УДК 519.614

О ДВУХ СПОСОБАХ ПОСТРОЕНИЯ МАТРИЦ АДАМАРА — ЭЙЛЕРА

Н. А. Балонин,
доктор техн. наук, профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения
М. Б. Сергеев,
доктор техн. наук, профессор, директор
НИИ информационно-управляющих систем Национального исследовательского университета информационных технологий, механики и оптики, г. Санкт-Петербург

Дается определение обобщенных матриц Адамара — Эйлера, рассмотрены их свойства, описаны алгоритмы их построения, приведены числовые примеры.

Ключевые слова *— ортогональные матрицы, матрицы Адамара, матрицы Белевича, числа Мерсенна, числа Ферма.*

Введение

В теории обработки и передачи информации широко используются ортогональные базисы преобразований с матрицами Адамара и сходными с ними [1]. Такие матрицы существуют не для всех порядков, что в значительной степени сужает возможности по выбору наиболее удачного базиса в ряде применений.

В работах [2, 3] вводятся базовые понятия и освещаются алгоритмы вычислений обобщенных матриц Адамара (М-матриц) на случай значений порядков, равных числам Ферма и Мерсенна, принадлежащих подмножествам нечетных чисел $n = 4k + 1$ и $n = 4k + 3$ соответственно. В случае четных порядков $n = 4k + 2$ не существующие на них матрицы Адамара дополняются матрицами Белевича [4].

Напомним, что матрица Адамара — квадратная двухуровневая 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.

Матрица Белевича (C-matrix, conference-matrix) — квадратная трехуровневая матрица $\mathbf{C}_n$ порядка n, состоящая из чисел {1, 0, –1}, столбцы которой ортогональны:

$$\tilde{\mathbf{N}}_n^{\mathrm{T}}\tilde{\mathbf{N}}_n = (n-1)\mathbf{I},$$

а нулевые элементы сосредоточены на диагонали.

Определение 1. Значения, которым равны элементы матрицы, будем называть ее уровнями. Значения уровней позволяют раскрашивать графические портреты матриц в разные цвета, и, соответственно, можно говорить не только об уровневости матрицы, но и о ее цветности.

■ *Леонард Эйлер* (4 апреля 1707 — 7 сентября 1783). Великий математик, автор более чем 800 работ по математическому анализу, дифференциальной геометрии, теории чисел, приближенным вычислениям, небесной механике, математической физике, оптике, баллистике, кораблестроению, теории музыки и др.

Например, матрица Адамара — двухцветная, а Белевича — трехцветная.

Согласно гипотезе Адамара, порядок матриц Адамара кратен четырем. Они превосходят матрицы Белевича по критерию минимума максимума абсолютных значений элементов, назовем этот признак m-нормой. Трехуровневые матрицы Белевича, помимо того, существуют для значений порядков $n = 4k + 2$, но, в свою очередь, необходимое условие их существования регламентирует критерий Эйлера о разложимости величины $n - 1$ на сумму двух квадратов. Матриц такого вида для значений порядков 22, 34, 58 и т. п. не существует. Это делает актуальным рассмотрение четырехуровневых замещений матриц Белевича, которые назовем, в свою очередь, матрицами Адамара — Эйлера.

Определение 2. Матрица Адамара — Эйлера — это квадратная матрица $\mathbf{E}_n$ порядка n, состоящая из чисел $\{a = 1, -a, b, -b\}$, столбцы которой ортогональны:

$$\mathbf{E}_n^{\mathrm{T}}\mathbf{E}_n = \xi\mathbf{I},$$

где $b = \frac{1}{2}$ при $n = 6$, в остальных случаях $b = \frac{q-\sqrt{8q}}{q-8}$, $q = n + 2$ (порядок матрицы Адамара); вес $\xi = \frac{(n+2)+(n-2)b^2}{2}$ учитывает, что $\frac{q}{2}$ модулей элементов каждого столбца такой матрицы имеют значения $a = 1$, модули остальных элементов равны $b < 1$.

