УДК 519.614
doi:10.31799/1684-8853-2023-1-2-16
EDN: KOMNBV

Научные статьи
Articles

Задачи разрешимые и неразрешимые. Алгоритм Прокруста получения матриц семейства Адамара

Н. А. Балонин[а], *доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
Дж. Себерри[б], *доктор наук, профессор, orcid.org/0000-0002-9558-4293*
М. Б. Сергеев[а], *доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277*
[а]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*
[б]*Университет Вуллонгонг, Вуллонгонг, Новый Южный Уэльс 2522, Австралия*

Введение: *развитие теории матриц Адамара столкнулось с препятствием, обусловленным не столько природой целочисленной задачи, сколько искусственным ограничением решения квадратичных уравнений переборным путем. Игнорирование прямого пути, отказ от иррациональности привели к появлению мнения, что гипотеза существования матриц Адамара недоказуема.* ***Цель:*** *обосновать разрешимость задачи Адамара ортогональными матрицами за счет выявления их устойчивой связи с матрицами с иррациональными элементами.* ***Результаты:*** *показано, что иррациональность проявляется в квадратичной норме столбцов матрицы Адамара второго порядка. Проанализирован перенос итерационных алгоритмов вычисления корней на матричный случай. Предложен алгоритм Прокруста минимизации максимального по абсолютному значению элемента ортогональной матрицы. Поскольку матрицы Адамара определены инвариантами вложенных в ее структуру матриц меньшего порядка, алгоритм оказывается универсальной основой для их совместного нахождения. Гипотеза о существовании матриц Адамара рассматривалась в оперативной области итерационных алгоритмов, определенных над полем вещественных чисел, дающих преимущества перед инструментами в форме конечных полей и групп.* ***Практическая значимость:*** *ортогональные последовательности, получаемые из строк (столбцов) матриц Адамара, и сами матрицы Адамара высоких порядков имеют большое практическое значение для задач помехоустойчивого кодирования, сжатия, маскирования и обработки изображений.*

Ключевые слова *— матрицы Адамара, конференц-матрицы, критские матрицы, алгоритм Прокруста, конечные поля, симметрии матриц.*

Для цитирования: Балонин Н. А., Себерри Дж., Сергеев М. Б. Задачи разрешимые и неразрешимые. Алгоритм Прокруста получения матриц семейства Адамара. *Информационно-управляющие системы*, 2023, № 1, с. 2–16. doi:10.31799/1684-8853-2023-1-2-16, EDN: KOMNBV

For citation: Balonin N. A., Seberry J., Sergeev M. B. Solvable and unsolvable problems. Using Procrustes analysis algorithm for obtaining a family of Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 1, pp. 2–16 (In Russian). doi:10.31799/1684-8853-2023-1-2-16, EDN: KOMNBV

Введение

Три знаменитые задачи античной древности на удвоение куба, трисекцию угла и квадратуру круга известны тем, что их не решить при помощи циркуля и линейки. Эти неразрешимые задачи были решены иначе выдающимися учеными, сумевшими систематизировать средства достижения цели и их эффективность. Изучение таких задач привело к понятию иррационального числа.

В современных обозначениях задача на удвоение куба сводится к решению уравнения $x^3 = 2$. Задача на трисекцию угла α связана с тригонометрическим уравнением $x^3 = 3x + 2\cos(\alpha)$. Если принять за единицу измерения радиус круга и обозначить через x длину стороны искомого квадрата задачи на квадратуру круга, то задача сводится к решению уравнения $x^2 = \pi$. Таким образом, неразрешимость задачи на квадратуру круга следует из неалгебраичности (трансцендентности) числа π, которая была доказана в 1882 г. Линдеманом. Из его теоремы следует, что осуществить решение нельзя с помощью прямых, окружностей или любых других алгебраических кривых и поверхностей, например эллипсов, гипербол или кубических парабол.

Аристотель в IV в. до н. э. писал: «Посредством геометрии нельзя доказать, что два куба составляют один куб». Однако эту неразрешимость следует понимать как неразрешимость при использовании *только* циркуля и линейки. Простейший механический способ решения предложил Леонардо да Винчи.

Противоречивый ход развития математики сначала отвергает очевидное (у диагонали равнобедренного прямоугольного треугольника есть длина, невыразимая числом), а потом находит решение, в котором сам этот «неразрешимый» треугольник становится генератором новых чи-

сел. Мы их «включаем» в систему за счет того, что множество рациональных чисел «расширяется» иррациональными числами, образуя новое понятие — вещественное число. С корнем из –1 это произошло позднее и иначе — комплексным числам приписали положение на плоскости. В этом проявляется пестрота математики.

Как известно, иррациональное число не может быть записано в виде обыкновенной дроби m/n, где m, n — целые числа, но может быть представлено в виде бесконечной непериодической десятичной дроби. Иррациональными являются, среди прочих, отношение длины окружности к диаметру круга (число π), число Эйлера e, золотое сечение φ, квадратный корень из двух. Все квадратные корни натуральных чисел, кроме полных квадратов, иррациональны. Каждое иррациональное число является либо алгебраическим, либо трансцендентным. Множество алгебраических чисел является счетным множеством корней полиномов с целыми коэффициентами. Простейшими являются квадратичные иррациональности. Поскольку множество вещественных чисел несчетно, то множество иррациональных чисел также несчетно.

К. Гаусс, рассматривая построение правильного семнадцатиугольника, пользовался тем, что с помощью циркуля и линейки можно выполнить все четыре арифметических действия и осуществить извлечение квадратного корня. Все остальное надо делать иначе. Подобное надо изучать подобным, иначе возникает коллизия. Однако не стоит думать, что переход к алгебраической форме записи автоматически упрощает рассмотрение проблемы. Так, например, количество и характер решений задачи, записанной в виде пары квадратичных уравнений, становится очевиднее, если видеть за уравнениями пару окружностей, описываемых ими. Две разные окружности со смещенными центрами могут пересекаться либо в одной, либо в двух точках. Для установления этого обстоятельства достаточно не столько углубленного знания геометрии, сколько жизненного опыта.

Иррациональные числа настолько абстрактны, что для их обозначения у нас нет привычных средств записи. Их обозначают, по сути, уравнениями (формулами), коэффициентами которых являются рациональные числа. Решения уравнений, включающих многочлены с рациональными коэффициентами, не всегда столь очевидны, как решения задач геометрии. Но если они имеют вещественные значения, то, в отличие от уравнений Диофанта, этот случай, согласно теореме Тарского, классифицируется как более простой.

Цель данной работы состоит в расширении теории матриц Адамара и демонстрации преодоления принципиальных трудностей их поиска за счет использования выявленной связи с иррациональными матрицами соседних порядков. Эта связь образует доказательную базу существования матриц Адамара, снимая ограничение, связанное с использованием комбинаторных методов.

Теорема Тарского и матричные квадратичные уравнения

А. Тарский обнаружил, что использование языка формул открывает путь для установления истинности утверждений относительно бесконечного числа объектов совершением конечного числа манипуляций.

В самом деле, значения полинома в промежутках между его корнями могут быть какими угодно, но они не меняют знака. Поэтому, несмотря на то, что функция определена над бесконечным множеством точек, существует конечный алгоритм построения таблицы Тарского (орнамента), помогающей вынести суждение о качествах всех их [1]. Иными словами, Тарский свел бесконечномерную задачу к задаче построения конечного орнамента, описываемого орнаментальными инвариантами (присущими узору параметрами).

Задачи на поиск корня уравнения $x^2 = n$, где n — целое число, относятся к числу фундаментальных, сложивших основание современной теории чисел и алгебраической геометрии. Итерационные алгоритмы систематизировал Ньютон, хотя их начали предлагать еще в глубокой древности. Таков, например, алгоритм Герона вычисления приближения к корню квадратному, начиная с некоторого любого положительного числа.

Задачи на поиск экстремума или (в иной трактовке) *неподвижной точки* отображения, задаваемого алгоритмом Герона, тесно взаимосвязаны. Поэтому в основании итерационных алгоритмов могут звучать как оптимизационные мотивы, так и мотивы, навеянные тематикой обобщений метода Герона. Важно понять, какой именно оптимизации и какого именно отображения, а также изучить их свойства.

Матричное расширение задачи

$$\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}, \qquad (1)$$

где $\mathbf{I}$ — единичная матрица того же порядка n, что и искомая матрица $\mathbf{H}$, уже при $n = 2$ расширяет пространство аргументов, элементов матрицы, среди которых находятся и целочисленные [2, 3].

Этот переход заметил в свое время основатель теории матриц Дж. Сильвестр в связи с получе-

нием на порядках, кратных степеням 2, орнаментов (матриц с элементами 1 и –1) [4], инверсия которых сводится к транспонированию и масштабированию элементов. Узор из знаков является общим инвариантом как прямой, так и обратной матриц.

