УДК 519.61:511-33 **DOI** 10.15622/sp.54.10

Н.А. Балонин, М.Б. Сергеев, В.С. Суздаль

ДИНАМИЧЕСКИЕ ГЕНЕРАТОРЫ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ СЕМЕЙСТВА АДАМАРА

Балонин Н.А., Сергеев М.Б., Суздаль В.С. **Динамические генераторы квазиортогональных матриц семейства Адамара.**

Аннотация. Исследуется задача построения нелинейных и линейных определенных в конечном поле генераторов квазиортогональных матриц семейства Адамара с малым количеством отличных между собой значений их элементов, не превосходящих по абсолютной величине 1, и глобальным или локальным значением детерминанта. Проанализированы свойства таких динамических систем, приведена классификация полученных с их помощью семейств матриц и их орнаментов, показан путь доказательства существования вещественных и целочисленных матриц, отличный от средств комбинаторного подхода. Значения, которым равны элементы матрицы, названы ее уровнями. Введены понятия адамаровой нормы и определителя квазиортогональной матрицы. Уровни, адамарова норма и определитель играют фундаментальную роль в определениях классов обобщенных матриц семейства Адамара. Выделены классы матриц Адамара, Белевича (конференц-матриц), Себерри (взвешенных матриц), Мерсенна, Эйлера, Одина (Зейделя), Ферма. Приведены формулы для значений их уровней. Орнаменты матриц Эйлера отвечают на вопрос максимальной сложности структуры матриц Адамара — бицикл с двойной каймой.

Ключевые слова: динамические генераторы, квазиортогональные матрицы, детерминированный хаос, конечные поля.

1. Введение Квазиортогональные матрицы — квадратные матрицы, ортогональные по строкам и столбцам с относительно простыми значениями элементов. К простейшим среди них относятся матрицы Адамара с элементами 1 и -1, применяемые в помехоустойчивом кодировании информации [1, 2]. Интерес к ним не проходит, за минувшее столетие вышло не поддающееся обозрению количество научных работ.

Тем не менее и сейчас публикуются таблицы матриц [3], пробелы таблиц изучаются специальными исследованиями [4, 5, 6]. Обуславливается это тем, что орнамент (узор) бинарных по знакам элементов матриц усложняется с ростом порядка.

Поясним, почему это важно. Матрицы Адамара — это матрицы максимума детерминанта, чей размер кратен 4 и отвечает числу оснований генетического кода. На первой международной конференции (AIMEE2017), организованной ИМАШ РАН совместно с ассоциацией RAMECS (Китай), отмечалась [7] связь структурной организации алфавитов ДНК с формализмами теории помехоустойчивого кодирования информации (функциями Уолша и Радемахера).

Эта точка зрения, развиваемая в книгах и статьях С.В. Петухова по матрично-алгебраическому анализу системы генетического кодирования живых организмов [8], оказывается привлекательной для

написания совместных работ международным коллективом исследователей, например [9]. Мун Хо Ли, давно работающий с обобщениями матриц Адамара, предложил использовать жакетные матрицы — не ортогональные матрицы, инвертируемые посредством всего лишь инверсии их элементов и масштабирования. Эта черта роднит их с симметричными матрицами Адамара.

На конференции прозвучал также доклад Ю.И. Манина , ныне автора классических работ по теории чисел, искусственному интеллекту и кодированию (публикация готовится). В задачах про орнаменты целочисленное решение в виде матриц Адамара зависит от иррациональных по своей природе бициклов Эйлера. Занимаясь в шестидесятые годы знаменитой гипотезой Морделла, Ю.И. Манин так сформулировал такого рода соответствия [10]: «Взаимодействие алгебраической геометрии с теорией чисел привело к пониманию удивительного и фундаментального принципа: ответы на Диофантовы вопросы о системе уравнений критически зависят от геометрической формы пространства всех комплексных решений этой системы. Например, пространство всех комплексных решений может выглядеть (топологически) как сфера или тор, или сфера с несколькими ручками. Количество ручек называется родом, это очень устойчивый инвариант системы уравнений и, кажется, что он имеет мало общего с арифметическими тонкостями и дискретными точками решетки целочисленных векторов (в проективном пространстве различие между целыми и рациональными точками стирается).

Тем не менее род определяет, когда множество всех рациональных решений может быть бесконечным: только если ручек не больше одной».

В работах сотрудника института сцинтилляционных монокристаллов НАН Украины В.С. Суздаля исследуется связь квазикристаллов Шехтмана [11] с квазиортогональными матрицами золотого сечения [12]. Такие матричные многомерные модели, дополняющие плоские мозаики Пенроуза, рассматриваются впервые. Динамические алгоритмы их получения — новые, неизвестные ранее в кристаллографии модели кристаллизации [13], описывающие иррациональности, присущие квазикристаллам. Строение химической таблицы Менделеева, кристаллы, структурные особенности ДНК — все это перекликается с темой построения матриц Адамара и их обобщений.

Вместе с тем динамические системы финитного времени [14] отличают собственные функции теплицева и ганкелева операторов, порождающих в ряде практически важных случаев ортогональные массивы, в том числе и интересующие нас матрицы. Эта точка зрения нова

и недостаточно освещена в научной литературе в силу долгого превалирования чисто комбинаторных методов исследования матриц Адамара. Итерационные процессы, ведущие к ортогональным матрицам, можно реализовать в конечных полях Галуа, но в этом случае приходится считаться с фактом существования поля. Поля не создать для составных размеров матриц, но, как показывает опыт, сохраняются присущие решениям задач в конечном поле явная или скрытая симметрии кодовых последовательностей [15-17].

Это наблюдение является предпосылкой для нахождения соответствующих орнаментов матриц на всех порядках матриц Адамара, выявляемых алгоритмами оптимизации детерминанта. По отношении к комбинаторным методам, оперирующим целочисленными матрицами, оптимизационный подход демонстрирует некоторые преимущества. Например, еще в античные времена было обнаружено, что диагональ прямоугольного с равными катетами треугольника не приблизить отношениями целых величин. Эта задача разрешима на более широком множестве чисел, порожденном изучением итерационных процессов и рядов. Квазиортогональные матрицы с их иррациональными элементами выступают как посредники в решении известной проблемы Адамара относительно существования матриц на всех порядках, кратных 4.

2. Предварительные сведения, определения и свойства. *Определение 1.* Квазиортогональной матрицей [15] будем называть квадратную матрицу A порядка *n* с приведенным к единице максимумом абсолютных значений ее элементов, удовлетворяющую квадратичному условию связи $A^{\mathrm{T}}A = \omega(n)I$, где n — любое натуральное число, $\omega(n)$ — некоторая весовая функция, определяющая тип матрицы, а I — единичная матрица.

