УДК 519.614
doi:10.31799/1684-8853-2021-5-2-9

Научные статьи
Articles

Матричные витражи и регулярные матрицы Адамара

А. А. Востриков*[a], *канд. техн. наук, доцент, orcid.org/0000-0002-8513-3683, vostricov@mail.ru
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

Введение: *кронекерово произведение матриц Адамара, когда одна матрица порядка n вставляется по месту каждого элемента другой матрицы порядка m, наследуя знак замещаемого элемента, рассматривается как основа получения этих ортогональных матриц порядка nm. Операция вставки, наследующая не только знаки, но и структурные элементы — орнаменты портретов матриц, рассматривается как операция создания витража — более общего результата. Витражи на базе типичных квазиортогональных матриц Мерсенна (**M**), Зейделя (**S**), Эйлера (**E**) и других, помимо наследования знака и орнамента (узора), иначе наследуют значение отличных от единицы (по амплитуде) элементов, вызывая необходимость пересмотреть и систематизировать накопленный опыт.* ***Цель:*** *описать новые алгоритмы обобщенного произведения матриц, выделяя конструкции, ведущие к регулярным матрицам Адамара высоких порядков.* ***Результаты:*** *предложен алгоритм получения матричных витражей вставкой матриц Мерсенна в матрицы Зейделя, позволяющий расширить аддитивные цепочки матриц вида **M-E-M-E-**… и **S-E-M-E-**…, получаемые удвоениями порядков и добавлением каймы. Операция формирования матричного витража позволяет получать матрицы высоких порядков с сохранением такого важного инварианта структуры, как орнамент. Показано, что формирование матричного витража наследует логику произведения Скарпи, но не сводится к ней, поскольку ненулевое расстояние между сомножителями **M** и **S** по порядку упрощает итоговый орнамент регулярной матрицы отсутствием циклических смещений. Чередование матриц **M** и **S** позволяет продолжить мультипликативные цепочки до известных пробелов в матрицах **S**. Это по-новому освещает теорию регулярных матриц Адамара как результатов произведения матриц Мерсенна и Зейделя.* ***Практическая значимость:*** *ортогональные последовательности с плавающими уровнями и алгоритмы эффективного нахождения регулярных матриц Адамара, выделенных рядом полезных свойств, имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

Ключевые слова *— ортогональные матрицы, регулярные матрицы, матрицы Адамара, матрицы Мерсенна, матрицы Зейделя, кронекерово произведение, алгоритм Скарпи, вставки матриц, матричные витражи.*

Для цитирования: Востриков А. А. Матричные витражи и регулярные матрицы Адамара. *Информационно-управляющие системы*, 2021, № 5, с. 2–9. doi:10.31799/1684-8853-2021-5-2-9
For citation: Vostrikov A. A. Matrix vitrages and regular Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 5, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2021-5-2-9

Введение

Квазиортогональные (ортогональные) матрицы широко используются в таких практических применениях, как обработка сигналов, сжатие, маскирование и помехоустойчивое кодирование изображений [1–4], криптография [5] и т. д. Это широко известные матрицы Адамара [6], матрицы Мерсенна [7] и др. Для поиска таких матриц известно большое количество методов и алгоритмов, отличающихся своей эффективностью при поиске матриц высоких порядков, или структурированных матриц, или матриц с целочисленными и вещественными элементами и пр. Наибольший интерес сегодня для задач обработки изображений представляет поиск квазиортогональных структурированных матриц высоких порядков [8–11], вычисления с которыми и их хранение наиболее эффективны [12].

Сегодня оборудование, осуществляющее обработку и передачу визуальной информации реального времени, оперирует разрешениями в 2, 4 и 8 тысяч пикселей внутри каждого видеокадра при скорости обновления от 30 до 120 и более кадров/с. Матрицы исследуемых порядков выступают в роли операторов преобразования с различными целями, и увеличение их порядка до сотен и тысяч существенно повлияет как на скорость обработки, так и на качество восстанавливаемого изображения для потребителя. Кроме этого, ввиду малого числа уровней (количества различных значений элементов таких матриц) в процессе вычислений ресурсоемкая процедура умножения заменяется значительно более быстрой и менее энергозатратной процедурой выборки из памяти. Совокупный эффект в результате нахождения и применения новых ортогональных матриц высоких порядков способен оказать существенное влияние на эффективность перспективных систем цифровой обработки сигналов и их двумерного представления — цифровых видеоизображений.

В настоящей работе предлагаются новые алгоритмы поиска матриц на основе обобщенного произведения матриц с выделением конструкций, ведущих к регулярным матрицам Адамара высоких порядков.

Необходимые термины и определения

Определение 1. Квазиортогональная матрица $\mathbf{A}$ порядка n — это квадратная матрица, удовлетворяющая уравнению $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$, где $\omega(n)$ — некоторая весовая функция, определяющая тип матрицы, а $\mathbf{I}$ — единичная матрица.