Заинтересованный в геометрическом толковании алгебраических задач Ж. Адамар дополнил это наблюдение [5]. Во-первых, он особо выделил порядки, кратные четырем, доказав, что только для них возможно целочисленное решение задачи матрицей с элементами 1 и –1. Во-вторых, он отметил важное свойство получаемых таким образом решений: они обладают еще одним инвариантом — максимумом детерминанта на классе матриц с элементами, по модулю не превышающими единицу. С тех пор задача остановилась в своем развитии, поскольку перекочевала в класс заведомо трудных задач с сугубо целочисленными решениями.

Комбинаторные методы, связанные с перебором индексов (адресов) отрицательных (положительных) элементов в матрице, изначально слабые, сильно развились с появлением эффективных алгоритмов теорий конечных полей и групп [6, 7]. Например, Н. Ито установил взаимно однозначное соответствие между орнаментами матриц Адамара и конструкциями, которые можно построить, вооружившись арифметикой дициклических групп [8, 9]. Тем не менее эта попытка и иные приемы использования конечномерной математики не дают основания однозначно судить, разрешима ли задача Адамара на всех выделенных им порядках или нет.

Это все большей частью методы ускорения решения при некоторых благоприятных условиях, но условия не одинаковы для различных областей порядков вида $n = 4t$, где t — натуральное число. Перебор, как бы сложно ни был оформлен использующий его метод через теорию групп или полей, не дает повода определенно заключить, закончится ли поиск нужной для решения комбинацией элементов 1 и –1. В итоге с помощью комбинаторного подхода отказались от попыток доказать гипотезу Адамара, что отмечается в публикациях, начиная с основополагающих работ Р. Пэли и Дж. Вильямсона [10, 11].

Между тем породивший это направление скалярный случай относится в настоящее время к тривиальным, разрешимым даже не одним известным способом.

Мы отмечаем отход от общего пути решения (итерацией), чем и вызвано данное недоразумение. В самом деле, достаточно нормировать столбцы матрицы второго порядка, делая ее ортогональной в смысле $\underline{\mathbf{H}}^{\mathrm{T}}\underline{\mathbf{H}} = \mathbf{I}$, чтобы элементы стали обратно пропорциональными корню квадратному из двух. Выход темы орнаментов, поднятой Сильвестром, за пределы достижимости их итерационными методами не обязателен. Можно сформулировать ту же проблему иначе, а именно как поиск ортогональной матрицы $\underline{\mathbf{H}}$ с минимальным максимальным элементом [12], и тогда задача не относится к классу целочисленных задач Диофанта.

Такая оптимизационная, а не переборная задача имеет с точки зрения фиксации орнамента (узора) то же самое решение, но по значениям элементов оно окажется рациональным или иррациональным. Целочисленное толкование задачи появилось ввиду того, что, если элементы матрицы равны друг другу по абсолютной величине, их значения можно исключить делением на неудобное нам иррациональное число. Если это исключение постулировать и положить в основу определения матрицы Адамара, как сделано в большинстве работ, мы отсекаем все то, с чего это начиналось. Трактовка проблемы как переборной задачи, осуществленная на раннем этапе ее постановки, оказалась удобной для приложения эффектных методов комбинаторной теории. Но она не согласована с целью поиска ответа на вопрос, а всегда ли есть искомое решение?

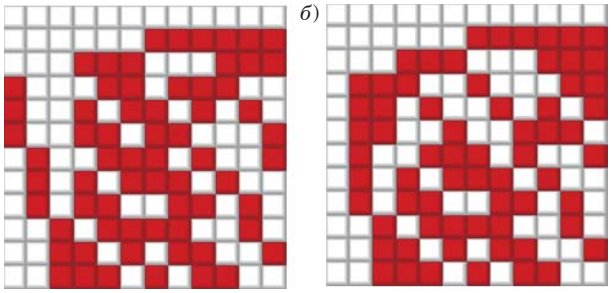
Мы намерены дать более полное представление об этом пути развития теории ортогональных матриц, поскольку это кажется нам назревшим и более важным, чем очередной комбинаторный алгоритм.

Инварианты матриц семейства Адамара

Для матриц Адамара (1) порядка n с элементами 1, –1, полученных каким-либо методом, не обнаруживаются, на первый взгляд, свойства для их идентификации. Однако вычисленные Адамаром матрицы порядков 12 и 20 эквивалентными преобразованиями путем умножения строк или столбцов на –1 и структурирующими перестановками можно привести к нормальному виду с «каймой» из единиц, располагаемых в первых ее строке или столбце.

После добавления к матрице каймы обнаруживаются два инварианта, характерных для всех матриц Адамара. Ими являются количество единиц (или –1), определяемое в любой ее строке или столбце как $k = n/2$ (без учета каймы), и $\lambda = n/4$ — количество единиц (или –1), совпадающих по местоположению в любой паре строк и столбцов [2, 3]. Проверить это обстоятельство можно на примере портретов взятой из статьи Адамара матрицы порядка 12 ($k = 6$ и $\lambda = 3$) (рис. 1, *а*) и ее нормальной формы (рис. 1, *б*) [13].

В статьях встречаются как нормальные формы, так и инварианты блочных конструкций [12, 14]. Допустим, блочно-составная матрица



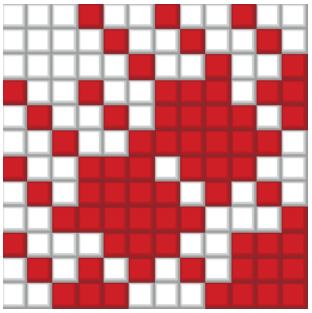
■ ***Рис. 1.*** Портреты матрицы Адамара порядка 12 (*а*) и ее нормальной формы (*б*)

■ ***Fig. 1.*** Portraits of the Hadamard matrix of order 12 (*а*) and its normal form (*б*)

Адамара с частными инвариантами блоков k_1, k_2, ..., подсчитываемыми для элемента –1, не приведена к нормальному виду, как это видно на портрете матрицы конструкции Пропус [12], представленной на рис. 2.

Естественно, суммарный инвариант $k = k_1 + k_2 + \ldots$ будет отличаться от инварианта нормальной формы. Формула для подсчета второго инварианта $\lambda = k - n/4$ универсальна, но в силу отличия k она дает иную (тоже верную) оценку, опираясь на иное упорядочивание 1 и –1 в пределах выделяемой блоками части всей матрицы. Симметричная конструкция Пропус (см. рис. 2) опирается на равенство двух (из четырех) средних блоков и удобна тем, что ее инварианты $k_1 = (v - x)/2$, $k_2 = k_3 = (v - y)/2$, $k_4 = (v - z)/2$, где $v = n/4$ — размер блока, можно классифицировать с помощью точек Гаусса на сфероиде $x^2 + 2y^2 + z^2 = n$, связывая разрешимость этого уравнения с теоремами Гаусса и Лиувилля [15, 16].

Как видно, диагональный блок размера 3×3 блочно-составной матрицы порядка 12 состоит из единиц и $k_1 = 0$. Три оставшихся блока содержат отрицательный элемент на диагонали. Суммарное $k = 3$, а для нормальной формы $k = n/2 = 6$.



■ ***Рис. 2.*** Матрица Адамара порядка 12 конструкции Пропус

■ ***Fig. 2.*** Propus construction of Hadamard matrix of order 12

Соответственно, $\lambda = k - n/4 = 3 - 3 = 0$ (для нормальной формы $\lambda = 3$), и ортогональность всей матрицы гарантируется конструкцией этого массива. Для кососимметричного массива Себерри [2] базовым является уравнение сферы $x^2 + y^2 + z^2 = n - 1$, а не сфероида из работы [17]. Все остальные соображения сохраняются.

Комбинаторика толкует о недоказуемости гипотезы Адамара. Да, но недоказуемость с использованием каких инструментов? Решение задачи о трисекции угла не позволяет говорить о неразрешимости вообще. Неразрешимость — следствие неверного выбора инструментов. Действительно, вопрос о разрешимости квадратичного матричного уравнения перебором не решить, хотя можно найти большое количество строк и столбцов квадратной матрицы с $k = n/2$ положительными и отрицательными элементами. Однако обеспечение второго инварианта $\lambda = n/4$ и тем самым получение матрицы Адамара не гарантировано.

Это те же «циркуль и линейка», но для поставленной Адамаром задачи, имеющей и другую формулировку. Согласно ей матрицы Адамара являются матрицами максимума детерминанта на множестве матриц с ортогональными строками и столбцами. При этом значения элементов не превышают единицу по абсолютной величине. Следовательно, имеется возможность находить матрицу Адамара путем оптимизации детерминанта ортогональной матрицы того же порядка. Про матрицы *максимума детерминанта* известно то, что они существуют всегда и имеют элементы 1 и –1 [3], а на порядках $4t$ совпадают с матрицами Адамара.

Инвариантов у таких матриц много, и они могут находиться переборными процедурами, но будут ли инварианты ортогональными? Ответ на данный вопрос получить с помощью комбинаторной математики невозможно, поскольку алгоритмы на основе переборного подхода могут гарантировать только оптимум, но не ортогональность.

Теперь зададимся вопросом: а является ли матрицей матрица Адамара?