Квазиортогональными в широком смысле будем называть любые ортогональные по столбцам (и строкам) матрицы. В этом случае они включают в себя также ортогональные матрицы с весом $\omega = 1$ и максимальным по модулю элементом $m < 1$.

Определение 2. Значения, которым равны элементы матрицы, будем называть ее уровнями.

Например, матрица Адамара с элементами {1, −1} имеет два уровня (двухуровневая), а матрица Белевича (конференц-матрица, взвешенная матрица) с элементами {0, 1, −1} — трехуровневая [1]. Квазиортогональные матрицы семейства Адамара с элементами, не превышающими по модулю единицы, лежат на пересечении M двух классов (рисунок 1): D-матриц абсолютного максимума детерминанта (не ортогональных по столбцам) и квазиортогональных W-матриц (безотносительных к оптимуму детерминанта) с некоторым (желательно небольшим) количеством уровней.

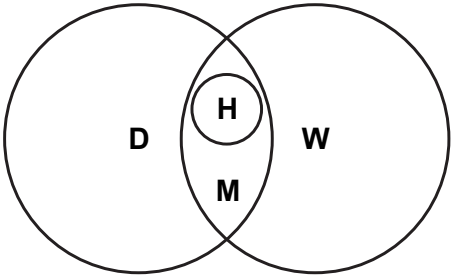

Рис. 1. Диаграмма Венна пересечения M множеств D-матриц и W-матриц, отражающая подмножество H матриц Адамара

Теорема. Утверждается, что $\left|\det\left(A\right)\right| \le n^{n/2}$ для всех матриц A с элементами, не превышающими по модулю единицы [1].

Теорема вводит в рассмотрение нестрогое *неравенство* Адамара, равенство достижимо только на матрицах Адамара H с их экстремально малым количеством уровней (два) при экстремально большом детерминанте. Классические матрицы Адамара образуют на пересечении D-матриц и W-матриц подмножество H всех матриц с единичными по модулю элементами. Возможность обобщения матриц Адамара базируется на том, что матрицы класса H существуют не для всех значений порядков *n*. Соответственно, можно сформулировать задачу поиска квазиортогональных матриц с максимально достижимым значением детерминанта, то есть матриц M, к которым принадлежит, например, часть матриц Белевича.

Вес $\omega = 1$ характерен для ортогональных матриц, к которым квазиортогональные матрицы, в частности матрицы Адамара, помимо тривиальной матрицы первого порядка, не относятся. Вместе с тем это матрицы весьма близкие к ортогональным, получаемым из A элементарным нормированием их столбцов, после чего максимальный по модулю элемент (*m*-норма) уменьшается до $m < 1$ для порядков, больших 1.

Определение 3. Минимаксными квазиортогональными M-матрицами [15, 17] в строгом смысле будем называть матрицы, обладающие минимумом *m*-нормы на классе квазиортогональных матриц порядка *n*.

Несложно заметить, что $\left|\det\left(A\right)\right| = \omega^{n/2}$, причем $\omega = 1/m^2$.

Матрица Адамара H, обладающая максимумом модуля детерминанта, имеет минимальное значение $m = 1/\sqrt{n}$, то есть является частным случаем M-матриц с весом $\omega = n$. Отсутствие оптимального решения на границе неравенства Адамара искусственное, поскольку возможен поиск достижимого максимума модуля детерминанта.

Определение 4. Минимаксными квазиортогональными М-матрицами [15, 17] в общем смысле будем называть матрицы, обладающие глобальным или локальным минимумом m-нормы на классе квазиортогональных матриц порядка n.

Такие М-матрицы более широко представлены, они обладают глобальным или локальным максимумами модуля детерминанта.

Определение 5. Адамаровой нормой (h-нормой, взвешенной m-нормой) матрицы будем называть показатель $h = m\sqrt{n}$.

Адамарова норма отражает близость матрицы к матрице Адамара, у которой она имеет минимально возможное значение $h = 1$. Модуль детерминанта квазиортогональной матрицы $\left|\det(A)\right| = 1/m^n = n^{n/2}/h^n$ включает в себя правую часть неравенства Адамара $n^{n/2}$, пониженную до достижимой величины делением на n-ю степень h-нормы.

Определение 6. Приведенным определителем или адамаровым определителем матрицы будем называть величину $D = 1/h^2 = 1/(nm^2)$.

Вычислить адамаров определитель несложно, он удобен тем, что выступает множителем в выражении $\left|\det(A)\right| = (Dn)^{n/2}$, $D \le 1$. Уровни, адамаровы норма и определитель играют фундаментальную роль в определениях классов обобщенных матриц семейства Адамара [3, 16]. Для всех матриц Адамара $D = 1$. Для остальных малоуровневых матриц семейство определяется не константой, а значением функций уровней и вытекающих из них зависимостей $D = D(n)$ или $h = h(n)$.

3. Орнаменты ортогональных матриц. Циклические и бициклические матрицы с малым количеством уровней объединяют в себе черты орнаментов, обладающих фиксированным узором, и матриц, обладающих детерминантом. Семейство орнаментов с *двумя значениями* элементов a, $-b$ описывается тремя инвариантами $\{n, k, \lambda\}$, где n — порядок матрицы, характеризующий величину узора, k — количество одинаковых элементов каждой строки и столбца, λ — количество одинаковых элементов, имеющих одну и ту же позицию в каждой паре строк или столбцов. Для квазиортогональных матриц с элементом $a = 1$ модуль второго элемента $0 \le b \le 1$. В том случае, когда ортогональность строк и столбцов недостижима назначением двух элементов, она достигается введением особого уровня для диагонали $0 \le d \le b$ или каймы из элементов первой строки и столбца матрицы с уровнем $b \le s \le 1$. В обоих случаях это требуется для матриц, превосходящих размер матриц Адамара на 1. Выбор наименований орнаментов в работе [17] согласован

с порядками, образующими числовые последовательности, на которых они наблюдаются. На порядках, равных числам Мерсенна $2^k - 1$ (здесь k — натуральное число), существуют двухуровневые циклические матрицы, называемые матрицами Мерсенна. Трехуровневые матрицы Ферма существуют на порядках, равных числам Ферма $2^{2^k} + 1$.

