УДК 519.614
doi:10.31799/1684-8853-2021-4-2-17

Научные статьи
Articles

Алгоритмы конечных полей и групп поиска ортогональных последовательностей

Н. А. Балонин[a], *доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
А. М. Сергеев[a], *канд. техн. наук, доцент, orcid.org//0000-0002-4788-9869*
О. И. Синицына[a], *аспирант, orcid.org/0000-0002-2819-4682*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *матрицы Адамара, состоящие из элементов 1 и –1, представляют собой идеальный объект для наглядного приложения конечномерной математики, оперирующей конечным числом адресов элементов –1. Системы нотаций методов абстрактной алгебры, в отличие от устоявшейся матричной алгебры, интенсивно менялись и, к тому же, не были повсеместно распространены, вызывая потребность пересмотреть и систематизировать накопленный опыт.* ***Цель:*** *описать набор алгоритмов конечных полей и групп в единых обозначениях для облегчения восприятия обширного материала, способствующего нахождению ортогональных и субортогональных последовательностей.* ***Результаты:*** *предложены формулы расчетов малоизвестных алгоритмов (и их версий) Скарпи, Зингера, Секереша, Гетхальса — Зейделя, Нобору Ито, а также полиномиальные уравнения, используемые для доказательства теорем существования конечномерных решений. Устранен существенный недостаток информации как в отечественной литературе (большинство затрагиваемых вопросов освещается у нас впервые), так и зарубежной систематизацией обширных знаний.* ***Практическая значимость:*** *ортогональные последовательности и методы их эффективного нахождения теорией конечных полей и групп имеют непосредственное практическое значение для задач помехоустойчивого кодирования, сжатия и маскирования видеоинформации.*

Ключевые слова *— матрицы Адамара, ортогональные матрицы, конечномерная математика, поля Галуа, конечные группы, алгоритм Скарпи, подход Зингера, метод Секереша, алгоритм Гетхальса — Зейделя, подход Нобору Ито.*

Для цитирования: Балонин Н. А., Сергеев А. М., Синицына О. И. Алгоритмы конечных полей и групп поиска ортогональных последовательностей. *Информационно-управляющие системы*, 2021, № 4, с. 2–17. doi:10.31799/1684-8853-2021-4-2-17
For citation: Balonin N. A., Sergeev A. M., Sinitsyna O. I. Finite field and group algorithms for orthogonal sequence search. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 4, pp. 2–17 (In Russian). doi:10.31799/1684-8853-2021-4-2-17

Введение

Теория ортогональных матриц Адамара с двумя значениями элементов (уровней) 1 и –1 закономерно относится к сфере привлечения теории конечных полей и групп, органично учитывающих фиксированные размеры матриц и их блоков. В циклических структурах положение отрицательных элементов этих матриц связано с характеристиками конечных полей — символами Лежандра и Якоби. Тем не менее, несмотря на эти знания, теория малоуровневых матриц далека от завершения.

Такие матрицы, как правило, имеют не один, а несколько характерных для них орнаментов (узоров) — взаимных расположений элементов с положительными и отрицательными знаками на «портретах» матриц. В зависимости от вида орнамента должен меняться алгоритм их нахождения. Однако многоклеточный, трехблочный и двухблочный орнаменты с одной или двумя каймами имеют существенно различающиеся между собой фиксированные размеры.

В научной литературе по данной тематике наблюдается дефицит информации относительно вариативного употребления конечномерной математики. Если размер блока может убывать и не только на единицу, возникает неопределенность: какой вид индикаторов положения отрицательного элемента в орнаменте матрицы применять. Использовать символы Лежандра повсеместно становится невозможно. Это обстоятельство редко или вовсе не учитывается в существующих научных работах. Более того, оно является причиной сегодняшних научных исследований.

Ортогональные матрицы нашли множество применений в современной технике, поэтому вопрос, как их найти, включая высокие порядки и вариации орнаментов, важен. Вместе с тем соответствующую классификацию того, что происходит при изменении размеров блоков, никто в общей совокупности возникающих при этом задач не проводил. Еще один факт заключается в том, что сама по себе наука о конечных объектах не является чем-то вполне законченным. За столетие сам ее язык меняется, меняются обозначения, причем настолько, что прежде полученное знание снова утрачивается ввиду малочисленности статей и малопонятного, не закрепившегося на практике специфического языка описания алгоритмов.

Языки науки естественно повторяют путь древнегреческого, латинского и прочих языков, со временем отмирая и выходя из употребления. Работая со статьей, нам пришлось переписать и перевести на современный более понятный язык забытые ныне алгоритмы или алгоритмы, которые не известны в нашей стране и описаны в редких статьях за рубежом. Таковы, например, оригинальные алгоритмы Н. Ито, описанные весьма кратко, а также алгоритмы, сложившиеся под влиянием продуктивной группы математиков, близких к П. Эрдешу, таких как Д. Секереш, Дж. Себерри, Д. Джокович и др.

Описание нами орнаментов матриц в их тесной связи с положениями точек Гаусса на квадратичных поверхностях закономерно подводит к этапу, когда обобщенных параметров орнаментов (координат целочисленных точек) становится мало. Нам нужен сам орнамент, а чтобы его найти, приходится выполнить большую и напряженную работу по сбору необходимой информации.

В такой совокупности настоящая статья будет нова и для российской, и для зарубежной аудитории. В ней ставится цель привести общие универсальные знания об орнаментах и симметриях, а также свойствах чисел и числовых последовательностей как порядках матриц, иллюстрируемые портретами ортогональных матриц. Часть приводимых алгоритмов при этом имеет значение для пограничных областей математики, далеко выходящих за пределы потребностей построения ортогональных базисов.

Введение в конечные поля и группы

Абстрактную систему элементов (матриц, векторов, полиномов) вместе с четырьмя операциями называют полем. Убрав умножение и деление, получаем кольцо. Оставив одну операцию умножения, получим группу, что не мешает размывать свойства этой составной операции, делая ее похожей на сложение [1–5].

Поля с конечным числом элементов — поля Галуа (Galois fields) обозначают как $GF(q)$, где q — простое число p или его степень. Числа 0, 1, 2, ..., $p-1$ с операциями, выполняемыми по модулю p, дают пример простого поля $GF(p)$. Таблицы сложения и умножения в поле отличаются от привычных лишь тем, что содержат остатки от деления на p, поэтому элементы поля принято называть вычетами.

Если вычет образован квадратом некоторого числа поля, он называется *квадратичным вычетом*, в противном случае — невычетом. Роль корней квадратных в конечномерной математике выполняют *инволюции* — элементы, квадрат которых равен единичному элементу.

Пример 1. Наименьшее число элементов, образующих поле, равно двум. Такое поле $GF(2)$ содержит два опорных элемента: **A** = 0 относительно операции сложения и **B** = 1 относительно операции умножения. Их можно записывать конкретно как 0 и 1 или абстрактно как **A** и **B** и исследовать таблицы на предмет соблюдения, для операций с ними, всех правил арифметики (рис. 1).

Пример 2. Попытка построить поле $GF(2^2) = GF(4)$ из **A** = 0, **B** = 1, **C** = 2, **D** = 3, дает расширенные таблицы (рис. 2). На них видно, что в центре таблицы умножения появился нулевой элемент A, и в этой строке сдвоились **CB** = **CD** = **B**, **B** — единица поля. Выходит, что на роль обратного к **C** элемента претендуют два кандидата: **B** и **D**.

Первая из таблиц, согласно классификации 1884 г., носит название четверной группы Клейна и обозначается как V_4. Чтобы отремонтировать вторую, в качестве элементов конечных полей $GF(p^m)$ рассматриваются полиномы или векторы их коэффициентов размера m. Полиномы удобны тем, что, задав всего одно дополнительное полиномиальное уравнение, формирующее поле, с его помощью можно убрать последствия повышения степени при произведениях, сумма таких хлопот не вызывает.

