ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

УДК 519.142.6
DOI 10.34822/1999-7604-2021-3-6-11

К ПРОБЛЕМЕ ПОИСКА МАТРИЦ АДАМАРА ПОРЯДКА 668

А. М. Сергеев ✉, Ю. Н. Балонин
Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, Россия
✉ *E-mail: aleks.asklab@gmail.com*

В статье рассматривается проблема вычисления матриц Адамара высоких порядков. Даны определения матриц-близнецов Пропус, Пропус-М и Пропус-Е, а также описан метод их вычисления с использованием матриц Мерсенна и Эйлера и модифицированного массива Вильямсона на основе двух базовых матриц. Показан путь приближения матрицы Адамара порядка 668 через Пропус-М на основе известной матрицы Мерсенна порядка 167 и даны определения уровней матриц и их портретов. Приведены уравнения связи уровней матриц Пропус-М и Пропус-Е; рассмотрены их свойства, числовые примеры и портреты матриц Пропус-М и Пропус-Е, вычисленные с использованием модифицированного массива Вильямсона.

Ключевые слова: ортогональные матрицы, матрицы Адамара, матрицы Мерсенна, матрицы Эйлера, числа Мерсенна, матрицы Пропус, массив Вильямсона.

ON PROBLEM OF SEARCH FOR HADAMARD MATRICES OF ORDER 668

A. M. Sergeev ✉, Yu. N. Balonin
Saint-Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia
✉ *E-mail: aleks.asklab@gmail.com*

The article describes the problem of calculation of Hadamard matrices of high orders. Definitions of twin matrices, Propus, Propus-M, Propus-E, is given. A method for their calculation via Mersenne and Euler matrices and modified Williamson array, based on two basic matrices, is described. A path of approximation of a Hadamard matrix of order 668 through Propus-M, based on a known Mersenne matrix of order 167, is shown, and definitions of matrices levels and their portraits are given. Equations of connection of Propus-M and Propus-E matrices levels are presented; their properties, numerical examples and portraits of Propus-M and Propus-E matrices calculated via modified Williamson array are analyzed.

Keywords: orthogonal matrices, Hadamard matrices, Mersenne matrices, Euler matrices, Mersenne numbers, Propus matrices, Williamson array.

Введение

Теория матриц Адамара $\mathbf{H}_n$ прошла несколько стадий развития. Изначально эти матрицы выделил и определил Сильвестр в рамках рекурсивной последовательности матриц (ортогональных базисов с простейшим проективным элементом ортов – единицей) вида

$$\mathbf{H}_n = \begin{pmatrix} \mathbf{H}_{n/2} & \mathbf{H}_{n/2} \\ \mathbf{H}_{n/2} & -\mathbf{H}_{n/2} \end{pmatrix} \qquad (1)$$

для порядков $n = 2^k$, где k – натуральное число.

Становление теории матриц до появления численных методов тесно связано с изучением свойств определителя [1]. Изучая матрицы с максимальным определителем, Адамар не

только заметил среди них матрицы сильвестровой последовательности, но и дополнил эту последовательность матрицами порядков 12 и 20, что было принципиально и ново. В его определении $\mathbf{H}_n$ – квадратные матрицы порядка n, состоящие из элементов {1, –1} и удовлетворяющие условию $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}$, где $\mathbf{I}$ – единичная матрица.

Указанные матрицы существуют только для порядков 1, 2 и далее – кратных четырем, причем Адамар своей работой способствовал формированию гипотезы об отсутствии пропусков в этой последовательности.

Матрицы Адамара оказались тесно связаны с теорией чисел уже потому, что сам факт их существования в виде циклического блока с каймой из 1 (нормальная форма) определяется простотой числа n – 1. Следовательно, чем сложнее это число (чем больше в его составе простых делителей и их степеней), тем труднее будет найти матрицу.

Сложность внутреннего строения матриц Адамара практически неограниченно увеличивается вместе с порядком, поэтому в ряду известных матриц порядков $n < 1000$ есть пропуски – до сих пор не найденные матрицы. Успешностью нахождения таких матриц, или матриц с фиксированными чертами симметрии (симметричных, кососимметричных и т. п.) [2, 3], измеряется уровень развития аппаратного и программного обеспечения развитых стран [4].

