УДК 519.614
doi:10.15217/issn1684-8853.2016.1.2

МАТРИЦЫ МЕРСЕННА И АДАМАРА

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: *показать соответствие чисел Мерсенна, Ферма и прочих числовых последовательностей малоуровневым матрицам локального максимума детерминанта, гарантирующее как существование матриц, так и взаимное соответствие матричных портретов видам чисел: простых, пар простых чисел, степеней простых чисел.* ***Методы:*** *поиск матриц глобального и локального максимумов детерминанта ведется итерационной вычислительной процедурой, ориентированной на минимизацию максимального абсолютного значения элементов ортогональной матрицы.* ***Результаты:*** *разработана теория взаимного соответствия чисел и экстремальных матриц, упрощающая поиск неизвестных матриц обращением к классификации матриц по типам чисел. Предложено расширительное толкование гипотезы Адамара адекватными ей гипотезами о существовании семейств малоуровневых квазиортогональных матриц. Приведено доказательство существования матриц Мерсенна и, следствием, доказательство существования матриц Адамара. На основе арифметики конечных полей Галуа построены алгоритмы вычисления матриц Мерсенна, согласованные по результатам с оптимизационными процедурами повышения детерминанта и дополняемые ими.* ***Практическая значимость:*** *малоуровневые матрицы локального максимума детерминанта ортогональны и имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

Ключевые слова *— ортогональные матрицы, матрицы Мерсенна, матрицы Адамара, гипотеза Адамара, конечные поля Галуа, циклические матрицы, негациклические матрицы, бициклические матрицы, вычислительные алгоритмы.*

Введение

Отношения чисел и математических объектов иной природы, таких как функции и матрицы, естественны, поскольку математика — единый предмет, разделенный на области. Выход на границы областей, как правило, лежит вне основного интереса отдельных научных направлений, и они развиваются автономно. Вместе с тем междисциплинарные исследования приносят свои плоды. Пример — гипотеза Таниямы. Любая эллиптическая кривая, заданная над полем рациональных чисел, характеризуется своими параметрами. Математический объект другой природы, модулярная форма, также дает некоторую последовательность чисел. В сентябре 1955 г. Ютака Таниама высказал предположение о том, что эллиптические кривые являются модулярами, т. е. нет такой эллиптической кривой, для которой не нашлась бы адекватная ей по набору параметров модулярная форма. Гипотезой заинтересовались, когда в 1985 г. Герхар Фрэй предположил, что она является обобщением Великой теоремы Ферма, поскольку любой контрпример к Великой теореме Ферма приводил в итоге к немодулярной эллиптической кривой. Гипотезу доказали, и эта история служит хорошей иллюстрацией продуктивности исследований в пограничных областях наук, когда устанавливаются связи между объектами совершенно различной, казалось бы, математической природы.

Интерес настоящей статьи связан с системами ортогональных векторов, далекими от числовых последовательностей, объектов не геометрической природы. Ортогональные базисы описываются ортогональными матрицами или *квазиортогональными* матрицами — масштабированными ортогональными матрицами с максимальным элементом, равным по модулю единице.

Наше видение состоит в том, что с числовыми последовательностями соотносятся не все такие матрицы, а только экстремальные, у которых детерминант максимален. То, что экстремальные квазиортогональные матрицы имеют порядки, соответствующие элементам числовой последовательности $4t$, где t — натуральное число, заметил еще Адамар [1]. Он высказал предположение, сходное с предположением Таниямы, о том, что экстремальные матрицы подобны «модулярам» для четных чисел вида $4t$. Гипотеза раскрывает разнообразие систем чисел и ортогональных базисов, которое в пределах даже такого сравнительно узкого предположения способно дать почву для столетних изысканий матриц Адамара.

Предположение, высказанное нами и подкрепленное примерами матриц в работе [2], состоит в том, что семейства экстремальных матриц существуют не только на четных порядках $4t$ и $4t-2$, но и на нечетных порядках $4t-1$ и $4t-3$.

Приведенные числовые последовательности распадаются на вложенные в них последовательности простых чисел p, степеней простых чисел p^m, где m — натуральное число, пар близких простых чисел p и $p+2$, чисел Мерсенна 2^k-1, где k — натуральное число, чисел Ферма $2^{2^k}+1$, где k — неотрицательное целое число, и др. Согласно

предположению, на соответствующие подсемейства распадаются также и матрицы, подробно рассмотренные в работе [2].

Опираясь на отмеченное разнообразие последовательностей чисел, можно отойти от универсальных алгоритмов и кардинально ускорить поиск экстремальных матриц.

Интерпретация теоремы Эйлера — Ферма

В качестве иллюстрации тесной связи чисел и ортогональных матриц приведем нашу интерпретацию теоремы Эйлера — Ферма.

Одна из знаменитых теорем теории чисел связана с заменой *в левой части* уравнения для триады чисел Пифагора (пифагоровы тройки) квадратичной зависимости, типичной для уравнения круга, на линейную зависимость с получением $p = x^2 + y^2$. Жирар и Ферма заметили, что любое натуральное число представляется суммой не более чем четырех квадратов целых чисел. Ни одно число вида $4t - 1$ не представимо в виде суммы двух квадратов. 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 двух квадратов всегда возможно для чисел $4t - 3$.

Форма представления ортогональных массивов (матриц Адамара) бициклом является специфической иллюстрацией теоремы Эйлера — Ферма для чисел $p = n/4 = x^2 + y^2$ (буквальная визуализация представления матрицы *двумя квадратами*). В популярной характеристике бинарных матриц в форме SDS($2p$; r, s; λ) разности $r = p - x$ и $s = p - y$ описывают число 1 или –1 матриц бицикла (просто проверяется по портретам матриц на рис. 1), $\lambda = p - x - y$ — четвертый параметр, равный числу сходных элементов в двух соседних строках.

Позднее результат развил Лагранж — теоремой о сумме четырех квадратов. Теорема утверждает, что всякое натуральное число можно представить в виде суммы четырех квадратов целых чисел. Она является основой поиска матриц Адамара в форме четырехблочного массива Гетхальса — Зейделя. С нашей точки зрения, это структурный избыток, поскольку достаточно бицикла и двойной каймы. Этой форме соответствует разложение матрицы Мерсенна (на единицу меньшего порядка) в виде бицикла и одинарной каймы.

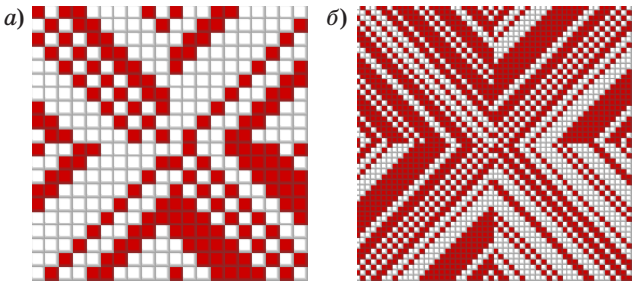
Важную для теоремы лемму о том, что произведение сумм четырех квадратов есть сумма четырех квадратов, доказал Эйлер, однако саму теорему доказал Лагранж в 1770 г. Доказательство теоремы представляет собой алгоритм, позволяющий находить разложение числа N с помощью $O(N^2 \log_2\{N\})$ арифметических операций.

Матрицы Ферма и золотого сечения

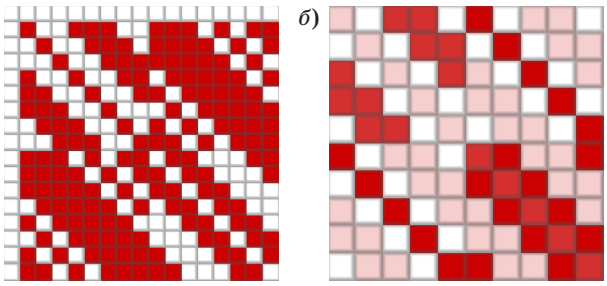
Матрицы Ферма [2, 3] порядка 17 и золотого сечения [4, 5] порядка 10 приведены на рис. 2.

Простые числа Ферма F_k являются классическими объектами теории чисел, известно пять таких чисел: 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.

