УДК 519.61:511-33

Матрицы Мерсенна и Адамара

Н. А. Балонин[а], М. Б. Сергеев[б]

[а]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ

[б]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, РФ

Подготовлено для журнала Информационно-управляющие системы. 2016. № 1

Введение

Отношения чисел и математических объектов иной природы, функций и матриц, естественны, поскольку математика – единый предмет, для удобства разделенный на области. Выход на границы лежит вне основного интереса отдельной науки и до поры до времени обособленные дисциплины развиваются автономно.

Тем не менее, наступает момент, когда междисциплинарные исследования приносят свои плоды. Пример тому дает история с гипотезой Таниямы. Содержание ее следующее. Любая эллиптическая кривая, заданная над полем рациональных чисел, характеризуется своими параметрами. Математический объект другой природы, модулярная форма, также дает нам последовательность чисел. В сентябре 1955 Ютака Таниама высказал мало тогда замеченное предположение о том, что эллиптические кривые являются *модулярами*, то есть, нет такой эллиптической кривой, для которой не нашлась бы адекватная ей по набору параметров модулярная форма.

Гипотезой заинтересовались, когда в 1985 году Герхар Фрэй предположил, что она является обобщением Великой теоремы Ферма, потому как любой контрпример к Великой теореме Ферма приводил в итоге к немодулярной эллиптической кривой. Гипотезу доказали, и этот случай 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 имеют своим представительством ортогональные матрицы, или, лучше для нас, *квазиортогональные* матрицы – масштабированные ортогональные матрицы с максимальным элементом, равным по модулю единице. Наше видение состоит в том, что с числовыми последовательностями соотносятся не все такие матрицы, а только экстремальные. Те, у которых детерминант максимален.

То, что экстремальные квазиортогональные матрицы отвечают (имеют порядки из) числовой последовательности $4t$, t – здесь и далее в таких случаях натуральное число, заметил еще Адамар [1]. Он высказал предположение (гипотеза Адамара), сходное с предположением Таниямы, о том, что экстремальные матрицы – своего рода “модуляры” 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.

Согласное с этим наблюдением новое предложение, которое мы высказали и подкрепили примерами матриц в [2], состоит в том, что не только четным $4t$ и $4t–2$, но и нечетным системам чисел $4t–1$ и $4t–3$ отвечают семейства экстремальных матриц.

Системы чисел эти слишком общие и распадаются на вложенные в них последовательности простых чисел p, степеней простых чисел p^m, m – натуральное число, пар близких простых чисел p и $p+2$, чисел Мерсенна $2^k–1$, k – натуральное число, чисел Ферма $2^{2^k}+1$, k – не отрицательное целое число и т. п. Согласно общей идее, распадаются на подсемейства также и матрицы, подробно рассмотренные нами в серии статей, предварявших собирательный обзор [2] (с необходимыми ссылками), подводящий итог нашей программы исследований.

За два года произошли изменения и появились новые наблюдения, в связи с чем возникла потребность в новом обзоре. Если ранее мы находили матрицы некоторым универсальным путем, то теперь выяснилась возможность кардинально ускорить их поиск, опираясь на отмеченное видовое разнообразие.

К тому же, любая такая ветвь, естественно, приводит к аналогу гипотезы Таниямы, и у нас появились новые соображения на этот счет. В конце концов, гипотеза стала теоремой, и у нашей программы исследований есть точно такая же перспектива, в которой предположение Адамара играет, как видно, весьма частную роль.

Речь идет о значительно большем обобщении, судя по количествам вовлеченных в рассмотрение систем чисел. Для полноценного восприятия материала статьи мы изложим сначала некоторые примеры, уточним новые понятия и дадим полезные сведения.

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 $p=x^2+y^2$.

Еще 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.

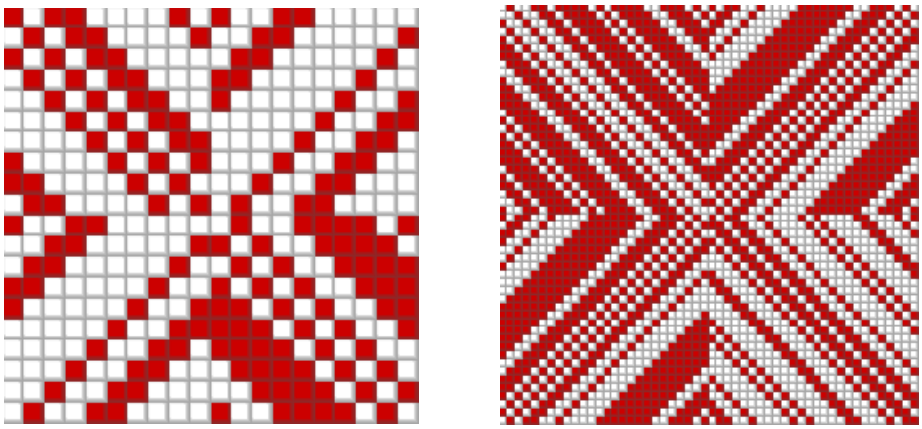


Рис. 1. Бициклические матрицы порядков n=20 и 52: p=5 и 13

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. На рис. 2 представлено универсальное 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.

Матрицы Ферма и золотого сечения

Классическими объектами теории чисел являются простые числа Ферма, известно пять таких чисел F_k = 3, 5, 17, 257, 65537. В 1796 году 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.

Так как 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 (рис. 2) – матрицы глобального максимума детерминанта $F_{k-1}/(2F_k-1)^{1/2}B$, где B – ограничение на детерминант сверху, данное Гвидо Барба.