Орнаменты иррациональных матриц семейства Адамара

То, что мы рассматриваем не матрицу, а гиперобъект как узор, подчеркивается тем, что он может быть представлен не одной ортогональной матрицей, а несколькими матрицами смежных порядков. То есть порядок матрицы (размер узора) в этой задаче понятие весьма растяжимое. Проекция какого-либо математического объекта — это тень, обладающая тем качеством, что

она не обязательно совпадает со всем объектом, но несет о нем информацию. Присмотримся к основе, взятой с обратным знаком от матрицы Адамара без нормализующей каймы порядка $m = n - 1$.

Количество положительных элементов в каждой строке у матрицы сохранится, как и второй инвариант, вычисляемый по ним. Эту матрицу можно сделать ортогональной по строкам (столбцам), заменив значения элементов 1 и –1 на $a = 1$ и $-b$. Тогда скалярное произведение двух соседних строк матрицы порядка $m = 4\lambda - 1$ будет иметь λ значений a^2, $2(k - \lambda) = 2\lambda$ произведений $-ab$ ($k - \lambda$ элементов a каждой из строк умножено на $-b$) и $\lambda - 1$ значений b^2. Таким образом, условие ортогональности определяется как $(\lambda - 1)b^2 - 2\lambda ab + \lambda a^2 = 0$.

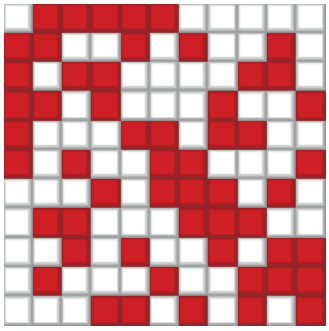
Положительный корень приведенного полинома $b = \frac{\lambda}{\lambda + \sqrt{\lambda}}\alpha$ является модульным уровнем ортогональных матриц, построенных на основе (core) матрицы Адамара. Едва ли две тесно связанные матрицы стоит рассматривать как самостоятельные объекты. Это две проекции гиперобъекта, который мы склонны рассматривать как две ортогональные по столбцам матрицы смежных порядков, но они не независимы, а сосуществуют друг с другом согласно тождеству инвариантов.

Как видно, матрица Адамара, не меняя внутренней сути, не является уже целочисленной матрицей, поскольку значение b иррациональное. Все, что будет далее говориться об итерационном процессе, дающем такую матрицу точно, независимо от значений ошибок вычислений, дает нам возможность забыть на время задачу Диофанта — можно находить иррациональную проекцию, а не целочисленную.

Однако и это еще не все, ведь ровно половину первой строки (или столбца) матрицы занимают элементы со значением 1, кроме первого элемента. Это означает, что эквивалентными операциями перестановок можно произвести разделение строк и столбцов матрицы на начинающиеся с $-b$, а потом с $a = 1$. Для удобства будем называть ее второй нормальной формой матрицы Адамара, или нормальной формой ее основы (рис. 3).

Чтобы далее не путаться, основу порядка $4t - 1$ будем называть матрицей Мерсенна $\mathbf{M}$, а основу порядка $4t - 2$ будем называть матрицей Эйлера $\mathbf{E}$ [12]. Операцию перехода от одной матрицы к другой в силу ее важности назовем «метаморфозой» гиперобъекта.

После *отделения* бинарной каймы и ортогонализации вторичным изменением уровня $b = \frac{\lambda}{\lambda + \sqrt{2\lambda}}\alpha$ останется разделенная на четыре части матрица блочных видов: знакосимметричного $\mathbf{E} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C}^{\mathrm{T}} & -\mathbf{D}^{\mathrm{T}} \end{pmatrix}$ или знакококосимметричного $\mathbf{E} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ -\mathbf{C}^{\mathrm{T}} & \mathbf{D}^{\mathrm{T}} \end{pmatrix}$. Они сводимы к версии с $\mathbf{A} = \mathbf{D}$, $\mathbf{B} = \mathbf{C}$ [12] размера $m - 1$.



■ ***Рис. 3.*** Портрет нормальной формы основы матрицы Адамара

■ ***Fig. 3.*** Portrait of normal form of Hadamard matrix core

Метаморфоза заключается в эквивалентных преобразованиях и перестановках строк и столбцов для выделения блоков, а также в инверсии их знаков и адаптации модуля уровня b. Указанные преобразования позволяют сохранить ортогональность строк и столбцов усекаемой или расширяемой матрицы. Матрица Мерсенна отличается от модульно одноуровневой матрицы Адамара тем, что имеет два уровня 1 и $-b$. Матрица Эйлера в экономном (каноническом) ее представлении является четырехуровневой и двухблочной при $\mathbf{A} = \mathbf{D}$ и $\mathbf{B} = \mathbf{C}$. Благодаря инверсии знака одного блока она содержит элементы $\{1, -1, b, -b\}$.

По отношению к матрице Адамара это менее «плоские» конструкции. Инверсия знака при $-b$ у них не порождает единицу, поэтому преобразование, благодаря которому матрица Адамара может рассматриваться как целочисленная матрица, для двух остальных граней гиперобъекта не проходит. Это объекты иррациональные, которые следует находить итерациями.

Ничто не мешает не удалять, а добавлять кайму к матрице. Матрица Ферма $\mathbf{F}$ может трактоваться как четвертая проекция гиперобъекта, которая требует увеличения числа уровней до трех: кроме единицы и $-b$ появляется уровень элементов каймы s [12]. Однако сделать это просто можно только по отношению к регулярным матрицам Адамара, которые характеризуются дополнительным инвариантом — суммы строк и столбцов одинаковы. К выделенным в $n + 1$ порядкам 5, 17, 256 и т. п. относятся числа Ферма, что привлекает к ним особое внимание.

Можно расширяться и дальше, но это будут многоуровневые матрицы, которые менее универсальны и менее интересны, поскольку состав стабилизирующих их свойства инвариантов исчерпывается описанными выше.

Изменение определения матрицы. В основу определения матриц с элементами 1 и $-b$ можно положить функцию уровня: для матриц Адамара $b = 1$, для матриц Мерсенна $b = \frac{\lambda}{\lambda + \sqrt{\lambda}}\alpha$ и для матриц Эйлера $b = \frac{\lambda}{\lambda + \sqrt{2\lambda}}\alpha$, — связав столбцы условием ортогональности. Но уравнение ортогональности не связано непосредственно с экстремальными свойствами этих матриц, и желательно определить их через итерационный алгоритм оптимизации детерминанта.

Алгоритм Прокруста

Детерминант любой ортогональной в смысле $\underline{\mathbf{A}}^{\mathrm{T}}\underline{\mathbf{A}} = \mathbf{I}$ матрицы порядка n равен единице. Это является удобной точкой отсчета. Разделив ее на максимальный по абсолютному значению элемент μ матрицы $\underline{\mathbf{A}}$, получаем квазиортогональную матрицу $\mathbf{A}$ такую, что $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega\mathbf{I}$, где $\omega \le 1$ — некоторый весовой коэффициент $\omega = 1/\mu^2$ [12].

Теорема. Чем меньше μ, тем выше детерминант $\det(\mathbf{A}) = \omega^{n/2} = 1/\mu^n$ матрицы, приведенной к форме с единицей в качестве максимального элемента.

Эта теорема напрямую следует из выражения для ω и элементарным следствием дает хорошо известную в теории матриц Адамара $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$ границу сверху $\det(\mathbf{A}) \le n^{n/2}$, достижимую *только* на порядках 1, 2 и кратных четырем. На прочих порядках приходится увеличивать число модульных уровней. При этом матрицы Мерсенна и Эйлера, будучи образованными от столь мощной по детерминанту основы, не утрачивают экстремальных свойств, однако приобретают специфику.

Приступим к описанию алгоритма их нахождения, целиком следующего из их определения как квазиортогональных матриц, характеризуемых максимальным элементом μ матрицы $\underline{\mathbf{A}}$.

Название алгоритма напрямую связано с мифом, согласно которому тиран Прокруст, накормив гостей, укладывал их на кровать. Выступающие за пределы кровати ноги он отрубал, а короткие — вытягивал, стремясь придать им эстетичные формы. Вкратце изложенное соответствует описанию алгоритма оптимизации детерминанта, подаренному античной традицией доводить все до совершенства.

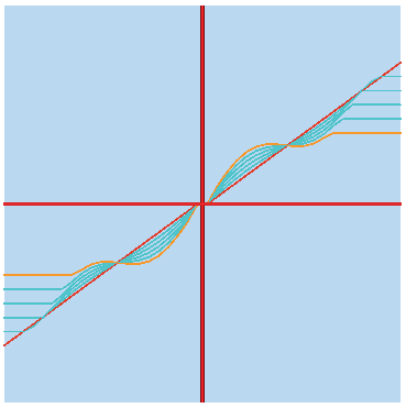
У квазиортогональной матрицы максимума детерминанта $\mathbf{A}$ максимальный по абсолютной величине элемент μ минимален. Это типичная минимаксная задача. Алгоритм Прокруста для матриц сводится к усечению максимального элемента. Первую фазу алгоритма назовем сжатием. При слишком примитивном прокрустовом сжатии матрица теряет ортогональность, но ее несложно восстановить известной процедурой Грама — Шмидта [18], которая вызывает растяжение. Возникает двухэтапный процесс, сжатие плюс растяжение, который итерациями действительно ведет матрицу к оптимуму.

