О ДВУХ ПРЕДИКТОРАХ ВЫЧИСЛЯЕМЫХ ЦЕПОЧЕК КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

Н.А. БАЛОНИН, *доктор технических наук, профессор*
А.А. ВОСТРИКОВ, *кандидат технических наук, доцент*
Санкт-Петербургский государственный университет аэрокосмического приборостроения
ул. Большая Морская 67, Санкт-Петербург 190000, Россия
E-mail: korbendfs@mail.ru, vostrikov.anton@ask-lab.com

М.Б. СЕРГЕЕВ, *доктор технических наук, профессор*
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (ITMO University)
Кронверкский просп. 49, Санкт-Петербург 197101, Россия
E-mail: mbse@mail.ru

Рассмотрены общее определение квазиортогональных матриц, определение малоуровневых матриц и частные определения квазиортогональных матриц Мерсенна, Эйлера. Введено определение новых квазиортогональных симметричных матриц Зейделя, существующих на нечетных порядках, а также трехуровневых символов Лежандра, на основе которых элементы этих матриц вычисляются. Приведен метод вычисления матриц Эйлера по матрицам Мерсенна. Показана родственность асимметричных и симметричных матриц нечетных порядков Мерсенна и Зейделя. Предложен новый модифицированный метод Сильвестра вычисления матриц Эйлера по симметричным циклическим матрицам Зейделя.

Ключевые слова: квазиортогональные матрицы, матрицы Адамара, матрицы Белевича, матрицы Мерсенна, матрицы Эйлера, матрицы Зейделя, трехуровневые символы Лежандра, двуциклические матрицы

1. ВВЕДЕНИЕ

Практический интерес к ортогональным матрицам, какими являются матрицы Адамара (*Hadamard*) [1] обусловлен их основными свойствами, обеспечивающими им широкое применение в цифровых системах обработки информации [2].

Матрица Адамара – квадратная матрица $\mathbf{H}_n$ порядка n, состоящая из чисел {1, –1}, столбцы которой ортогональны $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\,\mathbf{I}$, где $\mathbf{I}$ – единичная матрица.

Во-первых, всего два целых значения элементов этих матриц обеспечивают эффективность матричных операций, как при аппаратной, так и программной реализациях. Во-вторых, ортогональность матриц дает возможность создания симметричных технических систем, поскольку для матрицы $\mathbf{H}_n$, используемой в прямом преобразовании, матрица для обратного преобразования находится простым ее транспонированием $\mathbf{H}_n^{-1} = \mathbf{H}_n^{\mathrm{T}}$. В-третьих, существующие ортогональные базисы включают симметричные, циклические, двуциклические и др. матрицы, значительно расширяющие возможности выбора оптимальной матрицы для решения конкретной задачи преобразования информации.

В теории кодирования, например, столбцы ортогональных матриц Адамара являются основой построения кодов с большим кодовым расстоянием [3]. Специальный порядок нумерации столбцов матриц Адамара в цифровой обработке сигналов, сжатии и маскировании изображений интерпретируется как двухуровневое представление широко используемых функций Уолша [4].

Ортогональные матрицы Адамара существуют на порядках $n = 4k$, где k – натуральное число, и могут вычисляться в виде цепочек на основе матриц предыдущих порядков $n/2$ по правилу Сильвестра [5], а также алгоритмами Пэли [6] и Скарпи [7].

В работе [8], посвященной описанию и классификации матриц семейства Адамара, сформулирована задача о нахождении двух тесно взаимосвязанных семейств квазиортогональных матриц Мерсенна [9] и Эйлера [10], близких по свойствам к матрицам Адамара, но отличающихся от них порядками и значениями элементов.