Принцип вложения. Адамар первым сформулировал принцип вложения, согласно которому уровневые (не орнаментальные) свойства матриц базовой последовательности, в его случае — последовательности Сильвестра 2^k, распространяются на последовательность $4t$, в которую они вложены. Соответственно, матрицы Мерсенна существуют вне базовой последовательности на порядках $4t - 1$, в которую числа $2^k - 1$ вложены. Что касается чисел Ферма, то они вложены не в одну, а в несколько числовых последовательностей, среди них $2^k + 1$ (здесь k — четное целое число), поэтому на $4t + 1$ уровневые свойства этих матриц не соблюдаются.

На одном и том же порядке могут сосуществовать несколько видов орнамента, описываемых одним и тем же набором орнаментальных инвариантов. На рисунке 2 приведены две матрицы Мерсенна [15, 17] порядка 15 с инвариантами {15, 7, 3}, каждая имеет по 7 одинаковых клеток в каждой строке и столбце и по 3 — в каждой паре строк или столбцов. Два цвета клеток соответствуют двум уровням *a* и -*b*.

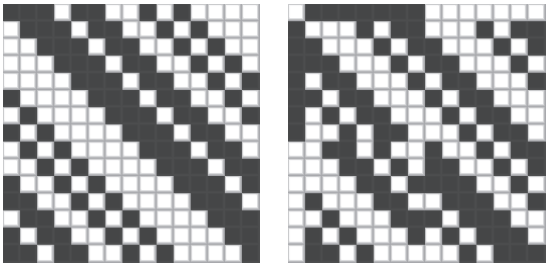

Рис. 2. Два {15, 7, 3}-орнамента матриц Мерсенна

Первый циклический орнамент характерен для порядков, равных числам Мерсенна, второй более универсальный бициклический орнамент разрешим для всех порядков $4t - 1$, в которые числа Мерсенна вложены. Таким образом, орнаменты сопровождают числовые последовательности и имеют с ними взаимно-однозначное соответствие. Это положение звучит более широко, чем гипотеза Адамара, поскольку последняя связывает порядки и не говорит о структурах. Как будет показано

далее, орнамент матриц Мерсенна с иррациональными уровнями с точностью до знака соответствует орнаментам целочисленных матриц Адамара в их нормализованной форме с каймой из 1.

Поскольку на поиск вещественных матриц Мерсенна нет ограничений, выдвигаемых комбинаторными методами, это путь доказательства гипотезы Адамара косвенно через рассматриваемый далее оптимизационный подход.

Возможные сочетания инвариантов $\{n, k, \lambda\}$ для матриц ограничивает их порядок. Реализуемые параметры связывает выделенное еще исследованиями матриц Адамара [1] квадратичное *диофантово уравнение* I вида $k(k-1)=\lambda(n-1)$. Второе столь же общее матричное квадратичное уравнение $A^{\mathrm{T}}A=\omega I$ отражает условие ортогональности столбцов и строк квадратной матрицы.

Для матриц с двумя элементами *a*, *-b* (матрица с положительными элементами не может быть ортогональной) скалярное произведение любых двух отличающихся индексами строк содержит λ произведений вида a^2, $2(k-\lambda)$ произведений ab ($k-\lambda$ элементов *a* каждой из строк умножено на *b*) и $n-2k+\lambda$ произведений b^2. Отсюда следует квадратичное *характеристическое уравнение* II ортогонального дизайна,

$$(n-2k+\lambda)b^2-2(k-\lambda)ab+\lambda a^2=0, \qquad (1)$$

записанное в виде, удобном для поиска корней при превалировании количества положительных элементов над отрицательными. Для матриц с целыми элементами *a*, *-b* оно дает квадратичное *диофантово уравнение* II.

4. Оптимизационный подход к поиску квазиортогональных матриц. Итерационная схема реализации оптимизационного подхода к поиску оптимальных и субоптимальных по детерминанту квазиортогональных матриц [17] показана на рисунке 3 в виде динамического генератора.

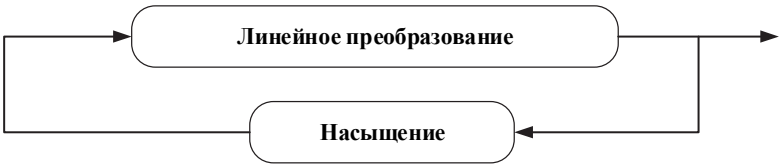

Рис. 3. Динамический генератор малоуровневых матриц

Эта схема напоминает классическую схему Айзермана, служащую для анализа аттракторов, возникающих в замкнутой нелинейным

элементом линейной системе посредством составления параметрически зависимых от амплитуды осцилляций передаточных функций. Состояние и выход дискретной линейной динамической системы в нашем случае описывается квадратной матрицей $Y = [y_1, y_2, ..., y_n]$, получаемой из матрицы входа $U = [u_1, u_2, ..., u_n]$ цепочкой ортогональных преобразований $y_1 = Q_1 u_1$, $y_2 = Q_2 u_2$, … , $y_n = Q_n u_n$, для поворота векторов входа до ближайшей к ним ортогональной конфигурации матрицы выхода. Содержание этих операций может быть разнообразным, взятым из практики вычислительных методов линейной алгебры: QR-преобразование, преобразование Грама-Шмидта, сингулярное разложение матрицы и обратный синтез с округленными до целых значений 1 и -1 собственными числами.

Цель динамической прямой связи — получить после нормирования амплитуд Y к 1 квазиортогональную матрицу A. Нормирование выполняет нелинейный элемент цепи обратной связи, дополняя ее насыщением $U = f(A)$ так, чтобы элементы U не превосходили по своей абсолютной величине некоторого порога $p \le 1$: $u_{ij} = a_{ij}$ для $|a_{ij}| \le p$, $u_{ij} = sign(a_{ij})\, p$, для $a_{ij} > p$, $i, j \in \{\overline{1,n}\}$.

Поскольку детерминант матрицы $|\det(A)| = 1/m^n$ обратно пропорционален значению степени от *m*-нормы, которую мы уменьшаем насыщением максимальных элементов, аттрактором динамического процесса является минимаксная матрица, принимающая характерную для нее малоуровневую конфигурацию. Этот процесс отражен на рисунке 4 при помощи трех гистограмм абсолютных значений элементов матрицы пятого порядка A_5. Модули элементов в этом случае представлены в виде амплитуд.

