УДК 519.614
doi:10.31799/1684-8853-2022-3-2-8

Научные статьи
Articles

Матрицы Адамара как результат произведения Скарпи без циклического смещения блоков

Н. А. Балонин[a]*, доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
А. М. Сергеев[a]*, канд. техн. наук, доцент, orcid.org/0000-0002-4788-9869*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *ортогональные матрицы Адамара, состоящие из элементов 1 и –1 (вещественное число), существуют для порядков, кратных 4. Рассматривается произведение ортогональной матрицы Адамара на ее основу (core), получившее название произведения Скарпи и близкое по смыслу к произведению Кронекера.* ***Цель:*** *выявлением симметрий блочных матриц Адамара показать, что соблюдение их способствует произведению, обобщающему метод Скарпи на случай отсутствия конечного поля.* ***Результаты:*** *показано, что ортогональность является инвариантом рассматриваемого произведения при соблюдении двух условий: один из сомножителей вставляется в другой с учетом знака элементов второго сомножителя (произведение Кронекера), но с выборочным действием знака на элементы и, главное, с циклическим смещением основы, зависящим от места вставки. Выявлено, что таких смещений можно избежать совсем при использовании симметрий, характерных для универсальных форм матриц Адамара. Кроме того, такой прием является общим для многих разновидностей корректируемых произведений Кронекера.* ***Практическая значимость:*** *ортогональные последовательности и методы их эффективного нахождения теорией конечных полей и групп имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

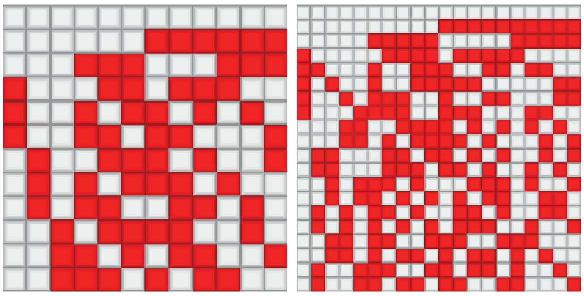
Ключевые слова *— матрицы Адамара, матрицы Мерсенна, произведение Скарпи, кососимметрические матрицы, симметрии матриц.*

Для цитирования: Балонин Н. А., Сергеев А. М. Матрицы Адамара как результат произведения Скарпи без циклического смещения блоков. *Информационно-управляющие системы*, 2022, № 3, с. 2–8. doi:10.31799/1684-8853-2022-3-2-8
For citation: Balonin N. A., Sergeev A. M. Hadamard matrices as a result of Scarpis product without cyclic shifts. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 2–8 (In Russian).

Введение

Матрицы Адамара — это матрицы порядка $n = 4t$ (помимо стартового порядка 2) с элементами 1 и –1, ортогональные в смысле $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, где $\mathbf{I}$ — единичная матрица [1, 2]. Почти сразу вслед за вычислением Адамаром двух матриц порядков 12 и 20, отличающихся от степеней двойки, возник вопрос об их симметрировании как более экономной форме представления.

На портретах матриц Адамара (рис. 1) красное поле соответствует элементу со значением –1, а белое — единице.



■ ***Рис. 1.*** Портреты матриц Адамара порядков 12 и 20
■ ***Fig. 1.*** Hadamard matrix portraits of orders 12 and 20

Как известно, «кронекерово умножение двух матриц $\mathbf{A}$ и $\mathbf{B}$ с элементами 1 и –1 реализуется вставкой матрицы $\mathbf{B}$ по месту элементов матрицы $\mathbf{A}$ с наследованием знака замещаемого элемента» [3] в следующем виде:

$$\mathbf{A}\otimes\mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \ldots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \ldots & a_{nn}\mathbf{B} \end{pmatrix}.$$

Результатом умножения, например, двух матриц Адамара порядков n и m будет матрица Адамара порядка nm. Именно произведение Кронекера первооснователями направления исследований Сильвестром и Адамаром использовалось для вычисления ортогональных матриц увеличенных порядков.