Можно использовать (с оговоркой) термин «взвешенная матрица», но это слово уже занято целочисленными ее представителями с элементами $\{0, 1, -1\}$ и линейной функцией веса $\omega(n) = n - k$, где k — целое число.

Случай $k = 0$ соответствует матрицам Адамара [6] с ее ненулевыми элементами; $k = 1$ соответствует матрицам Белевича (конференц-матрицам) [13]. Случай $k \geq 1$ относят к взвешенным матрицам $\mathbf{W}(n, n-k)$, рассматриваемым как *обобщение* матриц Адамара в работах [7, 14]. Для иррациональных значений k подходит обозначение $\mathbf{W}(n, \omega(n))$.

Иными словами, квазиортогональная матрица — это взвешенная $\mathbf{W}(n, \omega(n))$ матрица с вещественными элементами $\{a = 1, -b\}$ в ней или образующих ее блоках. Инверсия знака при блоках не меняет состав базисных элементов. Третий элемент обычно выделен (как и у матриц Белевича) позиционированием на диагонали $\{d, a = 1, -b\}$ $(d \leq b \leq 1)$ или кайме $\{a = 1, -b, s\}$ $(b \leq s \leq 1)$ матрицы.

Чтобы не путать $\mathbf{W}(n, n-k)$ с $\mathbf{W}(n, \omega(n))$, профессор Дж. Себерри предложила называть последние *критскими* матрицами, подчеркивая нецелочисленность значений их элементов.

Как известно, *кронекерово умножение* $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$ двух матриц $\mathbf{A}$ и $\mathbf{B}$ с элементами $\{1, -1\}$ реализуется вставкой матрицы $\mathbf{B}$ по месту элементов матрицы $\mathbf{A}$ с наследованием знака замещаемого элемента в виде

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

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

Определение 2. Портрет квазиортогональной матрицы — визуальное изображение, на котором ее элементы представлены в виде клеток разных цветов, соответствующих значениям элементов.

На портрете матрицы совокупность разных по цвету клеток создает орнамент [15]. Для рассматриваемых в работе матриц возможны не более трех цветов клеток, соответствующих наборам значений элементов $\{1, -1\}$, $\{1, 0, -1\}$, $\{d, 1, -b\}$ или $\{1, -b, s\}$.

Первооткрывателя направления Сильвестра привлекала именно орнаментальная составляющая портрета матрицы: при обращении матрицы орнамент ее сохраняется с точностью до транспонирования. Адамар, в свою очередь, расширил количество матриц, используемых в произведениях (вставках), предложенных Сильвестром.

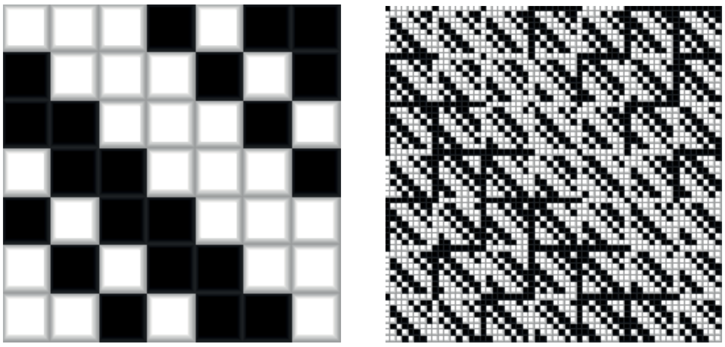
Определение 3. Витраж — это более общий результат кронекерова произведения двух матриц с косвенным наследованием числовых и структурных (орнамент матричного портрета) элементов.

У. Скарпи [16] предложил свой алгоритм реализации вставки спустя четыре года после опубликования Адамаром статьи [6], в которой тот сумел найти всего лишь пару новых матриц порядков 12 и 20, дополняющих порядки Сильвестра $n = 2^t$, где t — целое число.

Матрица Адамара после нормирования выведением в единицу элементов ее первых строки и столбца, называемых каймой, приобретает так называемую *основу* (core) отделением этой каймы. Порядки $2^t - 1$ представляют собой числа Мерсенна, причем полученную матрицу снова можно ортогонализовать введением плавающего уровня (изменением значения -1 на $-b$, где $|b| < 1$). Детерминант таких матриц выше, если число положительных элементов 1 выше числа отрицательных элементов $-b$ на единицу. Поэтому они инвертированы по знаку к основе (core), где это соотношение выдерживается с точностью до наоборот.

Получаемые в процессе этого преобразования ортогональные матрицы были названы матрицами Мерсенна [7]. Обнаружение существования таких матриц на порядках 11 и 19 позволило высказать предположение, что, как и матрицы Адамара, матрицы Мерсенна могут быть расширены на все порядки $n - 1$, где $n = 4t$ (гипотеза Н. А. Балонина). В этом виде гипотеза представляет собой альтернативную формулировку гипотезы Адамара о существовании всех выделенных им матриц на порядках, кратных 4 [17]. Но, поскольку матрицы Мерсенна — это, в том числе, и матрицы с иррациональными элементами (с учетом уровня $-b$), теория матриц с плавающим уровнем или уровнями открывает новые перспективы для доказательства упомянутых гипотез.