Алгоритмы построения матриц Адамара — Эйлера

Положение 1. Матрицы Адамара — Эйлера строятся на основе формулы Сильвестра

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

где $\mathbf{M}_{n/2}$ — двухуровневая матрица Адамара — Мерсенна [2] вдвое меньшего нечетного порядка, состоящая из чисел $\{a = 1, -b\}$ с пересчетом их уровня так, что $b = \frac{1}{2}$ при $n = 6$, в остальных случаях $b = \frac{q-\sqrt{8q}}{q-8}$, $q = n + 2$. Отсюда следует, что при этом преобразовании число уровней ввиду инверсии двухуровневой матрицы Адамара — Мерсенна удваивается.

Техника построения матриц Адамара — Эйлера наследует способ построения матриц Адамара удвоением порядка соответствующих им матриц Белевича с последующим преобразованием нулевых элементов в единичные по модулю. В обоих случаях дополнительным ресурсом для ортогонализации матриц выступает изменение варьируемого элемента. Помимо того, это матрицы, оптимальные по m-норме в рамках заявленной уровневой структуры, т. е. М-матрицы.

Сохраняется важное свойство обобщенных матриц — наследование структуры матриц Адамара, поскольку с ростом порядка модуль малоуровневых элементов b стремится к 1. Выделенный класс четырехуровневых М-матриц интересен тем, что они сосуществуют с матрицами Белевича на одних и тех же порядках, уступая последним по m-норме. Однако, как и в случае с матрицами Белевича по отношению к матрицам Адамара, значениям их элементов отведено на один уровень больше. Соответственно, условия их существования менее жесткие. Они дополняют матрицы Белевича тогда, когда последние не существуют. Это побочный продукт вычисления матриц Адамара — Мерсенна, более полно раскрывающий содержание гипотезы Адамара о существовании всех матриц порядка $4k$ (это относится и к матрицам Эйлера порядков $4k + 2$).

Пример 1. Последовательность чисел Мерсенна, задаваемая формулой $n = 2^k - 1$, начинается с чисел 1, 3, 5, 15, 31, ... и принадлежит подмножеству чисел вида $4k - 1$. Матрица Адамара — Мерсенна третьего порядка имеет вид

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix}.$$

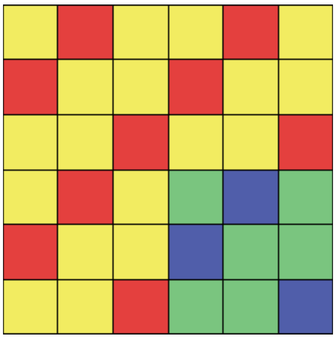
Соответственно, матрица Адамара — Эйлера

$$\mathbf{E}_6 = \begin{pmatrix} a & -b & a & a & -b & a \\ -b & a & a & -b & a & a \\ a & a & -b & a & a & -b \\ a & -b & a & -a & b & -a \\ -b & a & a & b & -a & -a \\ a & a & -b & -a & -a & b \end{pmatrix},$$

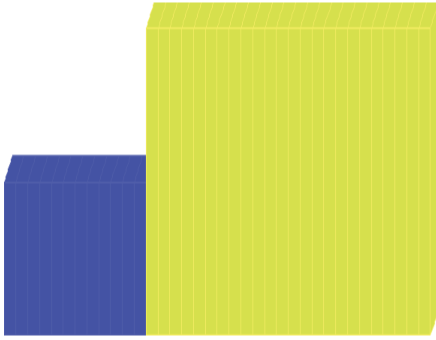
где $a = 1$; $b = 0{,}5$. Портрет и гистограмма модулей элементов приведены на рис. 1 и 2, где желтый и зеленый цвета соответствуют значениям элементов $\{1, -1\}$, синий и красный — элементов $\{0{,}5; -0{,}5\}$.

