УДК 519.61:511-33
doi:10.15217/issn1684-8853.2017.1.2

РАСШИРЕНИЕ ГИПОТЕЗЫ РАЙЗЕРА НА ДВУЦИКЛИЧЕСКИЕ СТРУКТУРЫ И РАЗРЕШИМОСТЬ МАТРИЦ АДАМАРА ОРНАМЕНТОМ В ВИДЕ БИЦИКЛА С ДВОЙНОЙ КАЙМОЙ

Н. А. Балонин[a], *доктор техн. наук, профессор*
М. Б. Сергеев[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Цель: *расширить границу предельных порядков гипотезы Райзера с циклических на бициклические квазиортогональные матрицы с двумя значениями элементов (уровней), исследовать разрешимость бициклических структур с одной и двумя каймами на известные типы ортогональных по столбцам (строкам) матриц.* ***Результаты:*** *показано, что ортогональные вещественные бициклы Эйлера с уровнями $a = 1, -b$, где $b = \frac{t}{t+\sqrt{2t}}$, существуют для всех значений $n = 4t - 2$ и с добавлением каймы переходят через промежуточную стадию вещественных матриц Мерсенна в целочисленные матрицы Адамара, определяя тем самым структуру матриц минимальной сложности, разрешимую для всех возможных для них порядков. Иными словами, гипотеза Адамара (хорошо известная своей недоказуемостью некомбинаторными методами) доказана при исследовании закономерностей «матричных переходов» от вещественных (не ограниченных запретом иметь иррациональные элементы) типов матриц к целочисленным матрицам Адамара с элементами 1, –1. Представлено родство матриц максимума детерминанта порядков $n = 4t - 2$ ортогональным бициклам с тем существенным отличием от матриц Эйлера, что их бициклическая структура так же, как бициклическая структура матриц Адамара, разрешима на отведенных им порядках не всегда. Произведены оценки границ симметрии различных семейств бициклических матриц максимального детерминанта, включая матрицы Адамара.* ***Практическая значимость:*** *алгоритмы нахождения бициклических матриц использованы при построении поискового программного комплекса. Субоптимальные по детерминанту матрицы составляют основу фильтров Эйлера и Мерсенна, применяемых для сжатия и маскирования изображений.*

Ключевые слова *— ортогональные матрицы, циклические матрицы, бициклические матрицы, гипотеза Райзера, гипотеза Адамара, матрицы Адамара, матрицы Мерсенна, матрицы Эйлера.*

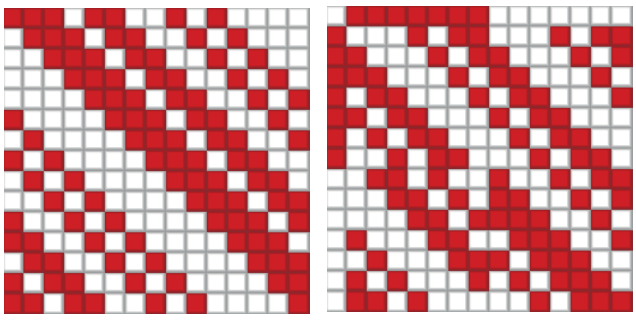
Введение

В теории финитных динамических систем [1], теории ортогональных матриц [2] часто рассматриваются теплицевы или ганкелевы формы, способствующие упрощению анализа. Их разновидность — циклические и бициклические матрицы с малым количеством значений их элементов (уровней) — объединяет в себе черты орнаментов (узоров) портретов матриц и собственно самих матриц.

Семейство орнаментов квадратных матриц с двумя значениями элементов описывается тремя инвариантами $\{n, k, \lambda\}$, где n — порядок матрицы, характеризующий величину узора; k — количество одинаковых элементов каждой строки и столбца; λ — количество одинаковых элементов, имеющих одну и ту же позицию в каждой паре строк или столбцов.

В качестве примера семейства на рис. 1 показаны две матрицы Мерсенна [3] порядка 15 с инвариантами {15, 7, 3}, каждая имеет по семь одинаковых клеток в каждой строке и столбце и по три — в каждой паре строк или столбцов (клетки иного цвета соответствуют параметрам некоторого зависимого дизайна).

Длительное время считалось, что циклические структуры (матрица слева на рис. 1) могут быть ортогональными матрицами с вещественными элементами только для простых порядков, пока не были обнаружены контрпримеры на составных порядках со значениями 15, 35 и 63. Первые два [4] образованы произведениями пар



■ ***Рис. 1.*** Два {15, 7, 3}-орнамента матриц Мерсенна

близких простых чисел 3, 5 и 5, 7. Порядок 63 входит в семейство чисел Мерсенна $2^k - 1$, которые образуют особое представительство в пределах $4t - 1$.

В настоящей работе рассматриваются задачи, связанные с изучением различных типов орнаментов матриц, определяющих возможность построения ортогональных массивов.