Произведение самим У. Скарпи было сформулировано громоздко, еще до введения понятия нормальной формы матрицы Адамара и ее основы, поэтому приведем его в нашей редакции. Формулировка даже значительно более простая по алгоритму вычисления произведения, чем предложенная Д. Джоковичем [18].



■ *Рис. 1.* Портрет матрицы Мерсенна $\mathbf{M}_7$ и витраж — портрет матрицы Адамара $\mathbf{H}_{56}$

■ *Fig. 1.* Portrait of the Mersenne matrix $\mathbf{M}_7$ and stained glass — portrait of the Hadamard matrix $\mathbf{H}_{56}$

Опираясь на определение матриц Мерсенна, произведение Скарпи можно переписать как обобщенное матричное произведение матриц $\mathbf{M}$, где роль множителя произведения Кронекера играет кайма, которая расширяет размер вставляемой основы до размера матрицы Адамара. Такие произведения не характерны для алгоритмов Сильвестра и Адамара, поэтому Скарпи сумел получить ряд новых матриц порядка $n(n-1)$, где $(n-1)$ — порядки матриц Мерсенна.

Поскольку итоговый порядок кратен четырем, значение плавающего уровня $-b$ в результирующей матрице снова становится равным -1. В результате получаем [19]

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

где $\mathbf{e}$ — вектор единичных элементов каймы; $\mathbf{T}$ — матрица циклического смещения всех элементов, каждый блок смещается на величину произведения $(i-1)(j-1)$, индексы для смещений нумеруются с нуля. Символ сложного произведения не меняем.

В качестве иллюстрации на рис. 1 приведены портреты матрицы Мерсенна порядка 7 и результата матричного произведения Скарпи — витража, в котором вставляемая матрица циклически смещается на величину, определяемую произведением индексов ее положения. Знак наследуется не прямо, а в виде знака каймы.

Приведенная на рис. 1 матрица Мерсенна порядка 7 вставляется сама в себя, с добавлением каймы (первая точка ее всегда отрицательная). В итоге получаем матрицу порядка матрицы Адамара $7(7+1)=56$, которая таковой и является, если считать элементы равными 1 и -1. Из приведенного примера видно, что это произведение напоминает кронекерово и описывает достаточно просто, как вставку (витраж), обширный класс матриц, порождаемых матрицами Мерсенна.

Изобретение Скарпи предлагается расширить на произведения иных квазиортогональных матриц, например, порядков $(m-1)$ и $(m+1)$. В итоге становятся достижимы квадратичные порядки m^2-1, характерные для основ регулярных матриц Адамара порядка $n=m^2=4u^2$, где u — целое число.

Определение 4. Матрицы Адамара являются регулярными, если имеют одинаковые значения сумм элементов строк и столбцов.

Предикторы цепочек критских матриц

Наиболее интересными критскими матрицами, в аспекте данной статьи, являются матрицы Мерсенна $\mathbf{M}$ и матрицы Одина, совпадающие орнаментом с матрицами Зейделя $\mathbf{S}$ с точностью до значений их плавающих уровней. Матрицы **M** и **S** (далее матрица Одина) являются двумя предикторами цепочек критских матриц вида **M**(или **S**)–**E**–**M**–**E**–... [20].

Прежде всего, их можно использовать для получения простейших витражей сильвестрова типа, получаемых умножением предикторов и членов цепочки на матрицу Адамара второго порядка $\mathbf{H}_2$, например $\mathbf{E} = \mathbf{H}_2 \otimes \mathbf{M}$, без коррекции элементов. Для произведения $\mathbf{H}_2 \otimes \mathbf{S}$ витраж корректируют, исправляя элементы диагоналей матрицы Одина для получения уровня матрицы Эйлера **E** [19]. Здесь **M** — это матрица Мерсенна порядка $n = 4t - 1 = 3(\mathrm{mod}\ 4)$, критская матрица с элементами $\{a = 1, -b\}$, $b = \dfrac{t}{t + \sqrt{t}}$, $k = (2t - 1) \times (1 - b^2)$, $\omega(n) = ((n + 1) + (n - 1)b^2)/2$, $t > 0$ — целое число. Рабочее предположение (гипотеза [17]) состоит в том, что эти матрицы существуют для любого выделенного для них порядка.

Для порядков значений простых целых чисел это циклические матрицы, для степеней целых чисел – блочные. Как видно из цепочки матриц **E** и **M**, большинство из них можно найти через бициклические матрицы Эйлера **E**. Будучи предиктором матриц Мерсенна, т. е. основой без специфической каймы, матрицы Эйлера тоже существуют на всех выделенных для них порядках $n = 4t - 2 = 2(\mathrm{mod}\ 4)$. Весовую функцию и элементы матрицы Эйлера **E** несложно определить с помощью связи $\mathbf{E} = \mathbf{H}_2 \otimes \mathbf{M}$, она сложена из двух циклических матриц Мерсенна. Аналогичен путь ее построения из циклических матриц Одина структуры Зейделя, с некоторыми поправками входящий в алгоритм [19, 21].