Поле $GF(p^2)$ связано по количеству востребованных коэффициентов с линейными функциями $a + bx$ или векторами (a, b) с параметрами, определенными в поле $GF(p)$. Произведение такого сорта элементов неприятно лишь в связи с появлением полинома второй степени: от x^2

+	A	B
A	A	B
B	B	A

×	A	B
A	A	A
B	A	B

■ ***Рис. 1.*** Таблицы сложения и умножения в $GF(2)$
■ ***Fig. 1.*** Addition and multiplication tables in $GF(2)$

+	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

×	A	B	C	D
A	A	A	A	A
B	A	B	C	D
C	A	B	A	B
D	A	D	C	B

■ ***Рис. 2.*** Таблицы с дефектом умножения по месту **A** = 0
■ ***Fig. 2.*** Tables with multiplication defect by location **A** = 0

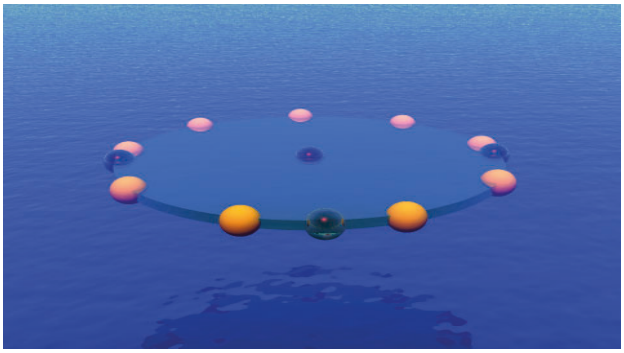
несложно избавиться, выразив через степени меньшего порядка. Образуемый переносом всех членов этого уравнения влево полином не должен разлагаться на произведение полиномов первого порядка, поэтому его называют *неприводимым*. Этих сведений достаточно, чтобы конструировать конечные поля.

Механическая интерпретация *циклической группы* известна по устройству часов, напоминающих расположением отметок времени другую распространенную конструкцию — позиции на комплексной плоскости корней из единицы: решений $g^n = 1$ (рис. 3).

Другой популярный источник полей и групп — матрицы — появился, потому что в качестве элементов можно брать члены прогрессии — показательной функции $1, g, g^2, \ldots, g^{n-1}$, где g — примитивный элемент (генератор).

Заметим, что операция умножения матриц составная, для получения элементов произведения работает конвейер из цепочек умножений и сложений, применяемых к элементам сомножителей. В теории циклических групп, оперирующей набором элементов с единственной операцией, обозначаемой знаком умножения «×», разрешено и вовсе не строить цепочек, подменяя операцию умножения сложением порядковых номеров a, b элементов, так как $g^a g^b = g^{a+b}$, различие этих двух операций относительное. Очевидно, что порядок циклической группы может быть любым, четным или нечетным. Это выгодно отличает группу от конечного поля, размеры которого лимитированы возможностями полиномиальной арифметики. Кажется, что для построения циклических групп нет препятствий. Однако это не так. Недостаток слишком просто устроенных групп прямо вытекает из их достоинства — простоты, которая не позволяет моделировать с их помощью более сложно устроенные математические объекты.

Сложнее устроена мультипликативная группа $GF(q)^*$, построенная усечением количества элементов конечного поля $GF(q)$, где q — простое число p или его степень, выбрасыванием ненужного группе 0. Соответственно, размер такой циклической группы не может быть любым, она обременена выброшенным сложением (а также вычитанием и делением). К мультипликативным группам примыкают по смыслу близкие к ним группы порядков $n = p^t u$, где множитель u взаимно прост с p, а p — простое число. Для абелевых групп (произведение коммутативно) принято выделять и использовать в доказательствах теорем циклические p-подгруппы Силова размера p^t.



■ ***Рис. 3.*** Расположение корней из 1
■ ***Fig. 3.*** Root location from 1

Тактика использования конечных полей и групп

В настоящее время теория групп кажется точной солидной наукой. Обилие книг. Некоторая торжественность и чопорность изложения. Однако есть одно смущающее обстоятельство. В теории принято одним и тем же символом обозначать очень разные вещи, если эти вещи считаются отражениями одного объекта. Например, элемент группы может быть номером элемента или матрицей, выбирай, что хочешь, обозначаем g.

Смысл конкретного наполнения элемента в теории групп и полей зависит от характера его употребления. Более щадят читателя разнесенные обозначения для индексов и матриц, но тогда его голову начинает сушить введенное в оборот большое количество символов, смысл которых не успевает закрепиться в сознании. Подчеркнем, что двусмысленность является рабочим методом решения задач, поскольку, следуя иному содержанию термина, мы иначе организуем вычисление, и это неожиданно может дать новое решение задачи, обладающее новыми свойствами. Отстригать такую приятную неожиданность — действовать против себя.

Например, в алгоритме Скарпи вычисления матриц Адамара [6, 7] фигурируют произведение и сумма индексов строк. Можно к двум прибавить три и получить пять. Но можно действовать иначе! Можно 2-й элемент поля сложить с 3-м элементом поля, получить элемент суммы, у него есть номер, и этот номер вовсе не обязан быть 5-м. В сложных полях это будет иной номер. Алгоритм Скарпи, разработанный его автором для простых полей [8], «неожиданно» даст верный результат, матрицу Адамара, если в более общем случае мы изменим ход вычислений. Что подсказало такой прием? Этот ход вычислений подсказала принципиальная двойственность обозначений.

Не только смысл элементов двойственен. Смысл функции тоже может переключаться в зависимости от характера ее употребления. Ведь

уже в алгоритме Скарпи мы имеем два итога вычислений, ход вычислений зависит от обрабатываемого материала.

Учитывая тезис о соответствии элементов группы символам или порядковым номерам 0, 1, 2, ... в таблице умножения, сводящейся к таблице сложения показателей степеней, при таком подходе приходится перешагивать через привычку аннулировать произвольный элемент умножением на единичный элемент, обозначаемый, в том числе, и 0.

С обозначениями в аддитивной по своему характеру арифметике, занятой умножениями, возникает сложность восприятия ввиду замены вычитания делением или умножением на обратный элемент. Так что с ab^{-1} вы освоитесь заметно быстрее, если будете иметь в виду, что это вполне знакомое вам $a - b$. В старых примерах таким (разностью) и бывшее, а потом переписанное в иных терминах в новые времена.

Разумеется, это вызывает внутренний протест, но что делать, если это так действенно и действительно сильно сокращает формулы.

Все это говорит о том, что употребление теории требует у читателя, привычного к иной работе с обозначениями, известной доли терпения и понимания, зачем это все нужно. Ортогональные и экстремальные по детерминанту матрицы являются превосходным иллюстративным материалом для демонстрации прикладной стороны абстрактной арифметики. Впрочем, всерьез делить, где здесь иллюстрация, а где инструмент, нет смысла, поскольку понятие ортогонального базиса первичное в математике, и речь идет, скорее, о тесной взаимной связи ее разделов.

Операция умножения чисел *по модулю*, не равному простому числу, не дает гарантии наличия среди соответствующих цепочек элементов генератора подгрупп силовского размера, хотя кажется почти очевидным, что они там должны быть. Подгруппы прочих размеров можно встретить, выделить и использовать в алгоритмах поиска матриц. Можно иначе строить подмножества, но тогда мы те подгруппы потеряем.

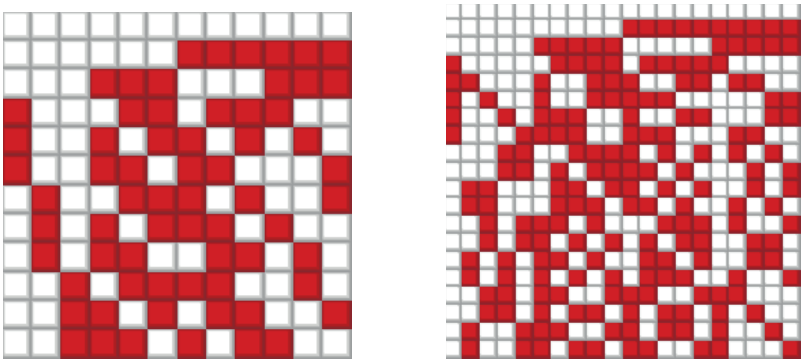
Алгоритм Скарпи

Определение. Квадратная матрица $\mathbf{H}$ порядка n с элементами {1, –1} и ортогональными столбцами $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, где $\mathbf{I}$ — единичная матрица, называется матрицей Адамара [6, 7].

Ввиду наличия только двух значений элементов, порядок матриц Адамара может быть равен только 1, 2 или $4t$, где t — натуральное число. Известно, что на классе матриц с элементами, не превышающими по модулю 1, матрицы Адамара имеют максимальный детерминант.