Квадратичные уравнения орнаментов

Порядок матрицы ограничивает возможные сочетания инвариантов $\{n, k, \lambda\}$, поскольку не все орнаменты реальны в рамках квадратной структуры. Реализуемые параметры [2] связывает квадратичное *диофантово уравнение* I вида

$$k(k - 1) = \lambda(n - 1).$$

Второе столь же общее матричное квадратичное уравнение $\mathbf{A}^T\mathbf{A} = \omega\mathbf{I}$, где ω — вес матрицы, а $\mathbf{I}$ — единичная матрица, отражает условие ортогональности столбцов матрицы. Для матриц с двумя элементами a, $-b$ (матрица с положительными элементами не может быть ортогональной) скалярное произведение любых двух строк, отличающихся индексами, содержит λ произведений вида a^2, $2(k - \lambda)$ произведений ab ($k - \lambda$ элементов a каждой из строк умножено на b) и $n - 2k + \lambda$ произведений b^2. Отсюда следует квадратичное *характеристическое уравнение* II ортогонального дизайна

$$(n - 2k + \lambda)b^2 - 2(k - \lambda)ab + \lambda a^2 = 0, \qquad (1)$$

записанное в виде, удобном для поиска корней при превалировании количеств положительных элементов над отрицательными. Для матриц с целыми элементами a, $-b$ оно дает квадратичное *диофантово уравнение* II.

Связь дискретных и непрерывных задач

Не следует думать, что квадратичное уравнение (1) касается поиска только ортогональных матриц. Оно возникает и в том случае, когда искомую неортогональную матрицу обязательно сопровождает ортогональная.

Значения параметров a, $-b$ инвариантами орнамента не фиксированы. Поэтому для его поиска важно лишь то, что ортогональная матрица существует и является необходимым условием решаемой задачи.

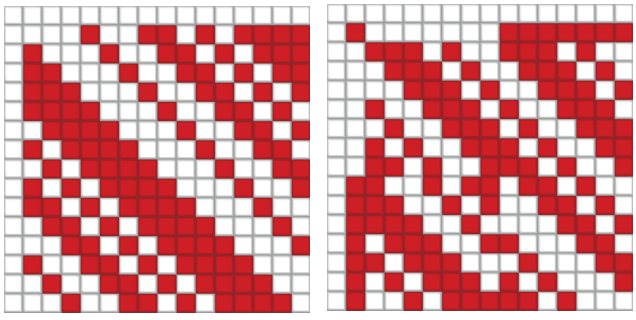
Среди матриц с элементами 1, –1 наиболее известны неортогональные матрицы *максимума детерминанта* [2] и ортогональные по столбцам (строкам) матрицы Адамара [5, 6] с весом $\omega = n$. Орнаменты первых отличаются лишь тем, что у матрицы Адамара свойства иметь 1, –1 и быть ортогональными совмещены в одной матрице, а у матриц максимума детерминанта ортогональность достигается параметрическим изменением уровней до некоторых фиксированных ортогональностью значений. Важным случаем является вариант ортогонализации матрицы без изменения количества уровней a, $-b$.

Это отчасти напоминает логику привлечения комплексных чисел для поиска вещественных корней полиномов. Вместо матрицы максимума детерминанта с элементами 1, –1, оказывается, можно искать ортогональную матрицу локального максимума детерминанта с вещественными рациональными или даже иррациональными элементами a, $-b$, а затем округлением до целых 1, –1 находить итоговое решение, так как орнамент у них один. Этот путь, через обращение к вещественным матрицам, не видят те, кто занят сугубо комбинаторным исследованием задачи.

Добавим, что изменение параметров a, $-b$ важное, но не единственное средство обратного перехода к целочисленной задаче.

В теории матриц Адамара [2, 6] структуру (орнамент), описываемую тремя инвариантами, как правило, имеет не сама матрица, а ее блок или блоки, в частности, основа (core) нормализованной матрицы с каймой в виде первой строки и столбца из 1. Лишенная каймы и инвертированная по знаку основа с элементами 1, –1 не ортогональна, но ортогональность ее столбцам и строкам можно вернуть изменением элементов a, $-b$. На рис. 2 показаны две матрицы Адамара, неортогональные внутренние блоки которых (при инверсии знаков) отвечают двум показанным на рис. 1 орнаментам {15, 7, 3} вещественных ортогональных по столбцам (и строкам) матриц Мерсенна.

Следовательно, узор неортогональных целочисленных блоков такой матрицы должен удовлетворять обоим квадратичным уравнениям, указанным выше.



■ ***Рис. 2.*** Две матрицы Адамара с блоками из матриц Мерсенна

Циклические и бициклические орнаменты матриц

Погружение задачи теории целочисленных матриц в более широкую область матриц с рациональными или иррациональными коэффициентами открывает дополнительные возможности. Например, итерациями можно проводить поиск значений вещественных элементов. Рассмотрим типичные структуры.

Циклическая матрица (моноцикл) — это регулярная структура, образуемая сдвигом верхней строки вправо с размещением вытесняемых элементов слева. В данном случае λ описывает количество близких пар отрицательных элементов строки, причем первый и последний элементы рассматриваются как соседствующие.

Бициклическая матрица (бицикл) $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$ образована двумя циклическими матрицами **A**, **B** с параметрами $\{v,\ k_1,\ \lambda_1\}$, $\{v,\ k_2,\ \lambda_2\}$. Нижняя часть узора зависима, ортогональность блоков нас, как правило, не интересует, поэтому для описания орнамента достаточно четырех параметров $\{n = 2v;\ k_1,\ k_2;\ \lambda\}$, где $\lambda = \lambda_1 + \lambda_2$.