Матрица **S** порядка $n = 4t - 3 = 1(\mathrm{mod}\ 4)$ — это критская матрица с элементами $\{d,\ a = 1, -b\}$, $b = 1 - 2d$, $d = \dfrac{1}{1 + \sqrt{n}}$, $k = 1 - d^2 + 2(t - 1)(1 - b^2)$, $\omega(n) = d^2 + ((n - 1) + (n - 1)b^2)/2$, где $t > 1$ — целое число. Эти матрицы существуют для любого выделенного для них порядка, если их порядок — сумма двух квадратов. Первые проблемные для матриц Одина порядки: 21, 33, 57 и т. п. До первой сотни существуют, но неизвестны (не найдены) матрицы Одина составных простых порядков 65 и 85.

Оригинальность бицикла **E** и его место в цепочках критских матриц состоит в том, что как связной элемент бесконечных цепочек итераций **M**(или **S**)–**E**–**M**–**E**–... он существует независимо от форм, которые принимают первоначальные матрицы Мерсенна и Одина. По сути, на старте это вполне себе независимая матрица, которую мы можем предопределять через предикторы **M** или **S** (служащих основой) только ради экономии сил и времени на ее отыскание.

Регулярные матрицы Адамара $\mathbf{H} = [\mathbf{S} \otimes \mathbf{M}]$ или $\mathbf{H} = [\mathbf{M} \otimes \mathbf{S}]$

Каждая из описанных нами цепочек в пределе стремится к матрице Адамара, но на бесконечно большом порядке, так как пара $\{a = 1, -b\}$ стремится к $\{a = 1, -1\}$. Иными словами, функция уровней $b(n)$ элементов матриц Мерсенна — монотонная, стремящаяся к единице. Особенность критских цепочек состоит в том, что формула Скарпи более универсальная и позволяет умножать не только матрицы Мерсенна (сами на себя), но и пары близко расположенных матриц $\mathbf{H} = [\mathbf{S} \otimes \mathbf{M}]$ или $\mathbf{H} = [\mathbf{M} \otimes \mathbf{S}]$. Используемые здесь квадратные скобки обозначают добавляемую к произведению (основе) кайму из единиц.

Формула не требует смещения, характерного для произведения Скарпи, диагональные элементы сомножителей замещены некоторыми компенсаторами, в остальном это обычное кронекерово произведение. Тем самым бесполезные, на первый взгляд, уровневые матрицы Одина выделены тем, что в сочетании с матрицами Мерсенна дают регулярные матрицы Адамара. Напомним, что в форме Буша (помимо тривиальных случаев, связанных с цепочкою матриц Сильвестра) за всю историю поисков найдено всего три регулярные матрицы Адамара первых порядков 36, 100 и 324. Матрица порядка 196 не найдена.

Витраж как основа построения регулярных матриц Адамара

Структура витража, опирающаяся на кронекерово произведение матриц, относится к простым структурам. Она порождает квазиортогональную матрицу с абсолютными значениями элементов, равными произведениям сомножителей. Эта версия произведения нам менее интересна, хотя она и имеет право на существование как источник ортогональных матриц. Основой регулярных матриц Адамара являются нормализованные произведения $\mathbf{H} = [\mathbf{S}^{(1)} \otimes \mathbf{M}^{(1)}]$ или $\mathbf{H} = [\mathbf{M}^{(1)} \otimes \mathbf{S}^{(1)}]$ двух смежных (отличающихся на 2) простых порядков.

Сложный витраж отличается от результата кронекерова произведения общей для всей матрицы каймой и матрицей компенсатором, размещенным вдоль оси симметрии (диагонали).

В качестве блоков на оси симметрии (диагональных блоков) используется матрица из единиц **J**, если первый сомножитель больше по порядку второго. В противном случае — матрица $\mathbf{J} - 2\mathbf{I}$, где **I** — единичная матрица (знак центральных элементов квадрата компенсируется), причем диагональ вставляемой матрицы варьируется в зависимости от знака замещаемого блоком элемента.

В остальном это произведение не отличается от кронекерова, чем и привлекательно. Вставки поднимают абсолютные значения элементов произведения квазиортогональных матриц до единицы. Это компенсационный принцип как у алгоритма Скарпи с его окаймлением блоков. Если порядки матриц Мерсенна составные, то используется сомножитель $\mathbf{M}^{(2)}$ порядка $(2m + 1)$, построенный из матриц простых порядков m.

В любом таком случае мы можем указать положение компенсатора на диагонали: у матриц Белевича это нули; у произведения роль нуля играют матричные блоки без орнамента, приходящиеся на ось симметрии или антисимметрии. Компенсатор помогает дополнять не равные по числу положительных и отрицательных элементов в строках (столбцах) матрицы сосредоточениями однородных элементов, обеспечивающих необходимый нулевой баланс.