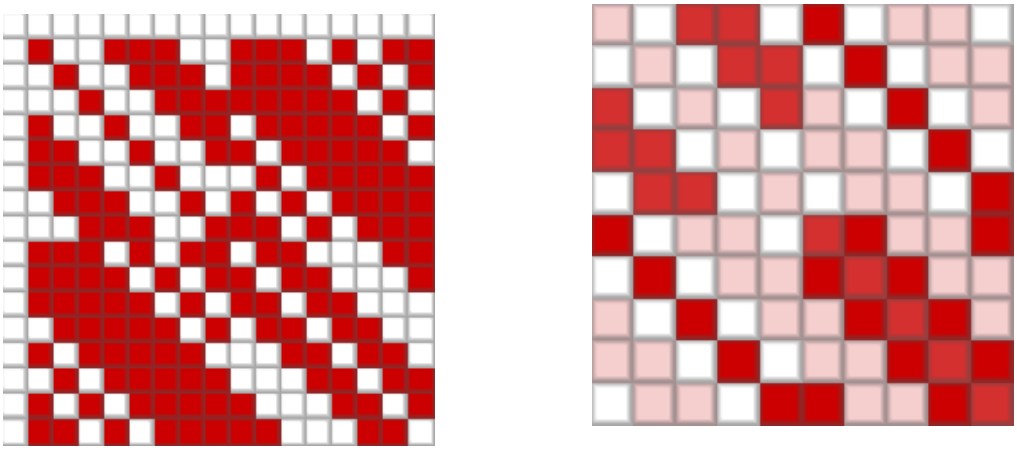


Рис. 2. Матрицы Ферма порядка 17 и золотого сечения порядка 10

Проверка оставшихся порядков 257, 65537 не проведена, но предположение (гипотеза), что они отвечают экстремумам, в слабом варианте – локальным, логично вытекает из знаменитой теоремы Гауса.

Другой пример не менее примечателен, в работах [4, 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 нового обширного материала, стоит остановиться, хотя бы вкратце, на общей картине, которую дают квазиортогональные матрицы. Приведем сначала их определение.

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

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

Определение 3. Локальный *максимум детерминанта* достигается тогда, когда любое достаточно малое по параметрам изменение матрицы, не нарушающее вида уравнения связи $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$ при свободно заданном значении веса $\omega(n)$, приводит к уменьшению детерминанта *).

Когда говорят о максимуме детерминанта, имеется в виду, что матрицы, имеющие максимум только лишь модуля детерминанта приводимы к экстремальной по детерминанту матрице инверсией знаков их элементов. Поэтому слово модуль чаще всего опускается, для простоты рассуждения, но иногда его надо указывать, чтобы выкладки не утрачивали корректность.

Тем самым, *допустимыми* являются любые изменения параметров варьируемой матрицы, не нарушающие условие ортогональности ее столбцов. Весовая функция в задачах поиска условного максимума $|\det(\mathbf{A})|$ на ограничении вида $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$ заранее не задана, и сама по себе является предметом поиска. В этом важное их отличие от задачи на поиск 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, отвечающее некоторой достаточно общей числовой последовательности, выражающей их порядки, отличается от прочих матриц количеством различных между собою элементов (уровней). Например, матрицы Адамара с элементами 1, –1, это двухуровневые матрицы. Только у них значения уровней не зависит от их порядков, функции уровней – константы.

Для экстремальных двухуровневых матриц один из уровней, по определению, равен 1 (или –1), иначе значение детерминанта матрицы можно повысить элементарным масштабированием.

Варьируемая функция уровня семейства двухуровневых матриц – всего лишь одна. К ним примыкают матрицы четных порядков, удвоение уровней наблюдается лишь в силу изменения знака при блоках.

Подсемействам квазиортогональных матриц отвечают порядки, вложенные в основные числовые последовательности. Элементы подсемейств отличаются между собой структурами матриц. Простейшими являются циклическая, бициклическая и негациклическая формы. Если регулярная структура не реализуема, появляются структура сложнее и блочные матрицы, содержащие в своем составе циклические, обратные циклические, негациклические и т.п. блоки, а также кайму.

Например, для матриц Адамара таковой являются конструкция из четырех блоков. Отделять универсальные структуры от частных полезно, они различимы для всех порядков $4t$, $4t–1$, $4t–2$, $4t–3$ ($4t+1$) основных семейств.

Семейство порядков $4t–3$ дисперсное, значения порядков вложенных матриц нарастают в нем не аддитивно ввиду того, что по своей конструкции матрицы являются специфичными производными от матриц основных ветвей. Есть здесь свои оригинальные подсемейства с нарастающими по величине пропусками порядков и особыми точками, где матриц не существует или их существование ставится под сомнение. Свойство числа 9 семейства $4t–3$ распадаться на пару множителей 3 семейства $4t–1$ находит свое воплощение в блочной структуре матрицы Якобсталя (основе матрицы Белевича порядка $4t–2$). Для разделения здесь подсемейств на виды удобно пользоваться разными обозначениями этих порядков как $4t–3$ и $4t+1$, не смешивая их между собой.

В этой общей картине не хватает одной детали.

Семейство двухуровневых матрицы Адамара порядков $4t$ характеризуется глобальным максимумом детерминанта. Как оказалось, для матриц соседних семейств важно не то, что максимум глобальный, а то, что это вообще некоторый максимум, пусть локальный, и число уровней минимально – два. Пройдя эту поворотную точку, мы уходим от матриц с глобальным максимумом по причинам, затронутым в прошлом обзоре [2].