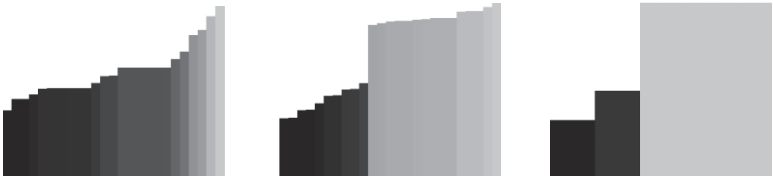

Рис. 4. Гистограммы амплитуд элементов матрицы A_5 трех стадий процесса

На рисунке 5 приведены орнаменты и гистограммы значений амплитуд их элементов квазиортогональных матриц абсолютного максимума детерминанта нечетных порядков, значения элементов матриц (уровни) отображены оттенками серого.

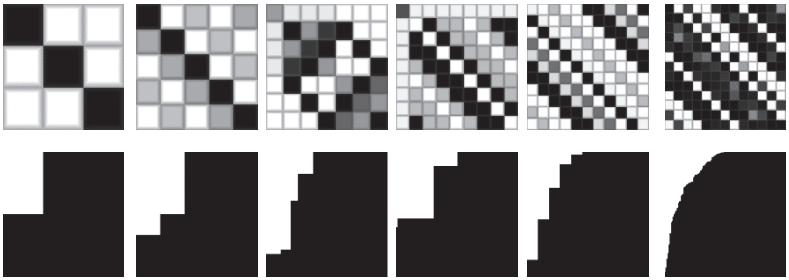

Рис. 5. Портреты матриц A_3, A_5, A_7, A_9, A_{11}, A_{13} с гистограммами

Для повышения эффективности схождения итераций к матрицам с заданным орнаментом помимо применяемых в практике вычислительных методов перестановок столбцов итерируемой матрицы на вход динамической системы на старте подается импульс в виде циклической, бициклической и других подобных матриц, после чего порог p плавно повышается от стартового значения к единице.

5. Критские матрицы. Качественный анализ аттракторов модифицированной схемы Айзермана (рисунок 3) позволяет выделить детали, роднящие ее (ввиду квадратичного характера уравнения связи $A^{\mathrm{T}}A = \omega(n)I$ с математическими моделями детерминированного хаоса. В задачах с матрицами четных порядков $4t$ или $4t-2$ наблюдается постепенный выход динамического процесса на аттрактор с элементами 1 и -1, в последнем случае с 0 на диагонали после сортировки элементов.

Цель комбинаторных методов [1] — достичь равенства $A^{\mathrm{T}}A = \omega(n)I$ последовательными изменениями знаков элементов с использованием переборных процедур. Оптимум детерминанта гарантирован свойствами матриц соответствующей размерности. В рассматриваемой схеме, наоборот, оптимизация детерминанта выступает в качестве основной мотивации ее построения, результатом ее работы являются матрицы с вещественными элементами.

В том случае, когда структура разрешима целочисленным решением, округление дает матрицы Адамара и Белевича, ранее получаемые совершенно иным путем. Количество уровней оптимальных по детерминанту матриц нечетного порядка с ростом размера растет почти ли-

нейно (с отклонением ±1). Есть и критическая точка, порядок 13, на котором экстремуму детерминанта, как видно из рисунка 5, соответствует дисперсное состояние уровней. В ранних работах этот эффект был отнесен к влиянию ограничений разрядной сетки компьютера, не позволяющей вычислить точный результат. Позже [17] было высказано подтвердившееся предположение, что как и у аттракторов Лоренца, дисперсное состояние уровней аттрактора обобщенной схемы Айзермана — свойство самой задачи, а не ошибка вычислительного инструмента. Строго оптимальной матрицы A_{13} с семью уровнями (±1) попросту нет, а если и есть, то она не оптимальна по детерминанту. Однако субоптимальная матрица была найдена.

Показатель D удобен для контроля качества вычислений и выработки критерия останова итераций в схеме 2. Значение адамарова детерминанта $D_{13} = 1/h^2$ равно примерно 0,8 (так же, как и константу Фейгенбаума, это критическое значение можно уточнять). Аттракторы оптимальных матриц порядков $n > 13$ с $D \geq 0,8$ отличаются дисперсным характером элементов. Преодоление указанной границы служит важным критерием выхода итерационного процесса на малоуровневую структуру.

Побочным, а для нас главным результатом работы оптимизатора детерминанта являются матрицы локального максимума детерминанта, отличающиеся от прочих малым количеством уровней. Детерминант D этих упорядоченных структур с ростом порядка стремится к 1. Такие малоуровневые структуры в [17] для краткости названы *критскими матрицами*, поскольку анонсированы были на Крите (2014 г.). В настоящее время это название широко используется как в отечественных, так и зарубежных публикациях.

6. Систематизация критских матриц. Малоуровневая матрица локального максимума детерминанта отличается от прочих матриц тем, что любая ограниченная вариация ее параметров, не выводящая их за пределы области разрешенных значений (амплитуды элементов ≤ 1), понижает значение модуля ее детерминанта. Кроме того, на порядках $4t - 3$, представимых суммой квадратов двух целых чисел 1, 5, 9, 13, … и т. п. (в первой сотне целых чисел исключениями являются 21, 33, 57, 69, 77, 93) встречаются трехуровневые матрицы Одина с выделенной уровнем диагональю, которые отвечают седловым точкам этой задачи. Со сделанной оговоркой мы отнесем их к критским матрицам ввиду того, что они дополняют двухуровневые матрицы Мерсенна порядков $4t - 1$, теория которых без них будет не полна. Матрицы Одина не только прерываются на некоторых порядках, но и являются более сложными, чем матрицы Мер-

сенна, поскольку не имеют ограничений на структуру. Для них нет понятия универсальной структуры, в рамках которой они могут быть найдены. Для порядка 45 орнамент включает неординарные блоки, для порядков 65 и 85 простых орнаментов заведомо нет, сложные орнаменты не найдены. Теория этих матриц в стадии развития.

Заметно проще бициклические матрицы Эйлера порядков $4t-2$, которые, в отличие от матриц Белевича, существуют для любого отведенного им порядка. В таблице 1 приведены семейства выделенных нами критских матриц с двумя и тремя уровнями.

Таблица 1. Значения уровней семейств критских 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 $b=\frac{t}{t+\sqrt{t}}$
E	$4t-2$	Эйлера	1, -b, где $b=\frac{t}{t+\sqrt{2t}}$
S	$4t-3$ (если разложимо на сумму 2 квадратов)	Одина (Зейделя)	1, -b, d, где $b=1-2d$, $d=\frac{1}{1+\sqrt{n}}$
F	$4t+1$ (если представимо числами Ферма или последовательностями, в которые они вложены)	Ферма	1, -b, s, где $q=n-1=4u^2$, $p=q+\sqrt{q}$, $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u}$, $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}=\frac{\sqrt{nu-1}}{2u+1}\times\frac{1}{\sqrt{u}}$

Как отмечалось ранее, для уровней диагональных элементов и элементов каймы в виде первых строки и столбца (за исключением первого, как правило, единичного элемента) сделаем исключение, помечая их персональными буквами d и s.