Поскольку между числами и матрицами есть соответствие, то эта связь должна иметь продолжение у матриц Ферма. Матрицы Ферма — матрицы, построенные расширением регулярных матриц Адамара (суммы элементов которых по строкам и по столбцам равны) каймой. Это матрицы ортогонализуемые параметрически без изменения структуры выбором значений элементов каймы и отрицательных элементов. Первые три целочисленные матрицы Ферма порядков 3, 5, 17 — матрицы глобального максимума детерминанта $F_{k-1}/(2F_k - 1)^{1/2}B$, где B — ограничение на детерминант сверху, данное Гвидо Барба. Проверка оставшихся порядков 257, 65 537 не проведена, но предположение (гипотеза), что они отвечают экстремумам, в слабом варианте — локальным, логично вытекает из знаменитой теоремы Гаусса.



■ ***Рис. 1.*** Бициклические матрицы порядков n = 20 и 52: p = 5 и 13



■ ***Рис. 2.*** Матрицы Ферма порядка 17 и золотого сечения порядка 10

Другой пример не менее примечателен — в работе [5] описана матрица золотого сечения порядка 10, ее бициклическая форма построена на паре последовательностей [g, 1, $-g$, $-g$, 1], [-1, 1, g, g, 1] с модулями элементов 1 и g. Условие ортогональности столбцов матрицы — уравнение золотого сечения $g^2 + g - 1 = 0$. В решении фигурирует иррациональный корень $g = 0{,}618...$, известный в теории чисел Фибоначчи.

Экстремальные квазиортогональные матрицы

Для правильного восприятия материала приведем некоторые определения.

Определение 1. Ортогональной матрицей называется квадратная матрица $\mathbf{A}$ порядка n такая, что $\mathbf{A}^T\mathbf{A} = \mathbf{I}$, где $\mathbf{I}$ — единичная матрица.

Определение 2. Квазиортогональной матрицей называется квадратная матрица $\mathbf{A}$ порядка n с ограниченными по модулю элементами $|a_{ij}| \le 1$ такая, что $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$, где $\mathbf{I}$ — единичная матрица; $\omega(n)$ — весовая функция.

Определение 3. *Локальный максимум* $|\det(\mathbf{A})|$ квазиортогональной матрицы достигнут, если любое достаточно малое по параметрам изменение матрицы не нарушает вида уравнения связи $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$ при свободно заданном значении веса $\omega(n)$, но приводит к уменьшению модуля детерминанта.

Таким образом, *допустимыми* являются любые изменения параметров варьируемой матрицы, не нарушающие условие ортогональности ее столбцов. Весовая функция в задачах поиска условного максимума $|\det(\mathbf{A})|$ при ограничении вида $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$ заранее не задана, и сама является предметом поиска. В этом состоит важное их отличие от задачи поиска матриц Адамара с жестко заданным заранее весом $\omega(n) = n$.

Квазиортогональные матрицы имеют следующие принципы деления их на семейства и подсемейства по аналогии с семействами и подсемействами чисел. Крупное семейство матриц порядков, равных числам некоторой достаточно общей числовой последовательности, отличается от прочих матриц количеством различных элементов (уровней). Например, матрицы Адамара с элементами 1 и -1 являются двухуровневыми матрицами, причем значения уровней не зависят от их порядков, функции уровней — константы.

Для экстремальных двухуровневых матриц один из уровней равен 1 (или -1), иначе значение детерминанта матрицы можно повысить элементарным масштабированием. Следовательно, варьируемая функция уровня семейства двухуровневых матриц — всего одна. К таким матрицам примыкают матрицы четных порядков, удвоение уровней наблюдается здесь лишь в силу изменения знака при блоках в блочных конструкциях.

Подсемейства квазиортогональных матриц строятся на порядках, вложенных в основные числовые последовательности. Элементы подсемейств различаются между собой структурами. Простейшими структурами являются циклические, бициклические и негациклические матрицы. Если регулярная структура не реализуема, появляются более сложные структуры, содержащие в своем составе циклические, обратные циклические, негациклические и др. блоки составных матриц, а также кайму.

Стоит отметить также возможность выделения некоторой универсальной структуры для всех подсемейств семейства матриц, разрешимой для любого вложения. Например, для матриц Адамара такой является структура из четырех блоков. Отделять универсальные структуры от частных полезно, они различимы на всех порядках $4t$, $4t-1$, $4t-2$, $4t-3$ ($4t + 1$) основных семейств.

Семейство квазиортогональных матриц порядков $4t-3$ дисперсное, значения порядков вложенных матриц нарастают в нем неаддитивно, поскольку по своей конструкции матрицы являются специфичными производными от основных матриц. В данном семействе есть оригинальные подсемейства с нарастающими по величине пропусками порядков и особыми точками, где матриц не существует или их существование ставится под сомнение. Свойство числа 9 последовательности $4t-3$ распадаться на пару множителей 3 последовательности $4t-1$ находит свое отражение в блочной структуре матрицы Якобсталя (основе матрицы Белевича из семейства порядков $4t-2$). Для разделения сугубо различных между собой подсемейств удобно пользоваться разными обозначениями $4t-3$ (матрицы Зейделя) и $4t+1$ (матрицы Ферма) этих порядков.

Семейство двухуровневых матриц Адамара порядков $4t$ характеризуется глобальным максимумом детерминанта. Как уже оказалось, для матриц соседних семейств важно не то, что максимум глобальный — он может быть и локальным, а то, что число уровней минимально — два.

Осознав это, можно уйти от исследования матриц с глобальным максимумом детерминанта по причинам, рассмотренным в работе [2]. Матрицы, отличающиеся *глобальным максимумом детерминанта* на уравнении связи $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$, соответствуют своему семейству чисел. На нечетных порядках $4t-1$ или $4t-3$ количество уровней не постоянно, оно растет почти линейно как $(n + 1)/2$. На порядках 3 и 5 имеются 2 и 3 уровня соответственно. На последующих порядках количество уровней отличается не более чем на 1 от оценочного. На четных порядках усложнения

матриц не наблюдаются, для $4t-2$ они являются трехуровневыми (иногда количество уровней больше). Особые точки на $4t-2$ — предмет отдельных исследований.

Порядок 13 специальный — это критическая точка; для него и далее *для всех нечетных порядков* количество уровней квазиортогональных матриц глобального максимума детерминанта значительно превышает приведенную выше линейную оценку. Переход от матриц с абсолютным условным экстремумом к матрицам локального максимума детерминанта принципиален.

Малое число уровней гарантирует лишь «слабый оптимум», но именно оно соответствует обширным семействам чисел. Отказ от поисков матриц глобального условного экстремума, характерного только для четных порядков, позволяет установить достаточно прочную связь между числами и квазиортогональными матрицами.

Неравенства Адамара

Неравенство Адамара 1. $|\det(\mathbf{A})| \le N_1 \times N_2 \times \ldots \times N_n$, где N_i — квадратичная норма столбца.

Соответствующая теорема доказана Адамаром [1]. На множестве квазиортогональных матриц неравенство Адамара сводится к следующему.

Неравенство Адамара 2. $|\det(\mathbf{A})| \le n^{n/2}$.

Из $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ следует, что $|\det(\mathbf{A})|^2 = |\omega(n)\mathbf{I}| = \omega(n)^n$, максимальное значение $\omega(n) = n$ достижимо при равенстве 1 модулей всех элементов каждого столбца. Равенство модулей и ортогональность столбцов совокупно достижимы лишь на порядках 1, 2 и далее на $4t$. На остальных порядках $|\det(\mathbf{A})| < n^{n/2}$.

Определение 4. Матрица Адамара — это квазиортогональная матрица $\mathbf{H}$ порядка n с элементами 1 и –1, для которой $\omega(n) = n$.

Значение $|\det(\mathbf{H})| = n^{n/2}$, и, соответственно, для нее достигается верхняя граница неравенства Адамара. Матрицы Адамара — это матрицы глобального максимума детерминанта, как условного, с учетом уравнения связи $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, так и безусловного, верхняя граница справедлива и для неортогональных по столбцам матриц.

Гипотеза Адамара состоит в том, что соответствующие матрицы существуют на порядках 1, 2 и $4t$.

Определение матриц Адамара через равенство, фиксирующее ортогональность их столбцов, и возможные уровни 1 и –1, не эквивалентно их определению через абсолютный максимум детерминанта. Оптимизационная постановка шире, это обстоятельство важно отметить в связи с другими нецелочисленными двухуровневыми матрицами.

Определение через равенство приводит к определению матриц основного семейства через совокупность всех его подсемейств. Так как подсемейства неисчерпаемы, как и вложенные в базисные порядки разнообразные подсистемы чисел, определение неконструктивно — оно не способствует собиранию подсемейств в единое семейство в рамках основной и общей для них черты — иметь максимум детерминанта.