Матрицы, отличающиеся *глобальным максимумом детерминанта* на уравнении связи $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \omega(n)\mathbf{I}$ (абсолютным условным экстремумом) отвечают своему семейству чисел. На нечетных порядках $n=4t–1$ или $n=4t–3$ количество уровней не постоянно, но оно растет почти линейно как $(n+1)/2$, на порядках 3 и 5 мы имеем 2 и 3 уровня, соответственно, далее показатели отличаются не более, чем на 1, от оценочного. На четных порядках усложнения матриц не наблюдается, кроме того, что для $4t–2$ востребовано не два, а три основных уровня, иногда (в особых точках), впрочем, больше. Особые точки на $4t–2$ – предмет отдельных исследований.

Порядок 13 особенный, это критическая точка, для него и далее *для всех нечетных порядков* количество уровней значительно приведенную выше оценку. Переход от матриц с абсолютным условным экстремумом к матрицам локального максимума детерминанта принципиален. Низкое число уровней гарантирует лишь “слабый оптимум”, но именно оно отвечает обширным семействам чисел. Отказ от поисков матриц глобального условного экстремума, характерного только для четных порядков, позволяет установить достаточно прочное соответствие между числами и квазиортогональными матрицами.

Неравенство Адамара

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

Соответствующая теорема доказана Адамаром [1].

На множестве квазиортогональных матриц неравенство Адамара сводится к следующему.

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

В самом деле, из $\mathbf{A}^T\mathbf{A} = \omega(n)\mathbf{I}$ следует, что $|\det(\mathbf{A})|^2 = |\omega(n)\mathbf{I}| = \omega(n)^n$, максимальное значение $\omega(n) = n$ достижимо при тождестве 1 модулей всех элементов каждого столбца. Извлекая корень квадратный, получаем выражение выше.

Ортогональность столбцов матрицы и тождество модулей всех элементов 1 совокупно достижимы лишь на порядках 1, 2 и далее кратных 4, т.е. $n=4t$, t − натуральное число. На остальных порядках имеет место быть $|\det(\mathbf{A})| < n^{n/2}$.

Определение 4. Матрица Адамара, это квазиортогональная матрица **H** с элементами 1 и –1.

Согласно определению, $\mathbf{H}^T\mathbf{H} = n\mathbf{I}$, $\omega(n) = n$.

Значение $|\det(\mathbf{H})| = n^{n/2}$, т. е. это матрица, на которой достигается верхняя граница неравенства Адамара. Матрицы Адамара, это матрицы не локального, а глобального максимума детерминанта, как условного, с учетом уравнения связи $\mathbf{H}^T\mathbf{H} = n\mathbf{I}$, так и безусловного, верхняя граница справедлива и для не ортогональных по столбцам матриц.

Гипотеза Адамара состоит в том, что соответствующие матрицы есть для любого $n=4t$**.** За пределами порядков 1, 2 и $n=4t$ матрицы Адамара не существуют.

Определение матриц Адамара через равенство, фиксирующее ортогональность ее столбцов, и возможные уровни (два, одинаковых по модулю), не эквивалентно определению их же через базовое их свойство, иметь максимум детерминанта.

Определение через равенство приводит нас 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. Не способствует собиранию подсемейств в единое семейство в рамках основной и общей для них черты – доставлять максимум детерминанта.

Матрицы Мерсенна

Возможны два определения матриц порядков $n=4t-1$, t − натуральное число. Первое определение в своем обосновании проходит тот же путь, который прошли матрицы Адамара. Основное подсемейство матриц Адамара было найдено примерно полстолетия назад, до выпуска центральной статьи [1].

Это квазиортогональные матрицы вложенных в $n=4t$ порядков $n = 2^k$, выделенные еще Сильвестром, признанным наряду с Кэли основателем теории матриц, ввиду их орнаментальных свойств − способности создавать сложный фрактальный узор совокупно с исключительно простым правилом инверсии (транспонированием с маштабированием). Адамар нашел пару матриц с аналогичными свойствами, но порядков 12 и 20, выходящими за пределы указанной последовательности, и предложил расширить семейство до $n=4t$, но не указал путь, как пополнять.

Далее оно начинялось подсемействами уже при имеющемся и ограничивающем возможности доказательства гипотезы Адамара определении.

Аналогично, можно построить квазиортогональные матрицы вложенных в $n=4t-1$ порядков $n = 2^k-1$, обладающих локальным экстремумом детерминанта, не включая это свойство в определение. Последовательность $n = 2^k-1$ называется последовательностью чисел Мерсенна, поэтому сопровождающие числа матрицы назовем матрицами Мерсенна.

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

Эти матрицы существуют, алгоритмы вычисления неоднократно описаны в наших статьях, отмеченных в обзоре [2].

Заметим теперь, что у этих матриц каждый второй порядок отличается тем, что их уровень иррационален. Поэтому, хотя мы можем найти, как и в случае Адамара, аналогичные матрицы на порядках 11 и 19 и сформулировать гипотезу о существовании матриц с нужной функцией уровня для порядков $n=4t-1$, что и было сделано [3], проще поступить иначе.

Возьмем за основу определения то, что сделано было ранее основным свойством.

Определение 6. Матрица Мерсенна, это двухуровневая квазиортогональная матрица порядка $n=4t-1$, доставляющая локальный максимум модуля детерминанта $|\det(\mathbf{M})|$ на уравнении связи $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \omega(n)\mathbf{I}$ при свободной правой части $\omega(n)$, с согласованной для последовательности чисел Мерсенна $n = 2^k-1$ функцией уровня $b = \dfrac{t}{t+\sqrt{t}}$.