Для освоения этой техники приведем примеры. Отметим, что циклическая форма матриц Мерсенна существует и для порядков, равных произведениям близких пар целых чисел, отличающихся на 2. Например, для порядков $3 \times 5 = 15$, $5 \times 7 = 35$, $7 \times 9 = 63$ и т. п., но они не отличаются явно выраженной осью симметрии. Такие ущербные матрицы наделены общей для всех матриц Мерсенна способностью порождать матрицу Адамара добавлением к этой основе каймы из отрицательных элементов — вид обобщенного умножения на матрицу Адамара первого порядка.

Регулярные матрицы Адамара

Регулярные матрицы Адамара существуют на порядках $4u^2 = (m + 1)(m - 1) + 1$, где u — целое число, т. е. 4, 16, 36, 100, 144, 196, 324, 196, 324, 676, 900, 1444, 1764, 2116, 2500, 2916 и т. п. Для вычисления промежуточных матриц порядков $21 \times 23 + 1 = 484$ и $33 \times 35 + 1 = 1156$ нет соответствующих матриц Одина.

Рассмотрим первые три циклические матрицы для получения витражей. Это матрицы Мерсенна $\mathbf{M}_3$, Одина $\mathbf{S}_5$ и Мерсенна $\mathbf{M}_7$. Будем далее обозначать $\mathbf{M} = (\mathbf{M}_n)$, $\mathbf{S} = (\mathbf{S}_n)$ округленные до целых значений элементов матрицы с нулями на диагонали. В таком случае эти матрицы перестанут быть ортогональными, и их портреты совпадут с матрицами $\mathbf{Q}$ квадратичных вычетов с выделенными диагональными (осевыми) элементами, представленными на рис. 2.

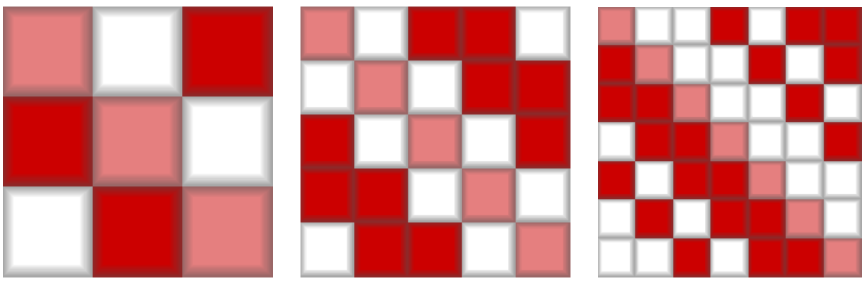
Для четных порядков 4 (тривиальный), 16, 36, 100, 144, (не $196 = 13 \times 15 + 1$), 324, (не 676), 900, (не 1444), 1764, (не 2116), 2500, (не 2916) возможны простые сомножители.

Алгоритм поиска. Для произведения $\mathbf{H} = [\mathbf{M} \otimes \mathbf{S}]$ вычисляем $\mathbf{A} = \mathbf{S} - \mathbf{I}$, $\mathbf{B} = -\mathbf{S} - \mathbf{I}$, а для $\mathbf{H} = [\mathbf{S} \otimes \mathbf{M}]$, наоборот: $\mathbf{A} = \mathbf{M} - \mathbf{I}$, $\mathbf{B} = -\mathbf{M} - \mathbf{I}$. Эти матрицы замещают положительный и отрицательный элементы первого сомножителя, диагональные элементы на оси симметрии замещаются $\mathbf{J} - 2\mathbf{I}$. Итоговую матрицу наращиваем каймой.

Тривиальный случай — это порядок $1 \times 3 + 1 = 4$, когда регулярная матрица Адамара получается расширением округленной матрицы Мерсенна $\mathbf{M}_3$ с помощью каймы из положительных элементов, кроме первого отрицательного элемента. На случай порядка $3 \times 5 + 1 = 16$ матрица $\mathbf{M}_3$ образует витраж с матрицей $\mathbf{S}_5$, ведущий к матрице $\mathbf{H}_{16}$ (рис. 3).

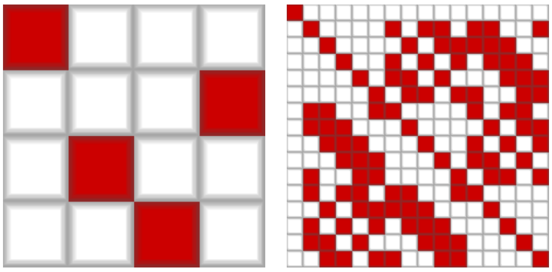
Для порядка $5 \times 7 + 1 = 36$ матрица $\mathbf{S}_5$ образует витраж с матрицей $\mathbf{M}_7$, ведущий к матрице $\mathbf{H}_{36}$. Произведем выравнивание сумм элементов строк и столбцов матриц Адамара инверсией второй половины блоков ее ядра. Регулярные матрицы $\mathbf{H}_{16}$ и $\mathbf{H}_{36}$ (рис. 4) сходны. Для синтеза матриц порядков $7 \times 9 + 1 = 64$ и $9 \times 11 + 1 = 100$ используем блочную матрицу $\mathbf{S}_9 = \mathbf{M}_3 \otimes \mathbf{M}_3$, соответствующую кратной степени.