Диофантово уравнение I бицикла имеет вид $k_1(k_1 - 1) + k_2(k_2 - 1) = \lambda(v - 1)$. Заменой переменных $x = p - k_1,\ y = p - k_2$ при $p = k_1 + k_2 - \lambda$ оно сводится к уравнению окружности

$$x^2 + y^2 = p + \lambda(v - 2p), \qquad (2)$$

решаемому в целых числах. Характеристическое уравнение

$$\lambda b^2 - 2(k_1 + k_2 - \lambda)ab +$$

$$+ (n - 2(k_1 + k_2) + \lambda)a^2 = 0 \qquad (3)$$

отражает условие ортогональности строк бицикла с элементами a, $-b$, оно записано в виде, удобном для поиска корней при превалировании количества положительных элементов над отрицательными.

Ортогональные моноциклы

Циклические структуры разрешимы, например, на порядках простых чисел, но целочисленные варианты жестко ограничены решением пары квадратичных диофантовых уравнений I, II. Согласно гипотезе Райзера [7], циклических матриц Адамара порядка выше 4 не бывает. Этот порядок разрешим единственной в своем роде не тривиальной по порядку (скалярный случай тривиален) симметричной матрицей с негативными элементами на диагонали.

Тем самым структуры с равными по своим абсолютным величинам элементами обладают недостаточной гибкостью для изготовления ортогональных моноциклов. Неравенство абсолютных величин элементов a, $-b$ создает дополнительный ресурс, которым можно пользоваться. Кроме того, мы можем рассматривать такие блоки как строительный материал для расширяемых каймой матриц с равными значениями $a = b$.

Диофантово уравнение I вида $k(k - 1) = \lambda(n - 1)$ с параметрами $\lambda = t,\ k = 2t$ заведомо разрешимо для порядков $n = 4t - 1$.

После подстановки параметров в уравнение связи (1) оно упрощается до $(t - 1)b^2 - 2tba + ta^2 = 0$, положительный корень этого полинома дает уровень вещественных ортогональных моноциклов Мерсенна [3, 5] $b = \dfrac{t}{t + \sqrt{t}}$ при $a = 1$.

Это не означает, что такое решение возможно именно в виде моноцикла, решение справедливо для всех гипотетически возможных орнаментов семейства с указанными параметрами. Циклический тип орнамента не универсален, зато тесно связан с числовой системой. Он сопровождает все числа Мерсенна, парные произведения близких простых чисел и простые числа — специфический индикатор простоты числа, если убрать два исключения.

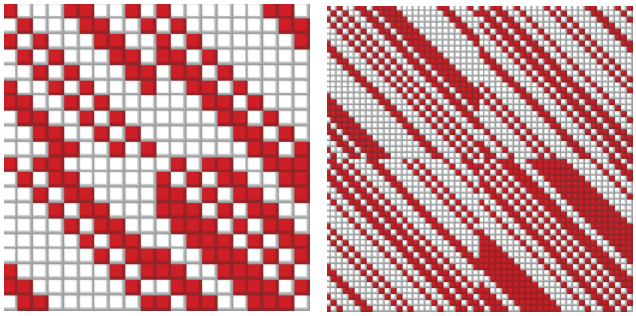
Ортогональные бициклы Адамара

Центральный вопрос относительно разрешающей силы орнаментов поставлен, по сути, формулировкой проблемы Райзера [7]: существуют ли бициклы, ортогональные независимо от значения их порядка?

В теории чисел есть две теоремы, одна из которых дает условия разложения нечетного числа на суммы квадратов двух чисел (теорема Ферма, доказательство которой опубликовал Эйлер), и теорема Лагранжа о разложимости любого числа на сумму двух квадратов. Теория матриц-орнаментов сопровождает эти теоремы графическими иллюстрациями, являясь их интерпретацией.

То, что теорема Лагранжа отвечает разрешимости матриц Адамара орнаментов в виде четырехблочной конструкции, было очевидно уже в середине прошлого века Вильямсону [8]. Для сокращения переборов он предложил искать только симметричные решения блоков, первый неразрешимый порядок матриц Вильямсона 35 обнаружил Драгомир Джокович [9]. Границу известного очерчивает таблица матриц Вильямсона [10] с предельно достижимым современной вычислительной техникой размером блока 59 (более общая форма была предложена Гетхальсом — Зейделем [2, 11]).

Буквальная визуализация представления матрицы Адамара *двумя квадратами* является иллюстрацией теоремы Эйлера — Ферма для нечет-



■ ***Рис. 3.*** Бициклические матрицы Адамара порядков $n = 20$ и $n = 52$

ных чисел $p = n/4 = x^2 + y^2$, разности $k_1 = p - x$ и $k_2 = p - y$ описывают количества элементов одного знака в строке (рис. 3).

Напомним, что в 1749 г. Эйлер после семи лет работы и почти через сто лет после смерти Ферма доказал теорему о простых числах, согласно которой разложение числа p на сумму квадратов всегда возможно для чисел $4t - 3$, к которым относятся числа p, равные $5 = 1 + 2^2$ и $13 = 2^2 + 3^2$.

В данном случае $k_1 = p - x = 4$ и $k_2 = p - y = 3$ отвечают матрице порядка $n = 20$, $k_1 = p - x = 11$ и $k_2 = p - y = 10$ отвечают матрице порядка $n = 52$. Требуемое значение одинаковых элементов в каждой паре строк $\lambda = p - x - y$.

Граница симметрии бициклов Адамара отодвинута с 4-го порядка Райзера (для моноциклов) до критического 32-го порядка [12].