Основа алгоритма Прокруста — нелинейный блок насыщения. Как мы его настроим, так он и будет работать. В простейшем случае это только насыщение, но можно добавить и вытягивание слишком малых элементов — ограничивать большие элементы и увеличивать малые. Уровень насыщения верхнего порога $p \le 1$ и искажение уровней малых элементов можно регулировать изменением профиля кривой, делая порог и искажения сильнее в начале итераций (рис. 4).

Повысить качество алгоритма можно еще несколькими способами, например перестановкой наиболее изменяемых столбцов на первое место или выбором начальной матрицы. Однако это уже второстепенные детали численного метода [19, 20]. Для двухуровневых матриц 1, $-b$ малых элементов (в итоговом решении) не бывает, но и задирать слишком сильно насыщение (снизу) до значения b нельзя, поскольку важна возможность изменять знаки элементов матрицы в процессе итераций. Это сказывается на эффективности поиска локальных экстремумов.

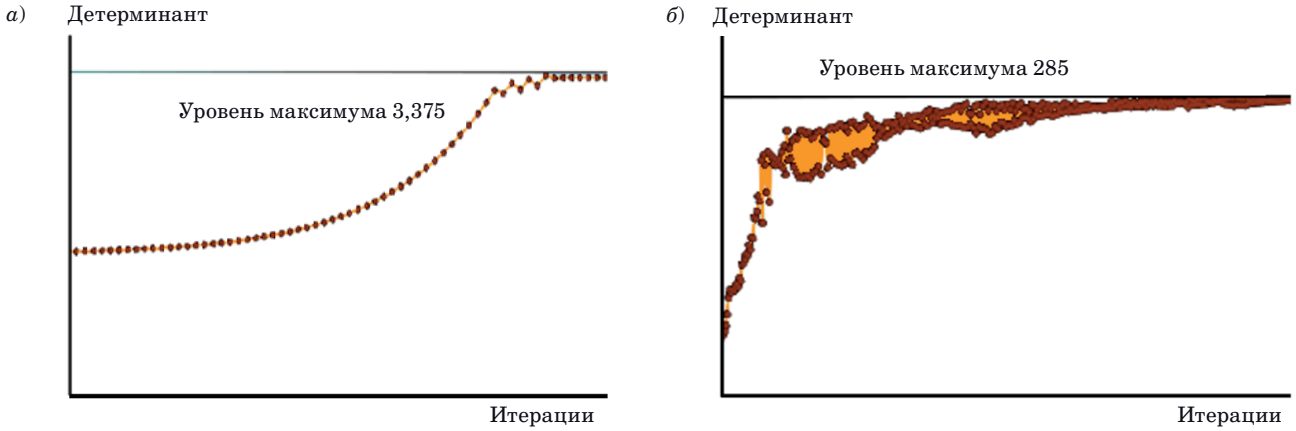
Матрица Адамара является естественным продуктом алгоритма Прокруста. У нее все элементы одинаковы по абсолютной величине, так что они определенно побывали в «прокрустовой кровати».

Сам по себе нелинейный блок статический, но в итерациях с порогом p, постепенно стремящим-



■ ***Рис. 4.*** Диаграмма пропускания нелинейного блока насыщения

■ ***Fig. 4.*** Transmission diagram of a nonlinear saturation block



■ ***Рис. 5.*** Кривые роста детерминантов матриц порядков 3 (*а*) и 7 (*б*)
■ ***Fig. 5.*** Curves of determinant growth for matrices of 3rd (*а*) and 7th (*б*) orders

ся к максимуму (к единице) — это динамическая система [19], хорошо известная в теории автоматического управления. Например, таков контур астатического регулирования системы с интегратором в цепи обратной связи по ошибке регулирования. Точка статического равновесия (неподвижная точка) приходится на искомую матрицу.

Ортогональная матрица с изменениями элементов, ортогонализацией и нормализацией столбцов вынужденно движется к экстремуму. Приложение теоремы о неподвижной точке отражения ограничено здесь наличием локальных экстремумов, нежелательных препятствий на порядках, кратных четырем, но результативных для матриц нечетных порядков. Матрица нечетного порядка не может достичь успокоения в форме с одинаковыми уровнями элементов — ее попросту нет. Элементы имеют два неравных значения или более двух при большем детерминанте. Однако это мало что меняет в работе алгоритма (рис. 5, *а* и *б*).

Условия останова алгоритма Прокруста

Для понимания условий останова алгоритма Прокруста следует учесть, что это алгоритм поиска не элементов, а орнамента. Как и в условиях теоремы Тарского [1], нарушим целочисленные значения элементов матрицы Адамара в любую сторону — к нулю или к бесконечности, не меняя знака. Значит ли это, что мы утратили эту самую матрицу Адамара? Судя по инвариантам $k = n/2$ и $\lambda = n/4$, — нет.

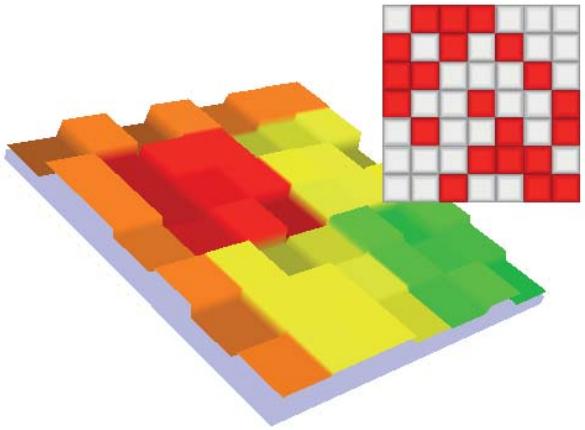
Отсюда следуют два вывода. Во-первых, найти исходную матрицу Адамара не составит труда. Для этого достаточно подтянуть элементы к значениям 1 и –1. Во-вторых, если некоторый итерационный процесс оптимизации детерминанта со сколь угодно большими ошибками выдаст такую матрицу до своего завершения, матрица Адамара будет найдена. Это процесс грубый, терпимый к большим неточностям. Мы ищем орнамент, а не матрицу. Инварианты у нее орнаментальные, описывающие узор, т. е. некий геометрически дискретный объект.

Пример. Матрицы Мерсенна являются двухуровневыми, с элементами 1 и $-b$. Допустим, в процессе итераций алгоритма Прокруста получается первая из приведенных ниже матриц порядка 7:

$$\begin{pmatrix} b & 1 & 1 & b & 1 & 1 & b \\ 1 & b & b & 1 & -1 & -1 & -b \\ 1 & b & -1 & -b & -1 & b & 1 \\ b & 1 & -b & -1 & 1 & -b & -1 \\ 1 & -1 & -1 & 1 & b & b & -b \\ b & -b & 1 & -1 & -b & 1 & -1 \\ 1 & -1 & b & -b & b & -1 & 1 \end{pmatrix};$$

$$\begin{pmatrix} -b & 1 & 1 & -b & 1 & 1 & -b \\ 1 & -b & -b & 1 & 1 & 1 & -b \\ 1 & -b & 1 & -b & 1 & -b & 1 \\ -b & 1 & -b & 1 & 1 & -b & 1 \\ 1 & 1 & 1 & 1 & -b & -b & -b \\ -b & -b & 1 & 1 & -b & 1 & 1 \\ 1 & 1 & -b & -b & -b & 1 & 1 \end{pmatrix}.$$

Уровень достигнут, достигнуты и инварианты: по $k = 4$ элемента 1 с положительным или отрицательным знаком в каждой строке и столбце и по $\lambda = 2$ соседствующих таких же элемента — в любой паре строк или столбцов. Так как инварианты соблюдены, мы можем не заниматься эквивалентными преобразованиями и заме-



■ ***Рис. 6.*** Матрица итога итераций и она же — решение
■ ***Fig. 6.*** Final iteration matrix and it is as the solution

нить все элементы ±1 на 1 и $\pm b$ на $-b$. При этом безразлично, как считать такие инварианты. Можно ориентироваться на знаки элементов, а можно на модули уровней (чего нет у матриц Адамара). Это означает, что останов алгоритма можно выполнить, не дожидаясь схождения величин элементов к заведомо недостижимым точно иррациональным значениям, которые мы знаем заранее. Можно селектировать их величины по порогу $(1 + b)/2$ на большие и малые, а по достижении нужных инвариантов привести итог к нормальному виду с бинарной каймой (рис. 6).

Функции поиска четко разделены. За вычисление уровня отвечает алгоритм вычисления корня квадратного с его более чем двухтысячелетней историей. Орнамент, а не матрицу с иррациональными элементами ищет алгоритм Прокруста. Он тянет матрицы к глобальному или к локальным экстремумам.