Матрицы Мерсенна

Квазиортогональные матрицы вложенных в $4t$ порядков $n = 2^k$ выделены еще Сильвестром ввиду их орнаментальных свойств — способности создавать сложный фрактальный узор совокупно с исключительно простым правилом инверсии (транспонированием с масштабированием).

Адамар нашел пару матриц с аналогичными свойствами на порядках 12 и 20, выходящих за пределы последовательности, и предложил расширить семейство до $4t$, но не указал путь его пополнения.

Аналогично можно построить квазиортогональные матрицы порядков $n = 2^k - 1$, вложенных в последовательность $4t-1$ и обладающих локальным максимумом детерминанта. Последовательность $2^k - 1$ называется последовательностью чисел Мерсенна, поэтому сопровождающие их матрицы названы матрицами Мерсенна [6].

Возможны два определения матриц порядков $4t-1$.

Определение 5. Матрица Мерсенна — это квазиортогональная матрица $\mathbf{M}$ порядка n с элементами $a = 1$ и $-b$, где $b = \dfrac{t}{t+\sqrt{t}}$ для $n = 2^k - 1$.

Эти матрицы существуют, алгоритмы их вычисления описаны в работах [2, 6, 7]. Заметим, что у матриц Мерсенна каждый второй порядок отличается тем, что один их уровень иррационален. Как и в случае с матрицами Адамара, матрицы Мерсенна найдены на порядках 11 и 19 [8], что позволило сформулировать гипотезу о существовании матриц с нужной функцией уровня на порядках $4t-1$ [9].

Определение 6. Матрица Мерсенна — это двухуровневая квазиортогональная матрица порядка $4t-1$, имеющая локальный максимум $|\det(\mathbf{M})|$ на уравнении $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega(n)\mathbf{I}$ при свободной правой части $\omega(n)$, с уровнем $b = \dfrac{t}{t+\sqrt{t}}$, согласованным с уровнем матриц чисел Мерсенна $2^k - 1$.

В отличие от матриц Адамара, отсутствие которых на соседних нечетных порядках необходимо еще доказать, какие-либо другие порядки, кроме $4t-1$, не включены, поскольку в них не содержится последовательность чисел Мерсенна.

Оптимизация при свободной правой части $\omega(n)$ существенно отличается от оптимизации при зажатом нормировании. Не получить решение

в таких условиях невозможно. Не все решения могут быть признаны матрицами Мерсенна, а только те, которые согласованы по функции уровня с матрицами Мерсенна в узком их смысле.

Функция уровня является основой классификации семейств квазиортогональных матриц и составляет дополнительный критерий отбора входящих в семейство матриц. Такой подход предлагается распространить на все семейства квазиортогональных матриц, связанных с вложенными числовыми последовательностями.

Задачи разрешимые и неразрешимые

В теории и практике разрешимых и неразрешимых задач хорошо известен пример системы линейных алгебраических уравнений (СЛАУ) $\mathbf{Ax} = \mathbf{b}$, где $\mathbf{b}$ — вектор правой части. Система считается разрешимой, если существует вектор $\mathbf{x}$, при котором соблюдается тождество левой и правой частей этого уравнения.

Неразрешимая система называется *несовместной*.

Неразрешимую задачу можно формально «решить». Большое значение для систематизации решений неразрешимых задач матричной алгебры имеют работы Пенроуза, предложившего определения псевдорешения и псевдообратной матрицы, основанные на свойстве экстремальности.

Для решения приведенной задачи необходимо изменить ее формулировку на оптимизационную. Рассмотрим невязку левой и правой части линейного уравнения $\boldsymbol{\xi} = \mathbf{Ax} - \mathbf{b}$. Поставим цель оптимизировать невязку в смысле минимума квадрата ее нормы $\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\xi} = \|\mathbf{Ax} - \mathbf{b}\|^2$.

Все обычные решения СЛАУ определяются вектором нулевых невязок, самым малым из возможных значений квадратичной нормы. Они являются также решениями оптимизационной задачи.

В отличие от исходной задачи точного решения СЛАУ, оптимизационная совместна при любом векторе правой части, поскольку при нежестких условиях на область поиска решения всегда есть некоторый минимум.

Следует отметить, что переход к оптимизационной трактовке переводит задачу решения формально неразрешимых задач к заведомо разрешимым.

Пенроуз предусмотрел минимизацию нормы самого решения как дополнительное условие, если основная оптимизация дает не одно решение, а множество. Так, менее ста лет назад в линейной алгебре появилось новое понятие: псевдорешение $\mathbf{x} = \mathbf{A}^{+}\mathbf{b}$, где $\mathbf{A}^{+}$ — псевдообратная матрица Пенроуза [10, 11].

Другой, более близкой рассматриваемой в данной статье задаче, является задача на разрешимость квадратичного уравнения с одной переменной $\mathbf{x}^2 = \mathbf{b}$. Для $\mathbf{b} = 2$ задача не разрешима, например, в целых числах или отношениях целых чисел. Вместе с тем геометрический объект, который уравнение описывает, — прямоугольный треугольник с катетами единичной длины — существует.

Для поиска такого «решения» нужна смена парадигмы. От равенства переходят к задаче минимизации невязки $\boldsymbol{\xi} = |\mathbf{x}^2 - \mathbf{b}|$, выражая x все более точно через значения частных сумм ряда. Иными словами, осмысленное решение формально неразрешимой задачи получено аккуратной аксиоматикой, приведшей к возникновению понятия иррационального числа.

Квадратичное ограничение $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega(n)\mathbf{I}$ — матричное обобщение уравнения $\mathbf{x}^2 = \mathbf{b}$. Поиск целочисленного решения при зажатой правой части, как это делается при ограничении $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, приводит к той же проблеме, что и в элементарном частном случае. Поступим иначе — будем искать экстремальные по детерминанту квазиортогональные матрицы определенных порядков $4t - 1$, не зажимая условие в правой части, т. е. не назначая $\omega(n)$. Эта функция задается не априорно, а узнается апостериорно. После оптимизации из имеющихся экстремальных решений должно быть выбрано одно, согласованное с решением для числовой последовательности Мерсенна.

Это иной путь решения, повторяющий в некоторых деталях логику определения псевдообратных матриц по Пенроузу.

Смена парадигмы

Новый подход приводит к широкой программе исследований, в которой, в силу наличия различных числовых последовательностей и связей чисел с матрицами, возникают предположения и утверждения.

Мы утверждаем, что:

— числам Мерсенна соответствуют специальным образом определенные матрицы Мерсенна, числам Ферма — матрицы Ферма и т. п.;

— вложенность числовой последовательности чисел Мерсенна $2^k - 1$ в последовательности нечетных чисел $4t - 1$ обусловливает существование обобщенных матриц Мерсенна, соответствующих более широкой области чисел. У матриц, как и у чисел, существует наследование признаков принадлежности к более широким семействам;

— семейства квазиортогональных матриц различаются инвариантами, в которые входят *значения их элементов* (уровни): все матрицы Мерсенна и обобщенные матрицы Мерсенна порядков $4t - 1$ имеют два возможных значения модулей уровней $a = 1$ и $b = \dfrac{t}{t + \sqrt{t}}$. Остальные

семейства квазиортогональных матриц также отличаются своими функциями уровней;

— несуществование квазиортогональных матриц на порядках, соответствующих некоторым числам определенной последовательности, означает их неэквивалентность друг другу по матрицам, и там, где для возникновения неэквивалентности нет основания, справедливы теоремы, аналогичные теореме Таниямы.

В последовательности чисел $4t-1$ нет пропусков. Это означает, что существуют все без исключения обобщенные матрицы Мерсенна. Заметим, что гипотезы о существовании всех матриц Мерсенна нечетных порядков $4t-1$ и матриц Адамара четных порядков $4t$ сходны. Следуя логике теоремы Таниямы, можно говорить о сопоставлении матриц Адамара и Мерсенна между собой по их числовым инвариантам (порядкам).

Иными словами, если существуют матрицы Мерсенна, то существуют и матрицы Адамара, и наоборот.

Тождество SBIBD для матриц Мерсенна и Адамара

Для бинарных матриц порядков v количество элементов одного знака (пусть $a = 1$) в строке принято описывать параметром k. Параметр λ равен числу элементов одного знака, встречающихся попарно в двух соседних строках или столбцах. Сочетание параметров $\{v, k, \lambda\}$, которое принято называть *симметричным блочным дизайном* и обозначать устоявшейся аббревиатурой SBIBD, предложено как средство поиска междисциплинарных связей.

