УДК 519.614
doi:10.31799/1684-8853-2018-6-2-13

Научные статьи
Articles

Как гипотезе Адамара помочь стать теоремой. Часть 1

***Н. А. Балонин[a]**, доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
***М. Б. Сергеев[a]**, доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277*
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

***Введение:** гипотеза Адамара о существовании специфических квадратных матриц сформулирована не Адамаром, а математиками начала прошлого века. В середине века проблема подверглась ревизии в работах Райзера с Бруком и Човлом, а также одним из основателей дискретной математики Холлом. Она относится к задачам пограничного смешанного типа, в ней присутствует и континуальная, и дискретная составляющие. Комбинаторный подход, используемый в рамках последней, за столетие исчерпал себя, в статье рассмотрена альтернатива, опирающаяся на обе образующие. **Цель:** рассмотреть причины, по которым гипотеза о существовании всех матриц Адамара на порядках $n = 4t$ считается недоказанной, и предложить возможные варианты ее доказательства. **Методы:** переход понижением порядка $n = 4t - 2$ к двухуровневым квазиортогональным матрицам с элементами 1 и $-b$, вопрос существования которых на всех указанных порядках не вызывает затруднений в силу возможной иррациональности их элементов, с последующим построением цепочки преобразований к матрицам порядков $n = 4t - 1$, $n = 4t$, $n = 4t + 1$. **Результаты:** доказано взаимно-однозначное соответствие точек Гаусса на сфероиде $x^2 + 2y^2 + z^2 = n$ с симметричными матрицами Адамара (построенными на основе массивов Балонина — Себерри), закрывающее известные в теории массивов Вильямсона пробелы неразрешимых порядков 140, 112 и т. п. Найдены и систематизированы таблицы решений, включающие так называемые «лучшие» трехблочные матрицы $\mathbf{L}(p, q)$, $p \geq q$ — количество несопряженных симметричных матриц рассматриваемого порядка, q — количество блочно-симметричных матриц, совпадающих с решениями Вильямсона. Предложен итерационный метод Прокруста, понижающий норму максимального элемента матрицы, для получения матриц Адамара поиском локального и глобального условных экстремумов детерминанта. **Практическая значимость:** полученные матрицы Адамара и квазиортогональные матрицы порядков $n = 4t - 2$, $n = 4t - 1$, $n = 4t + 1$ имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

***Ключевые слова** — ортогональные матрицы, матрицы Адамара, гипотеза Адамара, циклические матрицы, негациклические матрицы, бициклические матрицы, массив Вильямсона, массив Балонина — Себерри, алгоритм Прокруста.*

Цитирование: Балонин Н. А., Сергеев М. Б. Как гипотезе Адамара помочь стать теоремой. Ч. 1. *Информационно-управляющие системы*, 2018, № 6, с. 2–13. doi:10.31799/1684-8853-2018-6-2-13
Citation: Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 6, pp. 2–13 (In Russian). doi:10.31799/1684-8853-2018-6-2-13

Введение

Матрицы Адамара — квадратные матрицы $\mathbf{H}$ порядка n с элементами –1 и 1 такие, что выполняется

$$\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}, \tag{1}$$

где $\mathbf{I} = \mathrm{diag}(1,1,1...1)$ — единичная матрица.

Помимо тривиальных размеров 1 и 2 матрицы Адамара ищут на порядках, делимых на 4 [1–3]. Содержание так называемой гипотезы Адамара состоит в том, что такие матрицы есть на всех $4t$, где t — натуральное число. Попробуем разобраться, почему возникло сомнение в существовании матриц Адамара, и рассмотрим возможные пути, как это сомнение преодолеть.

Матрицы вида (1) принято называть квазиортогональными [4], имея в виду, что нормированием $\mathbf{H} = \mathbf{H}/\sqrt{n}$ их нетрудно свести к строго ортогональным матрицам $\mathbf{H}^{\mathrm{T}}\mathbf{H} = \mathbf{I}$. Их элементами в таком случае будут и иррациональные числа. Поэтому рациональными матрицы Адамара можно считать весьма условно в силу тождества значений их элементов, позволяющего упростить матрицу. В общем случае ортогональные матрицы имеют несколько значений элементов, называемых уровнями [5, 6]. Трехуровневыми, например, являются конференц-матрицы (С-матрицы) или их обобщения в форме взвешенных матриц [2, 5].

Матрицы Адамара могут быть разными по конструкции, в том числе симметричными. Вильямсон [7], выбирая форму блочного массива, взял его кососимметричным (здесь и далее — с точностью до диагонали), но с симметричными блоками, совместив в одной матрице два качества. Потом с интервалом примерно в десять лет выходят две работы [8, 9] пионеров компьютерных поисков матриц Адамара для первого раскрытого при помощи вычислительной машины порядка 92 (рис. 1).

Попытки сформулировать условия существования матриц Адамара на всех порядках, кратных 4, предпринимались до этих работ в середине прошлого века усилиями Брука, Райзера и Човлы [10, 11], сформулировавших теорему,

■ *Рис. 1.* Голомб, Баумерт и Холл с портретом матрицы порядка 92

■ *Fig. 1.* Golomb, Baumert and Hall with matrix portrait for order 92

комментируемую в монографии [12] Маршаллом Холлом (соавтором [8]).

В работе [9] первая блочная матрица берется кососимметричной, а остальные разворачиваются так, чтобы их симметрия (и отсутствие ее) не мешали матрице в целом быть кососимметричной. Это породило гипотезу Себерри [3, 9] о том, что матрицы Адамара не только существуют на каждом порядке, кратном 4, но они еще и все могут быть кососимметричны. Едва ли симметрия может претендовать на меньшую роль. Поэтому позднее внимание исследователей сосредотачивается на возможности существования матриц Адамара в симметричной форме с одним или несколькими циклическими блоками, расширяющей границу Райзера [13] с 4-го порядка для моноциклов до 32-го порядка для бициклов [14, 15] и далее на все порядки $4t$ при использовании не более трех блоков [16–19]. Два блока (а не три) достаточны для построения негациклической конструкции [20]. В работах [21, 22] рассматриваются трехуровневые взвешенные матрицы и последствия, к которым приводит несоответствие размера блока условию ортогональности. Структура матриц резко усложняется для размеров, не равных простым числам. На порядке 46 еще есть известные узоры, для порядков 66 и 86 решения не найдены.

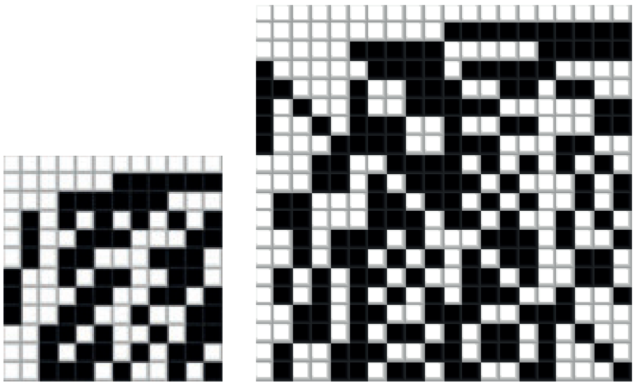
Предпосылки возникновения теории орнаментов

В отличие от теории чисел, с которой у рассматриваемой темы есть многочисленные пересечения, первые сведения о матрицах Дж. Сильвестр начал собирать около полутора столетий назад [23]. Он является автором наиболее известного алгоритма нахождения цепочки ортогональных по строкам и столбцам матриц $\mathbf{H}$, итерационно наращиваемых $\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$, где начальное $\mathbf{H} = 1$. Инверсия знака в правом нижнем блоке составной матрицы обеспечивает наличие в ней двух элементов: 1 и –1. В данном алгоритме рекурсия идет по порядку и зависит от начального выбора, поэтому найти матрицы всех возможных порядков при его помощи невозможно.