В работе [8] квазиортогональная матрица определена как квадратная матрица $\mathbf{A}_n$ порядка n с приведенными к единице максимумами модулей элементов каждого из столбцов, удовлетворяющая квадратичному условию связи

$$\mathbf{A}_n^{\mathrm{T}} \mathbf{A}_n = \omega(n)\, \mathbf{I}_n\,,$$

где $\mathbf{I}_n$ − единичная матрица, $\omega(n)$ − вес матрицы.

Вес $\omega(n) = 1$ характерен для ортогональных матриц, к которым квазиортогональные матрицы и, в частности, матрицы Адамара, помимо тривиальной матрицы первого порядка, не относятся [1]. Вместе с тем, эти матрицы весьма близки к ортогональным, получаемым из $\mathbf{A}_n$ нормированием их столбцов, после чего максимальный по модулю элемент (m-норма) уменьшается до m <1 для порядков $n > 1$.

Определение 1. Значения, которым равны элементы матрицы, будем называть ее уровнями. Например, матрица Адамара с элементами $\{1, -1\}$ имеет два уровня (двухуровневая), а матрица Белевича [11] с элементами $\{0, 1, -1\}$ – трехуровневая.

С учетом введенного *определения* квазиортогональными матрицами Мерсенна $\mathbf{M}_n$ называются двухуровневые матрицы порядков $n = 4k - 1$ со значениями элементов $\{1, -b\}$, где $|b|<1$, удовлетворяющие квадратичному условию связи

$$\mathbf{M}_n^{\mathrm{T}} \mathbf{M}_n = \omega(n)\, \mathbf{I}_n$$

с переменным весом $\omega(n) = \dfrac{(n+1)+(n-1)\,b^2}{2}$ [8, 9]. При $n = 3$ коэффициент $b = 1/2$, в остальных случаях $b = \dfrac{q+\sqrt{4q}}{q-4}$, где $q = n + 1$ – порядок соседствующей матрицы Адамара.

Название этих матриц связано с тем, что они обобщают вычисление квазиортогональных матриц Сильвестра [5] четных порядков $n = 2^k$ на нечетные значения порядков, равные числам Мерсенна $n = 2^k - 1$ [9].

Модульно двухуровневые матрицы порядков $n = 4k - 2$ [8, 10] с элементами $\{1, -1, b, -b\}$, где $|b| < 1$, удовлетворяющие квадратичному условию связи

$$\mathbf{E}_n^{\mathrm{T}}\,\mathbf{E}_n = \omega(n)\,\mathbf{I}_n$$

называются квазиортогональными матрицами Эйлера $\mathbf{E}_n$, для которых $\omega(n) = \dfrac{(n+2)+(n-2)b^2}{2}$.

Модульный уровень $b = 1/2$ при $n = 6$, в общем случае $b = \dfrac{q-\sqrt{8q}}{q-8}$, где $q = n + 2$ − порядок соседствующей матрицы Адамара.

Четырехуровневые матрицы Эйлера возникли как компромиссное замещение отсутствующих трехуровневых матриц Белевича, не существующих на порядках n, для которых число $n-1$ не разложимо на сумму двух квадратов целых чисел [12]. Критерий разложимости чисел основан на соответствующей теореме Эйлера, поэтому матрицы замещения получили соответствующее название.

В настоящей работе рассматривается правило вычисления матриц Мерсенна и Эйлера друг через друга, порождающее цепочки с взаимосвязанными их порядками. Такие цепочки значительно расширяют семейство матриц Адамара и являются механизмами упрощенного вычисления и хранения квазиортогональных матриц в симметричных системах обработки цифровой информации. Количество цепочек определяется стартовыми матрицами – предикторами, в качестве которых для двух уникальных цепочек матриц Мерсенна и Эйлера являются матрицы Зейделя.