Ни одно число вида $4t - 1$ не представимо в виде суммы двух квадратов, поэтому нет, например, бициклической матрицы Адамара порядка 12, $p = n/4 = 3$. Соответственно, в первой сотне существует всего 12 бициклических матриц Адамара порядков 1, 4, 8, 16, 20, 32, 40, 52, 64, 68, 80, 100.

Ортогональные бициклы Эйлера

Для всех матриц Эйлера [3, 5] порядков $n = 4t - 2$ (размер плеча $v = n/2 = 2p - 1$, $p = t$) диофантово уравнение (2) сводится к уравнению равнобедренного прямоугольного треугольника $x^2 + y^2 = 2$, разрешимое для точки $x = y = 1$ окружности с квадратом радиуса $p + \lambda(v - 2p) = 2$.

Поскольку $k_1 = p - x$ и $k_2 = p - y$, количества элементов одного знака в плечах бицикла равны $k_1 = k_2 = p - 1 = (v - 1)/2$, $\lambda = p - 2 = (v - 3)/2$.

Дизайн $\{n = 2v;\ k_1,\ k_2;\ \lambda\} = \{n = 2v;\ (v - 1)/2,\ (v - 1)/2;\ (v - 3)/2\}$ назовем *эйлеровым*.

Формальный переход от бициклической матрицы Эйлера к матрице Мерсенна с бинарной каймой [5] и (после добавления каймы с инверсией основы) к матрице Адамара иллюстрируется рис. 4.

Наиболее проста реализация бицикла Эйлера с равными плечами $\mathbf{A} = \mathbf{B}$, $\lambda_1 = \lambda_2$, $\lambda = \lambda_1 + \lambda_2$, которые представляют собой, в частности, циклические матрицы Мерсенна вдвое меньшего размера $v = 3 \pmod 4$, рассмотренные ранее.

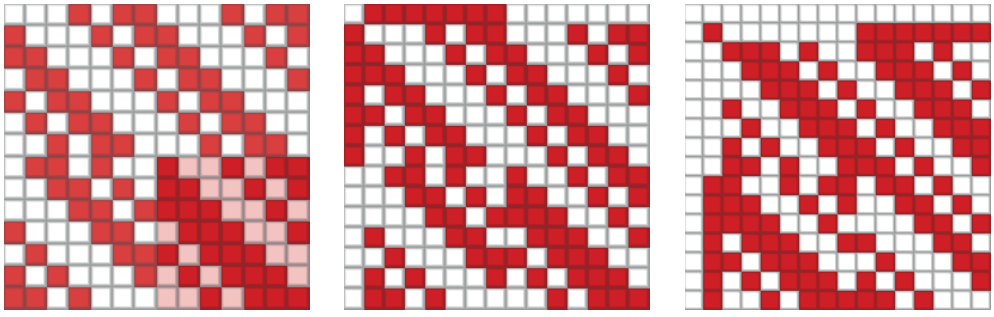
Пусть разложение на базе одной и той же матрицы в обоих плечах невозможно, тогда раскрывается скрытый ресурс бицикла: плечи его утрачивают равновесие $\mathbf{A} \neq \mathbf{B}$, отклонение $\lambda_1 = \lambda_2 + 1$ берет в расчет блоки, которым самим не обязательно быть ортогональными, ортогональна конструкция в целом.

Характеристическое уравнение (3) отражает условие ортогональности строк с элементами a, $-b$, причем $(n - 2(k_1 + k_2) + \lambda) = (n - 2p + \lambda) = p$ при $\lambda = p - 2$, $2(k_1 + k_2 - \lambda) = 2p$ и для $n = 4t - 2$, $p = t$. Положительный корень этого полинома дает уровень матриц Эйлера $b = \dfrac{t}{t + \sqrt{2t}}$ при $a = 1$.

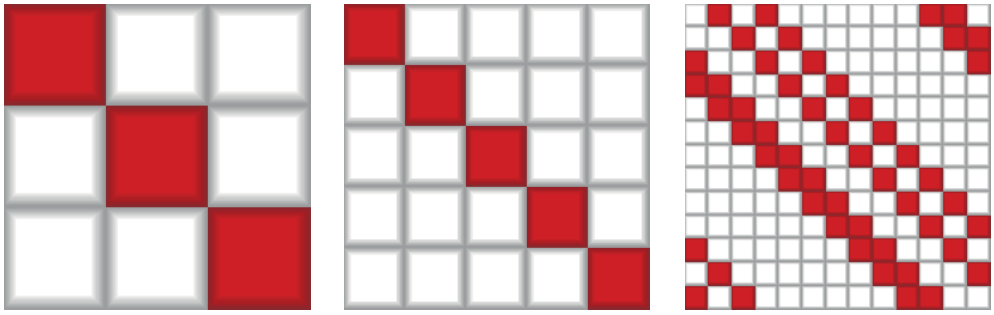
Неортогональные целочисленные бициклы

Отдельное от ортогональных матриц семейство составляют матрицы максимума детерминанта — абсолютное значение детерминанта максимально на множестве матриц с амплитудами элементов, не превышающими значения 1.

В силу исключительности свойств (детерминант максимален, элементы целочисленны) структура матриц максимума детерминанта нечетного порядка неограниченно усложняется по мере роста их размера, что затрудняет их поиск.