Сильвестра удивили орнаменты (узоры) цепочки матриц порядков 2^k и их свойство быть легко обращаемыми. В это время теория матриц только еще формировалась усилиями самого Сильвестра и Кэли. Было чему удивиться и написать подробнейший отчет с изображениями почти «морозных» ортогональных узоров. Далее пятьдесят лет ничего не происходило, что тоже обычно для задач, косвенно связанных с теорией чисел. Накануне нового столетия Адамар оживляет тему находкой матриц порядков 12 и 20, близких к сильвестровым [1], портреты которых приведены на рис. 2. Здесь и далее белая клетка соответствует значению элемента 1.

Адамар видит кратность порядков четырем и доказывает, что иных решений (кроме матриц порядков 1 и 2) не бывает. Он находит, что искомые матрицы достигают максимально возможного значения модуля детерминанта $n^{n/2}$.

Методов поиска матриц Адамар не предлагает, его собственный метод «проб и ошибок» несовершенен, орнаменты хаотичны. Правда, благодаря итерациям Сильвестра перечень достижимых вычислениями порядков заметно увеличился. Почти сразу вслед выходит статья специалиста по теории чисел Скарпи [24]. Он ищет ортогональные узоры иначе — вставками усеченных матриц



■ *Рис. 2.* Портреты матриц Адамара порядков 12 и 20

■ *Fig. 2.* Hadamard matrix portraits for orders 12 and 20 в самих себя с добавками каймы и циклическими сдвигами столбцов или строк. Хитроумный «замок Скарпи» по настоящее время находит как новые комментарии, так и продолжения [25–27].

Начиная со Скарпи, с предложенными им циклическими сдвигами, в расчеты матриц Адамара начинают проникать методы конечных полей.

Большой вклад в теорию вносит немецкий математик Эрнст Якобсталь, ученик Фробениуса и Шура, работавший в начале прошлого века над диссертацией по квадратичным вычетам. Далее Гилман [28] в начале тридцатых годов систематизирует матрицы порядков, отличающихся простыми значениями $n - 1$. Отсюда недалеко и до конструкций Пэли [29], учитывающих более сложный характер полей, когда $n - 1$ или $n/2$ — простые числа или их степени.

Если усеченный на единицу или вдвое размер матрицы представляет собой нечетное число, простое, то это ведет к нахождению матриц в виде особо простого орнамента, в частности циклического (с одной каймой) или бициклического. Метод Сильвестра тоже эксплуатирует особенности простых чисел, он базируется на степенях простого числа 2. Пэли подводит итог поискам, констатируя, что вставками Скарпи достигает вычисления матриц некоторых недосягаемых прочими методами порядков, связанных с составными числами.

Отсюда возникает представление, что матрицы Адамара порядков $n = 4t$ можно найти как пересечения семейств, каждое из которых содержит ограниченное или неограниченное число составляющих. Начинается поиск как отдельных матриц [8, 9], так и семейств матриц, выделяемых благодаря некоторому систематически применяемому приему по образцам, которые дали Сильвестр, Скарпи и Пэли.

Теорема Брука — Райзера — Човлы

Первые успехи в систематизации орнаментов матриц получены Райзером. Исследуя в шестидесятые годы прошлого века циклическую структуру [13], он замечает ее ограниченное порядком 4 применение (гипотеза Райзера). Впрочем, это простое наблюдение не имело бы такого резонанса, не продвинься Райзер с коллегами дальше.

Брук, Райзер и Човла [10, 11] оперируют привычными для циклических матриц параметрами их бинарных орнаментов — размером строки v, количеством отрицательных (или положительных) элементов в каждой строке и столбце k, а также количеством пар выбранных одинаковых элементов в каждых двух строках или столбцах матрицы λ. Понятно, что выбор набора параметров $\{v, k, \lambda\}$ не может быть произвольным, он стеснен общим количеством мест, которые предоставляет для узора квадратная матрица. Связывающее доступные значения параметров соотношение пришло из теории графов, поэтому его аббревиатура имеет невразумительное для матриц звучание — блочный дизайн. По смыслу — это диофантово уравнение реализуемого узора

$$k(k - 1) = \lambda(v - 1). \qquad (2)$$

Если равенство не выполняется, то узор реализовать нельзя, а если выполняется — можно. Заметим, узор в равной степени может описывать как целочисленные, так и иные бинарные матрицы — матрицы с двумя элементами. Поэтому их надо различать дополнительными условиями. Бинарные матрицы, удовлетворяющие условию (2), приводят к матричному уравнению связи, напоминающему условие ортогональности

$$\mathbf{A}^{\mathrm{T}}\mathbf{A} = (k - \lambda)\mathbf{I} + \lambda\mathbf{J}, \qquad (3)$$

где $\mathbf{J}$ — матрица из единиц; k описывает положительные, не равные нулю элементы. Определитель левой части $(k - \lambda)^{v-1}(k - \lambda + \lambda v) > 0$ [12] при нежестких ограничениях на параметры. Целочисленный корень этого матричного квадратичного уравнения с элементами 0 и 1 называется матрицей инцидентности.

Легко видеть, что в левой части (3) концентрируются суммы квадратов и взаимных произведений элементов искомой матрицы. Еще со времен исследований Эйлера и Лагранжа известно, что целое число раскладывается на сумму не менее четырех квадратов целых чисел. Иными словами, для квадратичных уравнений есть ограничения, когда они разрешимы. Углубленно этим занимались Хассе и Минковский, подробные комментарии приведены в обзоре Холла [12]. Между тем влиять на разрешимость уравнения (3) рациональными матрицами, к которым относится целочисленная матрица инцидентности $\mathbf{A}$, возможно только двумя целочисленными параметрами k и λ.

Теорема Брука — Райзера — Човлы [10–12] констатирует, что для матриц со строками четной длины v значение $(k - \lambda)$ должно быть квадратом некоторого числа. Для прочих матриц условие становится менее жестким и сводится к существованию наследующей у матричного аналога весовые коэффициенты квадратичной формы $z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ такой, чтобы ее можно было разрешить не только нулями. Райзер с коллегами и Холл приводят проблемные сочетания параметров проективного дизайна $v = q^2 + q + 1$, $k = q + 1$, $\lambda = 1$ при $q = 6$ и 14, в первом случае имеем $\{43, 7, 1\}$, а также пример меньшего порядка $\{29, 8, 2\}$.

Теорема Брука — Райзера — Човлы оперирует сугубо целочисленной матрицей инцидентности с элементами 0 и 1, описывающей не столько ортогональные матрицы (с их возможно вещественными элементами), сколько графы и другие сходные с ними дискретные конструкции, где не целые элементы исключены по смыслу самой задачи. Столбцы наращиваемой дополнительной каймой матрицы инцидентности можно сделать ортогональными путем изменения значений прежде нулевых элементов, ограничивая их отрезком от 0 до –1, получая в конечном итоге «рациональную» матрицу Адамара.

Это обстоятельство, получение одного из другого, стало играть роль краеугольного камня в вопросе о существовании матриц Адамара на всем диапазоне выделенных для них порядков, кратных 4. Так как условия теоремы видятся всего лишь необходимыми, но не достаточными для положительного заключения о существовании рациональных матриц инцидентности, то и на матрицы Адамара, с ними связанные, перешло сомнение [30].

Это сомнение разделяет, в том числе, автор обзора [12], который предпринял ревизию работ [10, 11]. В итоге Холл склоняется к мысли, что условия теоремы не только необходимы, но и достаточны, но не может этого обосновать, поскольку они описывают рациональные матрицы, а не матрицы с ограниченным набором элементов 0 и 1. Если условия достаточны, то гипотеза Адамара получает статус теоремы. Разумеется, опытные математики, в том числе Вильямсон [7] и Холл, наделенные немалой интуицией (об интуиции писал Адамар), давно видели пересечение строго доказанных в теории чисел теорем о разложениях чисел на квадраты с матричной тематикой.

