа Мерсенна, квазиортогональные матрицы, минимаксные матрицы, матрицы Адамара, матрицы Мерсенна

Широко известно использование в задачах обработки и преобразования информации матриц Адамара – квадратных матриц $\mathbf{H}_n$ порядка n, состоящих из чисел {1, –1}, столбцы которых ортогональны: $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}$, где $\mathbf{I}$ – единичная матрица.

Внедрение цифровых технологий в медицинскую технику, технологии представления и обработки данных в генетике, биомеханике, маскировании видеоданных в системах телемедицины [1]–[6] ставит задачу пересмотра основ, на которых базируются используемые цифровые методы.

Гипотеза Адамара о кратности числу 4 значений порядков $\mathbf{H}_n$ устанавливает период, с которым появляются сопутствующие типы квазиортогональных матриц [7]–[9] четных и нечетных порядков, соответствующих всем числам натурального ряда. Расширение ортогонального базиса способствует упрощению выбора конкретных матриц, оптимальных для соответствующей задачи. Особый интерес представляет обоснование существования и поиск минимаксных квазиортогональных матриц нечетных порядков.

Матрицы Адамара – минимаксные в том смысле, что на множестве полученных из них ортонормированных матриц того же порядка максимум m (m-норма матрицы) абсолютных значений их элементов минимален [9]. Любые другие типы ортонормированных матриц имеют более высокое значение m. Первый алгоритм вычисления минимаксных матриц порядков $n = 2^k$ предложил Сильвестр [7]. Обнаружив не входящие в последовательность Сильвестра матрицы $\mathbf{H}_{12}$ и $\mathbf{H}_{20}$ [8], Адамар предположил, что они встречаются чаще и существуют для всех порядков $n = 4k$.

Значения, которые принимают элементы минимаксных матриц, называются уровнями [9]. Матрицы Адамара – модульно одноуровневые матрицы. Такой степени совершенства – минимума модулей ортогональных элементов – достигают только эти минимаксные матрицы. В [10], [11] предложены версии двухуровневых (по количеству значений элементов матрицы) квазиортогональных матриц нечетных порядков, равных числам Мерсенна и Ферма. Последовательность Мерсенна, задаваемая как $n = 2^k - 1$, принадлежит

подмножеству чисел вида $4k-1$. Последовательность Ферма, определяемая формулой $n=2^{2^k}+1$, принадлежит подмножеству чисел вида $4k+1$.

В [12] Н. А. Балониным сформулирована гипотеза о существовании матриц Мерсенна на всех нечетных порядках n, при которых значение $n+1$ кратно 4. Несколько в иной формулировке эта теорема означает, что каждой матрице Адамара четного порядка $n+1=4k$ должна соответствовать матрица Мерсенна нечетного порядка n.

В настоящей статье показывается, что последовательности Мерсенна и Сильвестра, в отличие от последовательности Ферма, сходны тем, что ассоциированные с ними матрицы встречаются чаще, а матрица Мерсенна с округленными до целых значений коэффициентами является «ядром» (core) матриц Адамара особого вида.

Классификация минимаксных квазиортогональных матриц. Нечетные числа последовательностей $4k-3$ (или $4k+1$) и $4k-1$ (или $4k+3$) ввели Ферма и Эйлер. Ферма установил, что всякое простое число вида $4k+1$ может быть представлено в виде суммы двух квадратов, причем единственным образом. Например, $5=1+4$. Простые числа вида $4k+3$ в виде суммы квадратов не представимы. Это обстоятельство используется в теории квазиортогональных матриц четных порядков $n=4k-2$, поскольку критерий Эйлера–Ферма о разложимости числа $n-1=4k-3$ (не всегда простого) на сумму двух квадратов входит в проверку необходимых условий их существования.

Для того чтобы оперировать с любыми четными и нечетными порядками, понятие минимаксности квазиортогональных матриц расширяется. Минимум может быть двух сортов: абсолютный минимум функции и локальный – частный минимум. По отношению к m-норме матрицы применимо как то, так и другое понятие.