7. Динамические системы в конечных полях Галуа. Эффективным средством расчета критских матриц высоких порядков явля-

ется моделирование их структуры с помощью анализа поведения линейной динамической системы первого порядка в конечном поле $\mathrm{GF}\left(p^m\right)$. Роль ограничения в виде обратной связи расширенной схемы Айзермана, придающей необходимые свойства аттрактору, играет ограниченный размер поля.

Реакция линейной динамической системы в конечном поле качественно отличается от импульсной весовой характеристики апериодического звена в виде экспоненты. Число различных между собой значений показательной функции g^k, где g — ненулевой элемент поля Галуа, ограничено p^m-1. В отличие от сдвигового регистра, которым ищут иногда оригинальные матрицы порядков чисел Мерсенна в поле $\mathrm{GF}(2)$ [17], диапазон возможных значений элементов g не столь узок.

В поле $\mathrm{GF}\left(p^m\right)$ можно рассматривать g^k как адреса негативных рациональных или иррациональных элементов в последовательности чисел, формирующих первую строку циклической матрицы. В поле $\mathrm{GF}\left(p^m\right)$ значения показательной функции векторные, однако смысловую нагрузку адресов они не теряют, если вместо g^k рассматривать порядковый номер элемента. Кроме того, всегда имеется возможность рассматривать не одну, а две динамические системы первого порядка и фиксировать моменты пересечения значений этих векторных последовательностей, трактуя скалярные значения моментов пересечений как адреса.

В качестве примера поля Галуа $\mathrm{GF}(p)$ возьмем набор целых чисел 0, 1, …, $p-1$. Мультипликативная группа поля Галуа, образуемая операцией умножения по модулю p, обозначим ее как $\mathrm{GF}^*(p)$, состоит из всех элементов поля, кроме 0. Поскольку количество адресов негативных элементов заведомо меньше p (около половины), для построения циклической матрицы нам нужна не столько вся группа, сколько подгруппа, существование которой гарантируется теорией групп.

Пример. Рассмотрим группу Галуа размера $p=11$. Размеры ее подгрупп являются делителями числа $p-1=1\times2\times5=10$. Они отвечают длинам цепочек последовательностей g^k с неповторяющимися элементами — циклическим подгруппам группы $\mathrm{GF}^*(11)$, перечисленным в таблице 2.

Элементы 2, 6, 7, 8 первого столбца таблице 2 называются *примитивными*, они порождают циклическую подгруппу максимальной длины

$\mathrm{GF}^*(11)$. Такая орбита, как ее еще иногда называют, порождает ортогональную циклическую матрицу I (единичную) порядка 12 с элементами $a=1,\ b-0,$ где элементы орбиты — адреса элемента b в первой строке матрицы I, состоящей из 0, за исключением первой 1.

Таблица 2. Циклические подгруппы GF*(11)

g	g^k
1	1
2	1,2,4,8,5,10,9,7,3,6
3	1,3,9,5,4
4	1,4,5,9,3
5	1,5,3,4,9
6	1,6,3,7,9,10,5,8,4,2
7	1,7,5,2,3,10,4,6,9,8
8	1,8,9,6,4,10,3,2,5,7
9	1,9,4,3,5
10	1,10

Орбита минимальной длины, отвечающая $g=1,$ порождает ту же самую матрицу, если произвести изменение значения ее элементов на противоположные и добавить циклический сдвиг строк на один шаг назад.

Более содержательна орбита средней длины 5, образованная элементами 3, 4, 5, 9 первого столбца таблицы. Отметим, что эти элементы являются также значениями g^k, помимо первого единичного элемента $g^0=1$. Она порождает квазиортогональную циклическую матрицу размера 11 с элементами $a=1,\ -b$, изображенную на рисунке 6. Если индексировать элементы с 0, то числа 1, 3, 4, 5, 9 отвечают положениям элемента $-b$.

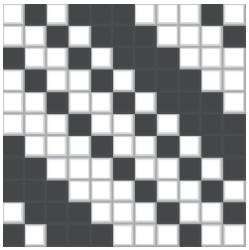

Рис. 6. Циклическая квазиортогональная матрица

Диофантово уравнение I вида $k(k-1)=\lambda(n-1)$ с параметрами $\lambda=t,\ k=2t$ заведомо разрешимо для порядков в виде простых чисел $n=4t-1$. После подстановки параметров в уравнение связи (1), оно упрощается до $(t-1)b^2-2tba+ta^2=0,$ положительный корень этого полинома дает уровень вещественных ортогональных моноциклов Мерсенна $b=\dfrac{t}{t+\sqrt{t}}$ при $a=1,$ отображенных в таблице 1.

Анализ таблицы 2 показывает, что есть еще бинарная матрица с двумя элементами. Такие матрицы отличаются сравнительно низким значением детерминанта (единица у единичной матрицы), они есть для многих порядков и мало интересны для приложений как слишком простые матрицы.

8. Бициклические матрицы. Моноциклы (циклические матрицы) существуют далеко не всегда. В связи с этим результативные поиски часто ограничивают бициклическими матрицами (бициклами) $\begin{pmatrix} A & B \\ B^{\mathrm{T}} & -A^{\mathrm{T}} \end{pmatrix}$ фиксированной сложности, ограниченной двумя циклическими блоками A, B с параметрами $\{n,k_1,\lambda_1\},\ \{n,k_2,\lambda_2\}.$

Нижняя часть этого орнамента зависима, ортогональность вложенных блоков, как правило, не интересует (ортогональны строки и столбцы матрицы в целом), поэтому для описания орнамента достаточно четырех параметров $\{n,k_1,k_2,\lambda\},$ где $\lambda=\lambda_1+\lambda_2$. Диофантово уравнение I бицикла имеет вид $k_1(k_1-1)+k_2(k_2-1)=\lambda(n-1).$ Заменой переменных $x=p-k_1,\ \ y=p-k_2,$ при $p=k_1+k_2-\lambda,$ оно сводится к уравнению окружности:

$$x^2+y^2=p+\lambda(v-2p), \tag{2}$$

решаемому в целых числах. Характеристическое уравнение:

$$\lambda b^2-2(k_1+k_2-\lambda)ab+(n-2(k_1+k_2)+\lambda)a^2=0, \tag{3}$$

в котором $k_1,k_2<p,\ \ p=k_1+k_2-\lambda=(n-2)/4,$ отражают условие ортогональности строк бицикла с элементами a, $-b$. Оно записано в виде, удобном для поиска корней при превалировании количества положительных элементов над отрицательными.