Более актуально, конечно, рассмотреть тот порядок, для которого С-матрицы найти нельзя. Первый такой случай соответствует порядку $n = 22$. Поскольку $n - 1 = 7 \times 3$ (эти множители свидетельствуют о неразложимости числа 21 на сумму двух квадратов), матрица Белевича $\mathbf{C}_{22}$ не существует.

Пример 2. Вычисление матрицы Адамара — Эйлера $\mathbf{E}_{22}$ основывается на вычислении двухуровневой матрицы $\mathbf{M}_{11}$, порядок которой отличается от чисел Адамара — Мерсенна, но это пре-



■ *Рис. 1.* Портрет матрицы $\mathbf{E}_6$



■ *Рис. 2.* Гистограмма модулей элементов $\mathbf{E}_6$

пятствует всего лишь применению модифицированной версии итерационного алгоритма Сильвестра [1]. Матрица $\mathbf{M}_{11}$, как и указанная выше матрица $\mathbf{M}_3$, является стартовой (для этого алгоритма) и вычисляется применением более универсальной процедуры оптимизации ортогональных матриц по m-норме, описанной в работе [5]. Двухцветный и четырехцветный портреты матриц $\mathbf{M}_{11}$ и $\mathbf{E}_{22}$ (двух- и четырехуровневых), полученных таким способом, показаны на рис. 3 и 4.

Следует подчеркнуть, что свойства матриц буквально дозируются симметрией и числом разрешенных уровней. На 22-м порядке найдена М-матрица [6], имеющая существенные прикладное и теоретическое значения. Она асимметрична, и диаграмма модулей ее элементов имеет 6 уровней, не достигая нижним из них нуля. Ее m-норма ниже, чем у матриц Адамара — Эйлера. В данной работе речь идет о принципиальной возможности ограничиться минимально необходимым числом уровней, которое у матриц Адамара — Эйлера, согласно способу их построения, равно четырем. Преимущество это сохраняется при всех возможных порядках $n = 4k + 2$, поэтому эти матрицы завершают построение малоуровневых ортогональных базисов.

Положение 2. Матрицы Адамара — Эйлера связаны, в свою очередь, с матрицами Адамара — Мерсенна, последние образованы дополнением их строкой и столбцом (каймой) в виде

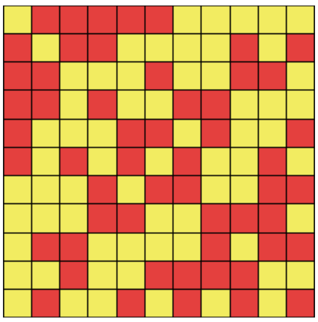
$$\mathbf{M}_{n+1} = \begin{pmatrix} -\lambda & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{E}^*_{2n} \end{pmatrix},$$

где $\lambda = -a$ — собственное число, а $\mathbf{e}$ — собственный вектор «сопряженной» матрицы $\mathbf{E}^*_{2n} = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & \mathbf{M}^*_{n/2} \end{pmatrix}$, $\mathbf{M}^*_{n/2}$ получается из матрицы Мерсенна соответствующего порядка взаимной заменой элементов $a = 1$ и $-b$ с пересчетом при $n > 3$ уровня $b = \dfrac{q-\sqrt{4q}}{q-4}$, $q = n + 1$ (порядок матрицы Адамара).

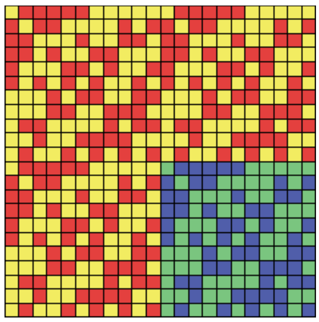
Пример 3. Используем матрицу Адамара — Эйлера $\mathbf{E}_{22}$ для вычисления двухуровневой матрицы Адамара — Мерсенна $\mathbf{M}_{23}$ (рис. 5).