Поиск локальных и условных экстремумов

Оптимальные по детерминанту матрицы отличаются характером своих экстремумов, это могут быть:

— глобальный (абсолютный) экстремум, как у матриц Адамара;

— локальный экстремум, отличающийся от глобального меньшим значением максимума;

— условный экстремум седловых точек, когда свобода вариации аргумента ограничена условием.

Задачи поиска корней уравнений дистанцируются от задач оптимизации тем, что положение корней не обязательно увязывать с максимумом какой-либо функции. Итерационный алгоритм рассматривают как систематически применяемое правило переноса (отображения) все новых и новых точек приближения к корню, а сам корень считается найденным, если находится в «неподвижной точке» такого отображения. Если точка только одна, схождение к ней обеспечивается из любых начальных условий.

Алгоритм Прокруста имеет регулируемый шаг по величине насыщения. При малом шаге на его итерациях не происходит изменение знаков элементов. Алгоритм ищет условный, а не абсолютный или локальный экстремум. Это удобно для поиска матриц в седловых точках, например матриц Ферма, когда ненужное направление изменения орнамента отсекается знаками. Орнамент таких матриц плавным изменением уровней (с изменением знаков) можно перевести в орнамент матриц глобального экстремума, уравнения перехода рассмотрим ниже.

Связь иррационального и целочисленного инвариантов

Матриц Адамара, а значит, и матриц Мерсенна бесконечно много. Согласно теореме Тарского о бесконечном числе математических объектов выносится определенное суждение на основании конечного числа манипуляций.

Допустим, оптимизацией детерминанта найдены несколько ортогональных в смысле $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega\mathbf{I}$ матриц с элементами 1, $-b$ разных порядков $m = n - 1$, где $\omega \le 1$ – некоторый весовой коэффициент. Для того чтобы идентифицировать функцию $b = b(m) = x_1(m)b^2 + x_2(m)b + x_3(m) = 0$, много матриц не потребуется. Параметры $x_1(m)$, $x_2(m)$, $x_3(m)$ — заранее неизвестные линейные рациональные функции от порядка m.

Они линейны, поскольку сводятся к подсчету числа элементов b^2, b^1, b^0 в скалярных взаимных произведениях столбцов $\mathbf{M}$, причем точное значение b не требуется. Уравнение $(m - 3)b^2 - 2(m + 1)b + (m + 1) = 0$ отвечает характеристическому уравнению матриц Мерсенна $(\lambda - 1)b^2 - 2\lambda ab + \lambda a^2 = 0$ при $a = 1$. Учитывая $\lambda = (m + 1)/4$, можно найти $b = \dfrac{\lambda}{\lambda + \sqrt{\lambda}} = \dfrac{m+1}{m + 2\sqrt{m+1} + 1}$, идентифицируя этот класс всего по нескольким его представителям.

Идентификация параметров на основании данных эксперимента давно используется в адаптивных системах. Для описания динамической системы, выполняющей маневр на отрезке времени любой протяженности, нет необходимости анализировать его весь. Достаточно по конечному числу точек найти параметры модели системы в форме дифференциального уравнения. Это касается установления эквива-

лентности между законами Ньютона и законами Кеплера описания движения планет. Никто не сверяет всю орбиту поточечно с решением дифференциального уравнения тяготения.

Если изучается класс бесконечного числа ортогональных матриц по конечному числу их представителей, обнаруженных алгоритмом Прокруста, можно установить аналитически точный вид функции уровня для всех них [20]. Далее важно то, что функция $b = b(m)$ монотонна, не содержит разрывов при всех значениях m, свидетельствующих об отсутствии решения. Уровень b помогает идентифицировать важнейший орнаментальный инвариант $\lambda = b^2/(1-b)^2$ через квадрат отношения отрезков, на которые $b < 1$ делит уровень $a = 1$. Следовательно, если из опыта экспериментов с алгоритмом Прокруста удалось установить значение b (даже не очень точно), можно оценить перспективу нахождения λ, т. е. того самого инварианта, который при поиске матриц Адамара перебором до завершения перебора аналитически установить невозможно. Это замечательное утверждение связывает два мира (дискретный и континуальный): целочисленный орнаментальный инвариант и иррациональный уровень.

Замкнутые орнаменты

Греческий математик и философ Прокл Диадох, сторонник чрезмерного лаконизма, разрабатывал концепцию числа как моста между двумя началами — умом и чувственным восприятием. Вспомнили мы о нем вот почему.

Рассмотрим матрицу Эйлера, которая в экономном своем варианте с блоками $\mathbf{A} = \mathbf{D}$ и $\mathbf{B} = \mathbf{C}$ может строиться на основе всего одной матрицы Мерсенна $\mathbf{M}$. Поскольку матрицы Мерсенна регулярны (суммы столбцов и строк совпадают), составная матрица Эйлера порядка $2m$ допускает назначение двух разных значений плеч $\mathbf{A} = \mathbf{M}(b_1)$, $\mathbf{B} = \mathbf{M}(b_2)$, причем можно выделить уравновешенное

$$b_1 = b_2 = \frac{\lambda}{\lambda + \sqrt{\lambda}} = \frac{m+1}{m + 2\sqrt{m+1} + 1}$$

решение $\mathbf{M} = \mathbf{A} = \mathbf{B} = \mathbf{C} = \mathbf{D}$ и экстремальное по детерминанту решение при $b_1 = 1$:

$$b_2 = \frac{\lambda - 1}{\lambda + \sqrt{2\lambda - 1}} = \frac{m-3}{m + 2\sqrt{2m+2} + 1}.$$

Первое решение назовем матрицей Эйлера, а второе — матрицей Прокла; усилив преобладание единичных по абсолютному значению элементов диагонального блока, поднимем значение детерминанта. Как и качели, они имеют два положения — уравновешенное и когда один край качелей вверху. В таких качелях важно то, что орнамент у обеих матриц общий. Они принадлежат континуальному множеству матриц, которые плавным координированным изменением параметров плеч переходят, без изменения рисунка из знаков, в состояние с бóльшим детерминантом.

Это означает, что алгоритм Прокруста, если его не останавливать, остановится на второй матрице, но находит-то он их обе. Таким образом, найден орнамент бесконечного множества матриц, одна из которых оставляет ему возможность быть в виде большого детерминанта.

Определение: Орнамент называется замкнутым, если любое малое изменение параметров узора приводит к понижению детерминанта.

Примеры замкнутых орнаментов: матрицы Адамара, Белевича, Мерсенна, Прокла. Стартовая матрица Прокла при $m = 3$ эквивалентна конференц-матрице с нулем на диагонали, что согласуется с ролью этой трехуровневой матрицы, замещающей матрицы Адамара на четных не достижимых ими порядков.

Примеры незамкнутых орнаментов: матрицы Эйлера как основа матриц Мерсенна и матрицы Одина как основа конференц-матриц [21]. Это параметрически изменяемые узоры. Алгоритм Прокруста к их поиску применим с рядом оговорок о поиске замкнутых орнаментов, к инвариантам которых имеют отношение нестабильные матрицы.

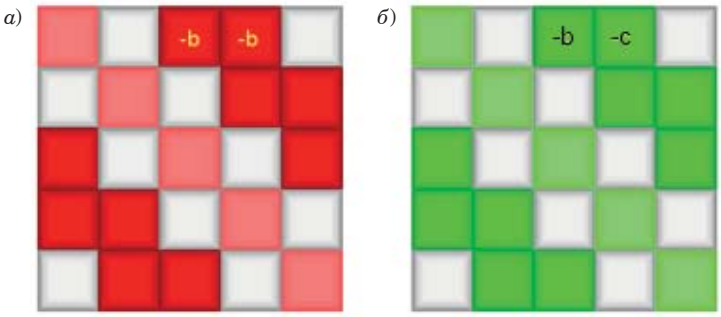
Устойчивость орнаментам первых трех матриц Адамара, Белевича и Мерсенна придает явно прослеживаемая в их конструкции кайма. Матрица Прокла зажата иначе — фиксированием половины ее параметров в –1, остальные находятся в блоках вне диагонали. Поскольку орнамент матрицы Мерсенна замкнут, то замкнут и орнамент матрицы Прокла.

Различие матриц Адамара и конференц-матриц

В тридцатых годах Пэли [10] обратил внимание, что если инвариант $k = n/2$ таков, что $p = k - 1$ разложимо на сумму двух квадратов, то симметричные четырехблочные матрицы Адамара можно строить на основе одного симметричного ортогонального блока с нулевой диагональю, варьируя знак диагонали:

$$\begin{pmatrix} \mathbf{C}+\mathbf{I} & \mathbf{C}-\mathbf{I} \\ \mathbf{C}-\mathbf{I} & -(\mathbf{C}+\mathbf{I}) \end{pmatrix}.$$

Особенно легко эта конструкция строится для простых p (или степеней простого числа), когда первая строка циклического блока $\mathbf{C}$ строится несложными алгоритмами конечных полей $GF(p)$.