Следует отметить, что для порядков 1, 2, 4, 8, 12 существует только одна матрица Адамара. Это означает, что все остальные матрицы на этих порядках сводятся к некоторой одной эталонной матрице эквивалентными преобразованиями: перестановками строк, их алгебраическими сложениями с масштабированием и инверсиями элементов по знаку. Так, на порядке 16 таких матриц 5, на порядке 20 – 3, на порядке 24 – 60, на порядке 28 – 487. На порядках 32, 36, 40 и выше счет идет на миллионы.

Несмотря на приведенное разнообразие неэквивалентных между собой матриц, на порядке 668 пока не найдено ни одной матрицы. Более того, в работе [4] К. Хорадам из Принстонского Университета напрямую ставит вопрос о существовании не менее трех проблемных матриц Адамара порядков, меньших 1 000, к которым относится матрица порядка 668.

Матрицы четных и нечетных порядков в проблеме матриц Адамара

Кратность порядков матриц Адамара четырем позволяет предположить, что должны быть матрицы вдвое и вчетверо меньших порядков: первые из них кратны двум, вторые – нечетные числа. Эти составляющие общий объект блоки (квадратные матрицы) сами по себе обладают свойствами матриц Адамара [5].

Конструирование матриц Адамара из ортогональных матриц вдвое меньшего и четного порядка по схеме (1) предложил Сильвестр, а следующий шаг сделал Пэли, найдя способ построения матриц Адамара из блоков (символов Лежандра) четных порядков, которые матрицами Адамара не являются, поскольку общее определение матриц Адамара, в отличие от подхода Сильвестра, этого не требует. Во второй половине прошлого века В. Белевич нашел следующую интерпретацию составных частей алгоритма Пэли.

Матрица Белевича (C-matrix, conference-matrix) – квадратная матрица $\mathbf{C}_n$ порядка n, элементами которой являются числа {1, 0, –1}, удовлетворяющая условию $\mathbf{C}_n^{\mathrm{T}}\mathbf{C}_n = (n-1)\mathbf{I}$. Нулевые элементы в ней сосредоточены на диагонали.

Составные блоки Пэли в виде симметричных матриц Белевича преемственны матрицам Адамара, конструкция удвоения порядка сводится к процедуре Сильвестра с коррекцией нулевых элементов до единичных по модулю. Амплитуда коррекции в данном случае составляет единицу:

$$\mathbf{H}_n = \begin{pmatrix} \mathbf{C}_{n/2} + \mathbf{I} & -\mathbf{C}_{n/2} + \mathbf{I} \\ -\mathbf{C}_{n/2} + \mathbf{I} & -\mathbf{C}_{n/2} - \mathbf{I} \end{pmatrix}.$$

Очевидно, что разделение матрицы на блоки нечетных порядков дает большие возможности, поскольку способ Пэли не позволяет построить матрицу Адамара уже порядка 92.

Пробел в нарождающейся теории матриц Адамара восполнил Вильямсон, предложив к рассмотрению матрицу, названную позже массивом:

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

где **A**, **B**, **C**, **D** – матрицы Вильямсона [6], удовлетворяющие условию для матриц Адамара $\mathbf{A}^{\mathrm{T}}\mathbf{A} + \mathbf{B}^{\mathrm{T}}\mathbf{B} + \mathbf{C}^{\mathrm{T}}\mathbf{C} + \mathbf{D}^{\mathrm{T}}\mathbf{D} = n\mathbf{I}$.

В отличие от метода Пэли здесь не предлагается алгоритм определения элементов этих матриц, а в отличие от метода Белевича – отсутствует алгоритм коррекции элементов матриц. Обе эти рабочие идеи здесь неприложимы, матрицы Вильямсона **A**, **B**, **C** и **D** нечетных порядков ищутся перебором их элементов в рамках какого-либо ограничения на структуру. В частности, задача перебора резко упрощается, если блоки имеют теплицев или ганкелев характер, т. е. генерируются не матрицами, а векторами.