В теории бициклов наиболее интересны те из них, которые разрешимы для $n=4t-2,$ не зависимо от разложимости числа $n-1$ на сумму

квадратов двух чисел. Напомним, что этим условием ограничены квазиортогональные матрицы с целочисленными элементами [1], в частности матрицы Белевича. После нормирования в 1 элементов каймы (помимо диагонального элемента 0) и отделения каймы, матрицы Белевича переходят в матрицы Одина нечетных порядков той же структуры. Ввиду пропусков и сложности орнаментов матрицы Одина имеют узко теоретическое значение. Так как критериями разложимости чисел на суммы квадратов целых чисел занимался Эйлер, бициклы, восполняющие пропуски матриц Белевича, названы матрицами Эйлера.

Для всех матриц Эйлера порядков $n = 4t - 2$ (размер плеча $v = n/2 = 2p - 1,\ \ p = t$) диофантово уравнение (2) сводится к уравнению равнобедренного прямоугольного треугольника $x^2 + y^2 = 2$, разрешимое для точки $x = y = 1$ окружности с квадратом радиуса $p + \lambda(v - 2p) = 2$. Поскольку $k_1 = p - x$ и $k_2 = p - y$, количества элементов одного знака в плечах бицикла равны $k_1 = k_2 = p - 1 = (v-1)/2$, $\lambda = p - 2 = (v-3)/2$. Дизайн вида $\{n = 2v; k_1; k_2; \lambda\} = \{n = 2v; (v-1)/2; (v-1)/2; (v-3)/2\}$ назовем *эйлеровым*.

Наиболее проста реализация бицикла Эйлера с равными плечами $A = B,\ \lambda_1 = \lambda_2,\ \lambda_1 = \lambda_1 + \lambda_2,$ которые представляют собой, в частности, рассмотренные ранее циклические матрицы Мерсенна вдвое меньшего порядка $v = 3 \pmod 4$. Пусть разложение на базе одной и той же матрицы в обоих плечах невозможно, тогда раскрывается скрытый ресурс бицикла: плечи его утрачивают равновесие $A \neq B$, отклонение $\lambda_1 = \lambda_2 + 1$ берет в расчет блоки, которым не обязательно быть ортогональными, ведь ортогональна конструкция в целом. Характеристическое уравнение (3) отражает условие ортогональности строк с элементами *a*, *-b*, причем $(n - 2(k_1 + k_2) + \lambda) = (n - 2p + \lambda) = p,$ при $\lambda = p - 2,\ \ 2(k_1 + k_2 - \lambda) = 2p,$ и для $n = 4t - 2,\ \ p = t$. Положительный корень этого полинома дает уровень матриц Эйлера $b = \dfrac{t}{t + \sqrt{2t}}$ при $a = 1$.

Возможно построение блоков матрицы Эйлера из двух циклических матриц Мерсенна, находимых итерациями в поле Галуа. Циклические матрицы Одина также порождают матрицу Эйлера, при росте размера матрицы вдвое уровень диагонального элемента перестает отставать от 1 (можно задать 1). В отличие от матриц Одина вдвое большая по размеру бициклическая матрица Эйлера имеет резерв на существование даже тогда, когда первых не существует. Ввиду экстремальности свойств эти критские матрицы локального максимума детерминанта

независимо от порядка находит динамическая система оптимизации, рассмотренная ранее.

9. Переход от матриц Эйлера к матрицам Адамара. Формальный переход от бициклической матрицы Эйлера к матрице Адамара опосредованно через промежуточную матрицу Эйлера венчает построение теории, показывающей конечность возможных структур матриц Адамара. Подсчет количества элементов матриц Эйлера показывает, что эти бициклы переходят в матрицы Мерсенна элементарным добавлением каймы из одинакового количества негативных и позитивных элементов (см. рисунок 7) с пересчетом уровней элементов, согласно таблице 1. Матрицы Мерсенна, в свою очередь, при помощи монотонной каймы и инверсии знаков элементов переходят в матрицы Адамара с приведением уровней элементов до 1 и -1.

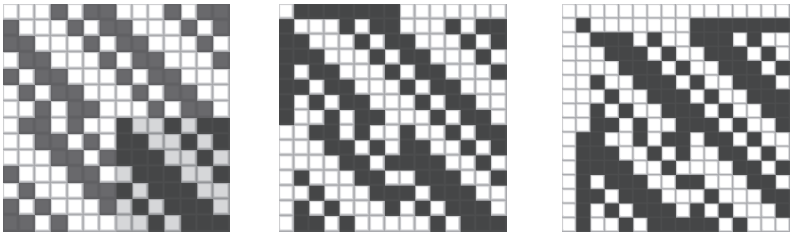

Рис. 7. Переход от бицикла Эйлера к матрице Мерсенна и Адамара

10. Получение квазиортогональных матриц в теории грамианов. В теории линейных динамических систем ортогональные матрицы возникают при диагонализации грамианов системных свойств управляемости, наблюдаемости и идентифицируемости. Впервые на это обратил внимание Гловер в работе [18], предложив использовать ненулевые элементы диагональных матриц грамианов управляемости и наблюдаемости в качестве аналогов сингулярных чисел матриц для задач редукции моделей динамических систем.

При реакции на импульсное воздействие вектор состояния модели динамической системы в сбалансированной форме Гловера содержит взаимно-ортогональные между собой функции. Обобщение этого метода состоит в рассмотрении широкого класса ассоциированных с линейной динамической системой линейных операторов, симметрия которых гарантирует ортогональность их сингулярных функций. Флип-метод определения сингулярных функций ганкелева оператора и оператора свертки позволяет выделить ортогональные последовательности в процессе математического или натурного моделирования [14].

Для нахождения малоуровневых матриц эти методы возбуждения динамических систем и создания условий, когда они выдают ортогональные последовательности, недостаточны, в связи с чем возникают аналитические методы поиска с помощью полей Галуа. Они очень эффективны для поиска матриц высокой размерности [17], но не отвечаю на все вопросы теории, поскольку относятся к комбинаторным методам. В их основе лежит перебор вариантов знаков элементов, поиск подгруппы и т. п. Комбинаторная теория широко оперирует орнаментами целочисленных матриц Белевича, также являющихся блоками матриц Адамара конструкции Пэли [1]. Проблематика матриц Белевича (заведомо существуют не всегда, орнамент не всегда ясен) сформировала точку зрения на орнаменты матрицы Адамара как неясные и, в общем, непредсказуемые. То же самое касается вопроса о существовании матриц на всех порядках $4t$.