Напрашивается естественный вывод, что разложение матриц на квадратные блоки — это всего лишь иллюстративный метод, позволяющий наглядно отразить содержание этих великих теорем о квадратах чисел.

Если матрицы низводятся до всего лишь иллюстраций доказанных разложений чисел на составляющие, то все необходимое для доказательства их существования на $4t$ есть. Отметим, что неразрешимые сочетания параметров квадратичного дизайна, для которых равенство (2) соблюдается, но (3) неразрешимо матрицей инцидентности, несущественны для ортогональных матриц. Даже если целочисленные матрицы инцидентности есть, они не обязательно ведут (ограниченным изменением их нулевых элементов) к вещественным ортогональным матрицам.

Например, для проективных планов $\{v, k, \lambda\}$, в которых были обнаружены критические неразрешимые точки, ортогонализация матрицы инцидентности вариациями нуля (ограниченными по норме единицей) вполне возможна, но она порождает матрицы с иррациональными элементами, к которым матрицы Адамара не относятся. Выходит, что и случаи, не вызывающие сомнения в разрешимости уравнения из теоремы Брука — Райзера — Човлы (3), не ведут к чему-либо приемлемому для построения целочисленных матриц с ортогональными столбцами.

Тем самым условия, столь тщательно исследуемые, к затронутой проблеме существования ортогональных конструкций имеют опосредованное отношение. Для полноценного исследования надо включать в сферу внимания матрицы с варьируемыми иррациональными элементами, а эта возможность не была использована.

Уравнения составных узоров

Наше дополнительное замечание состоит в том, что значениями квадратичной матричной формы стоит интересоваться не только для корней в виде матрицы инцидентности с ее 0 и 1, но и при экстремальных значениях параметров. Для ортогональных матриц диофантово уравнение реализуемости узора (2) — условие необходимое, но недостаточное в силу дополнительного уравнения связи $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$. Это условие можно выразить короче диофантовым уравнением ортогональности, задающим легко учитываемое ограничение на λ.

Лемма 3.1. Для квазиортогональных матриц с элементами –1 и 1, где k и λ ассоциированы с количеством отрицательных элементов, имеем

$$\lambda = k - n/4. \qquad (4)$$

Доказательство: Скалярное произведение пары любых не совпадающих между собой строк (и столбцов) ортогональной матрицы равно 0. Поскольку часть отрицательных элементов (–1) идут вместе попарно, сумма их взаимных произведений равна λ. В каждой из скалярно перемножаемых строк остается еще по $(k - \lambda)$ не нашедших пары отрицательных элементов, дающих вклад $-2(k - \lambda)$. Остаток состоит из суммы пар произведений положительных элементов, дающей $n - \lambda - 2(k - \lambda) = n - 2k + \lambda$. Все вместе $\lambda - 2(k - \lambda) + n - 2k + \lambda = 4\lambda - 4k + n = 0$ позволяет нам выразить значение целочисленного параметра ортогонального узора $\lambda = k - n/4$.

Лемма доказана.

Параметр k не может быть меньше четвертой части порядка, причем разность $k - \lambda = n/4$, что дает $n = 4(k - \lambda)$. Отсюда, кстати, видно, что для ортогональных матриц порядок должен делиться на четыре — необходимое условие, указанное Адамаром. Задачи, в которых $(k - \lambda)$ равно квадрату некоторого числа, приходятся на хорошо изученные четные порядки $n = 4u^2$, отвечающие цепочкам симметричных и (или) регулярных матриц Адамара.

Лемма 3.2. Диофантово уравнение реализуемого ортогонального узора имеет вид

$$x^2 = n, \tag{5}$$

где параметр $k = (v - x)/2$. Для одноблочных матриц, разумеется, длина строки блока $v = n$.

Доказательство: Подставив значение λ из леммы 3.1 в уравнение узора (2), имеем новое условие $k(k - 1) = (k - n/4)(n - 1)$, которое превращается в тождество тривиальной заменой переменных $k = (v - x)/2 = x(x - 1)/2$, $n = x^2$.

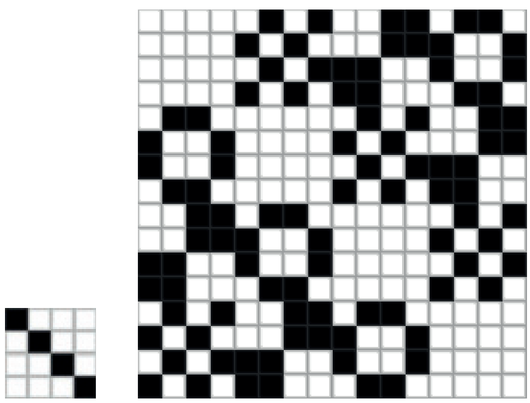
Лемма доказана.

Следствие 3.2.1. Регулярные матрицы Адамара, отличающиеся равными значениями сумм элементов строк и столбцов, порядков $n = 4u^2$ существуют. Условие (5) для них выполняется, к тому же выполняется первое условие теоремы Брука — Райзера — Човлы, так как $k - \lambda = n/4 = u^2$. Поэтому регулярные матрицы Адамара с параметрами дизайна Менона $\{v, k, \lambda\} = \{4u^2, u(2u - 1), u(u - 1)\}$ существуют.

Пример 3.2.1. Для порядка 4 регулярной является диагональная циклическая матрица с параметрами $k = 1$ и $\lambda = 0$. Согласно гипотезе Райзера [13], для следующего порядка 16 ресурсов циклического узора не хватает.

Разность $k - \lambda = n/4 = 4$ достигается при $k = 6$ и $\lambda = 2$, характерных для орнаментов в форме матриц Буша с их $n^{1/2} = 4$ клетками положительных элементов того же размера 4 на диагонали (рис. 3).

Переход к форме Буша усложнен концентрацией положительных элементов в ее крупных по размеру диагональных блоках, ввиду тривиальности которых узоры соседних блоков получаются довольно изощренными. В итоге орнамент промежуточной структуры порядка 196 не найден.



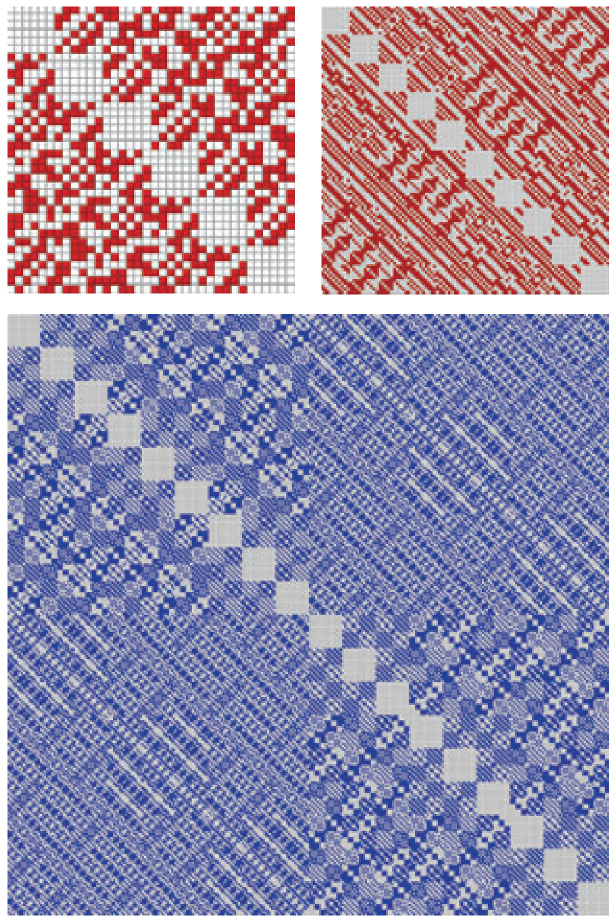
■ ***Рис. 3.*** Матрицы Райзера порядка 4 и Буша порядка 16

■ ***Fig. 3.*** Matrices of Ryser for order 4 and Bush for order 16

В качестве иллюстрации на рис. 4 представлены не приводившиеся ранее в виде орнаментов в литературе портреты матриц Буша порядков 36, 100 и 324 [31–33]. Второй орнамент найден первым автором данной статьи с помощью Владимира Тончева, одного из исследователей этих редких находок.