Вскоре после публикации Адамаром первых двух матриц $\mathbf{H}$ порядков 12 и 20, отличающихся от сильвестровых итераций $\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$ с началом $\mathbf{H} = 1$, оригинальным размещением элементов (рис. 4), появился первый и более общий метод синтеза, предложенный алгебраистом итальянского происхождения Умберто Скарпи [8].

Мы излагаем этот метод с использованием (введенной позднее) нормальной формы матрицы Адамара в виде $\mathbf{H} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{M} \end{pmatrix}$, где $\mathbf{e}$ — вектор единичных элементов каймы, и *произведения Скарпи* — кронекерова



■ ***Рис. 4***. Матрицы конструкции Адамара порядков 12 и 20

■ ***Fig. 4***. Construction of Hadamard matrices of orders 12 and 20

произведения *с коррекцией* знака каймы и нарастающим циклическим смещением строк основы, обозначаемого как «×». Тогда он описывается одной формулой (а не цепочкой преобразований)

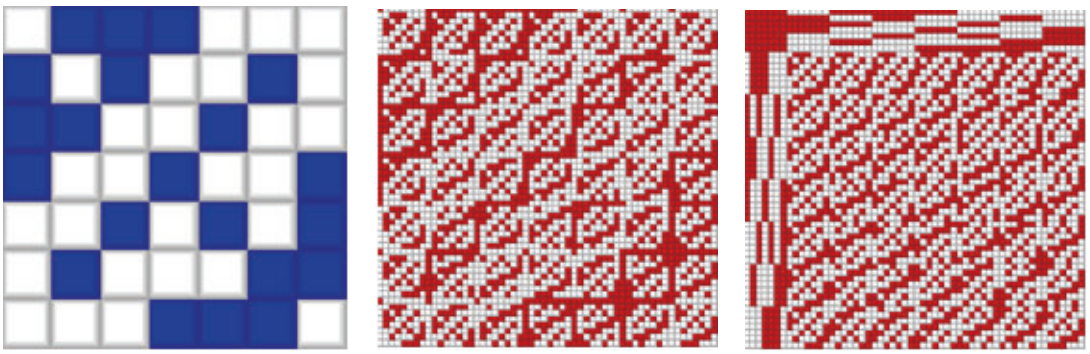
$$\mathbf{M}\times\mathbf{M}=\begin{pmatrix}
\begin{pmatrix}-1 & m_{00}\mathbf{e}^{\mathrm{T}}\\ m_{00}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}-1 & m_{01}\mathbf{e}^{\mathrm{T}}\\ m_{01}\mathbf{e} & \mathbf{M}\end{pmatrix} & \cdots & \begin{pmatrix}-1 & m_{0(\upsilon-1)}\mathbf{e}^{\mathrm{T}}\\ m_{0(\upsilon-1)}\mathbf{e} & \mathbf{M}\end{pmatrix}\\
\begin{pmatrix}-1 & m_{10}\mathbf{e}^{\mathrm{T}}\\ m_{10}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}-1 & m_{11}\mathbf{e}^{\mathrm{T}}\\ m_{11}\mathbf{e} & \mathbf{TM}\end{pmatrix} & \cdots & \begin{pmatrix}-1 & m_{1(\upsilon-1)}\mathbf{e}^{\mathrm{T}}\\ m_{1(\upsilon-1)}\mathbf{e} & \mathbf{T}^{\upsilon-1}\mathbf{M}\end{pmatrix}\\
\cdots & \cdots & \ddots & \cdots\\
\begin{pmatrix}-1 & m_{(\upsilon-1)0}\mathbf{e}^{\mathrm{T}}\\ m_{(\upsilon-1)0}\mathbf{e} & \mathbf{M}\end{pmatrix} & \begin{pmatrix}-1 & m_{(\upsilon-1)1}\mathbf{e}^{\mathrm{T}}\\ m_{(\upsilon-1)1}\mathbf{e} & \mathbf{T}^{\upsilon-1}\mathbf{M}\end{pmatrix} & \cdots & \begin{pmatrix}-1 & m_{(\upsilon-1)(\upsilon-1)}\mathbf{e}^{\mathrm{T}}\\ m_{(\upsilon-1)(\upsilon-1)}\mathbf{e} & \mathbf{T}^{(\upsilon-1)(\upsilon-1)}\mathbf{M}\end{pmatrix}
\end{pmatrix}.$$

Формула Скарпи работает корректно, если размер блока $\upsilon = n - 1$ представляет собой простое число, $\mathbf{T}$ — матрица циклического смещения строк $\mathbf{M}$.

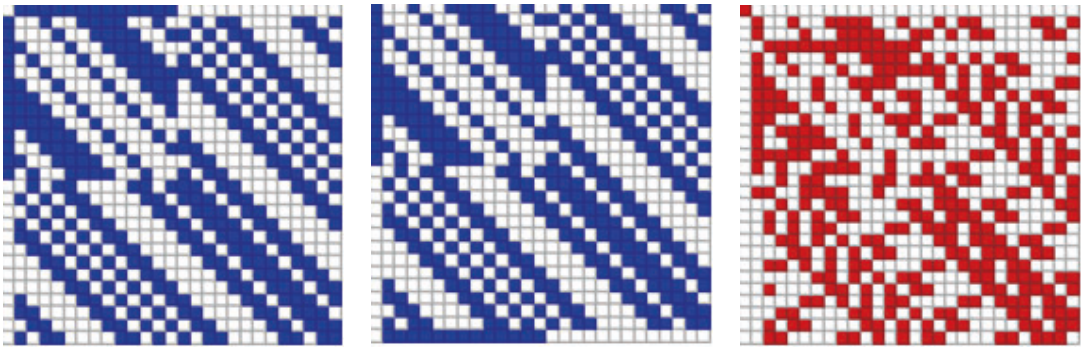
В кронекеровом произведении матриц

$$\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix}
a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B}\\
a_{21}\mathbf{B} & a_{22}\mathbf{B} & \ldots & a_{2n}\mathbf{B}\\
\vdots & \vdots & \ddots & \vdots\\
a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \ldots & a_{nn}\mathbf{B}
\end{pmatrix},$$

которым предлагал пользоваться Адамар, знаки элементов первого сомножителя влияют на всю матрицу второго сомножителя. Для сравнения на рис. 5 рядом приведены *основа* (ее называют в прикладной



■ ***Рис. 5.*** Основа и матрицы Адамара конструкции Скарпи порядка 56
■ ***Fig. 5.*** Basis and the Scarpy design Hadamard matrices of order 56



■ ***Рис. 6.*** Основа **M**, смещенная основа и смещение в алгебре полей Галуа *GF*(27)
■ ***Fig. 6.*** Basis **M**, basis offset and offset in algebra of Galois fields *GF*(27)

литературе *core*, она выделена синим цветом) **M** порядка $v = 7$ матрицы Адамара **H** порядка $n = 8$, произведение Скарпи и типичное для оригинала алгоритма размещение составной каймы, на которой отражаются знаки элементов основы, что дает две матрицы Адамара порядка $vn = 56$.

Заметим, что в алгоритме Скарпи циклическое смещение строки k основы **M** на величину $i \times j$ определяют индексы номера строки i и столбца j блока с нею, отсчитываемые от 0 — для блоков каймы смещение отсутствует.

Поправка к алгоритму формирования адреса смещаемой строки $k + i \times j$ на случай $v = p^k$ — степень простого числа, согласно концепции теории групп, не отражается на формуле расчета (рис. 6).

Как видно, при произведении в сложном поле меняется интерпретация номеров строк и столбцов номерами перемножаемых и потом складываемых элементов $GF(p^k)$. Итоги смещения строки матрицы **M** размера $v = 27$ обычным и модифицированным алгоритмами отличаются — во втором случае ее адрес определяется номером результирующего элемента в конечном поле.

Орнаментальные инварианты и разности Зингера

В алгоритме Скарпи [8] проявилась польза от деления матрицы на блок с каймой или блоки, используемые наравне с матрицами Адамара в операции, подобной кронекерову произведению. Моноблок **M** порядка $v = n - 1$ матрицы с каймой можно характеризовать двумя параметрами: числом –1 в каждой строке k и числом –1 в каждой паре строк λ.

Эти инварианты отвечают уравнению реализуемости орнамента $k(k - 1) = \lambda(v - 1)$, сводимому к *каноническому виду* $x^2 = 1$, $k = (v - x)/2$, учитывая, что для ортогональных матриц $\lambda = k - n/4$, что дает параметры $v = 7$, $k = 3$, $\lambda = 1$ первой матрицы на рис. 5.