Один и тот же SBIBD могут иметь различные между собой математические объекты, столь же далекие, как числа и матрицы. Понятие «блок» в него пришло от графических задач с блоками, а симметрия напоминает о симметрии таких схем. Пример: матроид Фано — объект конечномерной геометрии, имеющий общий SBIBD с матрицей Адамара порядка $n = 8$.

Все матрицы Адамара характеризует один и тот же SBIBD $\{4t-1, 2t, t\}$, называемый *адамаровым дизайном* [12].

Если существует один объект какой-либо одной математической природы (блок, схема или таблица чисел) с SBIBD $\{v, k, \lambda\}$, то существуют и другие объекты, описываемые тем же самым SBIBD. Этим свойством пользуются для нахождения особенно сложных матриц Адамара или сходных с ними трехуровневых конференц-матриц Белевича. Так была найдена матрица Белевича порядка $n = 46$ конструкции Матона [13].

В адамаровом дизайне $\{4t-1, 2t, t\}$ понятно все, кроме размера $v = 4t-1$, не имеющего прямого отношения к порядку матрицы.

Заметим, что числа положительных элементов k и попарных соответствий элементов λ рассчитываются на всю матрицу. Наиболее часто происхождение несогласованного с порядком матрицы числа $v = 4t-1$ объясняется тем, что оно описывает порядок основы (core) нормализованной матрицы Адамара без ее каймы в предположении, что она не несет информационной нагрузки.

Числа $4t-1$ являются порядками обобщенных матриц Мерсенна, которые имеют два уровня (бинарны) и могут быть описаны SBIBD. Размер дизайна соответствует *мерсеннову дизайну*, поскольку в нем фигурирует порядок матриц Мерсенна. Покажем, что приведенный выше дизайн является общим для матриц Адамара и Мерсенна.

Параметры k, λ связаны с коэффициентами квадратичного условия связи. Произведение двух соседних строк матрицы содержит λ произведений aa, $2(k-\lambda)$ произведений ab ($k-\lambda$ элементов a каждой из строк умножено на b), и остающиеся $n-2k+\lambda$ произведений b^2. Согласно $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$, оно равно нулю, что дает уравнение $(n-2k+\lambda) \times b^2 - 2(k-\lambda)ab + \lambda a^2 = 0$, которое будем называть *характеристическим*. Оно в сжатой форме выражает условие ортогональности бинарной по уровням матрицы.

После подстановки значений $\{n, k, \lambda\} = \{4t-1, 2t, t\}$ характеристическое уравнение сводится к $(t-1)b^2 - 2tba + ta^2 = 0$. Положительный корень полинома левой части $b = \dfrac{t}{t+\sqrt{t}}$ является модульным уровнем матриц Мерсенна.

Следовательно, SBIBD — прямое параметрическое описание матриц Мерсенна порядков $4t-1$, отвечающее характеристическому уравнению для искомого варьируемого уровня. Если матрицы порядков $4t-1$ с иррациональными уровнями, называемые матрицами Мерсенна, существуют, то существуют и целочисленные матрицы Адамара. И наоборот: если существуют матрицы Адамара, то существуют и матрицы Мерсенна.

Существование матриц Мерсенна

Заметим, что в задачах определения существования решения не требуется уметь находить оптимальные матрицы. Важно указать на неразрешимое противоречие, которое возникает, если решения задачи нет.

Переход от целочисленных задач к задачам с иррациональными элементами описан выше, остается доказать существование матриц Мерсенна, причем в облегченной постановке, когда они рассматриваются как результат оптимизации. Задача на оптимум не меняется для порядков, входящих в последовательность $4t-1$, она

одинаково формулируется для любого t, и нет причин выделять одну матрицу среди других, опираясь только на различие в значениях t. Хотя искомых матриц бесконечно много, для нахождения не самих матриц, а всего лишь функции модуля уровня в виде формул $b = b(n)$ или $b = b(t)$, не обязательно искать все такие матрицы.

Пусть матрица порядка $n = 4t-1$ имеет уровни $(a = 1, -b)$ при $b \le 1$.

Значение $b = b(t)$ удовлетворяет квадратичному условию связи $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega(n)\mathbf{I}$, т. е. это корень полинома второго порядка $a_2b^2 + a_2ba + a_0a^2 = 0$. Для идентификации зависимости трех коэффициентов полинома a_2, a_2, a_0 от порядка матрицы (а значит, и искомой формулы для корня) нам достаточно найти несколько таких матриц на порядках, все равно каких, поскольку они не отличаются и ничем не предпочтительны. В табл. 1 приведены найденные нами для порядков, равных первым числам Мерсенна $n = 2^k-1$, параметры матриц и полиномы, которым они удовлетворяют согласно условию $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega(n)\mathbf{I}$, отвечающих при свободно заданной правой части $\omega(n)$ локальному максимуму детерминанта. Они найдены не из уравнений, а строго в оптимизационной постановке, включая многие порядки $n = 4t-1$ (в табл. 1 содержится только часть обработанного нами материала, для иллюстрации).

Таблицу можно продолжить, заметив, что для $n = 4t-1$ все описанные ею полиномы являются частными случаями полинома $(t-1)b^2 - 2tba + ta^2 = 0$.

Отсюда, при уровне $a = 1$, имеем формулу для $b = \dfrac{t}{t+\sqrt{t}}$, график этой зависимости приведен на рис. 3.

Зависимость коэффициентов b матриц Мерсенна от порядка n не содержит особых точек, свидетельствующих об отсутствии матриц. Так как функция уровня монотонна и *не имеет особых точек* на области ее определения $n = 4t-1$, отсюда следует вывод, что такая оптимизационная задача совместна всегда. В противном случае мы пришли бы к противоречию: уровень предвычислен, включая даже возможный тут иррациональный уровень, а матрицы нет. Это свидетельствовало бы о неоднородности такой задачи, а она, как нам известно, одинакова для всех порядков.

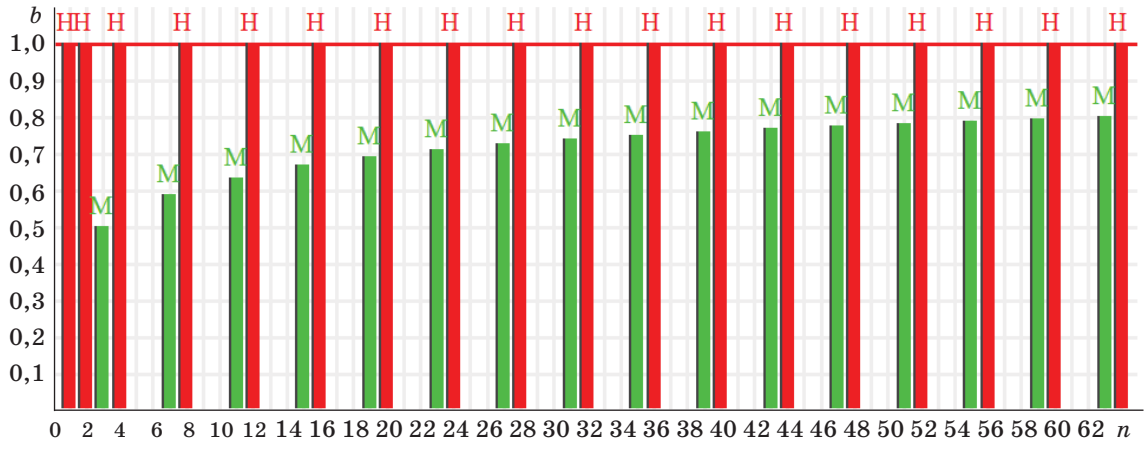
Итак, матрицы Мерсенна существуют для всей оси порядков вида $n = 4t-1$.