Для лучшей разрешимости узора в рассмотрение вводят два, три или четыре блока. Наиболее популярные блочные орнаменты матриц Адамара складываются в циклическую, бициклическую и т. п. конструкции, восходящие в своем содержании к более вариативному заполнению выделенных еще Сильвестром блоков $\mathbf{A}$, $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$, ... , здесь транспонирование «помогает» конструкции быть ортогональной. Условие ортогональности (1) для матрицы с парой блоков сводится к требованию ортогональности суммы $\mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B} = n\mathbf{I}$.

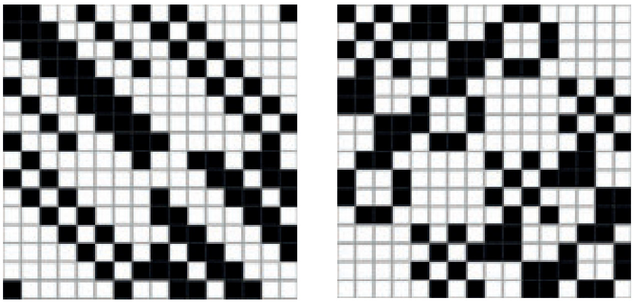
На рис. 5 приведена пара разных по своему характеру реализаций матриц с симметричными блоками $\mathbf{A}$, $\mathbf{B}$ размера 8×8 с параметрами $k_1 = 4$, $\lambda_1 = 2$ и $k_2 = 2$, $\lambda_2 = 0$. Первая матрица более про-



■ ***Рис. 4.*** Матрицы Буша порядков 36, 100, 324

■ ***Fig. 4.*** Bush matrices for orders 36, 100, 324

doi:10.31799/1684-8853-2018-6-6-fig4



■ ***Рис. 5.*** Орнаменты матриц Адамара порядков 16
■ ***Fig. 5.*** Hadamard matrix ornaments for order 16

ста, поскольку в качестве блоков взяты циклические матрицы.

Вторая матрица построена на основе отраженной относительно центральной вертикальной линии матрицы Буша порядка 16. Каждый блок **A**, **B** размера 8 × 8 состоит из трех разных по своему орнаменту субблоков. Так как это размер регулярной матрицы Адамара, структуру, напоминающую матрешку, порождает требуемый для реализации регулярной конструкции дизайн Менона с параметрами $k = k_1 + k_2 = 6$, $\lambda = \lambda_1 + \lambda_2 = 2$, $k - \lambda = n/4 = 4$. Таким образом, если циклическая структура недостаточно гибка, чтобы быть ортогональной на рассматриваемом порядке, узор усложняется. Важно вовремя остановиться в измельчении матрицы.

Диофантово уравнение реализуемого составного узора из нескольких блоков не претерпевает сколь-нибудь заметного изменения:

$$\Sigma k_i(k_i - 1) = \lambda(v - 1), \tag{6}$$

суммирование здесь и далее идет по всем индексам блоков, которых может быть 1, 2 и 4 (3 при равенстве двух блоков). Так как параметр $\lambda = \Sigma\lambda_i$ связан с условием ортогональности всей матрицы в целом, его можно не разделять на составляющие. Это общий коэффициент, условие ортогональности с ним не изменяется.

Лемма 3.3. Для ортогональных блочных матриц

$$\lambda = k - n/4, \tag{7}$$

где $k = \Sigma k_i$, k_i — параметры блоков, каждый из которых представляет собой количество элементов –1 строки блока; n — порядок матрицы.

Доказательство: При рассмотрении блочных конструкций, для которых выполняются тождество $\mathbf{A}^T\mathbf{A} + \mathbf{B}^T\mathbf{B} = n\mathbf{I}$ и сходные с ним для большего числа блоков, годятся все те же суждения, что и для леммы 3.1. Роль k выполняет суммарный коэффициент.

Разбиение всего массива на блоки фактически не сказывается на значениях суммарных параметров $k = \Sigma k_i$ и $\lambda = \Sigma\lambda_i$ первых v строк, где v — размер блока. Ортогональность остальных строк всей матрицы гарантируется блочной ортогональностью массива.

Лемма доказана.

Лемма 3.4. Диофантово уравнение реализуемого ортогонального узора имеет вид

$$\Sigma x_i^2 = n, \tag{8}$$

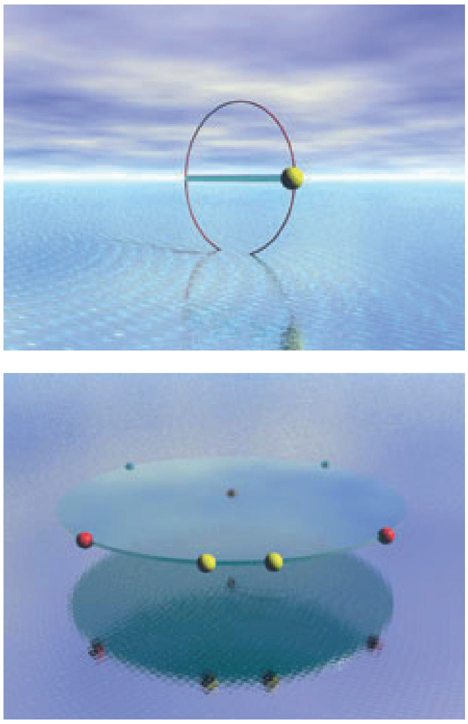
причем $k_i = (v - x_i)/2$. Для одноблочных матриц, разумеется, длина строки блока $v = n$.

Доказательство: Подставив значение λ из леммы 3.3 в уравнение узора, имеем новое условие $\Sigma k_i(k_i - 1) = (k - n/4)(n - 1)$, которое, как легко проверить, превращается в тождество заменой переменных $k_i = (v - x_i)/2$, $k = \Sigma k_i$.

Лемма доказана.

С увеличением числа блоков узора проблемы, описываемые теоремой Брука — Райзера — Човлы для одноблочного дизайна, отходят на второй план. На первое место выдвигаются теоремы Эйлера и Лагранжа. Гауссовы точки (рис. 6) — точки с целыми координатами на линии, удовлетворяющие условию $x^2 = n$, и на окружности $x^2 + y^2 = n$. При дальнейшем увеличении числа блоков они имеют продолжение в виде точек на сфере (или сфероиде).

Для первого примера циклический орнамент исчерпывается на порядке $x^2 = n = 4$. Целые точки на окружности $x^2 + y^2 = n$ помогают глубже понять логику орнаментов многоблочных матриц через бициклы.