Следующий пример кососимметрической циклической матрицы **M** (во всех таких случаях для краткости упускают уточнение — с точностью до диагонали) со строкой $a = [1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1]$ длины $v = 11$ кочует из книги в книгу, он принадлежит Зингеру [9], заметившему соответствие инвариантов $k = (v - x)/2 = 5$ и $\lambda = k - n/4 = 2$ инвариантам не связанной с матрицами Адамара системы разностей чисел D, образующей некоторое множество G.

Пример 3. Возьмем из работы [10] дифференциальный набор $k = 5$ чисел $D = \{1, 3, 4, 5, 9\}$ по mod 11. Он порождает (кроме 0) множество $G = \{1, 2, ..., 10\}$: $1 - 3 = -2 = 9$; $1 - 4 = -3 = 8$; $1 - 5 = -4 = 7$; $1 - 9 = -8 = 3$; $3 - 1 = 2$; $3 - 4 = -1 = 10$; $3 - 5 = -2 = 9$; $3 - 9 = -6 = 5$; $4 - 1 = 3$; $4 - 3 = 1$; $4 - 5 = -1 = 10$; $4 - 9 = -5 = 6$; $5 - 1 = 4$; $5 - 3 = 2$; $5 - 4 = 1$; $9 - 1 = 8$; $9 - 3 = 6 = 5$; $9 - 4 = 5$; $9 - 5 = 4$. Число совпадений разностей $\lambda = 2$.

Учитывая кососимметрию **M**, из нее можно построить матрицу Адамара добавлением каймы из 1 ее первого столбца и –1 (над блоком) ее первой строки. Заметим, что параметры набора D в точности совпадают с адресами –1 последовательности a.

Тем самым Зингер ввел в обиход дифференциальные наборы чисел, дав старт новому направлению исследования матриц Адамара при помощи групп, которыми такого сорта разности можно описать (напомним, что умножение в группе весьма условно), не опираясь на ресурсы поля. В своем решении он не избавился от перебора, поскольку метода формирования дифференциального набора он не предложил. Очевидно, что его подход игнорирует некоторую дополнительную информацию, которую несет в себе удачный для синтеза матриц Адамара выбор группы.

Потребность в полях или группах может исчезнуть совсем при симметрировании и перестановке порядка сомножителей с разницей их порядков, не большей 4. Соответствующая модификация алгоритма Скарпи [8] рассмотрена в работе [11]. Хороший вопрос, можно ли естественный для конечномерной математики ход вычислений, предопределенный изначально двусмысленностью записей абстрактной арифметики, считать *обобщением*, неведомым такому специалисту по теории чисел, как Скарпи? Скорее всего, Скарпи знал о таком продолжении. Тем более спустя тридцать лет об этом знал Пэли [12]. Пэли заметил, что комбинаторные алгоритмы, закрывая новые и новые порядки, кратные 4, фрагментарно пересекаются и никогда не закрывают область в целом.

Что свидетельствует о неограниченных способностях квадратичной задачи к усложнению. Похоже, решения в принципе нельзя охватить единой формулой или комбинаторным алгоритмом, хотя такие матрицы, безусловно, существуют вне исследованной зоны и, подчеркнем, поддаются изучению методами, связанными с максимумом детерминанта адамаровых матриц [13–15]. Теперь нам становится интересен пример, в котором блок или блоки ортогональной матрицы синтезируются на основе хотя бы мультипликативных групп $GF(q)^*$.

Алгоритм Секереша

В отличие от Скарпи и Зингера, Дьердь Секереш занялся алгоритмами поиска матриц Адамара спустя более половины столетия [16, 17]. Он руководствовался инвариантами канонического

уравнения $x^2 + y^2 = 2$, $k_1 = (v - x)/2$, $k_2 = (v - y)/2$, $\lambda = k_1 + k_2 - n/4 = (v - 2(x + y) + 1)/2$, $n = 2v + 2$, где v — размер блока бициклической основы (бицикла) $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^T & -\mathbf{A}^T \end{pmatrix}$ матрицы Адамара с парной каймой.

В таком случае размер порождающего мультипликативную группу $GF(q)^*$ поля $q = v$ соотносим с размерами клетки или всей матрицы за вычетом 1. Базовая идея первого алгоритма состоит в том, чтобы разделить элементы четной по размерам циклической группы на четыре части, сформировав из них два множества X и Y, пересекающиеся наполовину (рис. 7).

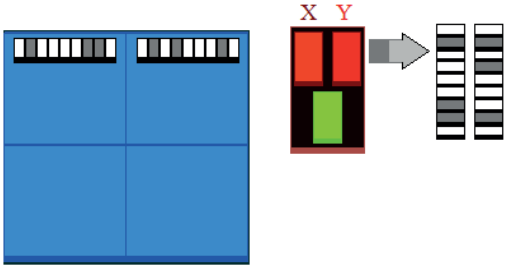
Синтез множеств происходит в два этапа. Сначала синтезируются общие части X и Y в виде последовательности g^{4k} длиною $(q - 1)/4$, где g — примитивный элемент группы. Умножив последовательность на g и на g^3, получим g^{4k+1} и g^{4k+3}, образующие два расходящихся между собой и дистанцирующихся от начала набора элементов для X и Y. Верхние части образуемой вилки можно поменять местами, но в таком случае нижнюю часть (ручку вилки) надо заменить оставшейся 1/4 элементов группы.

Теперь обратим внимание, что каждый элемент блока **A** или **B** описывается разностью его индексов, что касается первых строк, то это попросту индекс элемента без смещения. Разность индексов $(i - j)$ элемента блока — целое число, не имеющее прямого отношения к элементам мультипликативной группы. Но здесь начинает работать магия теоретико-группового подхода, не запрещающая считать его номером элемента группы. Если выбранный элемент группы принадлежит набору X (или Y), то блок **A** (или **B**) имеет вместе с заданными координатами значение –1. Идея Секереша в обращении со степенями изящна, она имеет ясный и понятный смысл в совокупности с простотой реализации.

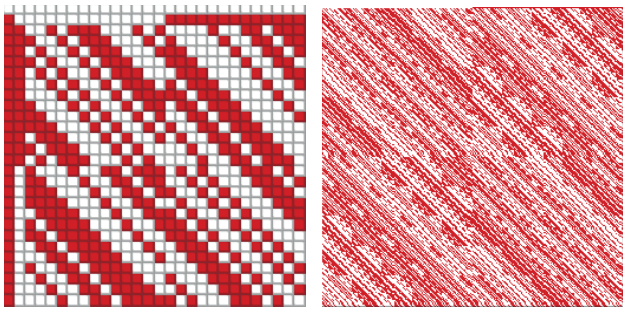
Для циклических блоков достаточно посчитать элементы первых строк блоков и получить из них смещением кососимметричный бицикл Адамара с парной каймой. Если группа сложная $GF(q^m)^*$, то и орнамент блоков **A** и **B** сложен, но матрица остается строго кососимметричной (рис. 8). К сожалению, именно поэтому она существует не всегда. Строгая структуризация приводит к появлению «дыр» в порядках матриц: алгоритм позволяет находить матрицы порядков $n = 4(4t - 1)$.

Если $q = n - 1$ — простое число или степень простого числа, то в $GF(q)^*$ генерируется подгруппа $X = g^k$ размера v. Элементы –1 последовательностей a и b отвечают пересечениям с X не пересекающихся между собой множеств $e + X$ и $e = X$, где e — единичный элемент группы. Порядок одной из приведенных на рис. 9 матриц равен 28, но он отвечает сложной группе (узор матрицы не усложняется). Как видно, эти решения отличаются типом симметрии синтезируемых матриц. Перестановкой блоков их можно сделать как симметричными, так и кососимметричными (см. рис. 9).