2. ЦЕПОЧКИ КВАЗИОРТОГОНАЛЬНЫХ МАТРИЦ

Особенность взаимосвязи квазиортогональных матриц состоит в том, что по каждой матрице Мерсенна нечетного порядка можно построить матрицу Эйлера удвоенного четного порядка. На порядках $n = 1$ и $n = 2$ формы этих двух типов матриц не имеют развитых отличительных признаков, а, соответственно, не ясно, первична матрица Мерсенна или Эйлера. Нельзя утверждать, что матрицы Мерсенна являются предикторами матриц Эйлера, поскольку существует правило перехода от любой матрицы Эйлера $\mathbf{E}_n$ к матрице Мерсенна $\mathbf{M}_{n+1}$ на единицу большего значения порядка.

Типичная цепочка матриц Мерсенна и Эйлера выглядит как $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$. Цепочка таких последовательно вычисляемых матриц может начинаться и с матрицы Эйлера. В работах [9, 10] доказывается, что порядок матриц Эйлера четен и равен $n = 4k - 2$, здесь как и ранее k – натуральное число. Поэтому на основе матриц Мерсенна порядков $n = 4k - 1$, принимающих значения 3, 7, 11, 15… и отличающихся на 4 (характерный период для всех типов матриц семейства Адамара), строятся матрицы Эйлера порядков 6, 14, 30….

Таким образом, имеется неопределенность относительно нахождения матриц Эйлера, когда половинное значение их порядка не равно порядку матриц Мерсенна. Это характерно, например, для существующей матрицы $\mathbf{E}_{10}$ [13]. До сих пор в статьях при описании взаимосвязи матриц Мерсенна и Эйлера порождающая матрица для такого случая не определялась.

3. МАТРИЦЫ ЗЕЙДЕЛЯ

Помимо асимметричных циклических матриц Мерсенна порядков $n = 4k - 1$ введем в рассмотрение во многом похожие на них симметричные циклические матрицы Зейделя $\mathbf{S}_n$ порядков $n = -4k + 1$.

Определение 2. Квазиортогональными матрицами Зейделя $\mathbf{S}_n$ будем называть трехуровневые матрицы порядков $n = 4k + 1$ со значениями элементов $\{1, -b, d\}$, где $d < b < 1$, удовлетворяющие квадратичному условию связи

$$\mathbf{S}_n^{\mathrm{T}} \mathbf{S}_n = \omega(n)\, \mathbf{I}_n .$$

Здесь $\omega(n) = d + (n-1)\,\dfrac{1+b^2}{2}$ – переменный вес. Диагональные элементы матрицы $d = \dfrac{1}{1+\sqrt{n}}$, $b = 1 - 2d$.

Матрицы нечетных порядков Мерсенна и Зейделя объединяет то, что их можно рассматривать как результат ортогонализации столбцов асимметричных и симметричных матриц Якобсталя [6, 14, 15], получаемых из нормализованных матриц Белевича отрезанием их каймы. В теории графов усеченному типу матриц соответствуют целочисленные не ортогональные матрицы смежности графов Зейделя [16], отсюда и вводимое название соответствующих квазиортогональных матриц. При такой общности матриц Мерсенна и Зейделя они обе могут использоваться при расчете матриц Эйлера.

Матрицы Мерсенна и Зейделя имеют нечетный порядок и могут использоваться при вычислении четных двуциклических матриц Эйлера. В первом случае матрица Эйлера строится на основе асимметричных составляющих, во втором – симметричных.

4. ВЫЧИСЛЕНИЕ МАТРИЦ ЭЙЛЕРА НА ОСНОВЕ МАТРИЦ МЕРСЕННА И ЗЕЙДЕЛЯ

Матрицы Эйлера можно вычислить по правилу Сильвестра, общему для всех адамаровых матриц [6], по матрицам Мерсенна [8, 9] в виде

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & -\mathbf{M}_{n/2} \end{pmatrix},$$

где $\mathbf{M}_{n/2}$ – двухуровневая матрица Мерсенна.