В отличие от матриц Адамара, отсутствие которых на соседних нечетных порядках надо еще доказать, какие либо другие порядки, кроме $n=4t-1$ 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. Однако не все из них мы признаем матрицами Мерсенна, а только те, которые согласованы по функции уровня с матрицами Мерсенна. Некоторая отдаленная аналогия есть у вырожденных систем линейных уравнений, когда решение неединственно, выбирается одно, минимальное по норме. По дополнительному условию. Функция уровня является основой классификации семейств квазиортогональных матриц, и она составляет дополнительный критерий отбора входящих в семейство матриц.

Задачи разрешимые и неразрешимые

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

Неразрешимая система называется *несовместной*.

Неразрешимую задачу можно формально “разрешить”. Большое значение для систематизации решений неразрешимых задач матричной алгебры сыграл Пенроуз, предложив упомянутое выше опирающееся на минимальность нормы, т. е. на экстремальность, определение псевдорешения и псевдообратной матрицы. Но он вообще сыграл большую роль во многих областях математики, необходимая на рассматриваемый случай информация есть в справочниках [4, 5].

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

Все обычные решения системы линейных алгебраических уравнений отвечают нулевому вектору невязки, самому малому из возможных значений квадратичной нормы. Они являются также решениями оптимизационной задачи.

В отличие от исходной задачи на точное решение уравнений, оптимизационная совместна при любом векторе правой части, поскольку при нежестких условиях на область поиска решения всегда есть некоторый минимум. Обратим внимание, что шагом, позволяющим перейти от задач формально не всегда разрешимых к заведомо разрешимым, т.е. совместным, является переход к их оптимизационной трактовке.

Кроме того, Пенроуз предусмотрел минимизацию нормы самого решения x, как дополнительное условие, если основная оптимизация дает не одно решение, а множество. Так, менее ста лет назад, в исхоженной вдоль и поперек области линейной алгебры, появилось новое понятие: псевдорешение $x=\mathbf{A}^{+}b$, где $\mathbf{A}^{+}$ − псевдообратная матрица Пенроуза [4].

Другой пример на ту же тему ближе нам по постановке, это античная задача на поиск диагонали равнобедренного треугольника. С древности известны пифагоровы тройки чисел, такие, что $a^2 + b^2 = x^2$, и алгоритм их построения. Близкая по смыслу тривиальная задача на разрешимость квадратичного уравнения с одной переменной $x^2 = b$ зависит (как и в случае линейных уравнений, выше) от правой части. Для b=2 задача неразрешима, 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. Вместо точного равенства переходят к задаче минимизации невязки $\xi = |x^2 - b|$ выражая x все более точно, в смысле ее минимума через значения частных сумм ряда. Иными словами, осмысленное решение формально неразрешимой задачи получено аккуратной аксиоматикой, приведшей к возникновению понятия иррационального числа.

Квадратичное ограничение $\mathbf{M}^{\mathrm{T}}\mathbf{M}=\omega(n)\mathbf{I}$ является матричным обобщением уравнения $x^2=b$.

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 $n=4t-1$, не зажимая условие в правой части, не назначая $\omega(n)$. Эта функция задается не априорно, а узнается апостериорно. После оптимизации из имеющихся экстремальных решений выбираем одно, согласованное с решением для числовой последовательности Мерсенна.

Это иной путь, он повторяет в некоторых деталях логику определения псевдообратных матриц по Пенроузу, поэтому мы ее напоминаем.

Смена парадигмы

Нетрудно видеть, что новый подход приводит к широкой программе исследований, в которой предположения возникают автоматически, в силу наличия различных семейств чисел и связи чисел с матрицами.

Мы, кратко перечисляя, утверждаем, что:

– числам Мерсенна (например), отвечают некоторые 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 влечет за собой существование обобщенных матриц Мерсенна, отвечающих уже более широкой области чисел, т. е. у матриц, как и у чисел, существует наследование признаков принадлежности к более широким семействам;

– семейства квазиортогональных матриц различаются между собой инвариантами, в которые входят *значения их элементов* (уровни) : все матрицы Мерсенна и обобщенные матрицы Мерсенна порядков $4t$–1 имеют два возможных значения противоположных по знаку элементов с модулями a, b, причем одно этих чисел равно 1, второе $\frac{t}{t+\sqrt{t}}$, и остальные семейства тоже отличаются своими функциями уровня;

– не существование сопровождающих числа матриц названной природы означает настолько глубокое различие чисел одного семейства, что можно говорить об их неэквивалетности друг другу (по матрицам), и там, где для возникновения неэквивалентности нет почвы, справедливы теоремы, аналогичные теореме Таниямы.

В работе [2] предпочтение было отдано системе обозначений, в которых первый элемент матрицы равен a=1, а второй, соответственно, равен $-b$. Так как модуль детерминанта матрицы индифферентен к смене знаков элементов матрицы, возможное альтернативное определение, в котором элемент с положительным знаком будет равен значению функции уровня $\frac{t}{t+\sqrt{t}}$, а второй, соответственно, примет значение -1.

Иными словами, если среди чисел $4t$–1 нет пропусков, а их нет, и семейство это отвечает множеству сопровождающих их матриц, то существуют все без исключения обобщенные матрицы Мерсенна. Заметим, что гипотезы о существовании всех матриц Мерсенна нечетных порядков $4t$–1 и матриц Адамара четных порядков $4t$ не просто сходны. Следуя логике теоремы Таниямы, можно говорить о сопоставлении, теперь уже, матриц Адамара и Мерсенна между собой по их числовым инвариантам (порядкам).