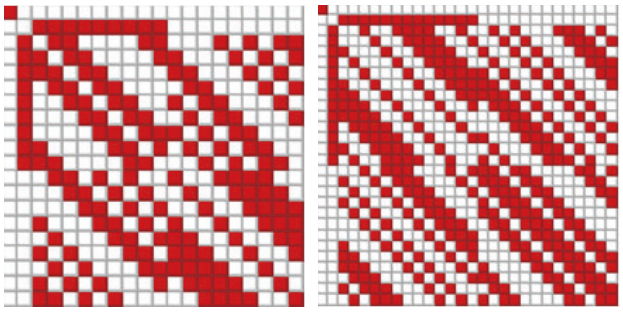
Очевидно, Секереш развил идею Зингера построением разностных семейств в ином, отличном от него, направлении. Это уже полноценные алгоритмы синтеза матриц Адамара, использующие четный размер мультипликативных групп для деления элементов на непересекающиеся подмножества. Поскольку размер группы совпадает здесь с удвоенным размером блока, очевидно, что



■ ***Рис. 7.*** Схема алгоритма Секереша
■ ***Fig. 7.*** Seckeresh algorithm diagram



■ ***Рис. 8.*** Матрицы Секереша порядков 28 и 256
■ ***Fig. 8.*** Seceresch matrices of orders 28 and 256



■ ***Рис. 9.*** Матрицы Секереша порядков 20 и 28
■ ***Fig. 9.*** Seceresch matrices of orders 20 and 28

основой построения является циклическая подгруппа, что объясняет относительно простой вид матрицы Адамара порядка 28 (27 — степень простого числа).

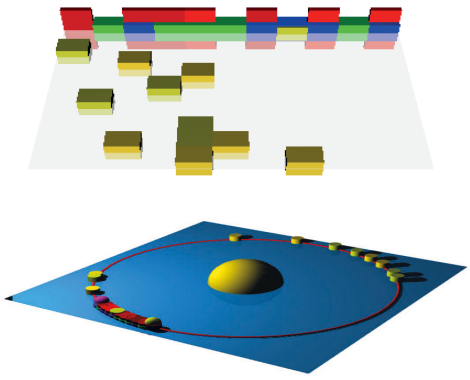
Алгоритмы Гетхальса — Зейделя

Переход математики от римского представления чисел к десятичной позиционной системе счисления дал преимущество — алгоритмы расчета стали короче. Усложнение конструкции числа облегчает вычисления. То же самое произошло при расширении поля вещественных чисел полем комплексных чисел — формулы для вычисления корней полиномов стали проще.

Излагаемая далее идея [18] противостоит идее Секереша: давайте не сокращать, а, наоборот, увеличивать размер поля $GF(q^2)$, где $q = n - 1$, n — порядок матрицы Адамара. На рис. 10 слева приведена форма представления конечной модели комплексных чисел, отображаемых кубиками песочно-желтого цвета, стартовый ряд состоит из начальных q элементов. При этом форму представления можно менять (представление модели справа).

Прогрессия g^k масштабируется умножением на g^v. Песочно-желтые элементы $X = \{g^v, g^{v+1}, g^{v+2}, \ldots, g^{2v-1}\}$ операция сложения $Y = X + X^q$ проецирует в более ограниченную область — конечную модель вещественных чисел, отображаемых на рис. 10 элементами красного цвета.

Что касается генерации квадратичных вычетов, то красные элементы на рис. 10 нам нужно рассортировать (элементы со значениями 1 и –1) по факту совпадения их с квадратичными вычетами и невычетами. Для этого используем элемент $\omega = g^n$, чьи четные степени будем интерпретировать как вычеты (зеленый цвет на рис. 10), а нечетные — как невычеты (синий цвет).



■ ***Рис. 10***. Формы представления конечной модели комплексных чисел

■ ***Fig. 10***. Representation forms of the complex numbers finite model

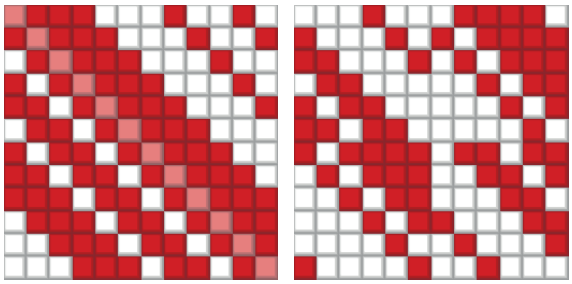
В силу расширения пространства группы квадраты элементов не реверсируются в ограниченную область, например, вычислениями по модулю q (размер поля вырос до q^2) и образуют семейство четных членов данной прогрессии.

В итоге получаем алгоритм, который завершается вычислением первой половины строки матрицы, стартовый элемент — нулевой. Вторая половина, ввиду симметрии, восстанавливается выписыванием элементов в реверсном порядке, игнорируя стартовый, при этом у негациклических матриц *знак каждого второго элемента* инвертируется. У конференц-матриц вся хвостовая часть еще раз инвертируется. Разделением четных и нечетных строк и столбцов матрица приводится к кососимметрическому виду с двумя блоками **A** и **B**, с исправлением диагонали в 1 (рис. 11).

Заметим, что во всех таких случаях мы всегда применяем один и тот же прием — вычисляем прогрессию. У негациклического блока строки получаются смещением с размещением слева вытесняемых элементов справа, но с инверсией знака. Отчетливо выраженных орнаментальных инвариантов такая матрица не имеет, с чем связана, возможно, продуктивность этого подхода.

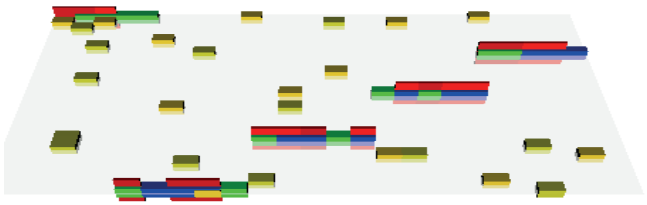
Для четных порядков матриц, кратных 2, но не делящихся на 4, метод ведет к так называемым конференц-матрицам, когда компенсировать нуль на диагонали не получается по соображениям совместности. После инвертирования знаков четных строк и столбцов блоков **A** и **B** они становятся циклическими симметричными и кососимметричными блоками. Дополнительно циклическое смещение второго блока на половину его размера решает проблему обеспечения блочной симметрии, характерной для этих бициклов.

В результате получается много ортогональных матриц двухблочной конструкции, что позволяет отнести этот метод едва ли не к основным и постулировать, что если поля нет, то соответствующим образом устроенная матрица Адамара все равно существует, теряя, разве что, вид симметрии.



■ ***Рис. 11***. Негациклическая матрица и негациклический бицикл

■ ***Fig. 11***. Negacyclic matrix and negacyclic bicycle



■ ***Рис. 12.*** Представление модели при работе в сложных полях

■ ***Fig. 12.*** Model representation when working in complex fields

При работе предлагаемого алгоритма в сложных полях меняется логика размещения расчетных элементов (рис. 12), но не тип матрицы, как это было с алгоритмами Секереша.

Заметим, что нам здесь пришлось воспользоваться двумя операциями поля, поскольку проецирование осуществляется сложением.

Алгоритмы Нобору Ито

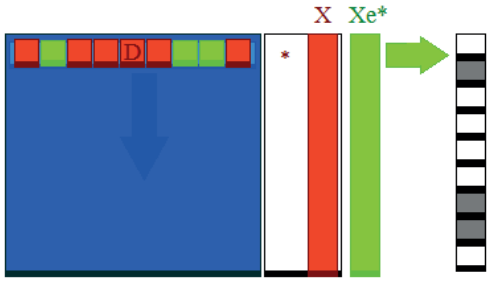
Ито начал работать в рассматриваемой тематике в 1993 г. [19, 20] с примера тетраэдральной группы $G = \{X, Y\}$, построенной с помощью трех генераторов a, b и c (бывает и такое). Первую ее половину составляет $X = \{e, a, b, ab, c, ac, bc, abc, c^2, ac^2, bc^2, abc^2\}$, вторую $Y = Xe^*$. Здесь e — единичный элемент, $e^* = a^2 = b^2$ — инволюция. Это близко идее Секереша в алгоритме, использующем для селекции знаков пару множеств (рис. 13).