В то же время матрицы Мерсенна связаны с матрицами Эйлера дополнением их строкой и столбцом (каймой) в виде [9, 14]

$$\mathbf{M}_{n+1} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{E}_n^* \end{pmatrix},$$

где $\lambda = -a$ – собственное число, а e – собственный вектор «сопряженной» матрицы $\mathbf{E}_n^* = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & \mathbf{M}_{n/2}^* \end{pmatrix}$, блок $\mathbf{M}_{n/2}^*$ получатся из $\mathbf{M}_{n/2}$ взаимной заменой элементов 1 и $-b$, и пересчетом уровня $b = \dfrac{q-\sqrt{4q}}{q-4}$, где $q = n + 2$ – порядок матрицы Адамара.

Содержательная сторона формул состоит в том, что матрицы Мерсенна и Эйлера рассчитываются на основе друг друга, образуя возрастающие по порядкам цепочки. Это обобщает правило Сильвестра – расчет возрастающих по порядку матриц Адамара [1, 5].

Теперь, пусть n − простое число, задающее порядок в виде $n = 4k + 1$. Это необходимое и достаточное условие существования [12, 14] трехуровневых квазиортогональных циклических матриц Зейделя $\mathbf{S}_n$ с элементами, равными трехуровневым символам Лежандра.

Определение 3. Трехуровневые символы Лежандра определим как $\chi\left(\frac{j-i}{n}\right) = \{1, -b, d\}$, вычисляемые через квадратичные вычеты по модулю n для разностей индексов i и j их строк и столбцов в матрице Зейделя порядка n. Здесь $d < b < 1$.

Напомним, что число a называется квадратичным вычетом по модулю n, если существует такое $x < n$, что $a = x^2 \pmod n$ [17]. Тогда, для $i = j$ полагаем $\chi\left(\frac{0}{n}\right) = d = \frac{1}{1+\sqrt{n}}$, а для $i \neq j$ полагаем $\chi\left(\frac{i-j}{n}\right) = 1$, если $i - j$ есть квадратичный вычет по модулю n и $\chi\left(\frac{i-j}{n}\right) = -b = 2d - 1$, в противном случае. Число d равно значениям диагональных элементов матрицы Зейделя.

Построим, например, квазиортогональную матрицу Зейделя пятого порядка $\mathbf{S}_5$ на основе символов Лежандра для набора чисел {0, 1, 2, 3, 4}, равных разностям индексов элементов первой строки матрицы. Их квадраты по mod5 равны {0, 1, 4, 4, 1}. Этому множеству принадлежат числа 1 и 4 – они являются квадратичными вычетами. Числа 2 и 3 квадратичными вычетами не являются. При этом значения диагональных элементов $d = \frac{1}{1+\sqrt{5}} \cong 0{,}309$, а $b = 1 - 2d \cong 0{,}382$.

Циклическая матрица Зейделя $\mathbf{S}_5$ строится по последовательности $\{d, 1, -b, -b, 1\}$, а сопряженная к ней матрица $\mathbf{S}_5^*$ – по последовательности $\{d, -b, 1, 1, -b\}$ парных символов Лежандра, с заменой 1 и $-b$ на $-b$ и 1, соответственно. В итоге имеем

$$\mathbf{S}_5 = \begin{pmatrix} d & 1 & -b & -b & 1 \\ 1 & d & 1 & -b & -b \\ -b & 1 & d & 1 & -b \\ -b & -b & 1 & d & 1 \\ 1 & -b & -b & 1 & d \end{pmatrix}, \quad \mathbf{S}_5^* = \begin{pmatrix} d & -b & 1 & 1 & -b \\ -b & d & -b & 1 & 1 \\ 1 & -b & d & -b & 1 \\ 1 & 1 & -b & d & -b \\ -b & 1 & 1 & -b & d \end{pmatrix}.$$

Стоит отметить, что на диагонали обоих матриц размещены числа d вдвое меньшие значения золотого сечения: $2d = 1/\psi = 0{,}618$, где $\psi = 1{,}618$. Разница между максимумом элемента (единица) и b в точности равно золотому сечению. Поэтому матрица Зейделя $\mathbf{S}_5$ может быть отнесена к разновидности квазиортогональных матриц золотого сечения [13].