■ ***Рис. 4.*** Переход от бицикла Эйлера к матрице Мерсенна и Адамара



■ ***Рис. 5.*** Циклические матрицы максимума детерминанта порядков 3, 5, 13

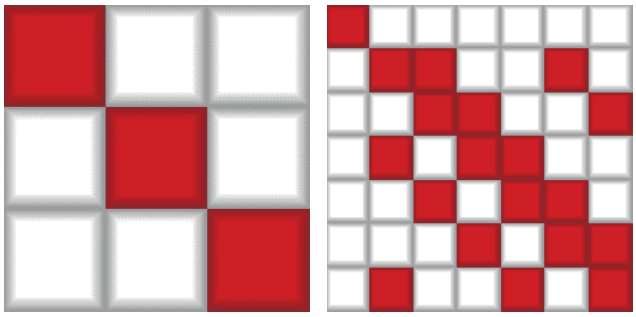
Семейство циклических матриц состоит (никто ранее не высказывал этого предположения, выскажем его) всего из трех представителей порядков 3, 5, 13 (рис. 5).

Помимо семейства циклических матриц, есть *моноциклы с каймой* из единиц порядков первых двух простых чисел Мерсенна 3, 7 (они же — бициклы с каймой без инверсии знака вида **[A B; B A]**) (рис. 6).

Семейству моноциклов Мерсенна вторит семейство бициклических матриц (тоже с каймой)

Ферма вида $\mathbf{F} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$ порядков 3, 5, 17,

повторяющих первые три простых числа Ферма, здесь **e** — вектор из единиц (рис. 7).



■ ***Рис. 6.*** Моноциклы с каймой порядков 3, 7

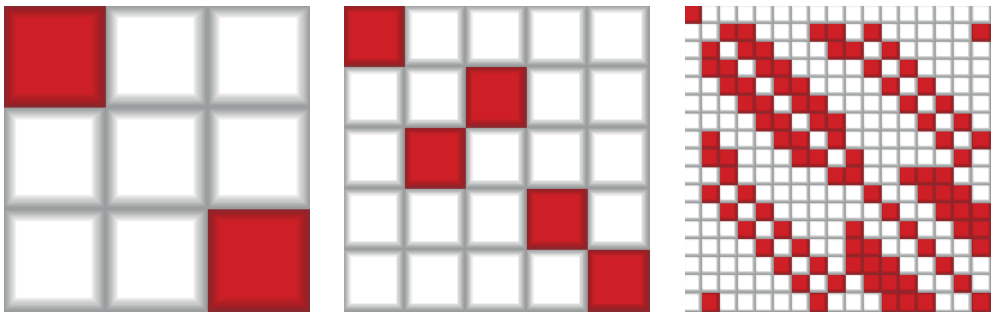
Простые числа Ферма — классические объекты теории чисел, известно всего пять таких чисел $F_k = 3, 5, 17, 257, 65\,537$.

В 1796 г. Карл Фридрих Гаусс обнаружил неожиданную связь между ними и геометрическими фигурами, вписав в круг правильный семнадцатиугольник и доказав более общее положение, что если число сторон правильного многоугольника равно простому числу Ферма, то его можно построить при помощи циркуля и линейки. Эта междисциплинарная связь глубока и может находить иные оригинальные проявления.

Гипотеза. Матрицы Ферма порядков простых чисел $n = F_k = 3,\ 5,\ 17,\ 257,\ 65\,537,\ \ldots$ — матрицы абсолютного максимума детерминанта, оцениваемого по формуле $F_{k-1}/(2F_k - 1)^{1/2} \times B$, где $B = (n - 1)^{(n-1)/2}(2n - 1)^{1/2}$ — оценка Гвидо Барбы [13] детерминанта сверху.

Матрицы Ферма [5] дополняются матрицами относительной простотой структуры нечетных порядков $4t + 1$, равных сумме квадратов ближайших (четное и нечетное числа) друг к другу чисел $n^B = q^2 + p^2$ при $p = q + 1$, выделенных Барбой [13]. За пределами этих двух семейств — орнаментальный хаос, отягощаемый предположением о его неограниченном усложнении (как у фракталов).

Часть матриц максимума детерминанта четных порядков $4t$ совмещают в себе качество быть экстремальными и ортогональными одновременно.



■ ***Рис. 7.*** Бициклические матрицы Ферма порядков 3, 5, 17

Прежде всего, это матрицы Адамара, которые, в отличие от вездесущих матриц Эйлера, к бициклам сводимы далеко не всегда. Бициклы максимума детерминанта иных четных порядков $4t - 2$ не ортогональны, но ортогонализуемы параметрически изменением одного из уровней от 1 до $-b$.

Узоры экстремального и ортогонального вариантов совпадают и описываются одинаковым набором орнаментальных инвариантов. Семейство неоднородно и распадается на два подсемейства Барбы четных порядков $n = n^B + 1$ и $n = 2n^B$ сложностью, не превосходящей сложность бицикла. Каждое имеет свое характеристическое уравнение и, соответственно, идентифицирующий семейство решений уровень $b = b(n)$.