Матрицы Адамара минимаксны в первом смысле абсолютного минимума максимума ее элементов. Остальные двухуровневые матрицы отвечают локальному максимуму, поскольку на нечетных порядках минимизация m-нормы приводит к значительному росту числа уровней с ростом порядка [9]. Только у матриц четных порядков число уровней с ростом порядка не растет. Таковы матрицы Адамара и трехуровневые матрицы Белевича (их называют **C**-матрицами) с элементами 0, 1, –1.

Таким образом, двух- и трехуровневые минимаксные в указанном широком смысле матрицы образуют специфическую расширенную семью матриц Адамара с малым числом уровней и произвольного четного или нечетного порядка. Это обстоятельство свидетельствует о значительном расширении базиса для ортогональных преобразований видеоизображений в прикладных задачах.

Рассмотрим 4 возможных варианта минимаксных квазиортогональных матриц с малым числом различающихся значений элементов [13] – малоуровневых M-матриц [9]. В зависимости от остатка r деления порядка n на 4 они могут быть классифицированы следующим образом [13]:

– $r=0$ – матрицы Адамара (**H**), включающие матрицы последовательности Сильвестра;

– $r=1$ – матрицы Ферма (**F**), включающие матрицы порядков последовательности чисел Ферма;

– $r=2$ – матрицы Эйлера (**E**), дополняющие матрицы Белевича (**C**) на исключениях, определяемых критерием Эйлера–Ферма;

– $r=3$ – матрицы Мерсенна (**M**), включающие матрицы порядков последовательности чисел Мерсенна.

Малоуровневые M-матрицы включают, таким образом, матрицы **H**, **F**, **E** и **M** множества квазиортогональных матриц, в которых последовательности Сильвестра и Мерсенна, по предположению [6], являются системообразующими. Оценки плотности охвата числовой оси значениями порядков матриц основываются, соответственно, на сходных гипотезах: гипотезе Адамара (Hadamard conjecture) – перенос свойств матриц порядков последовательности Сильвестра на **H**; гипотезе Балонина (Balonin conjecture) – перенос свойств матриц порядков последовательности Мерсенна на **M**.

Для обобщения понятия матриц Адамара–Мерсенна в [10], [12] предложено определение матрицы Мерсенна как квадратной матрицы **M** порядка n, состоящей из чисел $\{a=1, -b\}$, столбцы которой ортогональны: $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n=\mu\mathbf{I}$. Здесь $b=a/2$ при $n=3$, в остальных случаях $b=\dfrac{q-\sqrt{4q}}{q-4}$, где $q=n+1$ (порядок матрицы Адамара) [10].

Вес $\mu=\dfrac{(n+1)+(n-1)b^2}{2}$ учитывает, что $q/2$ элементов каждого столбца такой матрицы составляют $a=1$, остальные элементы равны $-b$. По m-норме превалируют эти решения, хотя, как и у

матриц Адамара, имеются сопутствующие «инверсные» решения с элементами $b = \frac{q + \sqrt{4q}}{q - 4}$.

Модифицированная последовательность Сильвестра [10] вычисления матриц Мерсенна начинается с вычисления блочной матрицы

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

и отличается от классической последовательности [7] тем, что матрица $\mathbf{M}_n^*$ образована перестановкой местами элементов $a = 1$ и $-b$ в отличие от простой смены знаков элементов модульно одноуровневых матриц Адамара.

Матрицы порядков, соответствующих числам как последовательности Мерсенна $n = 2^k - 1$, так и дополнительным $4k - 1$ (в которые числа Мерсенна вложены), образованы расширением указанной основы строкой и столбцом в виде

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

где $\lambda = -a$ – собственное число; $\mathbf{e}$ – собственный вектор матрицы $\mathbf{S}_{2n}$, половину элементов которого составляют $-b$, остальные элементы принимают значения a. Процедура вычисления матриц Мерсенна основной «сильвестровой» последовательности начинается с матрицы минимального размера 3 с каймой той же самой структуры

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix}.$$

Рассмотрение сходной основной последовательности матриц порядков $n = 2^k + 1$ (при четных k), включающих числа Ферма [10], также ведет к малоуровневым вариантам матриц. На этом, однако, сходство заканчивается, что отражает особое значение матриц Мерсенна в предложенной ранее классификации минимаксных квазиортогональных матриц.