Двуциклическая матрица Эйлера вычисляется по паре исходной и сопряженной матриц Зейделя согласно модифицированному правилу Сильвестра [14]

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{S}_{n/2} & \mathbf{S}_{n/2}^* \\ \mathbf{S}_{n/2}^* & -\mathbf{S}_{n/2} \end{pmatrix},$$

с учетом коррекции их элементов до значений соответствующих им элементов матрицы Эйлера: $b = 1/2$ при $n = 6$, иначе $b = \frac{q-\sqrt{8q}}{q-8}$, где $q = n + 2$ − порядок соседствующей матрицы Адамара. Модули диагональных элементов взаимно сопряженных блоков принимают значение 1. На рис.1 приведены портреты матрицы Зейделя пятого порядка и вычисленной по ней матрицы Эйлера десятого порядка. Здесь и далее белый квадрат портрета матрицы соответствует 1, черный – элементу –1 (или $-b$ у матрицы Зейделя). Остальные промежуточные по значениям элементы показаны оттенками серого.

Приведенное модифицированное правило Сильвестра обобщает правило Пэли вычисления матриц Адамара по матрицам Белевича, опираясь на взаимно однозначную связь матриц Адамара, Мерсенна и Эйлера.

Циклическое ядро нормализованных матриц Белевича и таблица смежности графов Зейделя [16] строится на основе округленной целочисленной последовательности $\{0, 1, -1, -1, 1\}$, самостоятельной ортогональности и связи с иррациональными числами такие массивы не имеют, хотя косвенно содержат их. Отсюда можно сформулировать формальное правило перехода от матриц Белевича к квазиортогональным матрицам Зейделя путем отрезания каймы и пересчета диагонального и отрицательных элементов матрицы с целью ее ортогонализации. Это правило может использоваться для вычисления блочных циклических матриц.

Кроме того, блочная циклическая матрица $\mathbf{S}_9$ вычисляется с помощью кронекерова произведения двух матриц $\mathbf{M}_3$ и является основой вычисления блочной матрицы Эйлера $\mathbf{E}_{18}$ (рис.2).

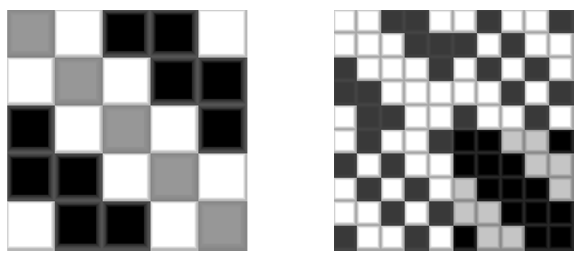

Рис.1. Портреты матриц Зейделя $\mathbf{S}_5$ и Эйлера $\mathbf{E}_{10}$.

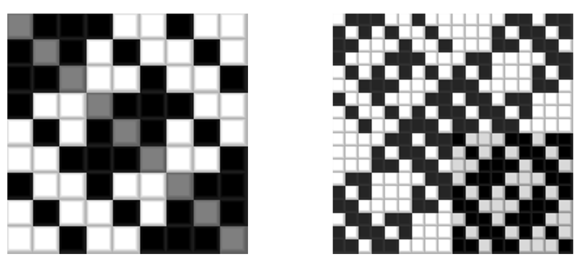

Рис.2. Портреты блочных матриц Зейделя $\mathbf{S}_9$ и Эйлера $\mathbf{E}_{18}$.