Трудоемкость такого подхода подтверждается тем, что вслед за первой найденной компьютером матрицей порядка $n = 92$ [7] матрица Адамара порядка $n = 428$ была найдена только в 2005 г. [1]. В обоих отмеченных случаях $(n - 1)$ представляет собой составное число. Комбинаторные методы перебора показали свою естественную ограниченность там, где структура недоопределена, а порядок матриц слишком велик.

Использование ортогональных матриц нечетных порядков

В работе [8] тема обобщения матриц Адамара на матрицы вдвое меньших, а также нечетных порядков получила свое продолжение исследованием матриц с ограниченным числом значений их элементов.

Определение 1. Значения целых, рациональных и иррациональных чисел, которым равны элементы матрицы, будем называть ее уровнями.

Введение уровней позволяет формировать графические портреты матриц, раскрашивая элементы различающихся уровней в разные цвета [9].

Например, портрет матрицы Адамара – двухцветный, а матриц Белевича – трехцветный.

Определение 2. Матрицей Мерсенна $\mathbf{M}_n$ порядка n с элементами $\{a, -b\}$ называется матрица, удовлетворяющая условию $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\mathbf{I}$, где $\mu = ((n + 1) + (n - 1)b^2)/2$ – весовой коэффициент, учитывающий, что $(n + 1)/2$ элементов каждого столбца $\mathbf{M}_n$ отрицательны. Элементы имеют значения $a = 1$, модули остальных элементов равны $b < a$. При $n = 3$ значение $b = 1/2$. В остальных случаях

$$b = \frac{q - \sqrt{4q}}{q - 4}, \qquad (2)$$

где q – порядок Адамара ($q = n + 1$).

Использование процедуры (1) удвоения порядков Сильвестра матрицы Мерсенна порождает матрицы четных порядков Эйлера [8], дополняющие (в ряду малоуровневых матриц с ортогональными столбцами) матрицы Белевича, если таковые не существуют. Таков, например, особый порядок 22 [10] и некоторые прочие: критерием существования матрицы Белевича является критерий Эйлера разложимости числа $(n - 1)$ на сумму двух квадратов и критерии, восходящие к нему, что дает название этому направлению.

Матрицы Пропус

В отличие от известных работ, в которых для удвоения порядка использовалась вычислительная схема Сильвестра, в настоящей работе показана продуктивность схемы Вильямсона

для модификации матриц Мерсенна и матриц Эйлера с учетверением их порядков. Модифицированный массив Вильямсона [11] перестановкой второй и третьей строк упрощается до блочно-симметричной модификации вида

$$\mathbf{W}_n = \begin{pmatrix} \mathbf{B} & \mathbf{A} & \mathbf{A} & \mathbf{A} \\ \mathbf{A} & \mathbf{A} & -\mathbf{B} & -\mathbf{A} \\ \mathbf{A} & -\mathbf{B} & -\mathbf{A} & \mathbf{A} \\ \mathbf{A} & -\mathbf{A} & \mathbf{A} & \mathbf{B} \end{pmatrix},$$

где в первом варианте используются матрицы Мерсенна $\mathbf{A} = \mathbf{M}_{n/4}$ с элементами $\{a, -a\}$ и $\mathbf{B} = \mathbf{M}_{n/4}$ с элементами $\{a, -b\}$, а во втором варианте – матрицы Эйлера $\mathbf{A} = \mathbf{E}_{n/4}$ с элементами $\{a, -a\}$ и $\mathbf{B} = \mathbf{E}_{n/4}$ с элементами $\{a, -a, b, -b\}$.

В отличие от переборного подхода такая задача заметно легче решается и дает значения уровней элементов двух матриц, порядок которых отличается на 4. Пропус (Propuse) – кратная звезда в созвездии Близнецов и подходящее название для матриц [12], порождаемых парами матриц Мерсенна (Пропус-М) или Эйлера (Пропус-Е).

Пропус-М. Уравнение связи уровней для матриц Мерсенна имеет вид

$$pb^2 - 2(p + 1)ab + (p - 2)a^2 = 0,$$

где $b = a$ при $n = 12$, и $b = (p + 1 - (4p + 1)^{1/2})a/p$, где $p = (n - 12)/16$, $n > 12$, n – порядок матрицы Вильямсона.