Ортогонализуемый бицикл максимума детерминанта, по аналогии с основой (core) матриц Адамара, отличается превалированием числа отрицательных элементов над положительными, поэтому его надо инвертировать либо оставить как есть, переписав характеристическое уравнение (3) к форме $(n - 2p + \lambda)b^2 - 2pab + \lambda a^2 = 0$ с учетом, что для его порядка $(n - 2(k_1 + k_2) + \lambda) = (n - 2p + \lambda)$, $2(k_1 + k_2 - \lambda) = 2p$, $p = k_1 + k_2 - \lambda = (n - 2)/4$. Его корни дают ортогональные матрицы с уровнем

$$b = \frac{p \pm \sqrt{p^2 - \lambda(n - 2p + \lambda)}}{n - 2p + \lambda} \text{ при } a = 1.$$

Семья Барбы 1. Порядки $n = n^B + 1 = 2(q^2 + q + 1) = 6, 14, 26, 42, 62, 86, 114, \ldots$ разрешимы на $k_1 = q(q + 1)/2$, $k_2 = q(q - 1)/2$, где $q = k_1 - k_2$ — радиус окружности; $x^2 + y^2 = k_1 + k_2 = q^2$, $p = k_1 = (n - 2)/4$, $\lambda = k_2 = p - q$, $q^2 = k_1 + k_2 = k$, $n - 2p - \lambda = n - 2k_1 - k_2$, формула для уровня упрощается до зависимости $b = \dfrac{k_1 \pm \sqrt{k_2^2 - (n - 2k_1 - k_2)}}{n - 2k_1 - k_2}$ от параметров k_1, k_2.

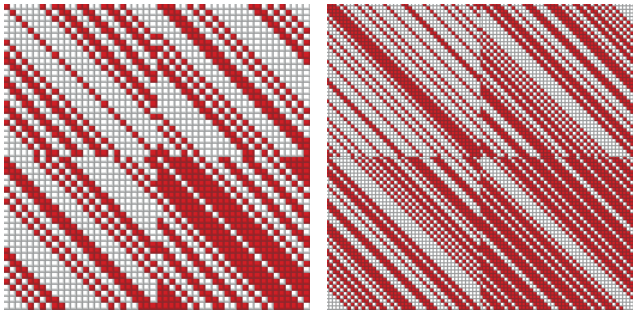
Матрица порядка 6 двоякосимметрична, в цепочке симметричных матриц 6, 14, 26, (не симметрична 42), 62, 86 порядок 86 предположительно последний симметричный.

Семья Барбы 2. Порядки $n = 2n^B = 2(2q^2 + 2q + 1) = 10, 26, 50, 82, 122, \ldots$ разрешимы на $k_1 = k_2 = q^2$, где $\sqrt{2}q$ — радиус окружности; $x^2 + y^2 = 2q^2$, $x = y = q$, $\lambda = q^2 + q$, $p = q^2 - q = (n - 2)/4$, $q^2 = (k_1 + k_2)/2 = k/2$, формула для уровня указана выше.

Матрица 10 двоякосимметрична, в цепочке симметричных матриц 10, (не симметрична 26), 50 порядок 50 предположительно последний симметричный.

Симметричные ортогональные бициклы двух выделенных семейств порядков 50 и 86 изображены на рис. 8.

Матрицы Адамара совмещают качество быть ортогональными и целочисленными, а параметры бициклических матриц максимума детерминанта нужно «уводить» от целых значений, в остальном это одинаковые по содержанию матрицы, образующие на четных порядках семейства и существующие на них, в отличие от бициклов Эйлера, далеко не всегда.



■ ***Рис. 8.*** Симметричные ортогональные бициклы порядков 50, 86

Метод орбит

Динамические системы первого порядка в поле Галуа используются как генераторы первых строк бициклов. Метод орбит состоит в следующем. В обычном вещественном поле показательная функция (выход динамической системы) монотонно возрастает. В конечном поле GF(p) рост функции заведомо ограничен теоремой Ферма $g^{p-1} = 1$, где g — элемент поля Галуа. Это напоминает поведение бильярдных шаров: динамика их несложна, но столкновения с бортом придают сложность движению.

В качестве примера поля Галуа рассмотрим набор целых чисел 0, 1, ..., $p - 1$ с умножениями по модулю p (простое число). Мультипликативная группа поля Галуа, обозначаемая как GF*(p), состоит из всех элементов поля, кроме 0. Необходимость введения подгрупп заключается в том, что показательная функция может закончиться единицей для степени, меньшей, чем $p - 1$, но пропорциональной ей.

Пример. Рассмотрим подгруппы GF*(p) для $p = 11$ (таблица), разложение $p - 1 = 1 \times 2 \times 5 = 10$ указывает на размеры 1, 2, 5, 10 циклических подгрупп.

Элементы 2, 6, 7, 8 левого столбца таблицы называются *примитивными*, они порождают циклическую подгруппу максимальной длины, совпадающую с GF*(11). Такая орбита, как ее еще иногда называют, дает ортогональную циклическую матрицу (единичную) порядка 12 с элементами $a = 1$, $b = 0$, где элементы орбиты — адреса элемента b в первой строке, т. е. все 0, за исключением первой единицы. Вторая орбита (минимальной длины), отвечающая $g = 1$, дает ту же самую матрицу, если поменять значения ее элементов на противоположные и добавить циклический

■ Циклические подгруппы GF*(11)

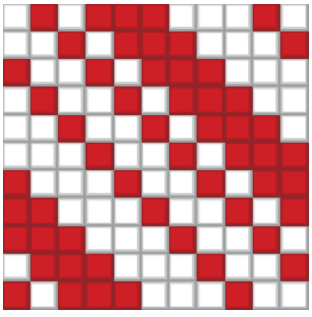
g	g^k
1	1
2	1, 2, 4, 8, 5, 10, 9, 7, 3, 6
3	1, 3, 9, 5, 4
4	1, 4, 5, 9, 3
5	1, 5, 3, 4, 9
6	1, 6, 3, 7, 9, 10, 5, 8, 4, 2
7	1, 7, 5, 2, 3, 10, 4, 6, 9, 8
8	1, 8, 9, 6, 4, 10, 3, 2, 5, 7
9	1, 9, 4, 3, 5
10	1, 10

сдвиг строк на один шаг назад. Есть еще бинарная матрица с двумя элементами. Такие матрицы отличаются сравнительно низким значением детерминанта (единица у единичной матрицы).