Так что если существуют матрицы Мерсенна, то существуют и матрицы Адамара, и наоборот. Дополним это положение дополнительными аргументами.

Тождество SBIBD для матриц Мерсенна и Адамара

Для бинарных структур количество элементов одного знака (пусть, a=1) в строке матрицы принято описывать параметром k. Вторым параметром λ отражают число элементов одного знака, встречающихся попарно в двух соседних строках или столбцах, все равно. Сочетание параметров $\{v, k, \lambda\}$ принято называть *симметричным блочным дизайном* (кратко) и обозначать устоявшейся аббревиатурой SBIBD.

Все матрицы Адамара характеризует один и тот же SBIBD $\{4t-1, 2t, t\}$, называемый *адамаров дизайн* [6].

В силу свободы выбора за основу положительных или отрицательных элементов, часто используют более распространенное описание $\{4t-1, 2t-1, t-1\}$, нам предпочтительнее вариант, когда положительных элементов больше отрицательных.

SBIBD предложен как средство поиска междисциплинарных связей.

Один и тот же SBIBD могут иметь весьма 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. Из книги в книгу ходит пример, иногда выносимый на обложку, схемы матроида Фано. Объекта конечномерной геометрии, имеющего общий SBIBD с матрицей Адамара порядка 8.

Смысл выделения SBIBD состоит в том, что если существует один объект, какой-либо одной математической природы, скажем, блок схема или таблица чисел с параметрами $\{v, k, \lambda\}$, то существуют и другие объекты, описываемые тем же самым SBIBD. Этим свойством иногда пользуются для нахождения особенно сложных матриц Адамара или сходных с ними трехуровневых матриц Белевича (конференц-матриц). Так найдена матрица Белевича порядка 46 конструкции Матона [7].

В адамаровом *дизайне* $\{4t-1, 2t, t\}$ понятно все, кроме размера $v=4t-1$, не имеющего прямого отношения к порядку матрицы. Заметим, что числа k положительных элементов и попарной встречи λ элементов рассчитываются на всю матрицу. Наиболее часто происхождение не согласованного с порядком матрицы числа $v=4t-1$ объясняется тем, что оно описывает порядок основы (core) нормализованной матрицы Адамара без ее каймы. Дескать, кайма не несет информационную нагрузку.

Заметим теперь, что число $n=4t-1$ описывает порядок обобщенных матриц Мерсенна, они тоже бинарны, у них два уровня, и по общей логике вещей этот междисциплинарный SBIBD касается и их. У него, пожалуй, больше прав называться *мерсеннов дизайн*, а не адамаров, поскольку размер дизана в точности соответствует порядку матрицы без каких-либо иных дополнительных соображений. Заметим, что происхождение термина туманно, и в литературе не приводятся обоснования, кроме исторического, почему данный дизайн назвали адамаров.

Матрицами Адамара начали интересоваться раньше, и не более того.

Покажем, что дизайн в самом деле общий.

Параметры k, λ связаны с коэффициентами квадратичного условия связи. Произведение двух соседних строк матрицы содержит λ произведений вида a^2, $2(k-\lambda)$ 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 отвечает условию $(n-2k+\lambda)\, b^2-2(k-\lambda)\, ab+ \lambda a^2 = 0$.

Будем называть его *характеристическим уравнением*. Оно в сжатой форме выражает условие ортогональности бинарной по уровням матрицы. После подстановки значений $\{n, k, \lambda\}=\{4t-1, 2t, t\}$, уравнение связи упрощается.

Оно дает $(t-1)\, b^2 - 2tba + ta^2 = 0$, положительный корень этого полинома $b = \dfrac{t}{t+\sqrt{t}}$ равен значению модуля уровня матрицы Мерсенна.

SBIBD, это прямое параметрическое описание матриц Мерсенна порядков $n=4t-1$, отвечающее характеристическому уравнению для искомого варьируемого уровня.

Таким образом, если матрицы с иррациональными уровнями порядков $n=4t-1$, называемые матрицами Мерсенна, существуют, то существуют и целочисленные матрицы Адамара. И наоборот. Если существует матрицы Адамара, то существуют и матрицы Мерсенна, поскольку их связывает один и тот же SBIBD.

Существование матриц Мерсенна

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

Переход, осуществленный выше, от целочисленных задач к задачам с иррациональными элементами, он довольно труден, но, как видно, проходим.

Остается доказать существование матриц Мерсенна, причем, в облегченной постановке, когда они не рассматриваются как продукт решения уравнений, а как продукт оптимизации, что, мы знаем, по примерам с псевдообратными матрицами, не одно и то же. Задача на оптимум не меняется от порядка к порядку для $n=4t-1$, она воспроизводится одинаково для любого t и нет причин выделять одну матрицу перед другой, опираясь только на различие в значениях t.

Далее, хотя искомых матриц бесконечно много, и найти их все невозможно, 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.

Допустим, матрица порядка $n=4t-1$ имеет элементы $(a=1,-b)$ 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 таблице 1, отнесенной в приложение, приведены найденные нами для порядков, равных первым числам Мерсенна $n=2^k-1$, параметры субоптимальных двухуровневых 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 детерминанту. Они найдены не из уравнений, а строго в оптимизационной постановке, включая многие порядки $n=4t-1$, в таблице содержатся, для иллюстрации, только часть обработанного нами материала.

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.