Пропус-Е. Уравнение связи уровней для матриц Эйлера имеет вид

$$(p - 1)b^2 - 2(p + 1)ab + (p - 5)a^2 = 0,$$

где $b = a$ при $n = 24$, и $b = (p + 1 - 2(2p + 1)^{1/2})a/(p - 1)$, где $p = (n - 8)/16$, $n > 24$, n – порядок матрицы Вильямсона.

Примеры портретов матриц Пропус-М и Пропус-Е порядков 12 и 24 приведены на рис. 1, где более светлый оттенок окраски элемента на портрете матрицы соответствует его положительному значению a, а значение $-b$ отображается более темным цветом.

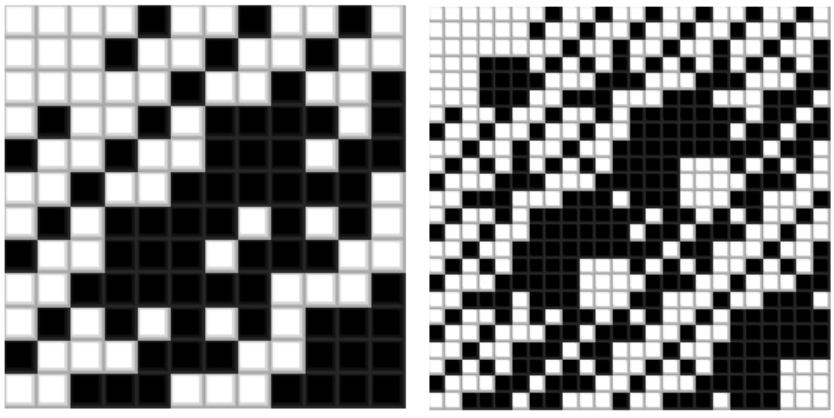

Рис. 1. Портреты матриц Пропус-М ($\mathbf{W}_{12}$) и Пропус-Е ($\mathbf{W}_{24}$)
Примечание: рисунок авторов.

На старте этого синтеза матрицы Мерсенна $\mathbf{M}_3$ и $\mathbf{M}_7$ порождают матрицу Адамара $\mathbf{W}_{12} = \mathbf{H}_{12}$ и отличную от матрицы Адамара матрицу $\mathbf{W}_{28}$, приведенную на рис. 2 с гистограммой ее элементов. Инверсия блоков матрицы Вильямсона повышает число отрицательных элементов $\{a, -a, b, -b\}$. Матрицы Эйлера $\mathbf{E}_2$ и $\mathbf{E}_6$ порождают их близнецов – матрицы Адамара $\mathbf{H}_8 = \mathbf{W}_8$, $\mathbf{H}_{24} = \mathbf{W}_{24}$.

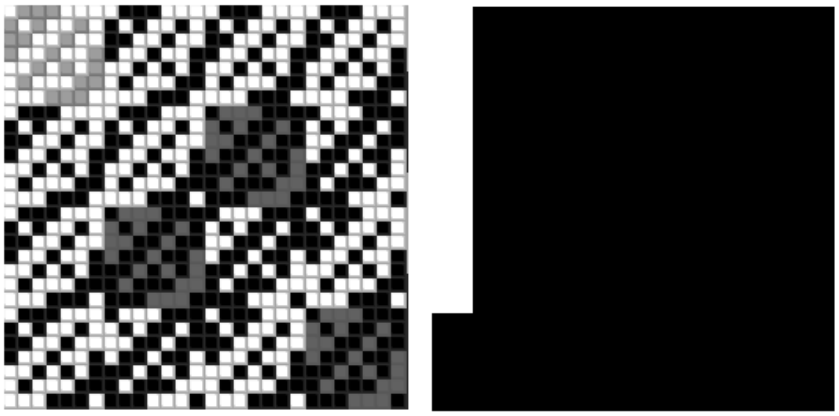

Рис. 2. Портрет матрицы Пропус-М (W_{28}) и гистограмма модулей ее элементов
Примечание: рисунок авторов.

Как видно, учетверение снижает количество блоков с плавающим значением уровня до 4, остальные элементы ортогональной матрицы такие же, как и у матриц Адамара.