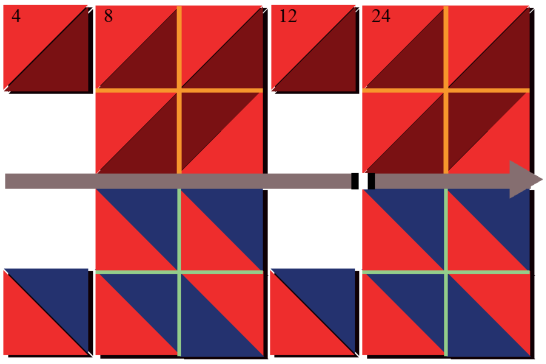
В мире таблиц, которыми являются матрицы Адамара, существуют два ярко выраженных симметричных начала: матрицы симметричные и кососимметричные (здесь и далее — с точностью до диагонали). Разновидность правила Сильвестра

$$\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix} \text{ и } \begin{pmatrix} \mathbf{H} & \mathbf{H} \\ -\mathbf{H}^{\mathrm{T}} & \mathbf{H}^{\mathrm{T}} \end{pmatrix}$$

позволяет распространить тип симметрии на удвоенные порядки (рис. 2), так что достаточно рассмотреть порядки $n = 4 + 8t = 4, 12, 20, \ldots$, идущие с шагом 8, при котором четверть n — нечетное число.

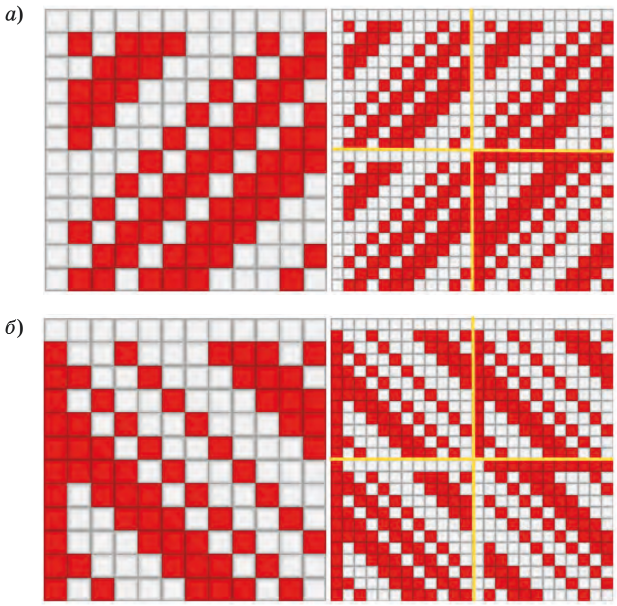
Далеко не сразу было осознано [4], что оба этих типа сосуществуют вдоль всей оси допустимых порядков одновременно. Для наглядности наших рассуждений на рис. 3, *а* и *б* матрицы приведены рядом с удвоенными основами.

Так получилось, что универсальные орнаменты, в которых можно найти матрицу Адамара независимо от ее порядка, были исследованы позднее. Наиболее простая форма — двоякосимметричная — содержит переставляемые местами



■ ***Рис. 2.*** Распространение обеих симметрий удвоением порядка

■ ***Fig. 2.*** Extending both symmetries by doubling the order



■ ***Рис. 3.*** Симметричные (*а*) и кососимметричные (*б*) матрицы Адамара

■ ***Fig. 3.*** Symmetric (*а*) and skew (*б*) Hadamard matrices

симметричный и кососимметричный блоки (матрицы) и парную кайму, тоже перестраиваемую. Эту форму легко найти при помощи полей Галуа [5, 6] на случай, если $n - 1$ представляет собой простое число или его степень. В некотором смысле она сопровождает простые числа и порождает легко находимые универсальные матрицы, отвечающие им.

Целью настоящей работы является представление новой реализации произведения Скарпи без смещений как основы упрощенного вычисления матриц Адамара.

Блочные конструкции матриц Адамара

Отсутствие поля делает невозможным совмещение обеих симметрий, но для симметрирования матрицы в целом это не обязательно. Косвенное свидетельство этому разработано в теории групп Ито, согласно которой есть взаимно однозначное соответствие между матрицами Адамара и дициклическими группами [6, 7]. Для нахождения симметричной или кососимметричной матрицы в универсальной форме без каймы число ее блоков — матриц порядка $v = n/4$ — увеличивается до четырех: **A**, **B**, **C**, **D**. Для матриц порядков, идущих с шагом 8: $n = 4 + 8t = 4(2t + 1)$, размер блока $v = 2t + 1$ — нечетное число.