■ ***Таблица 1.*** Полиномы связи и значения уровней матриц Мерсенна

k	Порядок $n = 2^k - 1$	Полином	Уровни
1	1	$b = a$	$b = a$
2	3	$2b - a = 0$	$b = a/2$
3	7	$b^2 - 4ab + 2a^2 = 0$	$b = \left(2-\sqrt{2}\right)a$
4	15	$3b^2 - 8ab + 4a^2 = 0$	$b = 2a/3$
5	31	$7b^2 - 16ab + 8a^2 = 0$	$b = \left(8-2\sqrt{2}\right)a/7$
6	63	$15b^2 - 32ab + 16a^2 = 0$	$b = 4a/5$
7	127	$31b^2 - 64ab + 32a^2 = 0$	$b = \left(32-4\sqrt{2}\right)a/31$
8	255	$63b^2 - 128ab + 64a^2 = 0$	$b = 8a/9$

Выводы из существования матриц Мерсенна

Выводы касаются не только порядков матриц Адамара, но и всей числовой оси — всех последовательностей чисел и всех квазиортогональных матриц. Выделенные числами экстремальные



■ ***Рис. 3.*** Зависимость уровней матриц Мерсенна (**M**) и Адамара (**H**) от порядка n

■ ***Таблица 2.*** Значения уровней и функции веса семейств матриц

Порядок матрицы n	Матрица	Возможные значения элементов матрицы	Функция веса $\omega(n)$
$4t$	Адамара	1, –1	n
$2t$, $4t$	Белевича	1, –1, 0	$n-1$
t, $2t$, $3t$, $4t$	Себерри (взвешенная)	1, –1, 0	$n-k$
$4t-1$	Мерсенна	1, $-b$, где $b=\dfrac{t}{t+\sqrt{t}}$	$((n+1)+(n-1)b^2)/2=2t+(2t-1)b^2$
$4t-2$	Эйлера*	1, $-b$, где $b=\dfrac{t}{t+\sqrt{2t}}$	$((n+2)+(n-2)b^2)/2=2t+(2t-2)b^2$
$4t-3$	Зейделя	1, $-b$, d, где $b=1-2d$, $d=\dfrac{1}{1+\sqrt{n}}$	$(n-1)(1+b^2)/2+d^2=2(t-1)(1+b^2)+d^2$
$4t-3$	Ферма	1, $-b$, s, где $q=n-1=4u^2$, $p=q+\sqrt{q}$, $b=\dfrac{2n-p}{p}=1-\dfrac{2u-1}{2u+1}\times\dfrac{1}{u}$, $s=\dfrac{\sqrt{nq-2\sqrt{q}}}{p}=\dfrac{\sqrt{nu-1}}{2u+1}\times\dfrac{1}{\sqrt{u}}$	$1+4u^2s^2=k+(q-k)b^2+s^2$, где $k=\dfrac{q-\sqrt{q}}{2}=2u^2-u$

* Для матрицы Эйлера четного порядка указаны значения двух блоков ее бицикла.

ортогональные базисы существуют, им отвечают как целочисленные, так и иррациональные матрицы.

К матрицам Мерсенна примыкают, например, матрицы Эйлера [2], дополняющие порядки $4k$ и $4k-1$ четными порядками $4k-2$, не кратными 4.

Порядки матриц Ферма $2^{2^k}+1$ погружены в более общее семейство чисел $2^{2k}+1$, на которые соответствующие матрицы можно распространить. Они вложены в $4t+1$ не прямо, а опосредованно. Более общее их описание состоит в том, что они соответствуют произведениям близких пар чисел $4t-1$ и $4t-3$ или (с точность до 1) взвешенным квадратам чисел, т. е. $4t^2+1$. Порядки идут неравномерно 3, 5, 17, 35, 65, ..., среди них встречаются все числа Ферма 3, 5, 17, ... Среди меньших на 1 чисел им соответствуют порядки регулярных матриц Адамара, для которых все суммы столбцов и строк равны друг другу.

Матрицы Ферма, Адамара, Мерсенна, Эйлера (соседствующие с ними матрицы Белевича и взвешенные матрицы) и Зейделя, описанные в работе [2], отвечают основным числовым системам для порядков $n=4t+1$, $n=4t$, $n=4t-1$, $n=4t-2$, $n=4t-3$ соответственно. Матрицы Зейделя порядков $n=4t-3$ сопровождают матрицы Белевича порядков $n=4t-2$, это не экстремальные матрицы, а матрицы седловых точек. Они существуют не всегда, но если нет матрицы Зейделя, то нет и матрицы Белевича, и наоборот. Матриц Зейделя нет, если их порядок $n=4t-3$ не выразить суммой двух целых чисел. Это повторение взаимоотношений матриц Адамара порядков $n=4t$ и Мерсенна порядков $n=4t-1$.

Основная ветвь матриц описывается SBIBD $\{4t-1, 2t, t\}$, включающим в себя непосредственно параметры матриц Мерсенна (табл. 2).

Примеры подсемейств матриц Мерсенна

Получение подсемейств матриц Мерсенна опирается на различие числовых последовательностей, входящих в $n=4t-1$. Эти нечетные числа, включая числа Мерсенна, распадаются на простые (или степени простых чисел) и прочие. Для вычисления матриц соответствующих порядков в первом случае естественно привлекать конечные поля Галуа. Второй случай сложнее, поскольку конечное поле не может быть использовано. Особняком стоят порядки, равные произведениям пар простых чисел $n=p(p+2)$. Близким соседством к степеням простого числа 2^m отличаются и числа Мерсенна $n=2^m-1$, поэтому для них существует процедура с использованием поля Галуа GF(2), хотя сами по себе числа Мерсенна могут быть простыми и составными.

Сказывается выделенность числовых последовательностей Мерсенна и Ферма, базовых для всех квазиортогональных матриц.

Расчеты в поле GF(2). Начнем примеры с этого случая. Матрицы, отвечающие порядкам чисел Мерсенна $n=2^m-1$, отличает самая простая

структура — циклическая. Циклические матрицы находят, рассматривая их первую строку как выход динамической системы $\mathbf{x}_k = \mathbf{F}\mathbf{x}_{k-1}$ с компонентами вектора состояния в поле GF(2), $\mathbf{F}$ — матрица фробениусовой формы порядка m.

В имеющейся на этот счет обширной литературе свойственно подчеркивать необходимость адекватного выбора вектора начального состояния и параметров матрицы фробениусовой формы. От них, на самом деле, мало что зависит. Основной параметр здесь — порядок динамической системы m, а влияние каких-либо других чисел на вычислительный расчет означает их внутреннюю связь с числами Мерсенна, которой нет. Поэтому почти любой выбранный случайным образом вектор начального состояния и параметры динамической системы, определенные в поле GF(2), генерируют матрицу.

Итерационные процессы такого сорта хорошо известны в практике нахождения собственных векторов, теории цепей Маркова и т. п., когда вектор состояния стремится от некоторого почти произвольного начального состояния к главному собственному вектору матрицы системы. Конечное поле вносит свои коррективы, но $n = 2^m - 1$ — максимальная длина генерируемой последовательности, после которой эволюции динамической системы утрачивают свое разнообразие. По истечении n тактов дискретная система может только воспроизвести тот же самый процесс, появляется период.

Заменяя в выходном сигнале 0 на $-b$, получаем первую строку циклической матрицы, генерируемую сдвиговым регистром. Заметим, что динамическая система тоже может быть реализована на сдвиговом регистре, и этот метод усиленно рекламируется, хотя он малопродуктивен для порядков вне основной зависимости. Кроме того, в литературе этот генератор не ассоциируют с матрицами Мерсенна, хотя он генерирует именно их.

Дополняя циклическую матрицу каймой, получим матрицу Адамара порядка Сильвестра $n = 2^m$, на ней и концентрируется внимание. Это иной метод придания ортогональности циклическому массиву, не связанный с адаптацией положительного или отрицательного уровня.

Отсюда родом твиттер Мерсенна, описывающий блок в виде полосы верхних элементов матрицы Мерсенна шириною m, используемый для бинарного кодирования символов (кодов столбцов этой полосы).

Расчеты в поле GF(p). Выше была описана несложная, но большая динамическая система порядка m, теперь поле большое, и наступает черед упростить порядок системы до первого. Выход такой динамической системы первого порядка — показательная функция $x^{\lambda k}$ (экспонента, для краткости); от основания x и параметра λ мало что зависит (противоположное означало бы связи внутри числовой системы, они почти произвольны).

Значения этой экспоненты непосредственно описывают индексы отрицательных элементов $-b$ первой строки циклической матрицы Мерсенна.