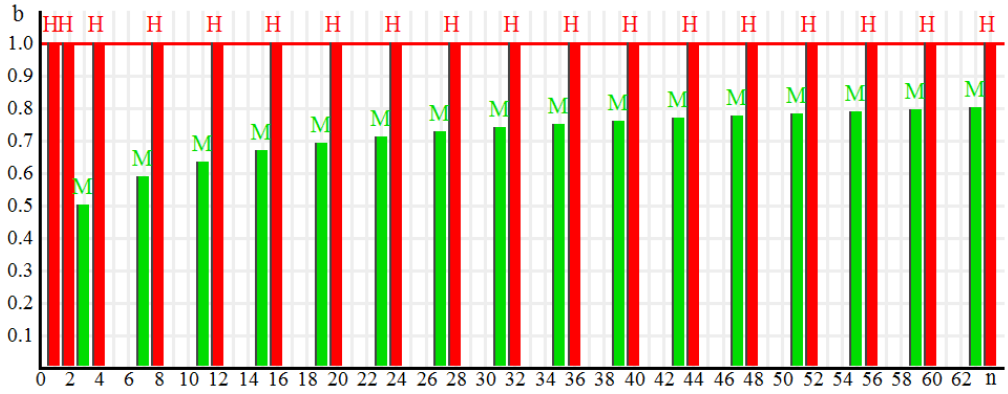


Рис. 3. Зависимость уровней матриц Мерсенна (**M**) и Адамара (**H**) от порядка n

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 $n=4t-1$.

Выводы из существования матриц Мерсенна

Выводы можно сделать самые широкие. Они касаются не только матриц Адамара, но всей числовой оси, всех этих систем чисел и всех квазиортогональных матриц. Выделенные числами экстремальные ортогональные базисы существуют, они разделяются на целочисленные и иррациональные, по описывающих их матрицам.

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 [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.

Примеры подсемейств матриц Мерсенна

В этой заключительной части нашей статьи нам хотелось бы показать, что расчет подсемейств матриц Мерсенна опирается на различие числовых последовательностей, входящих в $n=4t–1$.

Прежде всего, эти числа, включая числа Мерсенна, распадаются на простые (или степени простых чисел) и прочие. Для расчета сопровождающих их матриц естественно привлекать, в первом случае, поля Галуа. Второй случай заметно сложнее, поскольку мы не можем использовать поле. Особняком стоят в нем 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 не простыми.

Расчеты в поле GF(2). Начнем примеры с этого случая, он самый простой. 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 $\boldsymbol{x}_k=\mathbf{F}\boldsymbol{x}_{k-1}$, $\mathbf{F}$ – матрица фробениусовой формы, порядка m, с компонентами вектора состояния в поле GF(2).

Хотя 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 попавшийся случайным образом выбранный вектор начального состояния, и случайные же параметры динамической системы, также определенные в поле GF(2), дают нужную первую строку.

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, которую несложно генерирует сдвиговый регистр. Заметим, что сама по себе динамическая система тоже может быть реализована на сдвиговом регистре, и этот метод усиленно рекламируется, 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).

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

Расчеты в поле GF(p). В предыдущем разделе была описана не сложная, 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, как нетрудно догадаться, мало что зависит.

Противоположное означало бы связи внутри числовой системы.

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

Для большинства случаев подходит выбор x=2 и λ=1. Чтобы не гадать с начальным условием, часто переходят к иному сорту комбинаторике, вычисляя степенные функции k^2 mod 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 всеми полученными квадратами, возникает перебор. Так что метод экспонент, описанный выше, более прост. Не надо гадать, сразу имеем нужный нам индекс.

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

Расчет для пары простых чисел p, p+2. Поля Галуа размера n=p(p+2) нет. Можно вычислить p значений x^k mod (n) и q–p значений y^k mod (n) с основаниями x=y mod (p), x=0 mod (p+2), y – примитивный элемент групп GF(p) и GF(p+2), где q=(n–1)/2. Примитивный элемент, это любой элемент, степенная 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 не нет.

Все элементы поля 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, см. рис. 3.

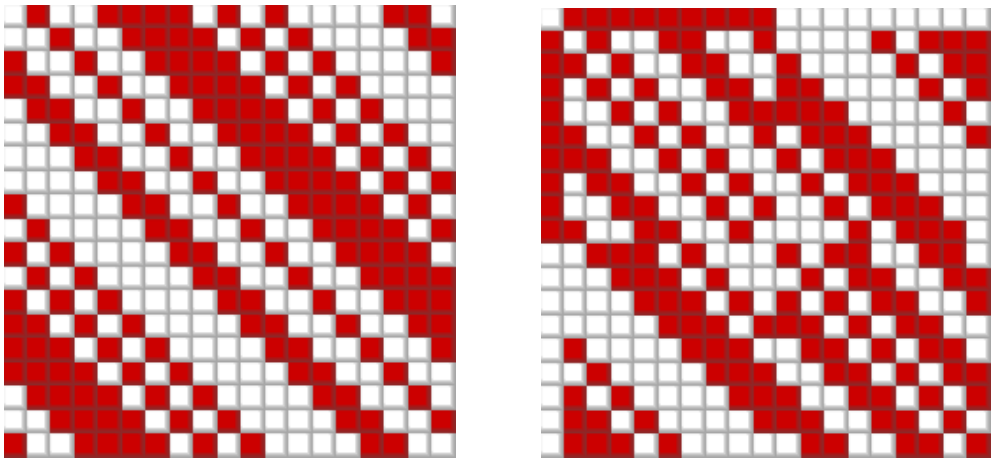


Рис. 3. Циклическая и бициклическая матрицы Мерсенна порядка 19

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 $n = p^m+1$.