5. ЗАКЛЮЧЕНИЕ

Описанный способ вычисления квазиортогональных матриц Эйлера на основе матриц Зейделя позволяет дополнить цепочку матриц вида $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$ цепочкой исключения $\mathbf{S}_5 - \mathbf{E}_{10} - \mathbf{M}_{11} - \mathbf{E}_{22} - \mathbf{M}_{21} - \ldots$ с вычислением матриц $\mathbf{E}_{10}$ и, в перспективе, $\mathbf{E}_{22}$, замещающей несуществующую трехуровневую матрицу Белевича, а также цепочку $\mathbf{S}_9 - \mathbf{E}_{18} - \mathbf{M}_{19} - \mathbf{E}_{38} - \mathbf{M}_{39} - \ldots$ на основе отмеченной выше блочной матрицы $\mathbf{S}_9$, хотя число 9 не простое и является четной степенью числа 3. Соответственно, блочные матрицы Якобсталя, Белевича и Зейделя существуют и строятся на обобщенных символах Лежандра для блоков размера 3.

Рассмотренный материал позволяет в научном плане существенно расширить направление исследований условий разрешимости циклических структур на одно- и двуциклические конструкции с двумя разрешенными значениями модульных уровней элементов матриц семейства Адамара. В практическом – дает возможность существенного упрощения процесса вычисления и хранения и механизма выбора матриц различных порядков для алгоритмов обработки цифровых данных.

СПИСОК ЛИТЕРАТУРЫ

[1] *Hadamard J.* Résolution d'une question relative aux determinants//Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.

[2] *Horadam K.J.* Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ, 2007.

[3] *Shalom E*. La conjecture de Hadamard (I) – Images des Mathématiques // CNRS. 2012. http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (accessed: 15.01.2015).

[4] *Walsh J.L.* A closed set of normal orthogonal functions. Amer. J. Math. 1923. V. 45. P. 5–24.

[5] *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. Vol. 34. P. 461–475.

[6] *Paley R.E. A.C.* On orthogonal matrices //J. of Mathematics and Physics. 1933. Vol.12. P.311-320.

[7] *Scarpis U.* Sui determinanti di valore massimo, Rendiconti della R. Istituto Lombardo di Scienze e Lettere 31 (1898). P. 1441–1446.

[8] *Сергеев А.М.* Обобщенные матрицы Мерсенна и гипотеза Балонина // Автоматика и вычислительная техника. 2014. № 4. С. 35–43.

[9] *Балонин Н.А., Сергеев М.Б., Мироновский Л.А*. Вычисление матриц Адамара - Мерсенна // Информационно-управляющие системы. 2012. № 5(60). С. 92–94.

[10] *Балонин Н.А., Сергеев М.Б.* О двух способах построения матриц Адамара - Эйлера // Информационно-управляющие системы. 2013. № 1(62). С. 7–10.

[11] *Belevitch V.* Theorem of 2n-terminal networks with application to conference telephony //Electr. Commun. 1950. Vol. 26. P. 231–244.

[12] *Балонин Н.А., Сергеев М.Б.* К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.

[13] *Балонин Н.А., Сергеев М.Б.* Матрица золотого сечения G_{10} // Информационно-управляющие системы. 2013. № 6(67). С. 2–5.

[14] *Balonin N., Sergeev M*. Quasi-orthogonal local maximum determinant matrices. Applied Mathematical Sciences, Vol. 9, 2015, no. 6, pp. 285-293. DOI 10.12988/ams.2015.4111000.

[15] *Gilman R.E.* On the Hadamard determinant theorem and orthogonal determinants //Bulletin Amer. Math. Soc. 37. 1931. P. 30–31.

[16] *Seidel J.J.* Strongly Regular Graphs with (–1,1,0) Adjacency Matrix Having Eigenvalue 3 //Lin. Alg. Appl. 1968. Vol. 1. P. 281–298.

[17] *Бухштаб А.А*. Теория чисел. – М.: Просвещение, 1966.

Рукопись получена 14.07.2014,
финальная версия – 24.03.2015.