Для большинства случаев подходит выбор $x = 2$ и $\lambda = 1$. Чтобы не выбирать с начальным условием, часто переходят к иному сорту комбинаторики, вычисляя степенные функции $k^2 \bmod p$. Те значения k, которые совпадут с любыми такими квадратами (мы ищем пересечение множества индексов с множествами квадратов индексов), называются квадратичными вычетами. Им присваивается значение *символа Лежандра*, равное 1. Остальным индексам соответствуют отрицательные символы Лежандра — в нашем случае выгодно считать их равными $-b$. Стартовому значению $k = 0$ отвечает 1. Трудность состоит в том, что k сравнивается не с собственным квадратом, а со всеми полученными квадратами, возникает перебор. Так что метод экспонент, описанный выше, более прост. Не надо подбирать, сразу имеем нужный нам индекс.

Для генерации матриц Мерсенна, поскольку эти матрицы пока малоизвестны, метод этот никогда не применялся, он описывается нами впервые.

Расчет для пары простых чисел p, $p + 2$. По́ля Галуа размера $n = p(p + 2)$ нет. Можно вычислить p значений $x^k \bmod(n)$ и $q - p$ значений $y^k \bmod(n)$ с основаниями $x = y \bmod(p)$, $x = 0 \bmod(p + 2)$, где y — примитивный элемент групп GF(p) и GF($p + 2$), $q = (n - 1)/2$. Примитивный элемент — это любой элемент, показательная функция от которого обходит всю группу, такие элементы связаны с размерами группы и подбираются несложно, можно случайным поиском. Этот расчет отличается от предыдущего только тем, что индексы отрицательных элементов $-b$ первой строки циклической матрицы Мерсенна генерируются совокупно двумя динамическими системами первого порядка.

Метод этот никогда не применялся для генерации матриц Мерсенна по той же причине, что и предыдущий, он описывается нами впервые.

Расчеты в поле GF(p^m). В данном случае также рассчитываются две функции, содержащие сумму и разность двух «экспонент» $x^{\lambda_1 k} + x^{\lambda_2 k}$, $x^{\lambda_1 k} - x^{\lambda_2 k}$, аналогов тригонометрических функций, косинуса и синуса (при равенстве, с точностью до знака, показателей, рассчитываемых в поле GF(p)). Бинарной последовательности или последовательности индексов в таком поле нет. Все элементы его имеют размер m, это векторы. Значения «парных символов Лежандра» рассчитаем сопоставлениями $x^{\lambda 0 k}$ с двумя указанными функциями. В этой удивительной математике

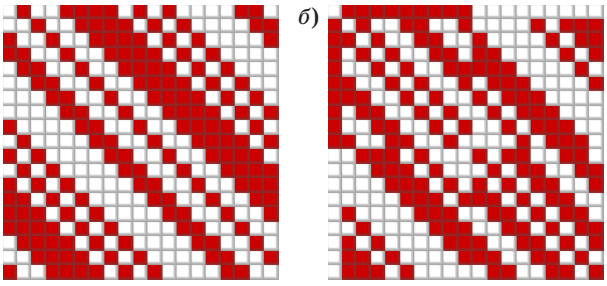
мало что зависит от второстепенных параметров, при выборе $\lambda_0 = \lambda_1 = 1$, $\lambda_2 = 0$ «экспонента» генератора упрощается до x^k, она сопоставляется на предмет пересечения с $x^k + 1$, $x^k - 1$.

Если экспонента пересекает функцию, то ставится 1, если нет, то –1, амплитудой отрицательного элемента заниматься пока рано. Отсюда получим две последовательности, для которых построим циклические матрицы **A**, **B** размера $(n-1)/2$, $n = p^m$.

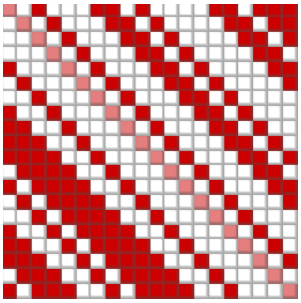
С их помощью складывается бициклическая форма (бицикл) $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$, охватываемая каймой с элементами из –1 и 1 напротив соответствующих матриц, первый элемент каймы 1 (рис. 4).

На завершающей стадии расчета отрицательный элемент –1 замещается на уровень матрицы Мерсенна $-b$. У этого метода есть альтернатива, когда вместо матрицы Мерсенна рассчитывается негациклическая матрица Белевича четного порядка $n = p^m + 1$. В данном случае нужна только одна последовательность (рис. 5). Она генерируется суммой экспоненты $\alpha = x^{\lambda_1 k + n/2}$ со своей степенью, т. е. функцией $\alpha + \alpha^{n-1}$. Сопоставляемая с нею на предмет пересечения вторая функция построена на квадрате основания $\beta = x^{2\lambda_2 k}$, в таком случае аддитивной добавкой в виде степени можно пренебречь, она не меняет расчет. Показатели $\lambda_1 = n - 1$ (нечетное число) и $\lambda_2 = n$ (четное число) можно упростить, взяв первый параметр равным 1. Вторую функцию рассчитываем для меньшего количества $(n-1)/2$ точек, остальные будут повторениями в силу ее четного показателя. Если сумма пересекает вторую функцию, то ставится –1, если нет, то 1, первое число последовательности равно 0.

а) *б)*



■ ***Рис. 4.*** Циклическая и бициклическая матрицы Мерсенна порядка 19



■ ***Рис. 5.*** Негациклическая матрица порядка 20

Далее матрица разбивается на четыре блока разделением четных и нечетных строк и столбцов, верхние два блока **A**, **B** после добавления к **A** единичной матрицы образуют бицикл четного порядка — матрицу Адамара. После нормирования от нее отнимают кайму, начинается стадия вытеснения –1 уровнем матрицы Мерсенна $-b$.

Этот метод расчета базируется на работах [14, 15], не соотнесенных, впрочем, с расчетом матриц Мерсенна, т. е. этот метод расчета матриц Мерсенна также нов. Упоминается он потому, что иллюстрирует сложный вид, который могут принимать матрицы подсемейств, основанных на разных системах чисел.

Нет никакого поля. Случай порядков $n = 4t - 1$ максимально общий, в него входят все предыдущие порядки. Сложность формы матрицы Мерсенна ограничена — это бициклическая матрица Мерсенна с одной каймой. Следовательно, все разнообразие числовой системы не повышает сложность структуры в сравнении с максимально сложным случаем расчета в полях Галуа. Алгоритм поиска универсален и нами освещен отдельно в работе [16]. Его общность и безотносительность к виду числовой системы, в которую входят порядки искомых матриц, подтверждают высказанные в работе [17] положения.

Произведение матриц Мерсенна. В силу тождества SBIBD матриц Мерсенна **M** порядка q и Адамара **H** порядка n имеет место тождество $\mathbf{H} = \begin{pmatrix} 1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{C} \end{pmatrix}$, где **e** — вектор единичных элементов; $\mathbf{C} = -\mathrm{sign}(\mathbf{M})$. Свойством округлять отрицательные элементы матрицы Мерсенна до –1 обладает также *произведение Скарпи* [18] (Scarpic product)

$$\mathbf{H}_{nq} = \mathbf{C} \times \mathbf{C} =$$

$$= \begin{pmatrix} \begin{pmatrix} 1 & c_{11}\mathbf{e}^{\mathrm{T}} \\ c_{11}\mathbf{e} & \mathbf{C} \end{pmatrix} & \begin{pmatrix} 1 & c_{12}\mathbf{e}^{\mathrm{T}} \\ c_{12}\mathbf{e} & \mathbf{C} \end{pmatrix} & \cdots & \begin{pmatrix} 1 & c_{1q}\mathbf{e}^{\mathrm{T}} \\ c_{1q}\mathbf{e} & \mathbf{C} \end{pmatrix} \\ \begin{pmatrix} 1 & c_{21}\mathbf{e}^{\mathrm{T}} \\ c_{21}\mathbf{e} & \mathbf{C} \end{pmatrix} & \begin{pmatrix} 1 & c_{22}\mathbf{e}^{\mathrm{T}} \\ c_{22}\mathbf{e} & \mathbf{TC} \end{pmatrix} & \cdots & \begin{pmatrix} 1 & c_{2q}\mathbf{e}^{\mathrm{T}} \\ c_{2q}\mathbf{e} & \mathbf{T}^{q-1}\mathbf{C} \end{pmatrix} \\ \cdots & \cdots & \ddots & \cdots \\ \begin{pmatrix} 1 & c_{q1}\mathbf{e}^{\mathrm{T}} \\ c_{q1}\mathbf{e} & \mathbf{C} \end{pmatrix} & \begin{pmatrix} 1 & c_{q2}\mathbf{e}^{\mathrm{T}} \\ c_{q2}\mathbf{e} & \mathbf{T}^{q-1}\mathbf{C} \end{pmatrix} & \cdots & \begin{pmatrix} 1 & c_{qq}\mathbf{e}^{\mathrm{T}} \\ c_{qq}\mathbf{e} & \mathbf{T}^{(q-1)(q-1)}\mathbf{C} \end{pmatrix} \end{pmatrix},$$

где **T** — матрица циклического сдвига в степени произведения индексов $(i-1)(j-1)$. Конструкция

симметричная, сдвигать можно как строки, так и столбцы. Это аналог кронекерова произведения матриц Адамара, ориентированный на вложение друг в друга матриц Мерсенна, знаки элементов **C** оказывают влияние только на кайму.