Гипотеза Балонина. Впервые гипотеза была сформулирована в [12] в следующем виде: матрицы Мерсенна существуют на всех порядках, равных $4k - 1$.

Для раскрытия содержания этой гипотезы на рис. 1 и 2 приведены портреты двух матриц Мерсенна $\mathbf{M}_{11}$ $\left(b = \frac{5 - \sqrt{5}}{2}\right)$ и $\mathbf{M}_{19}$ $\left(b = \frac{3 - \sqrt{3}}{2}\right)$, впервые опубликованные в [12]. Элементу $a = 1$ соответствует белый цвет на портрете матрицы, элементу $-b$, соответственно, черный цвет.

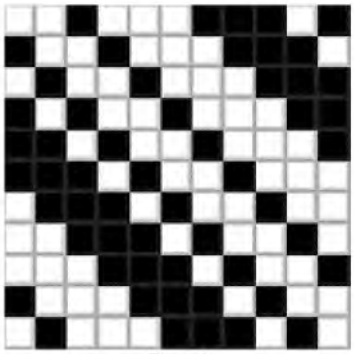

Рис. 1

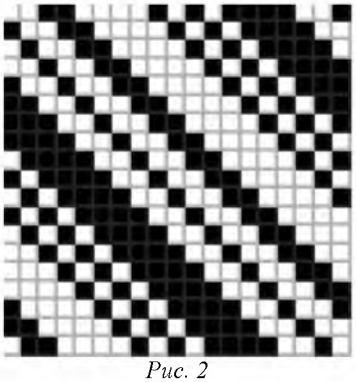

Рис. 2

Обе приведенные матрицы нечетных порядков являются циклическими квазиортогональными. Они, как и матрицы Адамара $\mathbf{H}_{12}$ и $\mathbf{H}_{20}$, находятся за пределами описанной ранее модифицированной итерационной последовательности Сильвестра, но их признаки (значения уровней элементов) соответствуют базовому определению матриц Мерсенна. Как и в случае матриц Адамара, вложенность последовательности чисел Мерсенна в более широкое множество нечетных чисел взаимно-однозначно соответствует вложенности сопутствующих им матриц.

Заметим, что согласно гипотезе Райзера порядок циклических матриц Адамара конечен и не превышает значения 4. Ввиду этого матрицы Адамара приходится искать в более сложном блочно-составном виде. Матрицы Мерсенна устроены проще, поскольку они связаны с менее жестким ограничением по норме максимального элемента. Они всего лишь минимаксны, но этот минимум – локальный. Для ортогональных базисов обработки видеоизображений простой циклический вид ортогонального массива переворачивает все привычные представления на этот счет.

В отличие от матриц Адамара, ограниченных всего лишь порядком 4, матрицы Мерсенна цик-

личны для порядка, равного любому числу Мерсенна. Кроме того, на расширенном множестве порядков простота вида матрицы (циклическая) однозначно связана с простотой числа. У этого правила есть исключение (если не считать непростых чисел Мерсенна). Порядки, равные произведениям пар близких простых целых чисел, разделяют с ними вид матрицы – циклический. Таковы матрицы Мерсенна порядков $15 = 3 \times 5$ и $35 = 5 \times 7$. Порядок $63 = 7 \times 9$ тоже соответствует циклической матрице, но по иной причине. Число 64 является числом Мерсенна, а они все связаны с ортогональными циклическими массивами.

Гипотеза Балонина утверждает, что матрица Мерсенна найдется для любого порядка $4k - 1$. Очевидно, что ее максимально общий вид не может значительно усложниться и существенно отличаться от моноциклического вида. Общее решение связано с бициклическим видом матриц. Бициклические матрицы Мерсенна состоят из пары циклических матриц и каймы. На них уже не отражается простота порядка или равенство порядка избранным числовым сочетаниям. Матрицы Мерсенна $\mathbf{M}_{11}$ (рис. 3) и $\mathbf{M}_{19}$ (рис. 4) можно сделать бициклическими. В общем случае матрицы Мерсенна ограничены в сложности и, соответственно, нет никаких ограничений на их построение. Как видно, это является предпосылкой доказательства гипотезы Адамара.