Первый по-настоящему не рабочий для такого алгоритма порядок это уже известный порядок 196 ($13 \times 15 + 1$). Заметим, что построение матрицы $\mathbf{S}_{13}$ проблем не вызывает. В разложении непростого числа $15 = 2 \times 7 + 1$ фигурирует простой порядок уже знакомой матрицы $\mathbf{M}^{(1)} = \mathbf{M}_7$, с помощью которой можно составить кососимметри-



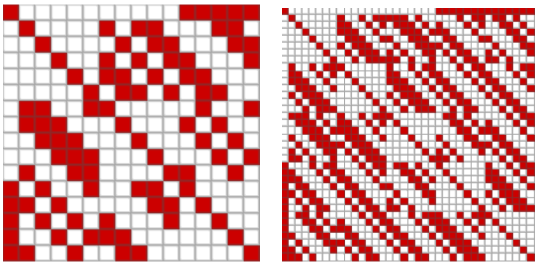
■ ***Рис. 2.*** Портреты трех циклических матриц квадратичных вычетов порядков 3, 5, 7

■ ***Fig. 2.*** Portraits of three cyclic matrices of quadratic residues of orders 3, 5, 7



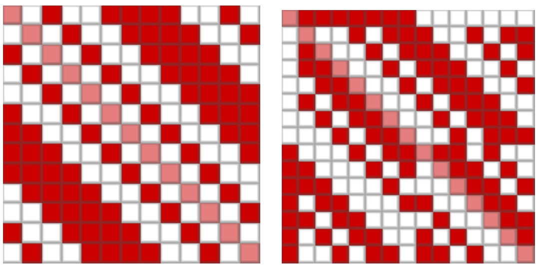
■ ***Рис. 3.*** Портреты матриц Адамара $\mathbf{H}_4$ и $\mathbf{H}_{16}$

■ ***Fig. 3.*** Portraits of the Hadamard matrices $\mathbf{H}_4$ и $\mathbf{H}_{16}$



■ ***Рис. 4.*** Портреты регулярных матриц Адамара $\mathbf{H}_{16}$ и $\mathbf{H}_{36}$

■ ***Fig. 4.*** Portraits of the regular Hadamard matrices $\mathbf{H}_{16}$ и $\mathbf{H}_{36}$



■ ***Рис. 5.*** Портреты матриц $\mathbf{S}_{13}$ и $\mathbf{M}^{(2)} = \mathbf{M}_{15}$

■ ***Fig. 5.*** Portraits of the matrices $\mathbf{S}_{13}$ и $\mathbf{M}^{(2)} = \mathbf{M}_{15}$

ческую матрицу $\mathbf{M}^{(2)} = \mathbf{M}_{15}$ с симметрией второго порядка (рис. 5). Тем самым путь к построению регулярных матриц Адамара порядка 196 открыт.

Заключение

Скарпи трактовал свое произведение как череду операций с матрицей Адамара. Предложенный в работе алгоритм построения регулярных матриц Адамара через витражи является новым, поскольку в качестве сомножителей произведения не используются матрицы Адамара — впервые для этого вводятся критские матрицы с плавающими уровнями и манипуляции с ними, в том числе повышение уровня по мере роста порядка матрицы.

Кроме матриц Адамара, результатом обобщенного кронекерова произведения являются и матрицы Мерсенна более высоких порядков. В обобщенном кронекеровом произведении вполне можно обойтись без процедуры общего окаймления, трактуя его именно как путь получения матриц Мерсенна.

Кроме аддитивных цепочек матриц вида **M–E–M–E–...** и **S–E–M–E–...**, получаемых удвоениями порядков и добавлением каймы, возникают мультипликативные цепочки генерации критских матриц.

Изложенный материал является основой для получения регулярной матрицы порядка 196 и далее матрицы порядка 676. Поскольку порядок матрицы $\mathbf{S}_{25}$ является квадратом простого числа, то для нее легко строится матрица квадратичных вычетов и регулярная матрица порядка 1444. Построение матрицы порядка 2116 зависит от блочной матрицы $\mathbf{S}_{45}$, являющейся ядром особой конференц-матрицы $\mathbf{C}_{46}$. И, наконец, матрицу $\mathbf{S}_{25}$ можно использовать при построении матрицы порядка 2916.

В практическом смысле результаты проведенных исследований существенно расширяют возможности применения цифровых систем обработки как одномерных сигналов, так и изображений высокого разрешения в целях их сжатия и защиты от несанкционированного доступа.