В теории матриц Адамара роль, сходную с матрицей Адамара — Эйлера, играет теплицева матрица символов Лежандра, называемая матрицей Якобсталя. Это обобщение конструкции Пэли, широко используемой при построении матриц Белевича и Адамара на основе теории квадратичных вычетов, учитывающее неравновесность значений положительного $a = 1$ и отрицательного $-b$ уровней элементов матрицы четного порядка с ортогональными столбцами.

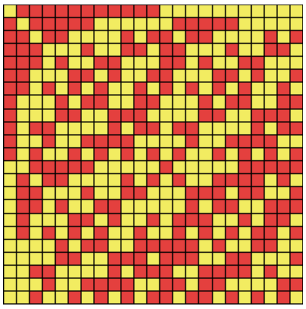
В пределах отмеченной структуры матриц Адамара — Эйлера существует еще одна претендентная матрица с элементом $b = \dfrac{q+\sqrt{8q}}{q-8}$ таким,



■ *Рис. 3.* Портрет матрицы $\mathbf{M}_{11}$



■ *Рис. 4.* Портрет матрицы $\mathbf{E}_{22}$



■ *Рис. 5*. Портрет матрицы $\mathbf{M}_{23}$

что $b > a$ (по сути, речь идет о взаимной замене параметров a, b местами). Данная матрица отвечает второму корню характеристического уравнения, следующего из условия ортогональности. Однако она существенно уступает по критерию минимума m-нормы основной матрице. Это частное решение может представлять некоторый самостоятельный интерес при построении общей теории М-матриц.

Заключение

В процессе поиска ортогональных матриц четных порядков, близких по своим свойствам к матрицам Адамара и замещающих не всегда существующие С-матрицы, удалось выделить в классе малоуровневых М-матриц [5] матрицы, названные обобщенными матрицами Адамара — Эйлера. Это увеличивает количество минимаксных ортогональных матриц, рассмотренных в работах [2, 3, 7].

На конкретных примерах показано, что матрицы Адамара — Мерсенна старших порядков могут быть получены двояко. Во-первых, обычным ходом модифицированного алгоритма Сильвестра, дающим, например, переход от $\mathbf{M}_{11}$ к $\mathbf{M}_{23}$, минуя актуальный 22-й порядок. Во-вторых, разделенным на стадии процессом с получением промежуточной матрицы $\mathbf{E}_{22}$. Отсюда следует, что условия ортогонализации матриц Адамара — Эйлера заведомо менее жесткие, чем у С-матриц Белевича, и, соответственно, они вычислимы тогда, когда требуемых критерием Эйлера предпосылок для существования матриц Белевича нет. При этом новые матрицы регламентируют структуру матриц справа от них, т. е. матриц Адамара — Мерсенна и Адамара включительно.

Хотя для разрешимости задачи ортогонализации на порядках $4k + 2$ значение уровней матриц Адамара — Эйлера равно четырем, число градаций их абсолютных значений всего на 1 больше, чем у матриц Адамара. В этом они родственны обобщаемым матрицам, вариация идет не столько за счет разнообразия уровней, сколько за счет выбора знаков. Проведенное исследование создает предпосылки к доказательству гипотезы Адамара [8] через рассмотрение вопроса о существовании матриц Адамара — Эйлера и Адамара — Мерсенна. Отмеченные закономерности не только расширяют понимание сложной проблемы, уходящей корнями в теорию чисел и теорию ортогональных базисов, но имеют и самостоятельное значение для теории обработки информации и моделирования.

Литература

1. **Мироновский Л. А., Слаев В. А.** Стрип-метод преобразования изображений и сигналов: монография. — СПб.: Политехника, 2006. — 163 с.
2. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92–94.
3. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Ферма // Информационно-управляющие системы. 2012. № 6. С. 90–93.
4. **Belevitch V.** Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
5. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14–21.
6. **Балонин Ю. Н., Сергеев М. Б.** М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
7. **Балонин Н. А., Мироновский Л. А.** Матрицы Адамара нечетного порядка // Информационно-управляющие системы. 2006. № 3(22). С. 46–50.
8. **Hadamard J.** Résolution d'une question relative aux determinants // Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.