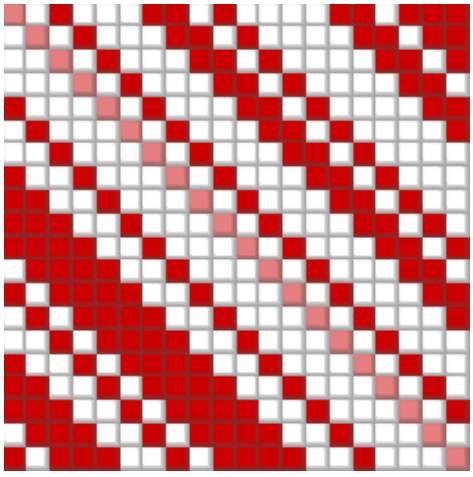


Рис. 4. Негациклическая матрица порядка 20

В данном случае нужна только одна последовательность.

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, кстати, 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.

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

Этот метод расчета базируется на работах [8, 9], не соотнесенных, впрочем, с расчетом матриц Мерсенна, то есть, этот метод расчета матриц Мерсенна также нов. Упоминается он потому, что иллюстрирует сложный вид, которые могут принимать матрицы подсемейств, основанных на разных системах чисел.

Нет никакого поля. Максимально общий случай порядков $n=4t-1$, в него входят все предыдущие порядки. Сложность формы матрицы Мерсенна ограничена – бициклическая матрицы Мерсенна с одной каймой. Все разнообразие числовой системы, следовательно, не повышает сложность структуры в сравнении с максимально сложным случаем расчета в полях Галуа. Алгоритм поиска универсален и нами освещен отдельно в работе [10]. Его универсальность и безотносительность к виду числовой системы, в которую входят порядки искомых матриц, подтверждают высказанные в [11] положения.

Произведение матриц Мерсенна. Произведение Скарпи известно применительно к матрицам Адамара, первое применение к матрицам Мерсенна с поднятием негативного уровня до –1 описано в данной работе. 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.

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

Заключение.

В заключение нам хотелось бы облегчить работу тех, кто собирается проверить наши выкладки. Несмотря на обилие литературы по полям Галуа, а может быть, ввиду этого, найти конкретное описание операции умножения, служащей для вычисления показательных функции, 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 $0\le i\le m$ как

S=C[i];

if (i<m–1) { S+=r*C[m+i];

if (i<d–1) S+=r*s*C[2*m–d+i]);

if (i>d–1) { S+=s*C[m+i–d]; if (i<2*d–1) S+=s*s*C[2*(m–d)+i]); }

C[i]=S%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=2 помимо случаев r=1, p+1 кратно 4, и r=3, p+1 кратно 6. Для более сложных полей параметры задаются таблично, см. таблицу 2 приложения.

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, также как и все прочие такие матрицы. Мы показали, что матрицы могут быть иррациональными, и 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 древнюю проблему поиска целочисленных решений. Гипотеза Адамара, как и прочие сходные с ней гипотезы, уступает в своей сложности Великой теореме Ферма. Ее проверка не должна быть столь же замысловатой.

В конечном поле показательная функция заметает собой все пространство и играет собой роль спирали, пронизывающей каждую его точку без пересечения, что свойственно хаосу. Именно таковы решения некоторых нелинейных дифференциальных уравнений в бесконечномерном трехмерном пространстве. 3D нужно, чтобы интегральной кривой было место, где разместиться без самопересечений. Интегральная кривая заметает объем, где размещается странный аттрактор, прошивает в нем любую точку один раз. В этом заключается подобие динамических систем им же, рассматриваемым в конечных поля. Аттракторы образованы степенями примитивного элемента мультипликативной циклической группы, выступающего в качестве начального условия “экспоненты” .

Нелинейность (сложность) содержится в логике модульной или полиномиальной арифметики. Не забываем и об оптимизируемом таким движением квадратичном критерии – детерминанте.

Матрицы абсолютного максимума детерминанта нечетного порядка увеличиваются в размерах путем бифуркации их уровней, причем есть критическая точка, порядок 13. Матрицы Адамара, это островные области, где ни количество уровней, ни сами эти уровни не меняются с ростом порядка.

Вся числовая система связана с малоуровневыми квазиортогональными матрицами. Варьируемый отрицательный уровень позволяет матрице Мерсенна удерживать ортогональность столбцов, причем с ростом порядка элемент $-b$ стремится к -1.

Матрицы высоких порядков, см. таблицу 3 в приложении и рис. 2, все менее отличаются друг от друга и от матриц Адамара.

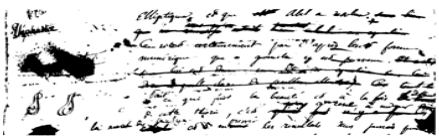
Даже если читатель не согласен с рядом выдвинутых здесь положений, или затрудняется их проверить самостоятельно, все же, согласитесь, это отрезок пути на познании чисел и матриц в их взаимосвязи, имеющий интересные перспективы в теории и практике вычисления экстремальных матриц ортогональных базисов.

Благодарности.

Наше обширное исследование циклических, бициклических, негациклических форм экстремальных матриц (называемых ради большей краткости *критскими* [12]) в том виде, как оно изложено, было бы невозможно без действенной помощи [8, 9, 12] и совета таких ученых, как профессоры Дженифер Себерри и Драгомир Джокович. В отношении доказательства гипотезы Адамара Дженнифер 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 описывающих их обоих одинаковых числовых инвариантов [13] (и не более того). С нашей точки зрения, осторожный подход уместен и не противоречит всему тому, что здесь изложено, поскольку он оперирует подсемействами матриц, тогда как оптимизационная постановка смещает акцент на большее обобщение.