■ ***Рис. 7.*** Портреты матриц Одина (*а*) и Модина (*б*)
■ ***Fig. 7.*** Portraits of Odin (*а*) and Modin (*б*) matrices

Позднее В. Белевич предложил рассматривать этот блок в качестве самостоятельной ортогональной матрицы, назвав ее конференц-матрицей в силу приложения ее к задачам телефонии. Конференц-матрица во многом напоминает матрицу Адамара и считается ее прямым продолжением на недостижимые матрицами Адамара четные порядки. После нормализации количество положительных и отрицательных элементов (вне каймы) симметричной матрицы Белевича совпадает в строках и столбцах.

Возможны построения аналогов матриц Мерсенна и Эйлера, названные матрицами Одина и Тени [20].

Ортогонализация матрицы Одина порядка $m = 4t - 3$ (и Тени порядка $m - 1$) невозможна без отрыва диагонального элемента от нуля $d = \frac{1}{1+\sqrt{m}}$, уровень $b = 1 - 2d$ компенсирует этот отрыв. Стартовая матрица Одина пятого порядка (рис. 7, *а*) не является матрицей локального максимума детерминанта. Доказать это несложно, разделив пару элементов первой строки $-b$ на $-b$ и $-c$. Чтобы не путаться, назовем вторую матрицу матрицей Модина (рис. 7, *б*).

По орнаменту обе приведенные матрицы являются матрицами «под-Белевичами». Орнаменты матриц Одина не замкнуты, при $m = 5$ диагональ $d = \frac{1}{1+\sqrt{m}} + \delta$ меняется за счет добавки δ, изменяющиеся в противоположные стороны параметры $b = \frac{1}{d+1} - c$, $c = \frac{1+\sqrt{8d^3+16d^2+4d-3}}{2(d+1)}$ играют ту же роль, что и плечи матриц Прокла.

Иными словами, детерминант матрицы Модина можно повысить в сравнении с детерминантом матрицы Одина, разорвав тождество $b = c$ сколь угодно малым изменением параметра d. Это означает, что матрицы Одина — седловые точки, а не точки локального оптимума детерминанта. У матриц Одина есть возможность при помощи варьируемой диагонали, позволяющей матрице измениться, повышать детерминант.

Это показывает существенное отличие матриц Мерсенна от матриц Одина. Элементы диагонали насыщены в единицы, так что «кредита доверия» для повышения детерминанта нет. Значение d максимально высоко.

Границы детерминантов критских матриц

Критские матрицы — это матрицы семейства Адамара $\mathbf{A}^T\mathbf{A} = \omega\mathbf{I}$ с небольшим числом уровней. Число уровней критских матиц нечетных порядков растет линейно (почти линейно) до критического порядка 13, где структура матриц резко усложняется возникновением почти хаотических матриц [12]. Детерминанты $\det(\mathbf{A}) = \omega^{n/2}$ и веса ω первых экстремальных по детерминанту матриц хорошо известны, это позволяет оценить то, насколько мало экстремумы локально оптимальных матриц Мерсенна уступают глобальным экстремумам при сравнении. Для этого используем тройки значений (порядок матрицы; вес матрицы Мерсенна; вес матрицы глобального экстремума): (3; 2,25; 2,25), (7; 5,03; 5,08), (11; 8,01; 8,5), (15; 11,11; 11,99).

Первая из этих матриц, приведенная к единице по максимальным значениям элементов, хорошо известная ортогональная матрица поворота на три угла Эйлера $\alpha = -\arcsin(2/3)$, $\beta = \gamma = \pi - \arctan(2)$:

$$\begin{pmatrix} \cos(\alpha)\cos(\gamma) & \cos(\alpha)\sin(\gamma) & -\sin(\alpha) \\ \sin(\alpha)\sin(\beta)\cos(\gamma) - \cos(\beta)\sin(\gamma) & \sin(\alpha)\sin(\beta)\sin(\gamma) + \cos(\beta)\cos(\gamma) & \cos(\alpha)\sin(\beta) \\ \sin(\alpha)\cos(\beta)\cos(\gamma) + \sin(\beta)\sin(\gamma) & \sin(\alpha)\cos(\beta)\sin(\gamma) - \sin(\beta)\cos(\gamma) & \cos(\alpha)\cos(\beta) \end{pmatrix}.$$

Функцию трех переменных невозможно представить в виде обычного графика поверхности с пиком экстремума, но можно показать детерминант диаметром шарика. Максимум в центре соответствует повороту, порождающему изображенную матрицу Мерсенна. Вариация углов в окрестности этой точки может только уменьшить сферы вокруг центральной точки (рис. 8, *а*).

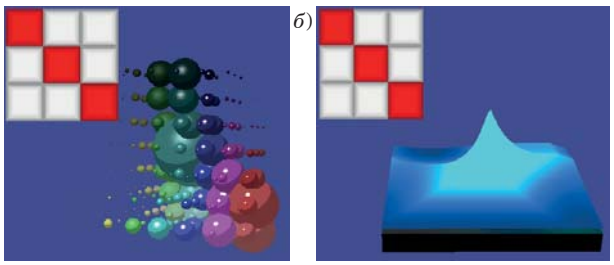
Традиционный рисунок максимума экстремума тоже можно увидеть, задавая развертку двумя углами, когда третий угол выбирается из условия максимума (рис. 8, *б*). На множестве матриц седьмого и более высоких порядков матрицы глобального **A** и локального **M** экстремумов не совпадают. Профиль экстремальной кривой можно изучать, ортогонализуя осредненную матрицу $\mathbf{A}t + \mathbf{M}(1-t)$, где t — вещественный параметр, регулирующий уход от матрицы локального в сторону глобального детерминанта (рис. 9).

Хороший рисунок в состоянии многое показать. Если детерминант любой критской матрицы $\omega^{n/2}$ поделить на оценку Адамара сверху $n^{n/2}$, то такой относительный детерминант не будет превышать единицу. Приведенный детерминант — это корень n-й степени из относительного детерминанта $\sqrt{\frac{\omega}{n}}$. Диаграмма с приведенными детерминантами экстремальных матриц, нанесенная с шагом 4, показывает их прижатыми к верхней границе, причем сжатие нарастает. Максимальные по возможному детерминанту матрицы Адамара находятся на верхней единичной полочке (рис. 10).

Порядки $4t$, $4t-1$, $4t-2$, $4t-3$, определяющие основные типы матриц семейства, отвечают еще трем границам. Более жесткую границу сверху дают оценки детерминантов конференц-матриц дополнительных четных порядков. На рис. 10 представлена граница детерминантов матриц Мерсенна (чуть ниже можно добавить границу для матриц Одина, основ матриц Адамара и конференц-матриц). Точки между ними являются значениями норм многоуровневых матриц максимума детерминанта. Портреты матриц и гистограммы их уровней представлены на рис. 11.

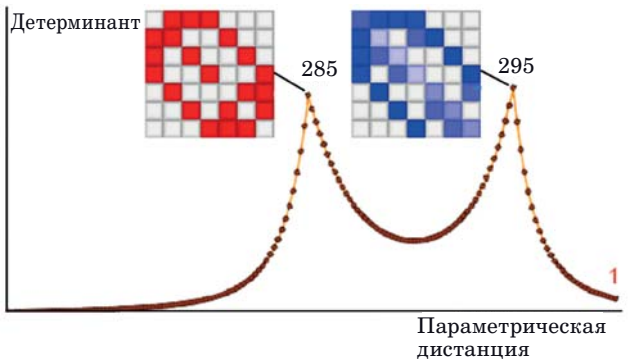
На порядке 22, где нет конференц-матрицы, есть шестиуровневая бициклическая и взвешенная матрицы. Детерминант последней дает точку, не дотягивающую до оптимистичной границы детерминантов конференц-матриц. Экстремальные многоуровневые матрицы приспосабливаются к порядку увеличением числа уровней и неограниченным нарастанием сложности их структур.

Как видно, граница детерминантов матриц Мерсенна — это наиболее удачное и относительно несложное приближение снизу. Так как матрицы Адамара и матрицы Мерсенна представляют объект с одним и тем же орнаментом (пренебрегая каймой), то получается, что критские матрицы зажаты между этими двумя проекциями гиперобъекта.