На старте синтезируемые матрицы не отличаются от адамаровых, далее, с ростом порядка, элементы b и $-b$ стремятся к 1 и –1 соответственно. Иными словами, матрицы Мерсенна и Эйлера, используемые в качестве матриц Вильямсона, порождают аппроксимацию матриц Адамара.

Старшая ветвь матриц-близнецов

Матрицы Мерсенна интересны тем, что их порядок кратен значениям, вчетверо меньшим значений неизвестных сегодня матриц Адамара порядков 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964, ...

В отличие от неизвестных матриц Адамара, матрицы Мерсенна значительно легче найти. Например, для вычисления матрицы Пропус-М порядка 668 нужен блок порядка 167 (668/4), который является простым числом, и значит, матрица Мерсенна указанного порядка существует и представляет собой циклический блок, первая строка которого состоит из элементов a и $-b$.

В комбинаторной математике [1] позиции отрицательных элементов принято рассчитывать нахождением символов Лежандра или значений прогрессии, вычисляемых в конечном поле GF(167). Обе эти процедуры не требуют много компьютерного времени, поэтому ветвь матриц Пропус-М можно считать «старшей», аппроксимирующей неизвестные матрицы Адамара самых актуальных порядков. Несложно посчитать по приведенной выше формуле (2), что для матрицы W_{668} уровень $b = 0{,}711\ldots$. Для более высоких порядков он будет только повышаться. Матрицы Пропус-Е в такой терминологии являются матрицами «младшей» ветви.

Заключение

Зная матрицу Адамара порядка 664, нельзя найти матрицу порядка 668 (и наоборот). Эти матрицы различаются сложностью.

Матрицы-близнецы Пропус описывают ортогональные массивы, не теряющие между собой связанность. Это увеличивает количество находимых малоуровневых минимаксных ортогональных матриц.

Матрицы Пропус-Е получаются удвоением матриц Мерсенна, а добавление каймы превращает их снова в матрицы Мерсенна, но более высокого порядка. Следовательно, матрицы Пропус-Е ориентированы на поиск аппроксимаций матриц порядка, меньшего на 4. В частности, они позволяют найти модель Пропус-Е порядка 664.

Благодарность

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

Литература

1. Colbourn C., Dinitz J. Handbook of Combinatorial Designs, 2nd edition. Chapman and Hall/CRC, 2006. 1016 p.

2. Di Matteo O., Doković D. Z., Kotsireas I. S. Symmetric Hadamard Matrices of Order 116 and 172 Exist // Special Matrices. 2015. Vol. 3, No. 1. P. 227–234.

3. Сергеев А. М., Востриков А. А. Специальные матрицы: вычисление и применение. СПб. : Политехника, 2018. 112 с.

4. Horadam K. J. Hadamard Matrices and their Applications: Progress 2007–2010 // Cryptography and Communications. 2010. Vol. 2. P. 129–154.

5. Craigen R., Kharaghani H. Hadamard Matrices and Hadamard Designs // In Handbook of Combinatorial Designs. 2006. P. 273–280.

6. Doković D. Z. Williamson Matrices of Order 4n for n=33;35;39 // Discrete Mathematics. 1993. Vol. 115. P. 267–271.

7. Baumert L., Golomb S. W., Hall M. Jr. Discovery of an Hadamard Matrix of Order 92 // Bull Amer Math Soc. 1962. Vol. 68. P. 237–238.

8. Балонин Н. А., Сергеев М. Б. Нормы обобщенных матриц Адамара // Вестник СПбГУ. Сер. 10. 2014. Вып. 2. С. 5–11.

9. 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. P. 135–143. DOI 10.1007/978-981-13-8303-8_12.

10. Балонин Ю. Н., Сергеев М. Б. М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.

11. Балонин Н. А., Сергеев М. Б. Матрицы Пропус 92 и 116 // Информационно-управляющие системы. 2016. № 2. С. 101–103. DOI 10.15217/issn1684-8853.2016.2.101.

12. Balonin N. A., Doković D. Z., Mironovskiy L. A., Seberry J., Sergeev M. B. Hadamard-Type Matrices. URL: http://mathscinet.ru/catalogue/index.php (дата обращения: 30.08.2021).