■ ***Рис. 6.*** Точки Гаусса на линии и на окружности
■ ***Fig. 6.*** Gauss's points at line and circle

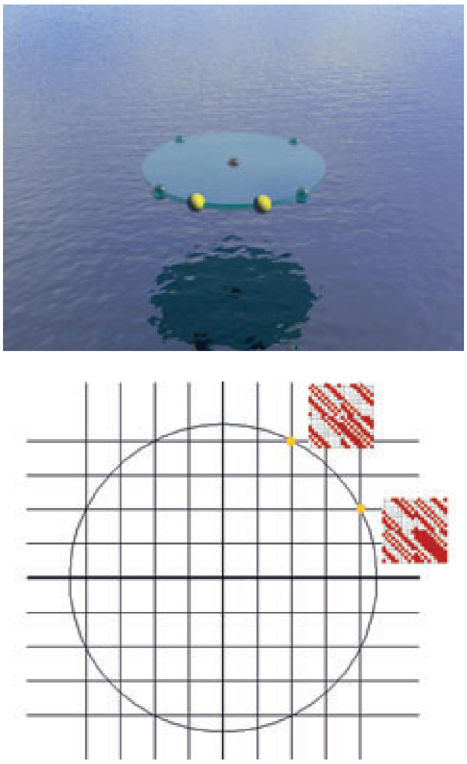
Теорема Эйлера. Любое число вида $4t + 1$ разлагается на сумму двух квадратов.

Это касается также составных чисел, в которых нечетные множители вида $4t + 3$ (или их нечетные степени) свидетельствуют о неразложимости числа на сумму двух квадратов. Содержимое теоремы, не раскрывая доказательства, Ферма описал математику Мерсенну. Кроме того, Ферма считал, что любое число последовательно представимо суммой трех треугольных чисел, четырех квадратов и т. п. Доказать последнее положение удалось Лагранжу.

Бициклический орнамент существует, соответственно, не всегда, а тогда, когда $n = 4p$ разложимо на сумму двух квадратов, т. е. когда значение p — простое число (или степень его) вида $p = 1 \bmod 4$. Точки идут парами, поскольку блоки бицикла всегда можно переставить местами. На рис. 6 пара красных точек соответствует регулярной бициклической матрице порядка 100. Если исключить из рассмотрения порядки регулярных матриц, то точек на окружности всего две. Например, для бициклической матрицы порядка 20 при $x = 2$, $y = 4$ матрицы $\mathbf{A}$ и $\mathbf{B}$ имеют параметры $k_1 = (v - x)/2 = 4$, $k_2 = (v - y)/2 = 3$, матрицы можно переставить местами.

Если $n = 4u^2$, $u = 3, 7, 11, \ldots = 3 \bmod 4$, то сумма квадратов существует, но влияние множителя $4t + 3$ даже в четной степени сказывается в том, что конструкция бициклической матрицы становится недостаточно гибка. Это порядки 36, 196, ... регулярных матриц, орнаменты которых должны существовать и в качестве моноблоков. Матрица Буша порядка 36 (см. рис. 5) дает представление о «заместителе» бициклической конструкции. Для удвоенного порядка 72 матрица разрешима блочным орнаментом, в блоках стоит сама регулярная структура. Если еще более увеличить размер, то добьемся разрешимости матрицы порядка 144 в бициклической конструкции — известное свойство матриц Адамара «вмещать» более простые конструкции по мере роста их размера: квадрат радиуса разрешимой окружности пришлось увеличить в 4 раза.

Таким образом, отсутствие бициклических матриц порядка 36 и наличие двух реализаций бицикла 100, среди которых один регулярный, неожиданно находит объяснение положением точек на окружности и характером радиуса этой окружности (см. рис. 6, 7).



■ ***Рис. 7.*** Точки Гаусса на окружности и бициклы

■ ***Fig. 7.*** Gauss's points at circle and two circulant matrices

Обращаясь к теореме Лагранжа о разложимости любого числа на сумму четырех квадратов, Вильямсон в сороковые годы предложил использовать четырехблочную конструкцию [7]. Он сэкономил на числе независимых элементов матрицы Адамара, взяв симметричные блоки (матрицы Вильямсона) $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, $\mathbf{D}$ вложенными в кососимметрическую конструкцию $\mathbf{W}$, называемую с тех пор массивом Вильямсона. Построенная на двух типах симметрий, облегченная форма позволила Голомбу, Баумерту и Холлу найти первую компьютерную матрицу порядка 92 [8]. На настоящий день массив идет в паре со своим обобщением $\mathbf{S}$, использованным [9] для поиска кососимметричной матрицы

$$\mathbf{W} = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & \mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & -\mathbf{B} & \mathbf{A} \end{pmatrix};$$

$$\mathbf{S} = \begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ -\mathbf{BR} & \mathbf{A} & -\mathbf{RD} & \mathbf{RC} \\ -\mathbf{CR} & \mathbf{RD} & \mathbf{A} & \mathbf{RB} \\ -\mathbf{DR} & -\mathbf{RC} & -\mathbf{RB} & \mathbf{A} \end{pmatrix}, \quad (9)$$

где $\mathbf{R}$ — обратная единичная матрица, т. е. матрица с единицами вдоль второй не главной диагонали квадрата. Если не обращать внимание на симметрию или кососимметрию блоков, то второй массив называют массивом Гетхальса — Зейделя.

Требование ортогональности матрицы в целом $\mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B} + \mathbf{C}^{\mathrm{T}}\mathbf{C} + \mathbf{D}^{\mathrm{T}}\mathbf{D} = n\mathbf{I}$ упрощается для симметричных блоков Вильямсона до вида $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$, $\mathbf{B}^{\mathrm{T}} = \mathbf{B}$, $\mathbf{C}^{\mathrm{T}} = \mathbf{C}$, $\mathbf{D}^{\mathrm{T}} = \mathbf{D}$. Леммы 3.3 и 3.4 для таких массивов применимы, число составляющих сумм возрастает до четырех. Ближе к завершению прошлого века Драгомир Джокович полным перебором доказал отсутствие матриц Адамара порядка 140, построенных на циклических матрицах Вильямсона [34]. Позднее было найдено еще несколько неразрешимых порядков [35]. Дженнифер Себерри, пожалуй, первой обратила внимание на то, что кососимметричная конструкция **S** наделена в мире орнаментов большим выживанием.

С тех пор она называется массивом Себерри или Себерри — Вайтмана. Далее будет показан путь к симметричной трехблочной конструкции, называемой *массивом Балонина — Себерри* [16]. Появилась она в работах по аппроксимации матриц Адамара, включая порядок 668, симметричными трехуровневыми матрицами, имеющими одинаковый узор всех четырех блоков. Задача легко разрешима, если центральный блок вместо –1 имеет варьируемый уровень $-b$, он поднимается к –1 при освобождении узоров пары крайних блоков **A**, **D**.

Двухуровневые матрицы с варьируемым элементом

Посмотрим, что будет, если в силу возможного нормирования максимального элемента матрицы сохранить его равным $a = 1$. Отрицательный элемент обозначим как $-b$, полагая, что b свободно варьируется в диапазоне от 0 до 1, проходя, в том числе, и иррациональные значения. На рис. 8 элемент с плавающим значением обозначен монотонной окраской.

Так как бинарность матрицы этим назначением сохраняется, диофантово уравнение реализуемого узора не меняется. Узор матриц из двух блоков $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$ порядка $n = 2v$ описывается, согласно (6), уравнением относительно параметров парного дизайна $k_1(k_1 - 1) + k_2(k_2 - 1) = \lambda(v - 1)$. Идея заключается в том, чтобы выбором λ свести его к уравнению окружности, заведомо касающейся точки с целыми координатами. Поскольку значения уровней не фиксированы жестко, имеется возможность выбора желаемой λ.