Условие ортогональности дает квадратичное уравнение связи $w^2 + x^2 + y^2 + z^2 = n$, регламентирующее число −1 в них: $k_1 = (v - w)/2$, $k_2 = (v - x)/2$, $k_3 = (v - y)/2$, $k_4 = (v - z)/2$ [8].

Для кососимметричного (более простого) варианта матрицы $\mathbf{A} - \mathbf{I} = (\mathbf{I} - \mathbf{A})^{\mathrm{T}}$ параметр $w = 1$ зажат этим видом симметрии, так что $k_1 = (v - 1)/2$, что сводит уравнение орнамента к уравнению сферы $x^2 + y^2 + z^2 = n - 1$. Для симметричного варианта решения $\mathbf{A} = \mathbf{A}^{\mathrm{T}}$ и $\mathbf{B} = \mathbf{C}$ (менее жестко $k_2 = k_3$, но это редко востребуемо) поменяв местами обозначения w и x, связав свободную переменную x с первой матрицей, имеем $w = y$, что сразу же дает уравнение сфероида $x^2 + 2y^2 + z^2 = n$.

В теории чисел (не матриц) разрешимостью в целых числах уравнений сферы и сфероида занимались еще Гаусс и Лиувилль. Замена $x^2 = 8\mathrm{T}_x + 1$, $y^2 = 8\mathrm{T}_y + 1$, $z^2 = 8\mathrm{T}_z + 1$ упрощает уравнения связи до линейного вида: $\mathrm{T}_x + \mathrm{T}_y + \mathrm{T}_z = t$ и $\mathrm{T}_x + 2\mathrm{T}_y + \mathrm{T}_z = t$, где t — натуральное целое, задающее номер матрицы в серии интересующих нас порядков, идущих с шагом 8. Согласно теореме Гаусса [9], любое целое число t, заданное в виде суммы, всегда разрешимо не более чем тремя треугольными числами — числами, взятыми из последовательности сумм натуральных чисел 0, 1, 3, 6, 10 и т. п. (аддитивный факториал). Лиувилль распространил это правило на второе линейное уравнение, близкое по смыслу [10].

Тем самым матрицы Адамара с их целочисленными элементами 1 и –1 представляют собой матричную иллюстрацию теорем теории чисел Гаусса и Лиувилля. Это строго доказанные факты, дающие четкие гарантии существования не только всех матриц Адамара, как это предположил Пэли [11], но и, что сильнее, всех матриц Адамара в симметричной и кососимметричной форме. Некоторая нерешительность Пэли объясняется тем, что он разбирал частный случай симметрий, зависящих от конечных полей. Но ведь поля существуют не всегда.

Историческое недоразумение состоит в том, что во второй половине XX столетия компьютеры были еще слабы, и восполнять недостатки матриц, которые не могли быть вычислены аппаратом конечных полей Пэли, решили, симметрируя не матрицы Адамара, а их блоки **A**, **B**, **C** и **D**. Эти блоки назвали именем автора этой идеи — матрицами Вильямсона [12]. Его подход представляет собой матричную иллюстрацию к другой хорошо известной теореме Лагранжа о разложимости любого целого числа на сумму не более чем четыре целых чисел.

Это направление мысли обязывает пользоваться четырьмя не симметричными, в общем, блоками в составе не симметричного массива Гетхальса — Зейделя, что уводит в сторону от наиболее простых и интересных нам форм. Основной недостаток внедрения симметричных блоков состоит в том, что пропуски порядков вследствие чрезмерной жесткости произвольно выбранного условия обнаруживаются опытным путем. Теории несовместимости с этим типом симметрии нет.

Недостаток подхода Вильямсона стал очевиден не сразу, но к концу XX века профессор Др. Джокович обнаружил первую не закрытую этим подходом матрицу порядка 140 [13], а специальное исследование уже начала XXI века [14] отметило довольно часто идущие пропуски порядков.