Орбита средней длины 5 из таблицы порождает ортогональную циклическую матрицу размера 11 с элементами $a = 1$, $-b$ (рис. 9). Если индексировать элементы с 0, то числа 1, 3, 4, 5, 9 отвечают положениям элемента $-b$, отличаемого цветом.

В данном случае для построения ортогонального моноцикла хватило одной орбиты. В теории мультипликативных групп принято выделять орбиты, называемые также *действием группы* на элемент m или множество элементов. Под действием подразумевается умножение m на элементы группы или подгруппы. Итог зависит от выбранного элемента. Например, если умножать единичный элемент $m = 1$ на группу, то итогом будет вся группа. А если умножать $m = 2$, то у этого числа иные продуктивные способности: в бесконечномерном случае оно порождает четные числа (идеал).

Вследствие умножения орбита перестает быть подгруппой. Содержательная сторона выделения орбит состоит в том, что циклические блоки размера p базируются на бинарных последовательностях элементов, причем адреса (индексы) элементов одного знака представляют собой, что особенно важно для матриц максимума детерминанта двух отмеченных выше семейств, совокупность частных орбит mg^k, включая тривиальную 0.



■ ***Рис. 9.*** Циклическая ортогональная матрица

Заключение

Прибавление каймы к *всегда существующему вещественному бициклу* Эйлера приводит его, после коррекции уровней, к вещественной же матрице Мерсенна и далее — к *целочисленной* матрице Адамара, что создает предпосылку для доказательства существования всех матриц Адамара и указывает на ограничение ее сложности: любая матрица Адамара не сложнее бицикла с парной каймой.

В статье рассмотрен подход, раскрывающий разрешимость бициклов ортогональными матрицами не в пользу матриц Адамара, а в пользу матриц Эйлера соседних с ними четных порядков. Общий алгоритм дискретизации за два прохода переводит нецелочисленные матрицы Эйлера путем структурных дискретных преобразований (добавлением каймы) в целочисленные матрицы Адамара: матрицы Эйлера порождают, при их расширении каймой, матрицы Мерсенна, а матрицы Мерсенна являются строительными блоками матриц Адамара.

Поскольку матрицы Эйлера не стеснены требованием целочисленности, это позволяет поновому взглянуть на проблему «недоказуемости» существования матриц Адамара комбинаторными методами. Перебором можно найти любой конечный орнамент, но нельзя гарантировать обязательность существования решения. В этом корень этой уже столетней проблемы. Заметим, что без использования иррациональных чисел ровно так же озадачивает вычисление длины гипотенузы прямоугольного треугольника с равными катетами.

Вещественные матрицы Эйлера выступают как «обычные» локально оптимальные по детерминанту матрицы. Разрешимость задачи поиска локального экстремума гарантируется общностью положения, никакой проблемы существования при этом не обнаруживается. Элементы матриц Эйлера — вещественные, в том числе рациональные и иррациональные, числа. Их теория никак не стеснена целочисленностью или рациональностью возможных решений. Они могут быть продуктом оптимизации детерминанта и впервые были получены итерациями как локально оптимальные по детерминанту матрицы.

Существующие на порядках с шагом 4 бициклы Эйлера, как антитеза известной гипотезе Райзера о существовании единственной матрицы Адамара (скалярный вариант не рассматриваем)

в форме моноцикла 4-го порядка, представляют собой законченное решение вопроса о гипотезе Адамара.

Обзоры и примеры найденных новых порядков матриц максимума детерминанта сосредоточены обычно на более простых четных порядках. Семейство матриц порядков, равных числам Ферма, выделено нами впервые. Оно дополняет матрицы нечетных порядков Барбы, более того, это главное и единственное семейство, отличное от прочих как тем, что мы умеем его орнаменты строить, так и тем, что оно связано с теоремой Гаусса о семнадцатиугольнике.

Работа выполнена при поддержке Минобрнауки РФ при проведении научно-исследовательской работы в рамках проектной части государственного задания в сфере научной деятельности по заданию № 2.2200.2017/ПЧ.