Цель Ито состоит в том, чтобы ясно показать, что ортогональная матрица Адамара отвечает симметриям, описываемым группой тетраэдра (рис. 14). Чтобы убедиться, что это именно группа, необходимо сконструировать умножением по модулю 11 все $n = 12$ ее элементов, опираясь на следующее матричное представление a, b и c:

$$\mathbf{A} = \begin{pmatrix} 0 & 10 \\ 1 & 0 \end{pmatrix}; \ \mathbf{B} = \begin{pmatrix} 1 & 3 \\ 3 & 10 \end{pmatrix}; \ \mathbf{C} = \begin{pmatrix} 4 & 7 \\ 8 & 6 \end{pmatrix},$$

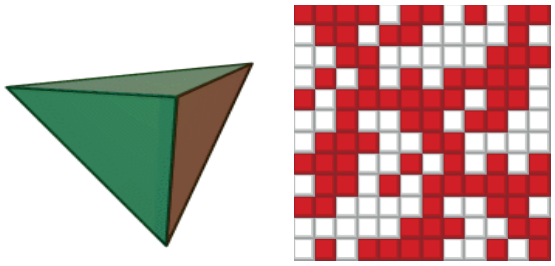
и проверить свойства $c^3 = e$, $b^{-1}ab = ae^*$, $c^{-1}ac = b$, $c^{-1}bc = ab$, обеспечивающие основное качество группы: нет такого сочетания элементов, которое не сводилось бы к элементам группы G. В качестве e берется единичная матрица $\mathbf{I}$, $e^* = a^4 = b^2$ — инволюция здесь и далее $(n - 2)\mathbf{I}$.

$D = \{e^*, ae^*, be^*, abe^*, c, ace^*, bce^*, abc, c^2e^*, ac^2, bc^2e^*, abc^2e^*\}$ задает первую строку кососимметричной матрицы Адамара тем, что элементы, входящие в первую половину группы, генерируют 1 и –1, если во вторую. Заметим, что если не учитывать элемент e^*, она повторяет порядок следования элементов группы.



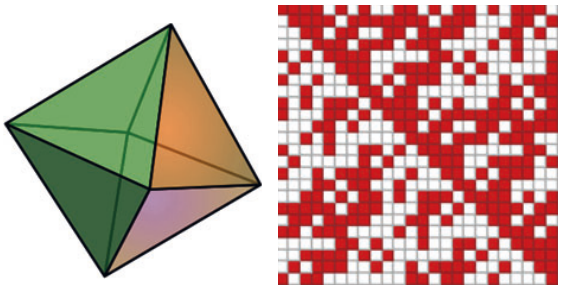
■ ***Рис. 13.*** Схема алгоритма Нобору Ито

■ ***Fig. 13.*** Noboru Ito algorithm diagram



■ ***Рис. 14.*** Тетраэдр и матрица Адамара с его симметриями

■ ***Fig. 14.*** Tetrahedron and Hadamard matrix with its symmetries



■ ***Рис. 15.*** Октаэдр и матрица Адамара с его симметриями

■ ***Fig. 15.*** Octahedron and Hadamard matrix with its symmetries

Остальные строки определяются последовательными произведениями D на элементы g первой половины группы. Перед синтезом элементы Dg тоже переставляются в соответствии с порядком их следования в группе. Если отказаться от перестановки, элементы –1 строки кососимметрической матрицы определяются вхождением $Y = Xe^*$ в Dg, поскольку Y содержит нужный порядок.

Следующий пример разнообразит ассоциативный ряд фигура-матрица группой октаэдра (рис. 15) с $D = \{e^*, ae^*, a^2e^*, a^3e^*, b, abe^*, a^2b, a^3be^*, c, ac, a^2ce^*, a^3ce^*, bc, abce^*, a^2bc, a^3bce^*, c^{-1}e^*, ac^{-1}, a^2c^{-1}e^*, a^3c^{-1}, bc^{-1}e^*, abc^{-1}e^*, a^2bc^{-1}e^*, a^3bc^{-1}\}$.

Остается сконструировать умножением по модулю 23 все $n = 24$ элемента, опираясь на следующее матричное представление a, b, c и c^{-1}:

$$\mathbf{A} = \begin{pmatrix} 7 & 19 \\ 4 & 11 \end{pmatrix}; \ \mathbf{B} = \begin{pmatrix} 10 & 9 \\ 22 & 13 \end{pmatrix};$$

$$\mathbf{C} = \begin{pmatrix} 18 & 11 \\ 19 & 4 \end{pmatrix}; \ \mathbf{C}^{-1} = \begin{pmatrix} 4 & 12 \\ 4 & 18 \end{pmatrix},$$

и проверить свойства $c^3 = e$, $b^{-1}ab = a^3e^*$, $c^{-1}a^2c = b$, $c^{-1}bc = a^2be^*$ и $(ab)^{-1}c^2b = c^{-1}$, обеспечивающие качество сочетания элементов быть группой.

Ито построил пример с группой икосаэдра (рис. 16).

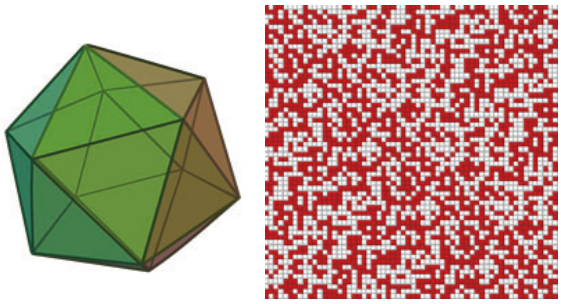
Остается сконструировать умножением по модулю 59 все $n = 60$ элементов, опираясь на следующее матричное представление a, b, c и d:

$$\mathbf{A} = \begin{pmatrix} 6 & 8 \\ 47 & 53 \end{pmatrix}; \ \mathbf{B} = \begin{pmatrix} 17 & 51 \\ 51 & 42 \end{pmatrix};$$

$$\mathbf{C} = \begin{pmatrix} 51 & 9 \\ 33 & 7 \end{pmatrix}; \ \mathbf{D} = \begin{pmatrix} 46 & 3 \\ 56 & 46 \end{pmatrix},$$

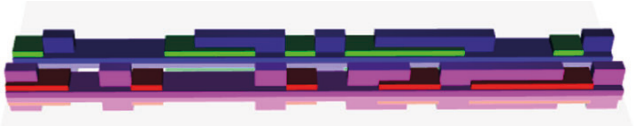
и проверить свойства $c^3 = e$, $d^5 = e$, $(da)^3 = e^*$, $d^2a = cde^*$, обеспечивающие качество сочетания элементов быть группой, инволюция $e^* = a^4 = b^2$, $D = \{e^*, a, be^*, abe^*, c, ac, bc, abc, c^2e^*, ac^2, bc^2, abc^2, d, ad, bd, abd, cde^*, acde^*, bcd, abcd, c^2d, ac^2de^*, bc^2de^*, abc^2d, d^2e^*, ad^2e^*, bd^2e^*, abd^2, cd^2, acd^2e^*, bcd^2e^*, abcd^2e^*, c^2d^2, ac^2d^2e^*, bc^2d^2e^*, abc^2d^2e^*, d^3, ad^3, bd^3e^*, abd^3, cd^3, acd^3e^*, bcd^3, abcd^3e^*, c^2d^3e^*, ac^2d^3, bc^2d^3, abc^2d^3, d^4e^*, ad^4, bd^4e^*, abd^4, cd^4e^*, acd^4e^*, bcd^3, abcd^4e^*, c^2d^4e^*, ac^2d^4e^*, bc^2d^4, abc^2d^4\}$.

Для нахождения обратной матрицы применяется обычный алгоритм инверсии матрицы, описанный еще Гауссом, но в конечном поле заданного модулем размера. Этот небольшой, но яркий набор примеров показывает богатство групп и возможных ассоциаций с ними. В нем отчетливо видны особенности идеи, к которой Ито позднее пришел,



■ ***Рис. 16.*** Икосаэдр и матрица Адамара с его симметриями

■ ***Fig. 16.*** Icosahedron and Hadamard matrix with its symmetries



■ ***Рис. 17.*** Трансверсали D и Dg

■ ***Fig. 17.*** Transversals D и Dg

подыскивая универсальную группу на роль такого описания: минимальная конструкция должна обходиться двумя генераторами, причем для ортогональных матриц характерна дихотомия в разделении элементов группы на равные по размерам подмножества, что может быть использовано как признак ортогональности.

Дициклическая группа $G = \{e, a, a^2, ..., a^{2v-1}, b, ab, a^2b, ..., a^{2v-1}b\}$, образованная двумя генераторами a и b, годится на роль такого посредника. Ее элементы имеют вид a^kb^m, и эта конструкция получена сращиванием пары циклических групп. Конечной ее делают соглашения: $a^{2v} = b$, $a^{4v} = e$, $bab^{-1} = a^{-1}$. Элемент $e^* = b^2 = a^{2v}$ обладает свойством $(e^*)^2 = e$, это единственная центральная (перестановочная с любым элементом) инволюция группы (у вещественных чисел это корень квадратный).