Кососимметричный вариант **G** матриц Адамара впервые возник в работе Дж. Себерри [15], сохранив, в силу инерции мысли, ненужную в этом подходе симметрию блоков **B**, **C** и **D**. Проблема хороших матриц **G** (Good matrices) [16] с симметричными вставками аналогична проблемам использования матриц Вильямсона.

Размер блока 35 благополучно преодолевается, но уже на порядке 100 (размер блока 25) на сфере обнаруживается точка Гаусса, не обслуживаемая такой симметрией. Проблема несовместимости лишь откладывается до матрицы порядка 188, где обнаружено решение с несимметричными свободными блоками.

Симметричная конструкция **P**, называемая массив Балонина и Себерри [17], а для краткости — Пропус, с $\mathbf{A} = \mathbf{A}^\mathrm{T}$ и $\mathbf{B} = \mathbf{C}$ возникла как альтернатива довольно долго державшейся моде на кососимметричные массивы, породив ряд симметричных матриц на прежде не раскрытых порядках [18–21]. В этих работах и близких к ним блок **R** встречается записанным по другую сторону от циклической матрицы (тогда первая строка реверсируется и циклически смещается на позицию, чтобы сохранить ортогональность массива в целом):

$$\mathbf{G} = \begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ -\mathbf{BR} & \mathbf{A} & \mathbf{RD} & -\mathbf{RC} \\ -\mathbf{CR} & -\mathbf{RD} & \mathbf{A} & \mathbf{RB} \\ -\mathbf{DR} & \mathbf{RC} & -\mathbf{RB} & \mathbf{A} \end{pmatrix};$$

$$\mathbf{P} = \begin{pmatrix} \mathbf{A} & \mathbf{BR} = \mathbf{CR} & \mathbf{CR} = \mathbf{BR} & \mathbf{DR} \\ \mathbf{CR} & \mathbf{RD} & -\mathbf{A} & -\mathbf{RB} \\ \mathbf{BR} & -\mathbf{A} & -\mathbf{RD} & \mathbf{RC} \\ \mathbf{DR} & -\mathbf{RC} & \mathbf{RB} & -\mathbf{A} \end{pmatrix},$$

где **R** — обратная единичная матрица, т. е. матрица с единицами вдоль второй, не главной, диагонали квадрата. Массив Гетхальса — Зейделя не пользуется упрощением вида $\mathbf{B}^\mathrm{T}\mathbf{R} = \mathbf{RB}$, характерным для циклических блоков.

В совокупности с теоремами Гаусса и Лиувилля образуется значительно более емкая и компактная теория симметричных и кососимметричных матриц Адамара, тесно опирающаяся на полный сет теорем теории чисел. На настоящий момент обе эти конструкции как факт общественного сознания состоялись. Немаловажно подчеркнуть, что тот же вид симметрии присущ основам (core) этих матриц, т. е. блокам, получаемым отсечением первой строки и первого столбца нормализованной матрицы Адамара (когда они состоят только из 1).

Итак, мы выяснили, что матрицы Адамара бывают двоякосимметричными, сопровождая собой простые числа $n - 1$ (или степени простых чисел) [5], или симметричного типа, и тогда они существуют на всем диапазоне порядков $4t$ в виде симметричных или кососимметричных конструкций.

Состав операций с матрицами существенно отличается в сторону простоты реализации, если матрица симметрирована. Очевидно, что если матрица не приведена к некоторой простой симметричной форме, то ее придется к ней приводить, используя аппарат конечных полей. При этом создается иллюзия, что аппарат этот в корне необходим.

Новый метод Скарпи

Так и произошло с методом [22], который возник едва ли не вместе с аппаратом матриц Адамара. Его автор У. Скарпи обнаружил, что, помимо произведения Кронекера, когда одна матрица Адамара вставляется в другую с множителем, равным заменяемому элементу матрицы, матрицу **H** можно вставлять в ее основу **M** размера $p = n - 1$. Описание на итальянском языке практически невозможно встретить в научной литературе, а те, кто встретят его, потеряют время на изучение ненужных подробностей. Приведем его в нашей заметно более короткой редакции, структурно похожей на витражи в работе [23]:

$$\mathbf{M}\times\mathbf{H}=\begin{pmatrix} \begin{pmatrix}1 & m_{11}\mathbf{e}^{\mathrm{T}}\\ m_{11}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}1 & m_{12}\mathbf{e}^{\mathrm{T}}\\ m_{12}\mathbf{e} & \mathbf{M}\end{pmatrix} & \cdots & \begin{pmatrix}1 & m_{1(n-1)}\mathbf{e}^{\mathrm{T}}\\ m_{1(n-1)}\mathbf{e} & \mathbf{M}\end{pmatrix}\\ \begin{pmatrix}1 & m_{21}\mathbf{e}^{\mathrm{T}}\\ m_{21}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}1 & m_{22}\mathbf{e}^{\mathrm{T}}\\ m_{22}\mathbf{e} & \mathbf{TM}\end{pmatrix} & \cdots & \begin{pmatrix}1 & m_{2(n-1)}\mathbf{e}^{\mathrm{T}}\\ m_{2(n-1)}\mathbf{e} & \mathbf{T}^{n-2}\mathbf{M}\end{pmatrix}\\ \cdots & \cdots & \ddots & \cdots\\ \begin{pmatrix}1 & m_{(n-1)1}\mathbf{e}^{\mathrm{T}}\\ m_{(n-1)1}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}1 & m_{(n-1)2}\mathbf{e}^{\mathrm{T}}\\ m_{(n-1)2}\mathbf{e} & \mathbf{T}^{n-2}\mathbf{M}\end{pmatrix} & \cdots & \begin{pmatrix}1 & m_{(n-1)(n-1)}\mathbf{e}^{\mathrm{T}}\\ m_{(n-1)(n-1)}\mathbf{e} & \mathbf{T}^{(n-2)(n-2)}\mathbf{M}\end{pmatrix} \end{pmatrix},$$

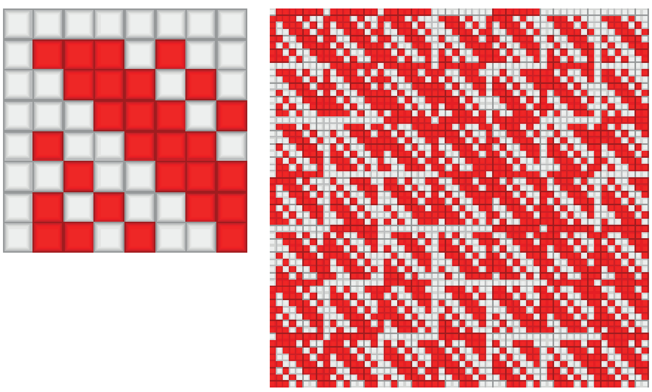
где $\mathbf{H}=\begin{pmatrix}1 & \mathbf{e}^{\mathrm{T}}\\ \mathbf{e} & \mathbf{M}\end{pmatrix}$ является нормальной формой матрицы Адамара; **M** — ее основой, элементы которой используются для модификации знака каймы; **e** — вектор единичных элементов каймы; **T** — матрица циклического смещения.

Пользуясь своим предложением, Скарпи нашел новую матрицу Адамара порядка 56 (7×8), не достижимую кронекеровым произведением адамаровых матриц. На рис. 4 в качестве примера приведено решение с матрицей Адамара указанного порядка.

По правилам кронекерова произведения на месте элемента матрицы **M** стоит модифицируемая знаком этого элемента матрица **H**. У Скарпи модификации подвергается только вектор каймы **e**. Этот алгоритм неработоспособен на случай сложных полей $GF(q)$, $q = p^m$, исключительно ввиду краткой формы его записи.

Недостаток, впрочем, легко поправить [24]. Согласно оригинальному алгоритму k-я строка (или столбец) матрицы **M** меняет номер k на величину $k + i \times j$ по mod q. Это общее место теории сложных полей: алгебраические операции ведутся не над тремя числами, а над элементами поля, номера которых эти числа задают. Номер итогового элемента поля служит указанием, куда именно строку (или столбец) перенести.