11. Заключение. Существующие на порядках с шагом 4 бициклы Эйлера составляют антитезу известной гипотезе Райзера [17] о существовании матрицы Адамара в форме моноцикла не выше 4-го порядка. Орнаменты матриц Эйлера отвечают на вопрос максимальной сложности структуры квазиортогональных матриц, к которым матрица Адамара относятся, сводя основную трудность решения задачи к поиску блоков бицикла. Добавление одинарной или двойной каймы сложностей не привносит. Переход к динамическим моделям оптимизации детерминанта, разумеется, не делает трудные задачи поиска матриц Адамара высоких порядков легким занятием. Эти трудности сохраняются в виде сложности указания областей устойчивости матриц локального максимума детерминанта. Но перспектива доказательства существования квазиортогональных матриц с возможно иррациональными элементами выглядит иначе. Сам по себе факт существования области сходимости к локальному максимуму безотносителен к порядку.

Таким образом, намечается продуктивный и независимый от прежних воззрений путь рассмотрения одной из наиболее интригующих гипотез прошлого века (гипотезы Адамара).

Литература

1. *Awyzio G., Seberry J.* On good matrices and skew Hadamard matrices // Algebraic Design Theory and Hadamard Matrices. 2015. pp. 13–28.
2. *Kim J., Susilo W., Au M.H., Seberry J.* Efficient semi-static secure broadcast encryption scheme // 6th International Conference Pairing-Based Cryptography (Pairing 2013). 2014. LNCS 2738. pp. 62–76.
3. *Holzmann W.H., Kharaghani H., Tayfeh-Rezaie B.* Williamson Matrices up to Order 59 // Designs, Codes and Cryptography. 2008. vol. 46. pp. 343–352.
4. *Doković D.Ž.* Williamson Matrices of Order 4n for n=33;35;39 // Discrete Math. 1993. vol. 115. pp. 267–271.
5. *Matteo O.Di, Djokovic D.Z., Kotsireas I.S.* Symmetric Hadamard matrices of order 116 and 172 exist // Special matrices. 2015. vol. 3. pp. 227–234.
6. *Doković D.Ž.* Generalization of Scarpis' theorem on Hadamard matrices // Linear and Multilinear Algebra. pp. 1–3. URL:

http://www.tandfonline.com/doi/abs/10.1080/03081087.2016.1265062?journalCode=glma20. (дата обращения: 21.11.2016).
7. *Petoukhov S.V.* The Genetic Coding, United-Hypercomplex Numbers and Artificial Intelligence // Advances in Artificial Systems for Medicine and Education. 2017. pp. 2–13.
8. *Петухов С. В.* Матричная генетика, алгебры генетического кода, помехоустойчивость // Москва: РХД. 2008. 316 с.
9. *Lee M.H., Hai H., Lee S.K., Petoukhov S.V*. A Mathematical Proof of Double Helix DNA to Reverse Transcription RNA for Bioinformatics // Advances in Artificial Systems for Medicine and Education. 2017. pp. 23–38.
10. *Манин Ю.И.* Математика как метафора // Москва: МЦМНО. 2008. 400 с.
11. *Shechtman D., Blech I., Gratias D., Cahn J.W.* Metallic Phase with LongRange Orientational Order and No Translational Symmetry // Physical Review Letters. 1984. vol. 53. pp. 1951–1953.
12. *Balonin N.A., Suzdal V.S.* Symmetry of Life in Crystals // Functional materials. 2016. vol. 23(4). pp. 1–7.
13. *Балонин Н.А., Сергеев М.Б., Суздаль В.С.* Матричные модели обобщенной кристаллографии // Информационно-управляющие системы. 2016. № 4(83). С. 27–33.
14. *Балонин Н.А.* Дискретные частотные характеристики элементарных динамических звеньев // Информационно-управляющие системы. 2015. № 4 (77). С. 17–24.
15. *Sergeev A.M.* Generalized Mersenne Matrices and Balonin's Conjecture // Automatic Control and Computer Sciences. 2014. vol. 48. no. 4. pp. 214–220.
16. *Балонин Ю.Н., Востриков А.А., Сергеев А.М., Егорова И.С.* О взаимосвязях квазиортогональных матриц, построенных на известных последовательностях чисел // Труды СПИИРАН. 2017. №. 1(50). С. 209–223.
17. *Балонин Н.А., Сергеев М.Б.* Расширение гипотезы Райзера на двуциклические структуры и разрешимость матриц Адамара орнаментом в виде бицикла с двойной каймой // Информационно-управляющие системы. 2017. № 1 (86). С. 2–10.
18. *Glover K.* All Optimal Hankel-norm Approximations of Linear Multivariables Systems // Intern. J. Control. 1984. vol. 39. no. 6. pp. 1115–1193.

Балонин Николай Алексеевич — д-р техн. наук, доцент, профессор кафедры вычислительных систем и сетей, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: вычислительные методы, теория управления, теория чисел, идентификация динамических систем, образовательные интернет-технологии, исполняемые алгоритмы. Число научных публикаций — 94. korbendfs@mail.ru; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +7(911)213-59-07.

Сергеев Михаил Борисович — д-р техн. наук, профессор, заведующий кафедрой вычислительных систем и сетей, института вычислительных систем и программирования, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП), директор института вычислительных систем и программирования, Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: численные методы, цифровая обработка данных, оптико-информационные системы. Число научных публикаций — 106. mbsergeev@gmail.com; ул. Большая Морская, 67, Санкт-Петербург, 190000; р.т.: +7(905)223-24-89.

Суздаль Виктор Семенович — д-р техн. наук, ведущий научный сотрудник лаборатории систем управления, Институт сцинтилляционных материалов Национальной академии наук Украины (НАНУ). Область научных интересов: теория управления, идентификация динамических систем, теория матриц, кристаллография. Число научных публикаций — 141. suzdal@isma.kharkov.ua; пр. Науки, 60, Харьков, 61072, Украина; р.т.: +380 97 914 6537.

Поддержка исследований. Работа выполнена при поддержке Минобрнауки РФ при проведении научно-исследовательской работы в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/4.6.