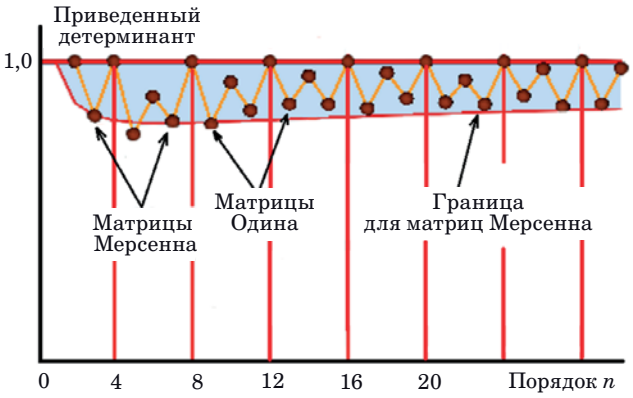
■ ***Рис. 8.*** Представление максимума детерминанта в 3D (*а*) и 2D (*б*) вариантах

■ ***Fig. 8.*** Maximum determinant in 3D (*а*) and 2D (*б*) versions



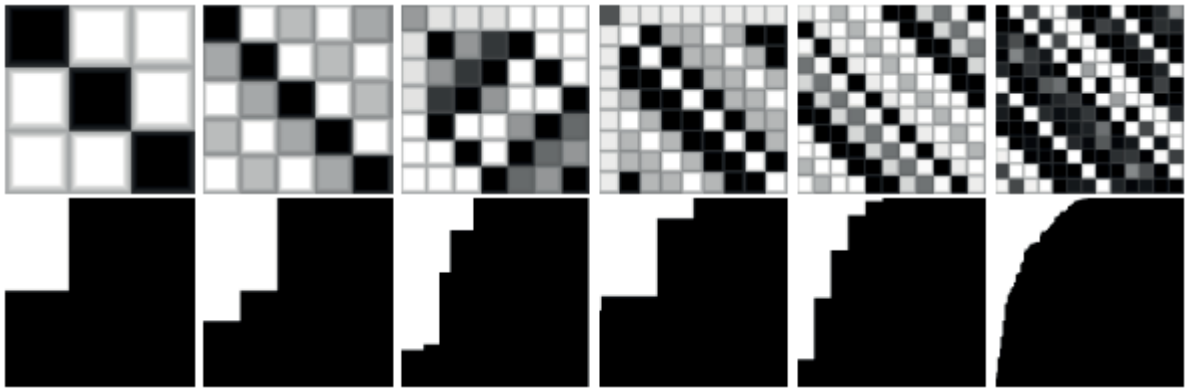
■ ***Рис. 9.*** Локальный и глобальный экстремумы детерминанта

■ ***Fig. 9.*** Local and global extremes of determinant



■ ***Рис. 10.*** Диаграмма максимальных детерминантов

■ ***Fig. 10.*** Maximum determinants diagram



■ ***Рис. 11.*** Портреты и диаграммы уровней элементов оптимальных матриц
■ ***Fig. 11.*** Portraits and element level diagrams of optimal matrices

Связь гиперобъекта с теоремой Дженнифер Себерри

Матрицы Адамара основной последовательности порядков Сильвестра отвечают числам Мерсенна $2^s - 1$, дающим размеры вложенных в них матриц, которые существуют вне зависимости от того, простые это числа, степени простых чисел или составные числа [22, 23].

Дженнифер Себерри доказала следующее [2].

Теорема. Минимальное расстояние $s > 0$ между нечетными простыми числами p и $2^s p - 1$ (размеров потенциальных основ конференц-матриц **C** или матриц Адамара конструкции Пэли) конечно и не превышает удвоенного логарифма от p.

Два — это максимальный коэффициент, его можно снижать, добавляя к логарифму константу смещения. Это называется оценкой асимптотики существования матриц Адамара, поскольку последующими удвоениями порядка можно получить неограниченное количество этих матриц. Для составных нечетных чисел оценки не меняются, так как матрицу Адамара можно получить кронекеровым произведением [24] матриц меньшего порядка, построенных для сомножителей по той же схеме.

Поскольку числа $2^s p - 1$ являются обобщением чисел Мерсенна, естественно предположить, что от расстояния s зависит не столько само существование матриц Адамара, сколько существование их в специфической форме Пэли. Кроме матриц, которые строятся на квадратичных вычетах, их можно найти в форме двояко-симметричных бициклов с парной каймой — описанных выше матриц Эйлера. За потерю возможности использовать поле есть чем платить: из симметричной и кососимметричной клеток универсального бицикла гарантированно остается одна.

Симметрии матриц принято описывать дициклическими группами или, как у коциклических матриц, таблицей умножения группы после дихотомии элементов группы на описывающие 1 или –1. Эта ясная точка зрения не разрешает вопрос существования, поскольку дихотомия неоднозначна и столь же трудна, как попытка найти матрицу Адамара прямым перебором. Тем не менее теорема Дж. Себерри об асимптотическом существовании матриц Адамара свидетельствует о том, что для выделяемого ею анклава матриц Адамара составной характер размера их основ не имеет никакого значения.

Заключение

В противопоставлении матриц Адамара и неортогональных матриц максимума детерминанта содержится доля противоречия. Выходит, что кроме экстремальных по детерминанту матриц Адамара есть еще какие-то экстремальные матрицы. Все это плохо согласуется между собой и будит желание разобраться глубже в проблеме. Матрицы Мерсенна, которые оказываются двойниками матриц Адамара, не утрачивают свойство быть экстремальными, и их находят алгоритмы поиска неподвижной точки отображения.

Экстремальные матрицы на любом разрешенном для них порядке идентифицируемы алгоритмом Прокруста — нет принципиальных препятствий найти экстремум, даже если этот экстремум локален и приблизиться к нему поиском области притяжения сложно. Алгоритм находит матрицы стартовых порядков различной природы, которые теоретически были открыты в разное время разными методами. Задача поиска раскладывается на субалгоритм вычисления иррационального уровня и субалгоритм поиска орнамента. Первый — это алгоритм Ньютона

для скалярного случая, а второй реализует поиск орнамента.

Благодаря модификации профиля нелинейного блока насыщения алгоритм может искать как локальные экстремумы, так и седловые точки — условные экстремумы, поскольку при малой амплитуде изменений, вносимых отображением, знаки элементов матрицы не меняются. Удержание знаков орнамента стабилизирует итерации на такой «невыгодной» точке, как седловая, из которой есть путь по увеличению значения детерминанта. Так, например, алгоритмом Прокруста были найдены матрицы Ферма, ошибочно классифицируемые изначально как матрицы локального экстремума именно потому, что алгоритм их ищет устойчиво и не теряет при отклонениях их параметров. Аналогичные «грубые» алгоритмы сыграли большую роль при поиске нулей дзета-функции, находить точные значения которой сложно.

Критские матрицы тесно связаны с числовой системой; всем особым числам: золотому сечению, числам Ферма, Мерсенна, числам-близнецам — отвечают соответствующие матрицы. На глубокое различие нечетных порядков $4t - 1$ и $4t - 3$ впервые обратили внимание Ферма и Эйлер в рамках так называемой Рождественской теоремы Ферма. Как видно, у матриц тоже есть это различие, выражающееся в том, что все матрицы Мерсенна порядков $4t - 1$ существуют без исключения, на что указывает наличие у них идентифицируемого экстремума.

Если фиксировать элементы уровнями, мостика между матрицей Мерсенна и матрицей глобального экстремума нет при том, что они близки по орнаменту. Поэтому, строя график изменения детерминанта матриц порядков $4t - 1$, нам приходится не просто усреднять, а еще и ортогонализировать промежуточные матрицы. Ничего подобного нет у седловых точек матриц порядков $4t - 3$, поскольку у них путь наверх заведомо облегчен структурой матрицы, будь это матрица Одина или матрица Ферма. Математический аппарат конечных полей и групп начала прошлого века ускоряет процесс поиска матриц. Эти инструменты, превосходные в своей эффективности на некоторых выделенных простотой порядках, уступают в мощности вычислений в поле вещественных чисел. Уже в скалярном случае полноценное рассмотрение задач алгебраической геометрии невозможно без привлечения итерационных процедур, с помощью которых было сформировано само понятие иррационального числа.

Финансовая поддержка

Статья подготовлена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004.

Благодарности

Авторы выражают искреннюю благодарность за многолетнюю помощь и поддержку профессору Д. Джоковичу. За помощь в технической работе с рукописью благодарят Т. В. Балонину.

Литература

1. **Матиясевич Ю. В.** Алгоритм Тарского. *Компьютерные инструменты в образовании*, 2008, № 6, с. 4–14.
2. **Jennifer S., Yamada M.** *Hadamard matrices: Constructions using number theory and linear algebra*. Wiley, 2020. 384 p.
3. **Colbourn C. J., Dinitz J. H.** *Handbook of Combinatorial Designs*. Second ed. Chapman and Hall/CRC, 2007. 967 p.
4. **Silvester 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, no. 34, pp. 461–475.
5. **Hadamard J.** Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.
6. **Балонин Н. А., Сергеев А. М., Синицына О. А.** Алгоритмы конечных полей и групп поиска ортогональных последовательностей. *Информационно-управляющие системы*, 2021, № 4, с. 2–17. doi:10.31799/1684-8853-2021-4-2-17
7. **Djocovic D. Z., Kotsireas I. S.** Periodic Golay Pairs of Length 72. In: *Algebraic Design Theory and Hadamard Matrices*. C. J. Colbourn (ed). Springer, 2015. Pp. 83–92.
8. **Ito N.** On Hadamard groups IV. *Journal of Algebra*, 2000, no. 234, pp. 651–663.
9. **Schmidt B.** Williamson matrices and a conjecture of Ito's. *Designs, Codes and Cryptography*, 1999, no. 17, pp. 61–68.
10. **Paley R. E. A. C.** On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
11. **Williamson J.** Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
12. **Балонин Н. А., Сергеев М. Б.** *Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские*. СПб.: Политехника, 2019. 196 с. doi:10.25960/7325-1155-0