Лемма 4.1. Диофантово уравнение реализуемого ортогонального узора для двухблочной конструкции порядка $n = 2v = 4t - 2$ с длиной строки $v = 2t - 1$ выбором $\lambda = (v - 3)/2 = t - 2$ сводится к паре разрешимых уравнений, описывающих общую точку окружности и линии, представленную на рис. 9, выражается как

$$x^2 + y^2 = 2,\ x + y = 2 \tag{10}$$

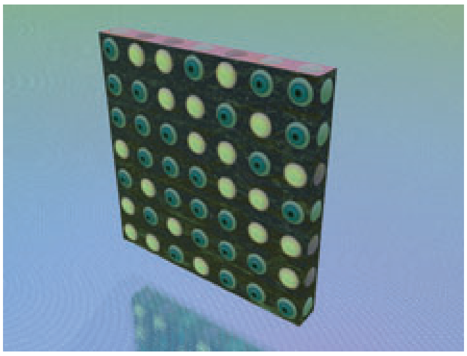
и получается после замены переменных $k_1 = t - x$, $k_2 = t - y$, приводящей для точки решения $x = 1$, $y = 1$ к равенству $k_1 = k_2 = t - 1 = (v - 1)/2$.

Доказательство заключается в подстановке указанных значений параметров $k_1 = k_2$, следующих из (10), при длине строки $v = n/2 = 2t - 1$ в уравнение ортогональности. Для случая $\mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B} = n\mathbf{I}$ имеем характеристическое уравнение $\lambda b^2 - 2(k - \lambda)ab + (n - 2k + \lambda)a^2 = 0$, $k = k_1 + k_2 = 2(t - 1)$. Оно сводится к всегда разрешимому относительно «плавающего» значения элемента b уравнению $(t - 2)b^2 - 2tb + t = 0$.

Доказательство закончено.

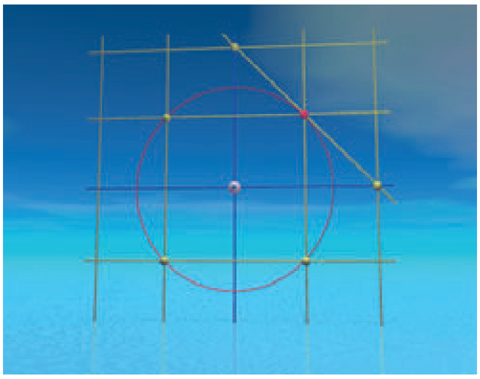
Достижимый дизайн $\{n = 2v;\ k_1, k_2;\ \lambda\} = \{n = 2v;\ (v - 1)/2,\ (v - 1)/2;\ (v - 3)/2\}$ назовем *эйлеровым*, поскольку разложениями чисел на сумму пары квадратов чисел занимался именно он. Попутно мы доказали важную теорему.

Теорема 3.1. Матрицы Эйлера, задаваемые *эйлеровым дизайном*, с уровнями $a = 1$ и $-b$, $b = \dfrac{t}{t + \sqrt{2t}}$, существуют для всех значений $n = 2v = 4t - 2$.



■ *Рис. 8.* Циклический моноблок с плавающим значением элемента

■ *Fig. 8.* Circulant monoblock with floating value of entry



■ *Рис. 9.* Общая точка окружности и линии

■ *Fig. 9.* Common point of circle and line

Доказательство сводится к нахождению положительного корня характеристического уравнения $(t-2)b^2 = 2tb + t = 0$. Так как мы не связаны с требованием рациональности элемента, нам нет необходимости заботиться о рациональном решении.

Доказательство закончено.

Теорема эта была высказана сначала в виде предположения относительно существования матриц Мерсенна на всех нечетных порядках $n = 4t-1$ [36–38] и матриц Эйлера на $4t-2$.

Ввиду инверсии знака блока в нижнем правом углу матрицы Эйлера $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$, это матрица с четырьмя элементами a, $-b$, $-a$, b. Добавим к ней составную кайму из строки и столбца, состоящих из 1, далее v отрицательных элементов и v положительных элементов, не обращая внимания на варьируемые элементы.

В таком случае значения параметров в каждой строке новой структуры порядка $n = 4t-1$ возрастут на 1, т. е. $k = k_1 + k_2 + 1 = 2(t-1)+1 = 2t-1$ и $\lambda = (t-2)+1 = t-1$. Эта операция превращает бициклическую конструкцию в моноблок с двумя элементами $a = 1$, $-b$ в каждой строке. Дизайн $\{n = 4t-1;\ k;\ \lambda\} = \{n = 4t-1;\ 2t-1;\ t-1\}$ назовем *мерсенновым* по причине вхождения чисел Мерсенна $M_p = 2^p - 1$ (с соответствующими решениями) в последовательность $n = 4t-1$. Этот дизайн комплементарен так называемому адамарову дизайну $\{4t-1;\ 2t;\ t\}$.

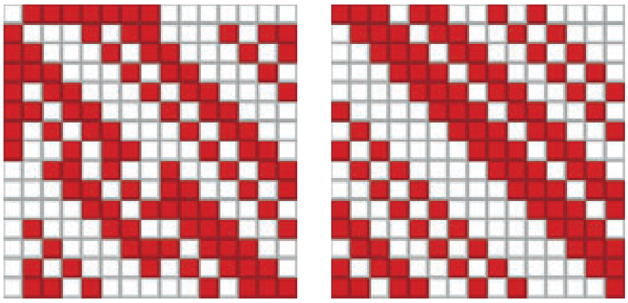
Теорема 4.2. Матрицы Мерсенна, задаваемые *мерсенновым дизайном* с уровнями $a = 1$ и $-b$, где $b = \dfrac{t}{t+\sqrt{t}}$, существуют для всех значений $n = 4t-1$.

Доказательство: Подстановкой параметров уравнение ортогональности моноцикла $\lambda b^2 - 2(k-\lambda)ab + (n-2k+\lambda)a^2 = 0$ сводится к $(t-1)b^2 - 2tb + t = 0$, разрешимому указанным выше значением b.

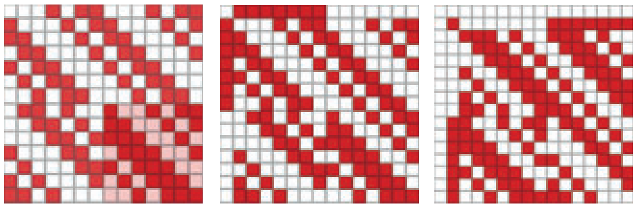
Доказательство закончено.

Более простой циклический орнамент матриц Мерсенна, представленный на рис. 10, существует только для порядков, равных числам Мерсенна 3, 7, 15, ..., простым числам или произведениям пар близких простых чисел, например, $15 = 3 \times 5$, $35 = 5 \times 7$, ... [38].

Квадратичные уравнения имеют два корня, описывающих значения элементов при превалировании и при дефиците отрицательных элементов матрицы. В качестве решения для значений элементов было выбрано то из них, которое обеспечивает большее значение детерминанта матрицы. Итак, мы доказали, что последовательно находимые друг из друга матрицы Эйлера и Мерсенна существуют. Матрицы эти почти неизвестны, они вещественные. Элементы не зажаты условием целочисленности — они «плавающие». И, казалось бы, в них мало удивительного.



■ *Рис. 10.* Два {15, 7, 3}-орнамента матриц Мерсенна
■ *Fig. 10.* Two {15, 7, 3}-ornaments of Mersenne matrix
doi:10.31799/1684-8853-2018-6-10-fig10



■ *Рис. 11.* Переход от бицикла Эйлера к моноблокам Мерсенна и Адамара
■ *Fig. 11.* Transition from a bicycle of Euler to monoblocks of Mersenne and Hadamard
doi:10.31799/1684-8853-2018-6-10-fig11

Следствие 4.2.1. Матрицы Адамара, задаваемые *мерсенновым дизайном* с уровнями $a = 1$ и $-b$, $b = 1$, существуют для всех значений $n = 4t$.

В самом деле, *мерсеннов дизайн* содержит всегда реализуемый ортогональный узор. Следуя предыдущей методике, добавим к нему монотонную кайму, состоящую из элементов $-b$.