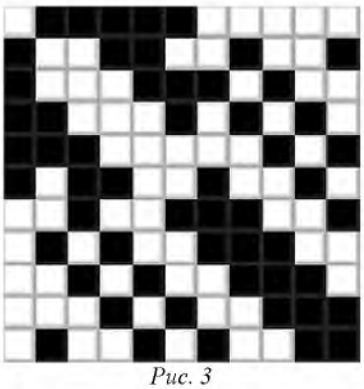

Рис. 3

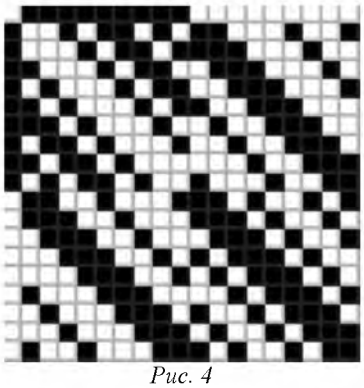

Рис. 4

Матрицы Мерсенна как «ядро» матриц Адамара. Для нахождения квазиортогональных матриц Адамара порядков $4k$ предлагается применять прием, который основан на свойствах собственных чисел и собственных векторов блочных матриц и позволяет получать матрицы Адамара одного особого вида по матрицам Мерсенна порядков $4k - 1$.

Матрица Адамара $\mathbf{H}_{4k}$ будет получена из матрицы $\mathbf{M}^*_{4k-1}$, в которой округлены до -1 значения элементов $-b$ матрицы Мерсенна $\mathbf{M}_{4k-1}$, с дальнейшим окаймлением в виде

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

где $\lambda = 1$, $\mathbf{e}$ – соответственно собственное число и собственный вектор матрицы $\mathbf{M}_{4k-1}$, состоящий из 1.

Обратный прием – усечением соответствующим образом нормированной матрицы Адамара и изменением отрицательных значений ее элементов до расчетного значения уровня $-b$ будет получена матрица Мерсенна, являющаяся в этом случае «ядром» (core) матрицы Адамара. Отметим, что, в отличие от так называемого *нормального* вида матриц Адамара с положительными элементами первых строк столбца, в данном случае согласно алгоритму построения первый элемент каймы отрицательный и равен -1.

Для перехода к классическому нормальному виду матриц Адамара надо изменить знаки элементов ее «ядра» на противоположные.

В качестве примера симметричных матриц на рис. 5 приведены портреты матриц Мерсенна $\mathbf{M}_7$ (слева) и найденной соответствующей ей матрицы Адамара $\mathbf{H}_8$ (справа), а на рис. 6 – портреты матриц Мерсенна $\mathbf{M}_{11}$ и Адамара $\mathbf{H}_{12}$ соответственно. Каждая из таких матриц, включая отмеченные ранее матрицы $\mathbf{M}_{11}$ и $\mathbf{M}_{19}$, является исходной для получения своей последовательности матриц применением модифицированного (на случай нечетных порядков) алгоритма Сильвестра. Следовательно, множество таких матриц расширяемо, в полном соответствии с тем, как это происходит у матриц Адамара.

В [14] понимание рассматриваемой гипотезы Балонина продвинуто за счет сравнения графиков m-норм матриц Адамара и Мерсенна. Решение вопроса о сходимости последовательности h-норм

(приведенных m-норм или адамаровых норм матриц) к единице при возрастании n ведет к осознанию факта сглаживания различий двух рассматриваемых классов матриц. При $k \to \infty$ матрицы Мерсенна и Адамара становятся практически не различимыми по m-норме.