Дженнифер Себбери и Драгомир Джокович, всеми своими интересными работами, творчеством внесли большой вклад в создание алгоритмов поиска экстремальных квазиортогональных матриц с использованием полей Галуа.



http://www.ega-math.narod.ru/Singh/Galois.htm

Литература

[1] Hadamard, J. Resolution d'une question relative aux determinants. *Bulletin des Sciences Mathematiques*. 1893. Vol. 17. pp. 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. О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2(63). С. 89–90.

[4] Bellman R. Introduction to Matrix Analysis, SIAM, Philadelphia, PA, USA, 1997, 395 p.

[5] Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. М.: Наука. Главная редакция физико-математической литературы, 1984. 320 с.

[**6**] Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications), 2nd Edition, by Charles J. Colbourn (Editor), Jeffrey H. Dinitz (Editor) Chapman and Hall/CRC, 2006, 1000 p.

[**7**] **Balonin N. A., Seberry, Jennifer**. A review and new symmetric conference matrices. *Informatsionno-upravliaiushchie sistemy*, 2014. № 4 (71), pp. 2–7.

[**8**] **Balonin N. A. and Đoković D. Ž.** Negaperiodic Golay Pairs and Hadamard Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 5(78), pp. 2–17.

[**9**] **Balonin N. A. and Đoković D. Ž.** Symmetry of Two Circulant Hadamard Matrices and Periodic Golay Pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3(76), pp. 2–16. doi:10.15217/issn1684-8853.2015.3.16 (in Russian).

[10] 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. С.2–9.

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

[12] Balonin N. A., and Seberry, Jennifer. Remarks on extremal and maximum determinant matrices with real entries ≤ 1. *Informatsionno-upravliaiushchie sistemy,* № 5 , (71) (2014), pp. 2–4.

[13] Seberry, Jennifer., Balonin N. A. Equivalence of the Existence of Hadamard Matrices and Cretan(4*t*–1,2)-Mersenne Matrices http://arxiv.org/abs/1501.07012v1

ПРИЛОЖЕНИЕ

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	$b^2-4\,a\,b+2a^2=0$	$b=(2-\sqrt{2})a$
4	15	$3b^2-8ab+4a^2=0$	$b=2a/3$
5	31	$7b^2-16ab+8a^2=0$	$b=(8-2\sqrt{2})a/7$
6	63	$15b^2-32ab+16a^2=0$	$b=4a/5$
7	127	$31\,b^2-64\,a\,b+32\,a^2=0$	$b=(32-4\sqrt{2})\,a/31$
8	255	$63\,b^2-128\,a\,b+64\,a^2=0$	$b=8a/9$

Таблица 2. Параметры неприводимого полинома

p	m	d	s	r
2	2	1	1	1
2	3	1	1	1
2	4	1	1	1
2	5	2	1	1
2	6	1	1	1
2	7	1	1	1
2	8	5	1	1
3	3	1	1	1
3	4	1	1	1
3	5	1	1	1
3	6	1	1	1
3	7	2	1	2
3	8	2	1	1
3	9	5	1	1
5	3	1	1	1
5	4	1	1	1
5	5	1	1	1
5	6	1	1	3
5	7	1	1	2
5	8	1	0	2

p	m	d	s	r
7	3	1	0	2
7	4	1	1	3
7	5	1	1	3
7	6	1	0	3
7	7	1	1	1
7	8	1	1	1
7	9	1	0	2
7	10	1	2	1
11	3	1	1	3
11	4	1	1	6
11	5	1	1	1
11	6	1	1	1
13	3	1	0	2
13	4	1	0	2
13	5	1	1	1
13	6	1	0	2
17	3	1	1	2
17	4	1	0	3
17	5	1	1	6
17	6	1	1	4

p	m	d	s	r
19	3	1	0	2
19	4	1	1	1
19	5	1	1	3
23	3	1	1	4
23	4	1	1	3
23	5	1	1	2
29	3	1	1	1
29	4	1	1	1
31	3	1	0	3
31	4	1	1	1
37	3	1	0	2
37	4	1	1	1
41	3	1	0	2
41	4	1	1	7
47	3	1	1	1
47	4	1	1	1
53	3	1	1	4
53	4	1	1	2
57	3	1	1	8
57	4	1	1	5

Таблица 3 Таблица наиболее важных видов 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 $b=\frac{t}{t+\sqrt{t}}$	$((n+1)+(n-1)b^2)/2=$ $2t+(2t-1)b^2$
$4t$–2	Эйлера *)	1, $-b$, где $b=\frac{t}{t+\sqrt{2t}}$	$((n+2)+(n-2)b^2)/2=$ $2t+(2t-2)b^2$
$4t$–3	Зейделя	1, $-b$, d , где $b=1-2d$, $d=\frac{1}{1+\sqrt{n}}$	$(n-1)(1+b^2)/2+d^2=$ $2(t-1)(1+b^2)+d^2$
$4t$–3	Ферма	1, $-b$, s , где $q=n-1=4u^2$, $p=q+\sqrt{q}$, $b=\frac{2n-p}{p}=1-\frac{2u-1}{2u+1}\times\frac{1}{u}$, $s=\frac{\sqrt{nq-2\sqrt{q}}}{p}=\frac{\sqrt{nu-1}}{2u+1}\times\frac{1}{\sqrt{u}}$	$1+4u^2s^2=$ $k+(q-k)b^2+s^2$ где $k=\frac{q-\sqrt{q}}{2}=2u^2-u$

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