Благодарность

Автор выражает благодарность профессорам Н. А. Балонину и М. Б. Сергееву за конструктивные замечания и помощь в подготовке статьи.

Финансовая поддержка

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

Литература

1. **Wang R.** *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis.* Cambridge University Press, 2010. 504 p.
2. **Mironovsky L. A., Slaev V. A.** *Strip-Method for Image and Signal Transformation.* De Gruyter, 2011. 175 p.
3. **Vostrikov A., Sergeev M.** Expansion of the quasi-orthogonal basis to mask images. *Smart Innovation,*

Systems and Technologies, 2015, vol. 40. pp. 161–168. doi:10.1007/978-3-319-19830-9_15
4. **Ahmed N., Rao R.** *Orthogonal Transforms for Digital Signal Processing*. Berlin-Heidelberg-New York: Springer-Verlag, 1975. 263 p.
5. **Koukouvinos C., Simos D., Varbanov Z.** Hadamard matrices, designs and their secret-sharing schemes. *Algebraic Informatics*, 2011, pp. 216–229. doi:10.1007/978-3-642-21493-6_14
6. **Hadamard J.** Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.
7. **Сергеев А. М.** О взаимосвязи одного вида квазиортогональных матриц, построенных на порядках последовательностей $4k$ и $4k$–1. *Известия ЛЭТИ*, 2017, № 7, с. 12–17.
8. **Di Matteo O., Djokovic D. Z., Kotsireas I. S.** Symmetric Hadamard matrices of order 116 and 172 exist. *Special Matrices*, 2015, vol. 3.1, pp. 227–234.
9. **Kharaghani H. and Tayfeh-Rezaie B.** A Hadamard matrix of order 428. *J. Combin. Designs*, 2005, vol. 13, pp. 435–440.
10. **Horadam K. J.** Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
11. **Seberry J., Yamada M.** *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. John Wiley & Sons, 2020. 352 p.
12. **Vostrikov A., Sergeev M., Balonin N., Sergeev A.** Use of symmetric Hadamard and Mersenne matrices in digital image processing. *Procedia Computer Science*, 2018, pp. 1054–1061. doi:10.1016/j.procs.2018.08.042
13. **Belevitch V.** Theorem of 2n-terminal networks with application to conference telephony. *Electrical Communication*, 1950, no. 26, pp. 231–244.
14. **Balonin Yu. N., Sergeev A. M.** Two-circulant Hadamard matrices, weighing matrices, and Ryser's conjecture. *Информационно-управляющие системы*, 2018, № 3, с. 2–9. doi:10.15217/issn1684-8853.2018.3.2
15. **Sergeev A., Sergeev M., Vostrikov A., Kurtyanik D.** Portraits of orthogonal matrices as a base for discrete textile ornament patterns. *Smart Innovation, Systems and Technologies*, 2019, vol. 143, pp. 135–143. doi:10.1007/978-981-13-8303-8_12
16. **Scarpis U.** Sui determinanti di valore massimo, Rendiconti della R. *Istituto Lombardo di Scienze e Lettere*, 1898, vol. 31, pp. 1441–1446.
17. **Сергеев А. М.** Обобщенные матрицы Мерсенна и гипотеза Балонина. *Автоматика и вычислительная техника*, 2014, № 4, с. 35–43.
18. **Djokovic D.** Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, iss. 10, pp. 1985–1987.
19. **Балонин Н. А., Сергеев А. М., Синицына О. И.** Алгоритмы конечных полей и групп поиска ортогональных последовательностей. *Информационно-управляющие системы*, 2021, № 4, с. 2–17. doi:10.31799/1684-8853-2021-6-2-17
20. **Balonin N. A., Vostrikov A. A., Sergeev M. B.** On two predictors of calculable chains of quasi-orthogonal matrices. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 3, pp. 153–158. doi:10.3103/S0146411615030025
21. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы максимума детерминанта. *Информационно-управляющие системы*, 2020, № 6, с. 2–11. doi:10.31799/1684-8853-2020-6-2-11