Теперь обратим особое внимание на то, что алгоритм Скарпи становится работоспособен с *любой* матрицей. Такая производительность излишняя, она не нужна при работе с заранее отсортированной кососимметричной матрицей **H**. Метод полей Галуа, по сути, здесь навязывается, он не нужен для реализации умножения. Оказывается, и в этом состоит смысл нашего нового предложения, секрет более быстрого и более универсального алгоритма заключается в *перестановке сомножителей* с модификацией теперь уже не каймы, а диагонали:



■ ***Рис. 4.*** Портреты матриц Адамара и произведения Скарпи

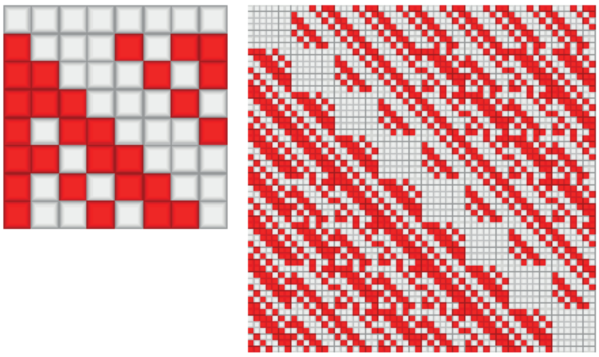
■ ***Fig. 4.*** Hadamard matrix and Scarpis product portraits

$$\mathbf{H}\times\mathbf{M}=\begin{pmatrix}\mathbf{J} & h_{12}\mathbf{M} & \dots & h_{1n}\mathbf{M}\\ h_{21}\mathbf{M} & \mathbf{J} & \dots & h_{2n}\mathbf{M}\\ \dots & \dots & \ddots & \dots\\ h_{n1}\mathbf{M} & h_{n2}\mathbf{M} & \dots & \mathbf{J}\end{pmatrix},$$

где $\mathbf{J}$ — матрица из единиц (рис. 5).

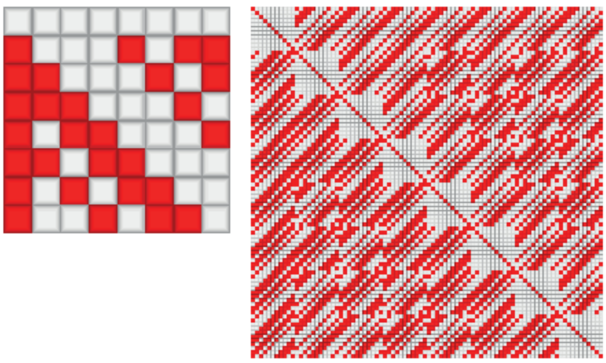
Размер вставляемой в кососимметричную матрицу $\mathbf{H}$ матрицы $\mathbf{M}$ не принципиален. Важно лишь, чтобы взаимная разница в размерах не превосходила 4. Если порядок $\mathbf{M}$ больше $\mathbf{H}$ на 3, блок коррекции $\mathbf{J} - 2\mathbf{I}$ на диагонали теряет парную симметрию, симметрируется и вставляемый блок $\mathbf{MR}$ или $\mathbf{RM}$, как это показано на рис. 6.

Вследствие небольшого рассогласования в размерах сомножителей произведение Кронекера получает небольшой легко поправимый центральными клетками дефект, порождая замечательно простую формулу произведения, дающего все матрицы Адамара независимо от простоты характерного размера сомножителей.



■ *Рис. 5.* Портреты матриц Адамара и быстрого произведения Скарпи

■ *Fig. 5.* Hadamard matrix and Scarpis fast product portraits



■ *Рис. 6.* Портреты матриц Адамара и второго произведения Скарпи

■ *Fig. 6.* Hadamard matrix and second Scarpis product portraits

В отличие от оригинала, предлагаемая реализация произведения выдерживает, например, работу с кососимметричной матрицей Себерри порядка 36 ($p = n - 1 = 35$, составное число), порождая произведение порядка $35 \times 36 = 1260$. Достижим и порядок $36 \times 37 = 1404$. Как Скарпи мог не заметить более простой формулы вставки в виде витража? Достаточно взглянуть на вид первых матриц Адамара, чтобы понять, что ни выделенных симметрий, ни нормальной и универсальных форм матриц в то время не было.