Литература

1. **Балонин Н. А., Мироновский Л. А.** Флип-метод определения сингулярных функций ганкелева оператора и оператора свертки // Автоматика и Телемеханика. 1999. № 11. С. 3–18.
2. Handbook of Combinatorial Designs. Ser. Discrete Mathematics and its Applications/ C. J. Colbourn (Ed.), J. H. Dinitz (Ed.). — London: Chapman and Hall/CRC, 2006. — 1000 p.
3. **Балонин Н. А., Сергеев М. Б.** Матрицы Мерсенна и Адамара // Информационно-управляющие системы. 2016. № 1. С. 2–15. doi:10.15217/issn1684-8853.2016.1.2
4. **Hall M.** A Survey of Difference Sets // Proc. Amer. Math. Soc. 1956. Vol. 7. P. 975–986.
5. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1. С. 2–15.
6. **Hadamard J.** Résolution d'une Question Relative aux Déterminants//Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.
7. **Ryser H. J.** Combinatorial Mathematics: The Carus Mathematical Monographs/ Published by the Mathematical Association of America. — N. Y.: John Wiley and Sons, 1963. N 14. — 162 p.
8. **Williamson J.** Hadamard's Determinant Theorem and the Sum of Four Squares // Duke Math. J. 1944. N 11. P. 65–81.
9. **Doković D. Ž.** Williamson Matrices of Order $4n$ for $n = 33;35;39$ // Discrete Math. 1993. Vol. 115. P. 267–271.
10. **Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B.** Williamson Matrices up to Order 59 // Designs, Codes and Cryptography. 2008. N 46. P. 343–352.
11. **Goethals J. M., and Seidel J. J.** Orthogonal Matrices with Zero Diagonal // Canadian Journal of Mathematics. 1969. Vol. 19. P. 1001–1010.
12. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея// Информационно-управляющие системы. 2015. № 3. С. 2–16. doi:10.15217/issn1684-8853.2015.3.2
13. **Barba G.** Intorno al Teorema di Hadamard Sui Determinanti a Valore Massimo// Giorn. Mat. Battaglini. 1933. N 71. P. 70–86.

UDC 519.61:511-33
doi:10.15217/issn1684-8853.2017.1.2

Ryser's Conjecture Expansion for Bicirculant Strictures and Hadamard Matrix Resolvability by Double-Border Bicycle Ornament

Balonin N. A.[a], Dr. Sc., Tech., Professor, korbendfs@mail.ru
Sergeev M. B.[a], Dr. Sc., Tech., Professor, mbse@mail.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: Our goal is to expand the border of critical orders for Ryser's conjecture from circulant to bicirculant structures of quasi-orthogonal matrices with two values (levels) of the entries, and to investigate the resolvability of bicirculant structures with one or two borders for the known types of column/row orthogonal matrices. **Results:** We have shown that orthogonal bicirculant Euler matrices with levels $a=1, -b$, where $b=\frac{t}{t+\sqrt{2t}}$, exist for all orders $n=4t-2$ and, with a border added, turn through an intermediate stage of real Mersenne matrices into integer Hadamard matrices, defining thereby a matrix structure of minimum complexity resolvable for all possible orders they have determined. In other words, the Hadamard matrix conjecture (well known by its irresolvability by non-combinatorial methods) is proved now through an appeal to "matrix transitions" from real matrix types (not limited by the ban to have irrational entries) to integer Hadamard matrices with entries 1, −1. We have demonstrated that maximum determinant matrices of orders $n=4t-2$ are related to orthogonal bicirculant matrices. They are essentially different from Euler matrices because their bicirculant structure, as well as the structure of bicirculant Hadamard matrices, is not always resolvable for their corresponding orders. We have

also estimated the symmetry borders for various families of bicirculant maximum determinant matrices, including Hadamard matrices. **Practical relevance:** The algorithms of calculating bicirculant matrices have been used in developing research software. Matrices suboptimal by their determinant are the basis of Euler and Mersenne filters used for image compression and masking.

Keywords — Orthogonal Matrix, Circulant Matrix, Bicirculant Matrix, Ryser's Conjecture, Hadamard Conjecture, Hadamard Matrix, Mersenne Matrix, Euler Matrix.

References

1. Balonin N. A., Mironovskii L. A. Flip Method for Obtaining Singular Functions of Hankel Operators and Convolution Operators. *Avtomatika i Telemekhanika*, 1999, vol. 60, no. 12, part 2, pp. 3–18 (In Russian).
2. *Handbook of Combinatorial Designs*. Ser. Discrete Mathematics and its Applications. 2nd ed. / C. J. Colbourn (Ed.), J. H. Dinitz (Ed.). London, Chapman and Hall/CRC, 2006. 1000 p.
3. Balonin N. A., Sergeev M. B. Mersenne and Hadamard Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 1, pp. 2–15 (In Russian). doi:10.15217/issn1684-8853.2016.1.2
4. Hall M. A Survey of Difference Sets. *Proc. Amer. Math. Soc.*, 1956, vol. 7, pp. 975–986.
5. Balonin N. A., Sergeev M. B. Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 1, pp. 2–15 (In Russian).
6. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
7. Ryser H. J. *Combinatorial Mathematics*. The Carus Mathematical Monographs. Published by the Mathematical Association of America, New York, John Wiley and Sons, 1963, no. 14. 162 p.
8. Williamson J. Hadamard's Determinant Theorem and the Sum of Four Squares. *Duke Math. J.*, 1944, vol. 11, pp. 65–81.
9. Doković D. Ž. Williamson Matrices of order 4*n* for *n*=33;35;39. *Discrete Math*., 1993, vol. 115, pp. 267–271.
10. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson Matrices up to Order 59. *Designs, Codes and Cryptography*, 2008, no. 46, pp. 343–352.
11. Goethals J. M., and Seidel J. J. Orthogonal Matrices with Zero Diagonal. *Canadian Journal of Mathematics*, 1969, vol. 19, pp. 1001–1010.
12. Balonin N. A., Djokovic D. Z. Symmetry of Two-Circulant Hadamard Matrices and Periodic Golay Pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
13. Barba G. Intorno al Teorema di Hadamard sui Determinanti a Valore Massimo. *Giorn. Mat. Battaglini*, 1933, vol. 71, pp. 70–86 (In Italian).

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.