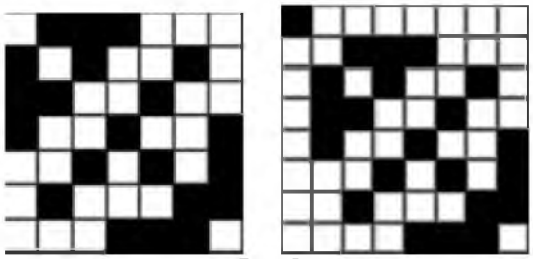

Рис. 5

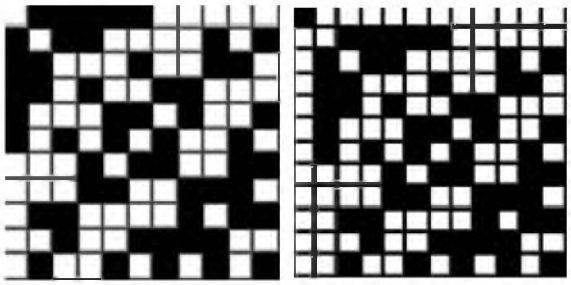

Рис. 6

Вид матрицы Мерсенна существенно зависит от характера приложения. Для генераторов криптографических кодов с помощью твистеров Мерсенна [2] используется циклическая форма этой матрицы. При циклическом сдвиге между первыми k элементами столбцов матрицы порядка $n = 2^k - 1$ наблюдается особенно простое соотношение, удобное для реализации генераторов и декодеров.

В связи с этим срезанный верх матрицы Мерсенна шириной k и длиной $n >> k$ используется как источник кодов букв, устойчивых к искажениям при передаче информации в канале.

Сортировка столбцов той же матрицы, полученной алгоритмом Сильвестра, дает коды Мерсенна–Уолша, отличающиеся от классических кодов Уолша нечетной длиной. Это столбцы матрицы Мерсенна, а не матрицы Адамара. Функции Мерсенна–Уолша ортогональны и могут использоваться для разделения сигналов в каналах ультразвукового сканирования местности.

Наконец, при маскировании видеоизображений [5] необходимы не только четные, но и нечетные размеры матриц при относительной простоте избираемого базиса. В таком случае используются бициклические матрицы Мерсенна с одной каймой.

Преимущества предложенной классификации. Гипотеза Адамара о кратности порядков квазиортогональных матриц числу 4 отвечает известной периодичности свойств в теории чисел (связанной также с периодичностью химических элементов в таблице Менделеева, с четырьмя основаниями генокода [3], [4]) и поднимает вопрос об оставшихся трех типах матриц, родственных матрицам Адамара. Этот вопрос естественен, поскольку в приложениях пропуски порядков чем-то надо заполнять, и заполнять их следует сходными с матрицами Адамара двухуровневыми конструкциями.

В процессе поиска квазиортогональных матриц нечетных порядков [9], [11]–[14], близких по своим свойствам к матрицам Адамара, выделен класс малоуровневых M-матриц, названных обобщенными матрицами Адамара–Мерсенна (на порядках, равных числам Мерсенна) или, для простоты, матрицами Мерсенна на всех нечетных порядках вида $4k - 1$. Точно такова же была логика перехода от матриц Сильвестра [7] к матрицам Адамара [2], когда программу вложения числовых последовательностей и сопутствующих им матриц выдвинул Адамар.

Этим матрицы Мерсенна существенно отличаются от многоуровневых обобщений матриц Адамара [15] на нечетных значениях порядков, чья сложность, к тому же, неограниченно нарастает. Невозможно указать общий вид этих альтернативных матриц.

Предложенная классификация включает в себя все возможные случаи четных и нечетных порядков, в том числе порядки, кратные двум [16]. В пояснение сформулированной Н. А. Балониным гипотезы о существовании матриц Мерсенна порядков $4k - 1$ (и их четных порождений, образуемых усечением каймы) найдены матрицы Мерсенна $\mathbf{M}_{11}$ и $\mathbf{M}_{19}$ [12]. Отмечено, что предположение, при его справедливости, значительно увеличивает количество малоуровневых минимаксных ортогональных матриц, рассмотренных в [11], [12], [16]. Таким образом, оно достаточно важное и принципиальное для теории малоуровневых квазиортогональных матриц.

Другие взаимосвязи последовательностей квазиортогональных матриц, построенных на известных последовательностях чисел, приведены в [16]–[18].

Построение матриц Мерсенна порядков $4k - 1$ регламентируют структуру матриц Адамара четных порядков $4k$ одного из возможных видов. Ги-

потезы о существовании матриц Адамара и матриц Мерсенна взаимно связаны – это сходные предположения о существовании квазиортогональных матриц четных и нечетных порядков. Из доказательства одной из гипотез будет следовать справедливость высказанного предположения для другой. Данное обстоятельство не было известно для матриц Адамара, поскольку случай нечетных порядков, в силу иррациональности значений уровней матриц, рассматривался ранее не достаточно подробно.