Трансверсалью D группы G по отношению к $<e^*>$ (единичному элементу и инволюции) называется такая половина ее элементов, что $\{D, De^*\}$ содержит все элементы группы, половинки не пересекаются. Если есть трансверсаль такая, что множества D и Dg наполовину пересекаются для любого элемента группы g, не совпадающего с $<e^*>$, то такой набор называется *адамаровым* (рис. 17).

На рис. 17 зелеными и красными модулями представлено размещение элементов трансверсали на парной подложке группы согласно их порядковым номерам. Высокие детали изображения показывают размещение элементов Dg.

Алгоритм Ито вычисления бинегациклической матрицы Адамара состоит в формировании половины элементов циклической группы a^* двух наборов a^*, ba^* в связанных с ними последовательностях, формирующих бинегациклическую матрицу Адамара, изображенную на рис. 11. Значения 1 или –1 обозначают пересечение их элементов с элементами трансверсали. Все познается в сравнении: после громоздких построений, описанных ранее, дициклическая группа в модели Ито уже не кажется сложной.

Теоретико-групповой подход

После 70-х годов XX века комбинаторная теория начала испытывать недостаток новых общих идей, способствующих ее развитию. Одна из та-

ких идей состояла в том, чтобы «увидеть» матрицу Адамара прямо в таблице, но не в таблице инцидентности графа, а, например, в «таблице умножения» $G \times G$ группы, благодаря некоторому преобразованию. Так появились *коциклические* матрицы [21], которые разберем на основе часто приводимого примера.

Допустим, для синтеза матриц Адамара мы решили обойтись одной таблицей четверной группы Клейна V_4. Теперь рассмотрим выражение

$$\psi: G \times G \to <1>$$

и поясним, что если $G = V_4$, операция «×» — это привычное сложение, а преобразование ψ переводит элементы таблицы в числа 1 и −1, содержащиеся в сэте <1>, по следующему правилу:

$$\psi(A) = \psi(B) = 1,\ \psi(C) = -1,\ \psi(D) = 1.$$

Легко проверить, что получающаяся таким образом из таблицы матрица **H** будет удовлетворять уравнению $\mathbf{H}^{\mathrm{T}}\mathbf{H} = n\mathbf{I}$, т. е. будет матрицей Адамара, представленной на рис. 18.

В случае матриц порядка 4 элементарными преобразованиями (перестановкой первых двух строк вниз) матрица **H** сводится к циклической форме, в которой ее чаще всего изображают. В целом это направление скорее иллюстративное, чем практическое. Дальнейшее развитие этой идеи потребовало разбирательства в том, каким уравнениям должна удовлетворять вспомогательная функция ψ.

Уже с появлением матриц у операций сложения и умножения появилась двойная нагрузка. С одной стороны, обе эти операции активно используются для манипуляций с элементами матрицы, позволяя сконструировать операцию умножения матриц. С другой стороны, есть сложение и умножение матриц, обозначаемое теми же символами и с теми же (если исключить коммутативность умножения) правилами употребления.

+	A	B	C	D
A	1	1	−1	1
B	1	1	1	−1
C	−1	1	1	1
D	1	−1	1	1

■ ***Рис. 18***. Коциклическая матрица Адамара
■ ***Fig. 18***. Cocyclic Hadamard matrix

С тех пор нагрузка на смысловое содержание операций только растет.

Теперь, внимание, к этой операции умножения вида «×», реализованной внутренним сложением, можно добавить внешнее сложение $g^2 + g^3$, порождая операцию группового кольца. Эти два типа сложения сосуществуют и вместе образуют то, что мы привыкли организовывать иным путем. Из школьного курса известна реализация операции умножения из ранее определенного сложения, но здесь сложение появляется после того, как мы определились с тем, что будем понимать под умножением.

Полиномиальные уравнения орнаментов

Разность пары элементов $a - b$ в абстрактной алгебре интерпретируют как операцию, противоположную операции «×» группы. Соответственно, ее обозначают не так, как выше, а делением или умножением на обратный элемент ab^{-1} (*right quotient*). Столь замысловатое обозначение можно было бы отнести к причудам абстрактной теории и не обращать на нее внимание, не получи она в настоящее время широкое распространение в литературе по ортогональным матрицам [22, 23].

Парадокс в том, что теперь этой операции «×» недостаточно. К циклической группе элементов $G = \{1, g, g^2, \ldots\}$, порожденных последовательными степенями примитивного элемента g, мы намерены добавить формальное сложение «+», выводящее на элементы группового кольца. Напомним, что «+» не позволяет пользоваться термином группа, у группы нет «суммы» ее элементов, кроме того, этот знак, как и у матриц, соотносим с надстраиваемым сверху групповым кольцом.

Переход на новый понятийный уровень позволяет элегантно записать условие Зингера для моноблока **M** порядка $v = n - 1$ матрицы $\mathbf{H} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{M} \end{pmatrix}$ с каймой в виде одного уравнения

$$DD^{(-1)} = k - \lambda + \lambda G \qquad (1)$$

и впредь оперировать уравнениями такого вида, связывающими количество −1 в каждой строке k и количество значений −1 в каждой паре строк λ с деталями орнамента матрицы. Для ортогональных матриц $\lambda = k - n/4$, так что может фигурировать просто $n/4$.

Пример 4. В самом деле, обращаясь к рассмотренному в примере 1 дифференциальному набору $D = \{1, 3, 4, 5, 9\}$, без угрозы путаницы обозначений запишем его как *элемент группового кольца* $D = g + g^3 + g^4 + g^5 + g^9$. Произведение

с $D^{(-1)} = g^{-1} + g^{-3} + g^{-4} + g^{-5} + g^{-9}$ порождает все описанные ранее разности показателей степеней по модулю $v = 11$. Одинаковые разности встречаются $\lambda = 2$ раза, порождая λG в (1) за вычетом не встречаемых комбинаций самого первого ее элемента $g^0 = 1$ (вычитаем λ). Кроме того, из-за k вычитаний у степеней g и g^{-1}, g^3 и g^{-3} и т. п. наберется-таки $k = 5$ элементов g^0, которые также учтены полиномиальной формулой.

Помимо модели (1) с ее детальным описанием узора D, есть модель попроще в виде условия реализуемости узора (орнамента) $k(k-1) = \lambda(v-1)$, которое можно переписать в каноническом виде как

$$x^2 = 1,\ k = (v - x)/2. \qquad (2)$$

Это условие действительно дает параметры в приведенном примере с $v = 11$, $k = 5$, $\lambda = 2$.

Правило, по которому детальная модель, например матрица, переходит к более простому ее описанию, например детерминанту матрицы, называется гомоморфизмом, причем алгоритм вычисления детерминанта фигурирует как описание этого соответствия. В отличие от изоморфизма, описывающего взаимно-однозначную связь моделей одной сложности, матрицу можно изменить так, чтобы детерминант ее не изменился. Обратное неверно, изменение детерминанта однозначно связано с тем, что изменилась матрица. То есть гомоморфизм — это путь от сложной модели к простой.

Для перехода от модели (1) к модели (2) построим нужный нам гомоморфизм, именуя его для простоты *характеристикой D* такой, что $\underline{x} = \chi(D) = \chi(D^{(-1)})$ — разность между числом *нечетных* и *четных* степеней, так что $\chi(G) = 0$. Благодаря этому можно записать почти нужное нам уравнение вида $\underline{x}^2 = n/4$. Замена переменных $nx = 4\underline{x}$ порождает уравнение $x^2 = 1$, описывающее решения в форме корней из единицы.

При рассмотрении матриц Адамара $\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}$ порядка $n = 2v$ полиномиальные уравнения, которые дублируют более простые квадратичные уравнения связи орнаментальных инвариантов, получили дополнительную работу. Условие реализуемости узора с параметрами $v/2 = k_1 + k_2 - \lambda$ такой матрицы имеет малое различие с (1)

$$D_0 D_0^{(-1)} + D_1 D_1^{(-1)} = k_1 + k_2 - \lambda + \lambda G \qquad (3)$$

для ортогональных матриц с $\lambda = k_1 + k_2 - n/4$, где v — размер блока основы, так что в правой части может фигурировать просто $n/4$ в сумме с λG.