UDC 519.614
doi:10.31799/1684-8853-2021-5-2-9

Matrix vitrages and regular Hadamard matrices

A. A. Vostrikov[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-8513-3683, vostricov@mail.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: The Kronecker product of Hadamard matrices when a matrix of order n replaces each element in another matrix of order m, inheriting the sign of the replaced element, is a basis for obtaining orthogonal matrices of order nm. The matrix insertion operation when not only signs but also structural elements (ornamental patterns of matrix portraits) are inherited provides a more general result called a "vitrage". Vitrages based on typical quasi-orthogonal Mersenne (**M**), Seidel (**S**) or Euler (**E**) matrices, in addition to inheriting the sign and pattern, inherit the value of elements other than unity (in amplitude) in a different way, causing the need to revise and systematize the accumulated experience. **Purpose:** To describe new algorithms for generalized product of matrices, highlighting the constructions that produce regular high-order Hadamard matrices. **Results:** We have proposed an algorithm for obtaining matrix vitrages by inserting Mersenne matrices into Seidel matrices, which makes it possible to expand the additive chains of matrices of the form **M**–**E**–**M**–**E**–... and **S**–**E**–**M**–**E**–..., obtained by doubling the orders and adding an edge. The operation of forming a matrix vitrage allows you to obtain matrices of high orders, keeping the ornamental pattern as an important invariant of the structure. We have shown that the formation of a matrix vitrage inherits the logic of the Scarpi product, but is cannot be reduced to it, since a nonzero distance in order between the multiplicands **M** and **S** simplifies the final regular matrix ornamental pattern due to the absence of cyclic displacements. The alternation of **M** and **S** matrices allows you to extend the multiplicative chains up to the known gaps in the **S** matrices. This sheds a new light on the theory of a regular Hadamard matrix as a product of Mersenne and Seidel matrices. **Practical relevance:** Orthogonal sequences with floating levels and efficient algorithms for finding regular Hadamard matrices with certain useful properties are of direct practical importance for the problems of noise-proof coding, compression and masking of video data.

Keywords — orthogonal matrices, regular matrices, Hadamard matrices, Mersenne matrices, Seidel matrices, Kronecker product, Scarpi algorithm, matrix inserts, matrix vitrages.

For citation: Vostrikov A. A. Matrix vitrages and regular Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 5, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2021-5-2-9

References

1. Wang R. *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis*. Cambridge University Press, 2010. 504 p.
2. Mironovskij L. A., Slaev V. A. *Strip-Method for Image and Signal Transformation*. De Gruyter, 2011. 175 p.
3. Vostrikov A., Sergeev M. Expansion of the quasi-orthogonal basis to mask images. *Smart Innovation, Systems and Technologies*, 2015, vol. 40. pp. 161–168. doi:10.1007/978-3-319-19830-9_15
4. Ahmed N., Rao R. *Orthogonal Transforms for Digital Signal Processing*. Berlin-Heidelberg-New York: Springer-Verlag, 1975. 263 p.
5. Koukouvinos C., Simos D., Varbanov Z. Hadamard matrices, designs and their secret-sharing schemes. *Algebraic Informatics*, 2011, pp. 216–229. doi:10.1007/978-3-642-21493-6_14
6. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
7. Sergeev A. M. On interconnection of one type of quasi-orthogonal matrices constructed by orders of $4k$ and $4k$–1 sequences. *Izvestia LETI*, 2017, no. 7, pp. 12–17 (In Russian).
8. Di Matteo O., Djokovic D. Z., Kotsireas I. S. Symmetric Hadamard matrices of order 116 and 172 exist. *Special Matrices*, 2015, vol. 3.1, pp. 227–234.
9. Kharaghani H. and Tayfeh-Rezaie B. A Hadamard matrix of order 428. *J. Combin. Designs*, 2005, vol. 13, pp. 435–440.
10. Horadam K. J. Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
11. Seberry J., Yamada M. *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. John Wiley & Son,s 2020. 352 p.
12. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Use of symmetric Hadamard and Mersenne matrices in digital image processing. *Procedia Computer Science*, 2018, pp. 1054–1061. doi:10.1016/j.procs.2018.08.042
13. Belevitch V. Theorem of 2n-terminal networks with application to conference telephony. *Electrical Communication*, 1950, no. 26, pp. 231–244.
14. Balonin Yu. N., Sergeev A. M. Two-circulant Hadamard matrices, weighing matrices, and Ryser's conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 2–9. doi:10.15217/issn1684-8853.2018.3.2
15. Sergeev A., Sergeev M., Vostrikov A., Kurtyanik D. Portraits of orthogonal matrices as a base for discrete textile ornament patterns. *Smart Innovation, Systems and Technologies*, 2019, vol. 143, pp. 135–143. doi:10.1007/978-981-13-8303-8_12
16. Scarpis U. Sui determinanti di valore massimo, Rendiconti della R. *Istituto Lombardo di Scienze e Lettere*. 1898, vol. 31, pp. 1441–1446 (In Italian).
17. Sergeev A. M. Generalized Mersenne matrices and Balonin's hypothesis. *Automatic Control and Computer Sciences*, 2014, no. 4, pp. 35–43 (In Russian).
18. Djokovic D. Generalization of Scarpis' theorem on Hadamard matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, iss. 10, pp. 1985–1987.
19. Balonin Yu. N., Sergeev A. M., Sinicyna O. I. Algorithms for finite fields and search groups for orthogonal sequences. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 4. pp. 2–17 (In Russian). doi:10.31799/1684-8853-2021-6-2-17
20. Balonin N. A., Vostrikov A. A., Sergeev M. B. On two predictors of calculable chains of quasi-orthogonal matrices. *Automatic Control and Computer Sciences*, 2015, vol. 49, no. 3, pp. 153–158. doi:10.3103/S01464116150 30025
21. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices, and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2020-6-2-11

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org