Поскольку дизайн Мерсенна представляет собой моноблок, получим матрицу порядка $n = 4t$, у которой $k = 2t$ элементов и $\lambda = t$. Уравнение ортогональности $\lambda b^2 - 2(k-\lambda)ab + (n-2k+\lambda)a^2 = 0$ сводится к $b^2 - 2b + 1 = 0$, разрешимому значением $b = 1$. Заметим, что мы не навязываем целочисленное значение «плавающего уровня». Обычно кайму матриц Адамара нормализуют, чтобы она состояла из положительных элементов, цепочку преобразований узоров описывает рис. 11.

Проверим условия Брука — Райзера — Човлы, они сводятся к существованию решения уравнения $z^2 = tx^2 - (t-1)y^2$ в целых, не равных одновременно 0. Очевидно, что $z = 1$, $x = 1$, $y = 1$ есть решение, и, значит, с этой стороны нет ограничений на существование матрицы Адамара, что отметил Холл в работе [12].

Окончание следует.

Литература

1. **Hadamard J.** Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.
2. **Seberry J., Yamada M.** *Hadamard matrices, sequences, and block designs*. J. H. Dinitz and D. R. Stinson eds. John Wiley and Sons, Inc., 1992. P. 431–560.
3. *Handbook of combinatorial designs* (Discrete mathematics and its applications). Ed. by Charles J. Colbourn, Jeffrey H. Dinitz. 2nd ed. Chapman and Hall/CRC, 2006. 1000 p.
4. **Балонин Н. А., Сергеев М. Б.** Нормы обобщенных матриц Адамара. *Вестник СПбГУ*. Сер. 10, 2014, вып. 2, с. 5–11.
5. **Balonin N. A., and Seberry, Jennifer.** Remarks on extremal and maximum determinant matrices with real entries ≤1. *Информационно-управляющие системы*, 2014, № 5, с. 2–4.
6. **Балонин Н. А., Сергеев М. Б.** Матрица золотого сечения G10. *Информационно-управляющие системы*, 2013, № 6, с. 2–5.
7. **Williamson J.** Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
8. **Baumert L., Golomb S. W., Hall M.** Discovery of an Hadamard matrix of order 92. *JR. Communicated by F. Bohnenblust, California Institute of Technology*, Bull. Amer. Math. Soc., 1962, vol. 68, pp. 237–238.
9. **Seberry Wallis J.** A class of Hadamard matrices. Communicated by Marshall Hall. *Journal of Combinatorial Theory*, 1969, vol. 6, pp. 40–44.
10. **Bruck R. H., Ryser H. J.** The nonexistence of certain finite projective planes. *Canadian J. Math.*, 1949, vol. 1, pp. 88–93. doi:10.4153/cjm-1949-009-2
11. **Chowla S., Ryser H. J.** Combinatorial problems. *Canadian J. Math.*, 1950, vol. 2, pp. 93–99. doi:10.4153/cjm-1950-009-8
12. **Hall M.** *Combinatorial theory*. 2nd ed. New York, Wiley, 1998. 464 p.
13. **Ryser H. J.** *Combinatorial mathematics*. The carus mathematical monographs. The mathematical association of America, New York, JohnWiley and Sons, 1963, no. 14. 162 p.
14. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея. *Информационно-управляющие системы*, 2015, № 3, с. 2–16. doi:10.15217/issn1684-8853.2015.3.2
15. **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, с. 2–10. doi:10.15217/issnl684-8853.2017.1.2
16. **Balonin N. A., Seberry J.** Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
17. **Balonin N. A., Balonin Y. N., Đoković D. Ž., Karbovskiy D. A., Sergeev M. B.** Construction of symmetric Hadamard matrices. *Информационно-управляющие системы*, 2017, № 5, с. 2–11. doi:10.15217/issn1684-8853.2017.5.2 (16 Aug 2017: arXiv:1708.05098).
18. **Balonin N. A., Đoković D. Ž., Karbovskiy D. A.** Construction of symmetric Hadamard matrices of order $4v$ for $v = 47, 73, 113$. *Special Matrices*, 2018, vol. 6, pp. 11–22 (9 Oct 2017: arXiv:1710.03037).
19. **Balonin N. A., Đoković D. Ž.** Symmetric Hadamard matrices of orders 268, 412, 436 and 604. *Информационно-управляющие системы*, 2018, № 4, с. 2–8. doi:10.31799/1684-8853-2018-4-2-8 (23 Mar 2018: arXiv:1803.08787)
20. **Balonin N. A., Djocovic D. Z.** Negaperiodic Golay pairs and Hadamard matrices. *Информационно-управляющие системы*, 2015, № 5, с. 2–17. doi:10.15217/issn1684-8853.2015.5.2
21. **Балонин Н. А., Сергеев М. Б.** Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке. *Информационно-управляющие системы*, 2013, № 5, с. 97–98.
22. **Balonin N. A., Seberry J.** A review and new symmetric conference matrices. *Информационно-управляющие системы*, 2014, № 4, с. 2–7.
23. **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.
24. **Scarpis U.** Sui determinanti di valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, no. 31, pp. 1441–1446.
25. **Đoković D. Ž.** Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, no. 10, pp. 1985–1987. doi:10.1080/03081087.2016.1265062
26. **Балонин Н. А., Сергеев М. Б.** Матрицы Мерсенна и Адамара. *Информационно-управляющие системы*, 2016, № 1, с. 2–15. doi:10.15217/issn1684-8853.2016.1.2
27. **Балонин Н. А., Сергеев М. Б.** Матрицы Мерсенна и Адамара, произведения. *Информационно-управляющие системы*, 2016, № 5, с. 2–14. doi:10.15217/issn1684-8853.2016.5.2
28. **Gilman R. E.** On the Hadamard determinant theorem and orthogonal determinants. *Bulletin Amer. Math. Soc.*, 1931, vol. 37, pp. 30–31.
29. **Paley R. E. A. C.** On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
30. **Malcolm W. Browne**. *Is a math proof a proof if no one can check it*? The New York Times. 1 december. 1988.
31. **Janko Z.** The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs. *Journal of Combinatorial Theory*, 2001, ser. A, vol. 95, no. 2, pp. 360–364.

32. **Janko Z., Kharaghani H., Tonchev V. D.** Bush-type Hadamard matrices and symmetric symmetric designs. *J. Combin*., 2001, no. 1, pp. 72–78.
33. **Janko Z., Kharaghani H., Tonchev V. D.** The existence of a Bush-type Hadamard matrix of order 324 and two new infinite classes of symmetric designs. *Des. Codes Cryptogr*, 2001, vol. 24, no. 2, pp. 225–232.
34. **Đoković D. Ž.** Williamson matrices of order $4n$ for $n = 33;35;39$. *Discrete Math*., 1993, vol. 115, pp. 267–271.
35. **Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B.** Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, no. 46, pp. 343–352.
36. **Балонин Н. А.** О существовании матриц Мерсенна 11-го и 19-го порядков. *Информационно-управляющие системы*, 2013, № 2, с. 89–90.
37. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара. *Информационно-управляющие системы*, 2013, № 5, с. 2–8.
38. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта. *Информационно-управляющие системы*, 2014, № 1, с. 2–15.