Итоговую матрицу Адамара порядка nq, q — простое число, можно, в свою очередь, представить в виде матрицы Мерсенна размера $nq-1$ и продолжить квадрирование. Матричная степенная функция дает связанные между собой пары матриц Мерсенна и Адамара новых порядков по отношению к матрицам, вычисляемым выше. Произведение Скарпи известно применительно к матрицам Адамара [18], первое применение к матрицам Мерсенна с поднятием негативного уровня до –1 описано в работе [19].

Некоторые рекомендации по исследованиям. Несмотря на обилие литературы по полям Галуа, а может быть, ввиду этого, найти конкретное описание операции, служащей для вычисления показательных функций, сложно. Правило сложения и вычитания векторов такое же, как и в обычной векторной алгебре. Операция умножения в полиномиальной арифметике полей Галуа основана на *свертке*, которая дает примерно вдвое (менее на 1, чем вдвое) больше коэффициентов, чем нужно элементу поля.

Нередуцируемый полином, с помощью которого образуется поле GF(p^m), по сути, представляет собой обратную связь, с помощью которой к m коэффициентам младшей части полинома произведения прибавляются старшие.

Чаще всего это $x^m = sx^d + r$, при $d = 1$ ко всем m младшим коэффициентам свертки прибавляются все старшие с множителями s, r за исключением крайних членов, к младшему коэффициенту произведения не дотягивается ветвь с весом s, к старшему коэффициенту — ветвь с весом r.

При $d > 1$ в этом алгоритме возникают поправки, описываемые следующей вычислительной схемой для векторов **C** = **AB**: на начальной стадии **C** = conv(**A**, **B**), это обычное произведение коэффициентов полиномов, поправки формируем в цикле для индекса $0 \le i \le m$:

c = **C**[i];
if ($i < m-1$) {c += r * **C**[$m + i$];
if ($i < d-1$) c += r * s * **C**[2 * $m - d + i$]};
if ($i > d-1$) {c += s * **C**[$m + i - d$];
if ($i < 2 * d-1$) c += s * s * **C**[2 * ($m - d$) + i])};
C[i] = c%p.

Схема полиномиального умножения напоминает нейронную, вспомогательный полином дает веса обратных связей, желательно, чтобы большую часть ветвей ликвидировали нулевые коэффициенты. Потребность в s-ветви отпадает совсем для GF(p^2), p — нечетное простое, произведение пары чисел $(a, b)(c, d) = (ac - rbd), (ad + bc)$. Это поле сходно с полем комплексных чисел, где $-r$ — аналог –1 (квадрат невычета). Параметр $r = 1$ (при $p + 1$ кратно 4) или $r = 3$ (при $p + 1$ кратно 6), в остальных случаях $r = 2$. Для более сложных полей параметры полинома приведены в табл. 3.

■ ***Таблица 3.*** Параметры неприводимого полинома

p	m	d	s	r	p	m	d	s	r	p	m	d	s	r
2	2	1	1	1	7	3	1	0	2	19	3	1	0	2
2	3	1	1	1	7	4	1	1	3	19	4	1	1	1
2	4	1	1	1	7	5	1	1	3	19	5	1	1	3
2	5	2	1	1	7	6	1	0	3	23	3	1	1	4
2	6	1	1	1	7	7	1	1	1	23	4	1	1	3
2	7	1	1	1	7	8	1	1	1	23	5	1	1	2
2	8	5	1	1	7	9	1	0	2	29	3	1	1	1
3	3	1	1	1	7	10	1	2	1	29	4	1	1	1
3	4	1	1	1	11	3	1	1	3	31	3	1	0	3
3	5	1	1	1	11	4	1	1	6	31	4	1	1	1
3	6	1	1	1	11	5	1	1	1	37	3	1	0	2
3	7	2	1	2	11	6	1	1	1	37	4	1	1	1
3	8	2	1	1	13	3	1	0	2	41	3	1	0	2
3	9	5	1	1	13	4	1	0	2	41	4	1	1	7
5	3	1	1	1	13	5	1	1	1	47	3	1	1	1
5	4	1	1	1	13	6	1	0	2	47	4	1	1	1
5	5	1	1	1	17	3	1	1	2	53	3	1	1	4
5	6	1	1	3	17	4	1	0	3	53	4	1	1	2
5	7	1	1	2	17	5	1	1	6	57	3	1	1	8
5	8	1	0	2	17	6	1	1	4	57	4	1	1	5

Заключение

Описав конкретные методы нахождения матриц Мерсенна, теперь позволим себе несколько фраз об общей философии рассматриваемого нами подхода. Достаточно очевидно, что матрицы Адамара — это фрактальный объект (его сравнивают с треугольником Серпинского), так же, как и все прочие такие матрицы. Мы показали, что матрицы могут быть иррациональными. Такой подход преимущественен с точки зрения меньших сомнений в существовании искомых матриц. Нет матриц — нет и соответствующих им чисел, а они есть, такая привязка дает существенные гарантии и позволяет по-новому взглянуть на старую проблему поиска целочисленных решений. Гипотеза Адамара, как и прочие сходные с ней гипотезы, уступает в своей сложности Великой теореме Ферма. Их проверка не должна быть столь же замысловатой.

В конечном поле показательная функция заметает собой все пространство и играет роль спирали, пронизывающей каждую его точку

без пересечения, что свойственно моделям детерминированного хаоса. Таковы решения некоторых нелинейных дифференциальных уравнений в бесконечномерном трехмерном пространстве. 3D нужно, чтобы интегральной кривой было место, где разместиться без самопересечений. Интегральная кривая (странный аттрактор) прошивает любую точку заполняемого ею объема один раз. В конечных полях происходит нечто аналогичное. «Аттракторы» динамических систем с пространством состояния в конечном поле образованы степенями примитивного элемента мультипликативной циклической группы (или подгруппы), выступающего в качестве начального условия показательной функции. Системы просты, сложность их поведения содержится в логике модульной или полиномиальной арифметики.

Не забываем и об оптимизируемом таким движением квадратичном критерии — детерминанте. Задача в любом случае — квадратичная. Квазиортогональные матрицы глобального максимума детерминанта нечетного порядка увеличиваются в размерах путем бифуркации их уровней, причем есть критическая точка — порядок 13. Матрицы Адамара — островные области, где ни количество уровней, ни сами эти уровни не меняются с ростом порядка.

Вся числовая система связана с малоуровневыми квазиортогональными матрицами. Матрицы высоких порядков (см. рис. 3 и табл. 3) при увеличении их размера все менее отличаются друг от друга и от матриц Адамара. Варьируемый отрицательный уровень позволяет матрице Мерсенна удерживать ортогональность столбцов, причем с ростом порядка элемент $-b$ стремится к -1.

Даже если читатель не согласен с рядом выдвинутых здесь положений или затрудняется их проверить самостоятельно, все же, согласитесь, это полезные примеры познания чисел и матриц в их взаимосвязи, имеющие перспективы в теории и практике вычисления экстремальных матриц ортогональных базисов.

Благодарности

Наше исследование циклических, бициклических, негациклических структур экстремальных матриц (называемых ради большей краткости *критскими* [20]) в том виде, как оно изложено, невозможно было бы без действенной помощи и совета профессоров Дженифер Себерри (Jennifer Seberry) и Драгомира Джоковича (Dragomir Đoković).

Дж. Себбери и Д. Джокович своими интересными работами и творчеством внесли большой вклад в создание алгоритмов поиска экстремальных квазиортогональных матриц с использованием полей Галуа.

В отношении доказательства гипотезы Адамара Дж. Себерри поддерживает ту часть утверждения, которая констатирует эквивалентность матриц Мерсенна и Адамара. Согласно более осторожному подходу, если нет матрицы Адамара, то нет и матрицы Мерсенна в том первом ее определении, где она задана равенством и сопоставляется с матрицей Адамара по системе совместных числовых инвариантов [21].