DOI 10.15622/sp.54.10

N.A. BALONIN, M.B. SERGEEV, V.S. SUZDAL

DYNAMIC GENERATORS OF THE QUASIORTOGONAL HADAMARD MATRIX FAMILY

Balonin N.A., Sergeev M.B., Suzdal V.S. **Dynamic Generators of the Quasiortogonal Hadamard Matrix Family.**

Abstract. The problem of constructing non-linear and linear finite-field generators of quasi-orthogonal matrices of the Hadamard family with a small number of distinct values of their elements not exceeding by absolute value 1 and a global or local maximum of determinant is investigated. The properties of such dynamical systems are analyzed; the classification of the matrix families and their ornaments, obtained with their help, is described; the way of proving the existence of real and integer matrices different from the combinatorial approach is shown. The values to which the elements of the matrix are equal are called its levels. The concepts of the Hadamard norm and the determinant of a quasiorthogonal matrix are introduced. Levels, Hadamard norm and determinant play a fundamental role in the definitions of classes of generalized matrices of the Hadamard family. The classes of the Hadamard, Belevich (conference matrices), Seberri (weighing matrices), Mersenne, Euler, Odin (Seidel), Fermat matrices are described. The formulas for the values of their levels are given. Ornaments of Euler matrices answer to the question of the maximum complexity of Hadamard matrices — two border two circulant structure.

Keywords: dynamical systems, quasiorthogonal matrices, deterministic chaos, finite fields.

Balonin Nikolay Alekseevich — Ph.D., Dr. Sci., associate professor, professor 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 — 94. korbendfs@mail.ru; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +7(911)213-59-07.

Sergeev Mikhail Borisovich — Ph.D., Dr. Sci., professor, head of computer systems and networks department of Institute of computing systems and programming , Saint Petersburg State University of Aerospace Instrumentation (SUAI), director of Institute of computing systems and programming , Saint Petersburg State University of Aerospace Instrumentation (SUAI). Research interests: numerical methods, digital data performig, optical information systems. The number of publications — 106. mbsergeev@gmail.com; 67, B. Morskaia St., 190000, Saint-Petersburg; office phone: +7(905)223-24-89.

Suzdal Viktor Semenovich — Ph.D., Dr. Sci., leading researcher of control systems laboratory, Institute for Scintillation Materials of National Academy of Sciences of Ukraine. Research interests: control theory, identification of dynamic systems, crystallography. The number of publications — 141. suzdal@isma.kharkov.ua; 60, Nauky ave. Kharkiv, 61072, Ukraine; office phone: +380 97 914 6537.

Acknowledgements. The research leading to these results has received funding from the Ministry of Education and Science of the Russian Federation according to the project part of the state funding assignment No 2.2200.2017/4.6.

References

1. Awyzio G., Seberry J. On good matrices and skew Hadamard matrices. Algebraic Design Theory and Hadamard Matrices. 2015. pp. 13–28.

2. Kim J., Susilo W., Au M.H., Seberry J. Efficient semi-static secure broadcast encryption scheme. 6th International Conference Pairing-Based Cryptography (Pairing 2013). 2014. LNCS 2738. pp. 62–76.
3. Holzmann W.H., Kharaghani H., Tayfeh-Rezaie B. Williamson Matrices up to Order 59. *Designs, Codes and Cryptography*. 2008. vol. 46. pp. 343–352.
4. Doković D.Ž. Williamson Matrices of Order 4n for n=33;35;39. *Discrete Math*. 1993. vol. 115. pp. 267–271.
5. Matteo O.Di, Djokovic D.Z., Kotsireas I.S. Symmetric Hadamard matrices of order 116 and 172 exist. *Special matrices*. 2015. vol. 3. pp. 227–234.
6. Doković D.Ž. Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra.* pp. 1–3. Available at: http://www.tandfonline.com/doi/abs/10.1080/03081087.2016.1265062?journalCode=glma20. Published online: 07 Dec 2016. (accepted: 21.11.2016).
7. Petoukhov S.V. The Genetic Coding, United-Hypercomplex Numbers and Artificial Intelligence. Advances in Artificial Systems for Medicine and Education. 2017. pp. 2–13.
8. Petoukhov S.V. *Matrichnaia genetika, algebry geneticheskogo koda, pomekhoustoichivost*' [Matrix genetics, algebra of genetic code, noise immunity]. Moscow: RHD. 2008. 316 p. (In Russ.).
9. Lee M.H., Hai H., Lee S.K., Petoukhov S.V. A Mathematical Proof of Double Helix DNA to Reverse Transcription RNA for Bioinformatics. Advances in Artificial Systems for Medicine and Education. 2017. pp. 23–38.
10. Manin Yu.I. *Matematika kak metafora* [Mathematics as a Metaphor]. Moscow: MTsMNO. 2008. 400 p. (In Russ.).
11. Shechtman D., Blech I., Gratias D., Cahn J.W. Metallic Phase with LongRange Orientational Order and No Translational Symmetry. *Physical Review Letters*. 1984. vol. 53. pp. 1951–1953.
12. Balonin N.A., Suzdal V.S. Symmetry of Life in Crystals. *Functional materials*. 2016. vol. 23(4). pp. 1–7.
13. Balonin N.A., Sergeev M.B., Suzdal' V.S. [Matrix Models of Generalized Crystallography]. *Informatsionno-upravliaiushchie sistemy — Information and Control Systems*. 2016. vol. 4(83). pp. 27–33. (In Russ.).
14. Balonin N.A. [Discrete Frequency Characteristics of Elementary Dynamic Units]. *Informatsionno-upravliaiushchie sistemy — Information and Control Systems*. 2015. vol. 4(77). pp. 17–24. (In Russ.).
15. Sergeev A.M. Generalized Mersenne Matrices and Balonin's Conjecture. *Automatic Control and Computer Sciences*. 2014. vol. 48. no. 4. pp. 214–220.
16. Balonin Yu.N., Vostrikov A.A., Sergeev A.M., Egorova I.S. [On Relationships among Quasi-orthogonal Matrices Constructed on the Known Sequences of Prime Numbers]. *Trudy SPIIRAN — SPIIRAS Proceedings*. 2017. vol. 1(50). pp. 209–223. (In Russ.).
17. Balonin N.A., Sergeev M.B. [Ryser's Conjecture Expansion for Bicirculant Strictures and Hadamard Matrix Resolvability by Double-Border Bicycle Ornament]. *Informatsionno-upravliaiushchie sistemy — Information and Control Systems*. 2017. vol. 1(86). pp. 2–10. (In Russ.).
18. Glover K. All Optimal Hankel-norm Approximations of Linear Multivariables Systems. *Intern. J. Control*. 1984. vol. 39. no. 6. pp. 1115–1193.