Заключение

Подход Скарпи при всех недостатках, присущих ранней стадии обнаружения ортогональных конструкций (сложность описания, потребность в арифметике конечных полей), оказал соответствующее влияние на Пэли. Порядки матриц, достижимые витражами, не совпадают с порядками матриц, которые Пэли вычислял прямым применением конечных полей. Отсюда возникло представление, что поиск множества матриц Адамара невозможно закрыть одним каким-либо комбинаторным методом, требуется бесконечное «лоскутное одеяло». Появились матрицы Пэли, матрицы Скарпи, и смысл соревновательности математиков XX века состоял в предложении все новых и новых семейств матриц Адамара.

Апелляция к научному наследию в виде теорем Гаусса и Лиувилля решает проблему существования иным путем. Конечные поля позволяют упростить вычисление ортогональных малоуровневых матриц, но эти поля существуют далеко не всегда. Модифицированное произведение Кронекера в полях для проведения операций не нуждается.

Новый изложенный выше метод позволяет находить матрицы и при отсутствии полей, сохраняя свою основную черту — вставку матрицы Адамара в свою основу или наоборот.

Финансовая поддержка

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

Литература

1. **Hadamard J.** Résolution d'une question relative aux determinants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.

2. **Jennifer S., Yamada M.** *Hadamard matrices: Constructions using number theory and linear algebra*. Wiley, 2020. 384 p.
3. **Craigen R.** *Hadamard Matrices and Designs*. CRC Handbook of Combinatorial Designs. C. J. Colbourn and J. H. Dinitz eds. CRC Press, 1996. Pp. 229–516.
4. **Colbourn C. J., Dinitz J. H.** *Handbook of Combinatorial Designs*. Second ed. Chapman and Hall/CRC, 2007. 967 p.
5. **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
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. **Ito N.** On Hadamard Groups III. *Kyushu J. Math*, 1997, no. 51, pp. 369–379.
8. **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
9. **Гаусс К. Ф.** *Труды по теории чисел*/ пер. Б. Б. Демьянова; под ред. И. М. Виноградова, комментарии Б. Н. Делоне. М., АН СССР, 1959. 978 с.
10. **Liouville J.** Nouveaux théorémes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84.
11. **Paley R. E. A. C.** On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, no. 12, pp. 311–320.
12. **Williamson J.** Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
13. **Doković D. Ž.** Williamson matrices of order 4n for n = 33; 35; 39. *Discrete Math.*, 1993, vol. 115, pp. 267–271.
14. **Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B.** Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, no. 46 (3), pp. 343–352.
15. **Seberry J.** A skew-Hadamard matrix of order 92. *Bulletin of the Australian Mathematical Society*, 1971, no. 5, pp. 203–204.
16. **Awyzio G., Seberry J.** On good matrices and skew Hadamard matrices. *Proc. Algebraic Design Theory and Hadamard Matrices*, 2015, pp. 13–28. http://dx.doi.org/10.1007/978-3-319-17729-8_2
17. **Balonin N. A., Seberry J.** Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
18. **Balonin N. A., Balonin Y. N., Đjoković 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
19. **Balonin N. A., Doković 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.
20. **Balonin N. A., Doković 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
21. **Doković D. Ž.** Some new symmetric Hadamard matrices. arXiv:2101.05429v2. https://arxiv.org/abs/2101.05429.
22. **Scarpis U.** Sui determinanti di valore massimo. *Rendiconti della R. Istituto Lombardo di scienze e lettere*, 1898, no. 31, pp. 1441–1446.
23. **Востриков А. А.** Матричные витражи и регулярные матрицы Адамара. *Информационно-управляющие системы*, 2021, № 5, с. 2–9. doi.org/10.31799/1684-8853-2021-5-2-9
24. **Doković D. Ž.** Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, no. 10, pp. 1985–1987.