Литература

1. **Hadamard J.** Résolution d'une Question Relative aux Déterminants// Bulletin des Sciences Mathématiques. 1893. Vol. 17. P. 240–246.
2. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1(68). С. 2–15.
3. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Ферма // Информационно-управляющие системы. 2012. № 6(61). С. 90–93.
4. **Балонин Н. А., Сергеев М. Б.** Матрица золотого сечения G10 // Информационно-управляющие системы. 2013. № 6(67). С. 2–5.
5. **Balonin N. A., Vostrikov A. A., Sergeev M. B.** Two-Circulant Golden Ratio Matrices // Информационно-управляющие системы. 2014. № 5(72). С. 5–11.
6. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара — Мерсенна // Информационно-управляющие системы. 2012. № 5(60). С. 92–94.
7. **Балонин Ю. Н.** Программный комплекс MMatrix-2 и найденные им М-матрицы // Вестник компьютерных и информационных технологий. 2013. № 10(112). С. 58–64.
8. **Балонин Н. А.** О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2(63). С. 89–90.
9. **Сергеев А. М.** Обобщенные матрицы Мерсенна и гипотеза Балонина // Автоматика и вычислительная техника. 2014. № 4. С. 35–43.
10. **Bellman R.** Introduction to Matrix Analysis. — Philadelphia: SIAM, 1997. — 395 p.
11. **Воеводин В. В., Кузнецов Ю. А.** Матрицы и вычисления. — М.: Наука. Гл. ред. физ.-мат. лит., 1984. — 320 с.
12. Handbook of Combinatorial Designs. Second Edition (Discrete Mathematics and its Applications). 2nd Ed. / Charles J. Colbourn, Jeffrey H. Dinitz Ed. — Chapman and Hall, 2006. — 1000 p.
13. **Balonin N. A., Seberry J.** A Review and New Symmetric Conference Matrices // Информационно-управляющие системы. 2014. № 4(71). С. 2–7.

14. **Balonin N. A., Djokovic D. Z.** Negaperiodic Golay Pairs and Hadamard Matrices // Информационно-управляющие системы. 2015. № 5(78). С. 2–17. doi:10.15217/issn1684-8853.2015.5.2
15. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея // Информационно-управляющие системы. 2015. № 3(76). С. 2–16. doi:10.15217/issn1684-8853.2015.3.16
16. **Балонин Н. А., Сергеев М. Б.** О значении матриц начального приближения в алгоритме поиска обобщенных взвешенных матриц глобального и локального максимума детерминанта // Информационно-управляющие системы. 2015. № 6(79). С. 2–9. doi:10.15217/issn1684-8853.2015.6.2
17. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.
18. **Scarpis U.** Sui Determinanti di Valore Massimo// Rendiconti della R. Istituto Lombardo di Scienze e Lettere. 1898. Vol. 31. P. 1441–1446.
19. **Балонин Н. А., Балонин Ю. Н., Сергеев М. Б.** Вычисление матриц Мерсенна и Адамара методом Скарпи // Вестник информационных технологий, механики и оптики. 2014. № 3. С. 104–112.
20. **Balonin N. A., Seberry J.** Remarks on Extremal and Maximum Determinant Matrices with Real Entries ≤ 1 // Информационно-управляющие системы. 2014. № 5(71). С. 2–4.
21. **Seberry J., Balonin N. A.** Equivalence of the Existence of Hadamard Matrices and Cretan(4*t*–1,2)-Mersenne Matrices. http://arxiv.org/abs/1501.07012v1. (дата обращения: 20.12.2015).

UDC 519.614
doi:10.15217/issn1684-8853.2016.1.2

Mersenne and Hadamard Matrices

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: The goal of the paper is to show the correspondence of Mersenne numbers, Fermat numbers and numbers of other numerical sequences to multilevel matrices of local maximum determinant, which would guarantee both the existence of the matrices and the mutual correspondence of the matrix portraits to various kinds of numbers such as prime numbers, prime pairs or prime powers. **Methods:** The search for global or local maximum determinant matrices is performed by an iterative computational procedure focused on the minimization of the maximum absolute values of the elements of an orthogonal matrix. **Results:** A theory of mutual correspondence between numbers and extremal matrices has been developed, which simplifies the search for unknown matrices, classifying the matrices by types of numbers. We propose a broader interpretation of Hadamard conjecture by adequate hypotheses about the existence of multilevel quasiorthogonal matrices. A proof is given for the existence of Mersenne matrices and, as a consequence, of Hadamard matrices, too. For the calculation of Mersenne matrices, we propose algorithms based on Galois finite field arithmetics. These algorithms are concordant by results with the optimization procedures of increasing the determinant, being complemented by them. **Practical relevance:** Multilevel local maximum determinant matrices are orthogonal and have a direct practical value for the problems of error-correcting coding, video compression and masking.

Keywords — Orthogonal Matrices, Mersenne Matrices, Hadamard Matrices, Hadamard Conjecture, Galois Finite Fields, Cyclic Matrices, Negacyclic Matrices, Bicirculant Matrices, Numerical Methods.

References

1. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
2. Balonin N. A., Sergeev M. B. Local Maximum Determinant Matrices *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 1(68), pp. 2–15 (In Russian).
3. Balonin N. A., Sergeev M. B., Mironovsky L. A. Calculation of Hadamard Fermat Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 6(61), pp. 90–93 (In Russian).
4. Balonin N. A., Sergeev M. B. Matrix of Golden Ratio G10. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 6(67), pp. 2–5 (In Russian).
5. Balonin N. A., Vostrikov A. A., Sergeev M. B. Two-Circulant Golden Ratio Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5(72), pp. 5–11.
6. Balonin N. A., Sergeev M. B., Mironovsky L. A. Calculation of Hadamard–Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 5(60), pp. 92–94 (In Russian).
7. Balonin Yu. N. The Software Complex MMatrix-2 and Searched Minimax Matrices. *Vestnik komp'iuternykh i informatsionnykh tekhnologii* [Herald of Computer and Information Technologies], 2013, no. 10(112), pp. 58–64 (In Russian).
8. Balonin N. A. Existence of Mersenne Matrices of 11th and 19th Orders. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 2(63), pp. 89–90 (In Russian).
9. Sergeev A. M. Generalized Mersenne Matrices and Balonin's Conjecture. *Avtomatika i vychislitel'naia tekhnika*, 2014, vol. 48, no. 4, pp. 214–220 (In Russian).
10. Bellman R. *Introduction to Matrix Analysis*. Philadelphia, SIAM, 1997. 395 p.
11. Voevodin V. V., Kuznetsov Iu. A. *Matritsy i vychisleniia* [Matrices and Calculations]. Moscow, Nauka Publ., 1984, 320 p. (In Russian).
12. *Handbook of Combinatorial Designs. Second Edition* (*Discrete Mathematics and its Applications*). 2nd Ed. (Charles J. Colbourn, Jeffrey H. Dinitz Ed.). Chapman and Hall/CRC, 2006. 1000 p.
13. Balonin N. A., Seberry J. A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie*

sistemy [Information and Control Systems], 2014, no. 4(71), pp. 2–7.
14. Balonin N. A., Djokovic D. Z. Negaperiodic Golay Pairs and Hadamard Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 5(78), pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2
15. 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(76), pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.16
16. Balonin N. A., Sergeev M. B. Initial Approximation Matrices in Search for Generalized Weighted Matrices of Global or Local Maximum Determinant. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 6, pp. 2–9 (In Russian). doi:10.15217/issn1684-8853.2015.6.2
17. Balonin N. A., Sergeev M. B. On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 5(66), pp. 2–8 (In Russian).
18. Scarpis U. Sui Determinanti di Valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, vol. 31, pp. 1441–1446 (In Italian).
19. Balonin N. A., Balonin Yu. N., Sergeev M. B. Mersenne and Hadamard Matrices Calculation by Scarpis Method. *Vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2014, no. 3, pp. 104–112 (In Russian).
20. Balonin N. A., Seberry J. Remarks on Extremal and Maximum Determinant Matrices with Moduli of Real Entries ≤ 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5(71), pp. 2–4.
21. Seberry J., Balonin N. A. *Equivalence of the Existence of Hadamard Matrices and Cretan(4t–1,2)-Mersenne Matrices*. Available at: http://arxiv.org/abs/1501.07012v1 (accessed 20 December 2015).