13. **Сергеев А. М., Куртяник Д. В., Тарашкевичус К. Ф.** Матричный портрет как основа дискретного текстильного орнамента. *Известия высших учебных заведений. Технология легкой промышленности*, 2019, т. 44, № 2, с. 102–107.
14. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi:10.31799/1684-8853-2019-3-2-9
15. **Гаусс К. Ф.** *Труды по теории чисел*. М.: Изд-во АН СССР, 1959. 978 с.
16. **Liouville J.** Nouveaux théorémes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84.
17. **Awyzio G., Seberry J.** On Good Matrices and Skew Hadamard Matrices. In: *Algebraic Design Theory and Hadamard Matrices*: Springer Proceedings in Mathematics & Statistics/Ch. Colbourn (eds). Springer, Cham., 2015. Vol. 133. https://doi.org/10.1007/978-3-319-17729-8_2
18. **Pursell L. and Trimble S. Y.** Gram — Schmidt orthogonalization by Gauss elimination. *The American Mathematical Monthly*, 1991, vol. 98, no. 6, pp. 544–549.
19. **Балонин Н. А., Сергеев М. Б.** О значении матриц начального приближения в алгоритме поиска обобщенных взвешенных матриц глобального и локального максимума детерминанта. *Информационно-управляющие системы*, 2015, № 6, с. 2–9. doi:10.15217/issn1684-8853.2015.6.2
20. **Балонин Н. А., Сергеев М. Б.** Критские матрицы Одина и Тени, сопровождающие простые числа и их степени. *Информационно-управляющие системы*, 2022, № 1, с. 2–7. doi:10.31799/1684-8853-2022-1-2-7
21. **Belevitch V.** Theory of 2n-terminal networks with application to conference telephony. *Electrical Communication*, 1950, vol. 27, no. 3, pp. 231–244.
22. **Сергеев А. М.** Простые числа и симметрии квазиортогональных циклических матриц Мерсенна. *Математические методы и модели в высокотехнологичном производстве*: тезисы докл. I Междунар. форума, Санкт-Петербург, 10–11 ноября 2021 г. СПб., 2021, с. 14–15.
23. **Сергеев А. М.** Об одном подходе к вычислению квазиортогональных циклических матриц с симметриями как основы кодов. *Телекоммуникации*, 2022, № 9, с. 28–33. doi: 10.31044/1684-2588-2022-0-9-28-33
24. **Van Loan C.** The ubiquitous Kronecker product. *Journal of Computational and Applied Mathematics*, 2000, vol. 123, iss. 1-2, pp. 85–100. doi:10.1016/S0377-0427(00)00393-9

UDC 519.614
doi:10.31799/1684-8853-2023-1-2-16
EDN: KOMNBV

Solvable and unsolvable problems. Using Procrustes analysis algorithm for obtaining a family of Hadamard matrices

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
J. Seberry[b], Dr. Sc., Tech., Honorary Professor, orcid.org/0000-0002-9558-4293
M. B. Sergeev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[b]Department of Computing and Information Techology, University of Wollongong, NSW 2522, Australia

Introduction: The development of the Hadamard matrix theory encountered an obstacle caused not so much by the nature of the integer problem as by the artificial limitation of the solution of quadratic equations applying exhaustive search algorithms. Ignoring the direct path and rejecting irrationality led to the opinion that the hypothesis of the existence of Hadamard matrices was unprovable. **Purpose:** To prove the solvability of the Hadamard problem by orthogonal matrices via identifying their stable connection with matrices containing irrational elements. **Results:** We show that irrationality manifests itself in the quadratic norm of the columns of the Hadamard matrix of the second order. We consider the transfer of iterative algorithms for calculating roots to the matrix. To minimize the maximum absolute value element of the orthogonal matrix we propose the Procrustes analysis algorithm. Since Hadamard matrices are determined by invariants of smaller-order matrices embedded in their structure, the algorithm turns out to be a universal basis for finding them together. We consider the hypothesis of the existence of Hadamard matrices in the operational domain of iterative algorithms determined over the field of real numbers that give advantage over the tools in the form of finite fields and groups. **Practical relevance:** Orthogonal sequences obtained from rows (columns) of Hadamard matrices, and high-order Hadamard matrices themselves are of great practical importance for problems of noise-correcting coding, compression, masking and image processing.

Keywords — Hadamard matrices, conference matrices, Cretan matrices, Procrustes analysis algorithm, finite fields, matrix symmetries.

For citation: Balonin N. A., Seberry J., Sergeev M. B. Solvable and unsolvable problems. Using Procrustes analysis algorithm for obtaining a family of Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 1, pp. 2–16 (In Russian). doi:10.31799/1684-8853-2023-1-2-16, EDN: KOMNBV

Financial support
The article was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, agreement No. FSRF-2020-0004.

References

1. Matiyasevich Y. V. Tarski's algorithm. *Komp'yuternye instrumenty v obrazovanii*, 2008, no. 6, pp. 4–14 (In Russian).
2. Jennifer S., Yamada M. *Hadamard matrices: Constructions using number theory and linear algebra*. Wiley, 2020. 384 p.
3. Colbourn C. J., Dinitz J. H. *Handbook of Combinatorial Designs*. Second ed. Chapman and Hall/CRC, 2007. 967 p.
4. Silvester 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, no. 34, pp. 461–475.
5. Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
6. Balonin N. A., Sergeev A. M., Sinitshina O. I. Finite field and group algorithms for orthogonal sequence search. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 4, pp. 2–17 (In Russian). doi:10.31799/1684-8853-2021-4-2-17
7. Djocovic D. Z., Kotsireas I. S. *Periodic Golay Pairs of Length 72*. In: *Algebraic Design Theory and Hadamard Matrices*. C. J. Colbourn (ed). Springer, 2015. Pp. 83–92.
8. Ito N. On Hadamard groups IV. *Journal of Algebra*, 2000, no. 234, pp. 651–663.
9. Schmidt B. Williamson matrices and a conjecture of Ito's. *Designs, Codes and Cryptography*, 1999, no. 17, pp. 61–68.
10. Paley R. E. A. C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
11. Williamson J. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
12. Balonin N. A., Sergeev M. B. *Special'nye matricy: psevdoobratnye, ortogonal'nye, adamarovy i kritskie* [Special matrices: pseudo-return, orthogonal, Hadamardian and Cretan]. Saint-Petersburg, Politekhnika Publ., 2019. 196 p. (In Russian). doi:10.25960/7325-1155-0
13. Sergeev A. M., Kurtyanik D. V., Tarashkevichus C. A. Matrix portrait as the basis of discrete textile ornament. *Izvestiya vysshih uchebnyh zavedenij. Tekhnologiya legkoj promyshlennosti*, 2019, vol. 44, no. 2, pp. 102–107 (In Russian).
14. Balonin N. A., Sergeev M. B., Seberry J., Sinitshina O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9
15. Gauss J. K. *Trudy po teorii chisel* [Proceedings on number theory]. Moscow, AN SSSR Publ., 1959. 978 p. (In Russian).
16. Liouville J. Nouveaux théorémes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84 (In French).
17. Awyzio G., Seberry J. *On Good Matrices and Skew Hadamard Matrices*. In: *Algebraic Design Theory and Hadamard Matrices*: Springer Proceedings in Mathematics & Statistics. Ch. Colbourn (eds). Springer, Cham., 2015. Vol. 133. https://doi.org/10.1007/978-3-319-17729-8_2
18. Pursell L. and Trimble S. Y. Gram — Schmidt orthogonalization by Gauss elimination. *The American Mathematical Monthly*, 1991, vol. 98, no. 6, pp. 544–549.
19. Balonin N. A., Sergeev M. B. Initial approximation matrices in search for generalized weighted matrices of global or local maximum determinant. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 6, pp. 2–9 (In Russian). doi:10.15217/issn1684-8853.2015.6.2
20. Balonin N. A., Sergeev A. M. Odin and Shadow Cretan matrices accompanying primes and their powers. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 2–7 (In Russian). doi:10.31799/1684-8853-2022-1-2-7
21. Belevitch V. Theory of 2n-terminal networks with application to conference telephony. *Electrical Communication*, 1950, vol. 27, no. 3, pp. 231–244.
22. Sergeev A. M. Prime numbers and symmetries of quasi-orthogonal cyclic Mersenne matrices. *Tezisy dokladov I Mezhdunarodnogo foruma "Matematicheskie metody i modeli v vysokotekhnologichnom proizvodstve"* [Proc. of the I Int. Forum "Mathematical Methods and Models in High-Tech Production"], Saint-Petersburg, 2021, pp. 14–15 (In Russian).
23. Sergeev A. M. On one approach to calculation of quasi-orthogonal cyclic matrices with symmetries as basis of codes. *Telecommunications*, 2022, no. 9, pp. 28–33 (In Russian). doi:10.31044/1684-2588-2022-0-9-28-33
24. Van Loan C. The ubiquitous Kronecker product. *Journal of Computational and Applied Mathematics*, 2000, vol. 123, iss. 1-2, pp. 85–100. doi:10.1016/S0377-0427(00)00393-9