UDC 519.614
doi:10.31799/1684-8853-2022-3-2-8

Hadamard matrices as a result of Scarpis product without cyclic shifts

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
A. M. Sergeev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-4788-9869
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Orthogonal Hadamard matrices consisting of elements 1 and −1 (real number) exist for orders that are multiples of 4. The study considers the product of an orthogonal Hadamard matrix and its core, which is called the Scarpis product, and is similar in meaning to the Kronecker product. **Purpose:** To show by revealing the symmetries of the block Hadamard matrices that their observance contributes to a product that generalizes the Scarpis method to the nonexistence of a finite field. **Results:** The study demonstrates that orthogonality is an invariant of the product under discussion, subject to the two conditions: one of the multipliers is inserted into the other one, the sign of the elements of the second multiplier taken into account (the Kronecker product), but with a selective action of the sign on the elements and, most importantly, with the cyclic permutation of the core which depends on the insertion location. The paper shows that such shifts can be completely avoided by using symmetries that are characteristic of the universal forms of Hadamard matrices. In addition, this technique is common for many varieties of adjustable Kronecker products. **Practical relevance:** Orthogonal

sequences and effective methods for their finding by the theory of finite fields and groups are of direct practical importance for the problems of noiseless coding, video compression and visual masking.
Keywords — Hadamard matrices, Mersenne matrices, Scarpis product, skew-symmetric matrices, symmetric matrices.

For citation: Balonin N. A., Sergeev A. M. Hadamard matrices as a result of Scarpis product without cyclic shifts. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 3, pp. 2–8 (In Russian).

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. Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
2. Jennifer S., Yamada M. *Hadamard matrices: Constructions using number theory and linear algebra*. Wiley, 2020. 384 p.
3. Craigen R. *Hadamard matrices and designs*. In: *CRC Handbook of Combinatorial Designs*. C. J. Colbourn and J. H. Dinitz eds. CRC Press, 1996. Pp. 229–516.
4. Colbourn C. J., Dinitz J. H. *Handbook of combinatorial designs*. Second ed. Chapman and Hall/CRC, 2007. 967 p.
5. Balonin N. A., Sergeev M. B. 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
6. Balonin N. A., Sergeev A. M., Sinitsyna 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. Ito N. On Hadamard Groups III. *Kyushu J. Math.*, 1997, no. 51, pp. 369–379.
8. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna 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
9. Gauss K. F. *Trudy po teorii chisel* [Works on number theory]. Moscow, Akademiia Nauk SSSR Publ., 1959. 978 p. (In Russian).
10. Liouville J. Nouveaux théorémes concernant les nombres triangulaires. *Journal de Mathématiques Pures et Appliquées*, 1863, no. 8, pp. 73–84 (In French).
11. Paley R. E. A. C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, no. 12, pp. 311–320.
12. Williamson J. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
13. Đoković D. Ž. Williamson matrices of order 4n for n = 33; 35; 39. *Discrete Math.*, 1993, vol. 115, pp. 267–271.
14. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, no. 46 (3), pp. 343–352.
15. Seberry J. A skew-Hadamard matrix of order 92. *Bulletin of the Australian Mathematical Society*, 1971, vol. 5, pp. 203–204.
16. Awyzio G., Seberry J. On good matrices and skew Hadamard matrices. *Proc. Algebraic Design Theory and Hadamard Matrices*, 2015, 15 p. http://dx.doi.org/10.1007/978-3-319-17729-8_2
17. Balonin N. A., Seberry J. Two infinite families of symmetric Hadamard matrices. *Australian Journal of Combinatorics*, 2017, vol. 69(3), pp. 349–357.
18. 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 Systems], 2017, no. 5, pp. 2–11. doi:10.15217/issn1684-8853.2017.5.2
19. Balonin N. A., Djokovic D. Z., Karbovskiy D. A. Construction of symmetric Hadamard matrices of order 4v for v = 47, 73, 113. *Special Matrices*, 2018, vol. 6, pp. 11–22.
20. Balonin N. A., Đoković D. Ž. Symmetric Hadamard matrices of orders 268, 412, 436 and 604. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 2–8. doi:10.31799/1684-8853-2018-4-2-8
21. Djokovic D. Z. Some new symmetric Hadamard matrices. arXiv:2101.05429v2. https://arxiv.org/abs/2101.05429.
22. Scarpis U. Sui determinanti di valore massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, no. 31, pp. 1441–1446 (In Italian).
23. Vostrikov A. A. Matrix vitrages and regular Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 5, pp. 2–9. (In Russia). doi:10.31799/1684-8853-2021-5-2-9
24. Djokovic D. Z. Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, no. 10, pp. 1985–1987.