Работа выполнена при поддержке Минобрнауки РФ при проведении научно-исследовательской работы в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/ПЧ.

СПИСОК ЛИТЕРАТУРЫ

1. Ali Behrooz, Ali A. Eftekhar, Ali Adibi. Hadamard multiplexed fluorescence tomography // Biomedical Optics Express. 2014. Vol. 5, iss. 3. P. 763–777. DOI: doi.org/10.1364/BOE.5.000763.

2. Horadam K. J. Hadamard Matrices and Their Applications. Princeton, NJ: Princeton University Press, 2007. 263 p.

3. Петухов С. В. Матричная генетика, алгебры генетического кода, помехоустойчивость / НИЦ «Регулярная и хаотическая динамика». М., 2008. 316 с.

4. Петухов С. В. Вибрационная генетическая биомеханика и наследуемые системы биологических резонансов // Медицина и высокие технологии. 2015. № 2. С. 16–28.

5. Balonin N., Sergeev M. Construction of transformation basis for video image masking procedures // Frontiers in Artificial Intelligence and Applications. 2014. Vol. 262. P. 462–467. DOI 10.3233/978-1-61499-405-3-462.

6. Vostrikov A., Sergeev M. Expansion of the quasi-orthogonal basis to mask images // Smart Innovation, Systems and Technologies. 2015. Vol. 40. P. 161–168. DOI 10.1007/978-3-319-19830-9_15.

7. 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. P. 461–475.

8. Hadamard J. Résolution d'une question relative aux determinants // Bulletin des Sciences Mathématiques. 1893. № 17. P. 240–246.

9. Балонин Н. А., Сергеев М. Б. М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14–21.

10. Балонин Н. А., Сергеев М. Б., Мироновский Л. А. Вычисление матриц Адамара–Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92–94.

11. Балонин Н. А., Сергеев М. Б., Мироновский Л. А. Вычисление матриц Адамара–Ферма // Информационно-управляющие системы. 2012. № 6 (61). С. 90–93.

12. Балонин Н. А. О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 89–90.

13. Сергеев А. М. Обобщенные матрицы Мерсенна и гипотеза Балонина // Автоматика и вычислительная техника. 2014. № 4. С. 35–43.

14. Балонин Н. А., Сергеев М. Б. К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5 (66). С. 2–8.

15. Балонин Н. А., Мироновский Л. А. Матрицы Адамара нечетного порядка // Информационно-управляющие системы. 2006. № 3. С. 46–50.

16. Балонин Н. А., Сергеев М. Б. О двух способах построения матриц Адамара–Эйлера // Информационно-управляющие системы. 2013. № 1 (62). С. 7–10.

17. О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел / Ю. Н. Балонин, А. А. Востриков, А. М. Сергеев, И. С. Егорова // Тр. СПИИРАН. 2017. № 1 (50). С. 209–223. DOI: http://dx.doi.org/10.15622/sp.50.9.

18. 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, № 3. P. 153–158. DOI: 10.3103/S0146411615030025.

A. M. Sergeev
Saint Petersburg State University of Aerospace Instrumentation

THE INTERCONNECTION OF ONE KIND OF QUASI-ORTHOGONAL MATRICES BUILT ON THE ORDERS OF THE SEQUENCES 4*k* AND 4*k* – 1

The paper shows the interconnection among numbers, belonging to the sequences 4k and 4k – 1, and symmetric quasi-orthogonal matrices, existing on orders equal to these numbers. To show the interconnection of such matrices through the simplest transformations. As a result, sequences of natural numbers of the form 4k and 4k – 1 are considered, it is shown that the Mersenne matrices with rounded to integral values of the coefficients are the «core» of the Hadamard matrices. The Hadamard matrices of different orders and types of symmetry of its «portraits» are of great practical importance for solving problems of information processing in medical diagnostic equipment, in tasks of videoinformation compression and transformation. The evaluation of Hadamard matrices through Mersenne matrices is simple, allowing one to quickly obtain a matrix, which is optimal for a particular issue.

Medical equipment, information processing, image transformation, numerical sequences, Mersenne numbers, quasi-orthogonal matrices, minimax matrices, Hadamard matrices, Mersenne matrices