UDC 519.614
doi:10.31799/1684-8853-2018-6-2-13

Helping Hadamard conjecture to become a theorem. Part 1

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
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

Introduction: Hadamard conjecture about the existence of specific square matrices was formulated not by Hadamard but by other mathematicians in the early 20th century. Later, this problem was revised by Ryser together with Bruck and Chowla, and also by Hall, one of the founders of discrete mathematics. This is a problem of the boundary mixed type, as it includes both the continuous and discrete components. The combinatorial approach used in the framework of the discrete component has run its course by the end of the century. The article discusses an alternative based on both concepts. **Purpose:** To analyze the reasons why the conjecture about the existence of Hadamard matrices of all orders $n = 4t$ is considered unproven, and to propose possible ways to prove it. **Methods:** Transition, by lowering the order $n = 4t - 2$, to two-level quasiorthogonal matrices with elements 1 and −b whose existence on all specified orders is not a difficult problem due to the possible irrationality of their entries. Subsequent construction of a chain of transformations to matrix orders $n = 4t - 1$, $n = 4t$, $n = 4t + 1$. **Results:** It is proved that Gauss points on an $x^2 + 2y^2 + z^2 = n$ spheroid are in one-to-one correspondence with symmetric Hadamard matrices (constructed on the basis of the Balonin — Seberry arrays), covering up the gaps on the unsolvable orders 140, 112, etc. known in Williamson's array theory. Solution tables are found and systematized, which include so-called «best» three-block matrices $\mathbf{L}(p, q)$, where $p \geq q$ is the number of non-conjugated symmetric matrices of the order in question, and q is the number of block-symmetric matrices which coincide with Williamson's solutions. The iterative Procrustes algorithm which reduces the norm of the maximum entry in a matrix is proposed for obtaining Hadamard matrices by searching for local and global conditional extremes of the determinant. **Practical relevance:** The obtained Hadamard matrices and quasi-orthogonal matrices of orders $n = 4t - 2$, $n = 4t - 1$, $n = 4t + 1$ are of immediate practical importance for the problems of noise-resistant coding, compression and masking of video information.

Keywords — orthogonal matrices, Hadamard matrices, Hadamard conjecture, circulant matrices, negacirculant matrices, two-circulant matrices, Williamson array, Balonin — Seberry array, Procrustes algorithms.

Citation: Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 6, pp. 2–13 (In Russian). doi:10.31799/1684-8853-2018-6-2-13

References

1. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
2. Seberry J., Yamada M. Hadamard matrices, sequences, and block designs. *Contemporary design theory: A collection of surveys*. J. H. Dinitz and D. R. Stinson eds. John Wiley and Sons, Inc., 1992. P. 431–560.
3. *Handbook of combinatorial designs* (Discrete mathematics and its applications). Ed. by Charles J. Colbourn, Jeffrey H. Dinitz. 2nd ed. Chapman and Hall/CRC, 2006. 1000 p.
4. Balonin N. A., Sergeev M. B. The generalized Hadamard matrix norms. *Vestnik SPbGU*, ser. 10, 2014, vol. 2, pp. 5–11 (In Russian).
5. Balonin N. A., Seberry Jennifer. Remarks on extremal and maximum determinant matrices with real entries ≤1. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2014, no. 5, pp. 2–4.
6. Balonin N. A., Sergeev M. B. Matrix of golden ratio G10. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2013, no. 6, pp. 2–5 (In Russian).
7. Williamson J. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J*., 1944, vol. 11, pp. 65–81.
8. Baumert L., Golomb S. W., Hall M. Discovery of an Hadamard matrix of order 92. *JR. Communicated by F. Bohnenblust*, California Institute of Technology, Bull. Amer. Math. Soc., 1962, vol. 68, pp. 237–238.
9. Seberry Wallis J. A class of Hadamard matrices. Communicated by Marshall Hall. *Journal of Combinatorial Theory*, 1969, vol. 6, pp. 40–44.
10. Bruck R. H., Ryser H. J. The nonexistence of certain finite projective planes. *Canadian J. Math*., 1949, vol. 1, pp. 88–93. doi:10.4153/cjm-1949-009-2
11. Chowla S., Ryser H. J. Combinatorial problems. *Canadian J. Math*., 1950, vol. 2, pp. 93–99. doi:10.4153/cjm-1950-009-8
12. Hall M. *Combinatorial theory*. 2nd ed. New York, Wiley, 1998. 464 p.
13. Ryser H. J. *Combinatorial mathematics*. The carus mathematical monographs. The mathematical association of America, New York, John Wiley and Sons, 1963, no. 14. 162 p.

14. Balonin N. A., Đoković D. Ž. Symmetry of two-circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
15. 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 System], 2017, no. 1, pp. 2–10 (In Russian). doi:10.15217/issnl684-8853.2017.1.2
16. Balonin N. A., Seberry J. Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
17. Balonin N. A., Balonin Y. N., Đoković D. Ž., Karbovskiy D. A., Sergeev M. B. Construction of symmetric Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2017, no. 5, pp. 2–11. doi:10.15217/issn1684-8853.2017.5.2 (16 Aug 2017: arXiv:1708.05098).
18. Balonin N. A., Đoković D. Ž., Karbovskiy D. A. Construction of symmetric Hadamard matrices of order $4v$ for v=47, 73, 113. *Special Matrices*, 2018, vol. 6, pp. 11–22 (9 Oct 2017: arXiv:1710.03037).
19. Balonin N. A., Đoković D. Ž. Symmetric Hadamard matrices of orders 268, 412, 436 and 604. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2018, no. 4, pp. 2–8. doi:10.31799/1684-8853-2018-4-2-8 (23 Mar 2018: arXiv:1803.08787).
20. Balonin N. A., Đoković D. Ž. Negaperiodic Golay pairs and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2015, no. 5, pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2
21. Balonin N. A., Sergeev M. B. Weighted conference matrix generalizing Belevich matrix at the 22nd order. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2013, no. 5, pp. 97–98 (In Russian).
22. Balonin N. A., Seberry J. A review and new symmetric conference matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2014, no. 4, pp. 2–7.
23. 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.
24. Scarpis U. Sui determinanti di valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, no. 31, pp. 1441–1446 (In Italian).
25. Đoković D. Ž. Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, no. 10, pp. 1985–1987. doi:10.1080/03081087.2016.1265062
26. Balonin N. A., Sergeev M. B. Mersenne and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2016, no. 1, pp. 2–15 (In Russian). doi:10.15217/issn1684-8853.2016.1.2
27. Balonin N. A., Sergeev M. B. Mersenne and Hadamard matrices, products. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2016, no. 5, pp. 2–14 (In Russian). doi:10.15217/issn1684-8853.2016.5.2
28. Gilman R. E. On the Hadamard determinant theorem and orthogonal determinants. *Bulletin Amer. Math. Soc.*, 1931, vol. 37, pp. 30–31.
29. Paley R. E. A. C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
30. Malcolm W. Browne. *Is a math proof a proof if no one can check it*? The New York Times. 1 december. 1988.
31. Janko Z. The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs. *Journal of Combinatorial Theory*, 2001, ser. A, vol. 95, no. 2, pp. 360–364.
32. Janko Z., Kharaghani H., Tonchev V. D. Bush-type Hadamard matrices and symmetric symmetric designs. *J. Combin.*, Dec. 9, 2001, no. 1, pp. 72–78.
33. Janko Z., Kharaghani H., Tonchev V. D. The existence of a Bush-type Hadamard matrix of order 324 and two new infinite classes of symmetric designs. *Des. Codes Cryptogr*, 2001, vol. 24, no. 2, pp. 225–232.
34. Đoković D. Ž. Williamson matrices of order $4n$ for n=33;35;39. *Discrete Math.*, 1993, vol. 115, pp. 267–271.
35. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, no. 46, pp. 343–352.
36. Balonin N. A. Existence of Mersenne matrices of 11th and 19th orders. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2013, no. 2, pp. 89–90 (In Russian).
37. Balonin N. A., Sergeev M. B. On the issue of existence of Hadamard and Mersenne matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2013, no. 5, pp. 2–8 (In Russian).
38. Balonin N. A., Sergeev M. B. Local maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control System], 2014, no. 1, pp. 2–15 (In Russian).