Пример 5. Для матрицы Адамара порядка 16: $v = 8$, $k_1 = 2$, $k_2 = 4$, $\lambda = 2$, $D_0 = \{1, 7\}$, $D_1 = \{2, 3, 5, 6\}$, группа G размера v содержит все числа от 0 до $v - 1 = 7$. Плечи матрицы описываются тут двумя элементами группового кольца $D_0 = g^1 + g^7$, $D_1 = g^2 + g^3 + g^5 + g^6$, произведения $D_0 D_0^{(-1)} = (g^1 + g^7)(g^{-1} + g^{-7}) = 2 + g^{-6} + g^6 = 2 + g^2 + g^6$, $D_1 D_1^{(-1)} = (g^2 + g^3 + g^5 + g^6)(g^{-2} + g^{-3} + g^{-5} + g^{-6}) = 4 + 2g^1 + g^2 + 2g^3 + 2g^4 + 2g^5 + g^6 + 2g^7$. Их сумма равна элементу $G = 1 + g + g^2 + g^3 + g^5 + g^6 + g^7$, умноженному на $\lambda = 2$, за вычетом λ (при 1), тогда как первые члены 2 и 4 произведений дадут значение $k_1 + k_2 = 6$.

При сравнении полиномов мы сравниваем показатели степеней и коэффициенты полиномов отдельно, так что запись совокупности элементов группы $1, g, g^2, \ldots$ в виде одного элемента группового кольца $1 + g + g^2 + \ldots$ открывает возможность одним уравнением описать цепочку равенств. Как и в матричной алгебре, мы сокращаем количество уравнений. Теперь поясним, зачем все это нужно.

Пойдем проторенным путем, учтя, что, помимо модели (3) с ее детальным описанием узора, есть модель проще в виде уравнения реализуемости орнамента, которое можно переписать в каноническом виде уравнения окружности

$$x^2 + y^2 = n,\ k_1 = (v - x)/2,\ k_2 = (v - y)/2, \qquad (4)$$

причем для перехода от модели (1) к модели (2) годится построенный ранее нами гомоморфизм в форме характеристики, примененной к двум полиномиальным плечам $\underline{x} = \chi(D_0) = \chi(D_0^{(-1)})$, $\underline{y} = \chi(D_1) = \chi(D_1^{(-1)})$, выражающей разности между числом *нечетных* и *четных* степеней в полиномах, так что $\chi(G) = 0$. На первом этапе получим уравнение окружности меньшего радиуса $\underline{x}^2 + \underline{y}^2 = n/4$, которое переходит в нужное нам удваиванием квадрата радиуса, так что $x = 2\underline{x}$, $y = 2\underline{y}$.

В частности, для указанного выше примера $\underline{x} = \chi(D_0) = 2$, $\underline{y} = \chi(D_1) = 0$, так что алгоритм работает: $x^2 + y^2 = 16$.

Причина, по которой с этим формализмом пришлось подробнее разбираться, состоит в том, что нам хотелось бы, чтобы блоки **A** и **B** были циклическими, ввиду чего уравнение (4) становится необходимым, но не достаточным условием существования бицикла. Иными словами, помимо этого уравнения должно возникнуть дополнительное, ограничивающее область определения.

Это сужение того, из чего делается выбор переменных, описывающих точки Гаусса (точки с целыми координатами x, y) на окружности, лимитирующей количества элементов со значением -1 в каждой строке двух блоков бицикла $k_1 = (v - x)/2$, $k_2 = (v - y)/2$, а оно не может быть

дробным, и доопределяет задачу так, как нам хотелось бы ее доопределить. Предварительно известно, что согласно так называемой рождественской теореме Ферма целое число вида $n = 4t + 1$ всегда разложимо на сумму двух квадратов: $5 = 1 + 2 \times 2$, $9 = 0 + 3 \times 3$ и т. д., и целое число вида $4t + 3$ неразложимо: 3, 7, 11, ...

Соответственно, если порядок бицикла n имеет делители последнего вида (или их нечетные степени), то уравнение окружности с точками Гаусса на них составить невозможно. Сомнение в возможности существования бицикла возникает при наличии делителей в виде четных степеней простых чисел вида $p = 3 \pmod 4$. Во всех остальных случаях решение определенно существует. Вспомогательное уравнение $\underline{x}^2 + \underline{y}^2 = \upsilon/2$ требует, кстати, чтобы каждое слагаемое в нем было либо 0, либо разностью двух квадратов. Например, для случаев $\upsilon/2 = 9 = 0 + 9 = 0 + (25 - 16)$, $\upsilon/2 = 18 = 9 + 9$ и т. п. Остается вспомнить, что абелева группа G размера $p^{2t}u$ имеет силовскую p-подгруппу P, и нас интересует случай, когда эта подгруппа циклична. Тогда цепочка проецирований, гомоморфизмов, описанных выше, удлиняется на одно звено от исходных полиномов D_0, D_1 уравнения (3) к новым полиномам C_0, C_1 задачи, в которой вследствие первого сжатия размера появляются отличные от единичных коэффициенты при слагаемых группового кольца. Например, $C(\lambda G)$, равные λuP, удовлетворяющие уравнению

$$C(D_0)C(D_0)^{(-1)} + C(D_1)C(D_1)^{(-1)} = \\ = k_1 + k_2 - \lambda + \lambda uP \qquad (5)$$

и далее привычным $\underline{x} = \chi(C_0)$, $\underline{y} = \chi(C_1)$ в первом уравнении из (4). В работе [23], где проложен этот путь, уравнение записывается в максимально общей форме с комплексными переменными. Обычно чем менее мы сужаем решение задачи, тем проще добраться до сколь-нибудь вразумительного ответа. Прием погружения аргументов в комплексное пространство часто используется для упрощения вида уравнений, однако здесь это преимущество не ощущается.

Поэтому читатель при желании может заменять в ссылках на (4) в двух следующих леммах [23], имеющих в реферируемой литературе своих авторов, область определения аргумента с реальной на комплексную. Однако после такой замены (если она имеет иной смысл, помимо усложнения, не нужного задаче) при реальной правой части уравнение описывает *гиперсферу*, а не окружность, теряя иллюстрируемость рис. 3, призванного отражать корни из 1. Возможно, этот ритуал подчеркивает, что в работах на выяснение существования решения важен не столько рабочий вид гомоморфизма, сколько отыскиваемый признак разрешимости задачи с квадратичным уравнением общего вида, заданным над множеством решений уравнения (5).

Лемма 1. Если правая часть уравнения окружности из (4) имеет делитель p^{2t}, $p = 3 \pmod 4$ — простое число, то $\underline{x}$ и $\underline{y}$ делятся на p^t.

Такие пересчеты масштабов координат возникали у нас и ранее. Лемма доказывается от обратного. Выделим p^t из $\underline{x}$ и $\underline{y}$, элементарные правила арифметики позволяют вынести появившийся ввиду квадрирования общий множитель p^{2t} за скобки, правая часть (4) тоже должна его содержать. Условие реверсивно, если она его содержит, обратный процесс перераспределит навязываемое p^t по составным частям.

Лемма 2. Пусть $\underline{x}$ и $\underline{y}$ делятся на p^t, тогда C_0 и C_1 можно описать аддитивно значениями $p^tX + YP$, где множители X и Y, как это свойственно элементам окружности, взяты на том же множестве всех возможных решений уравнения (5).

Доказательство приведено у Ма [24]. Этот несколько искусственный прием позволяет сформулировать следующую теорему.

Теорема. Пусть $\upsilon = p^{2t}u$, $p = 3 \pmod 4$ — простое число, p и u взаимно просты, причем $(\upsilon/2 \parallel p^{2e})$, т. е. $\upsilon/2$ содержит делитель p^{2e} (причем остаток уже не делится на p), тогда уравнение окружности (4) разрешимо, если $u \geq p^e$.

Заметим, что по условиям формирования коэффициенты полиномов D_0 и D_1 не превосходят 1, их сведение к полиномам меньшей степени $C_0 = C(D_0)$ и $C_1 = C(D_1)$ дает весовые коэффициенты при степенях $1, g, g^2, \ldots$ примитивного элемента, не большие u.

Поскольку $\upsilon/2$ содержит делитель p^{2e}, то, согласно первой лемме, элементы C_0 и C_1 содержат делитель с вдвое меньшим показателем p^e. Соответственно, согласно второй лемме, их можно перегруппировать к приспособленной для доказательства аддитивной форме $C_0 = p^eX_0 + Y_0P$, $C_1 = p^eX_1 + Y_1P$. Эта форма удобна тем, что, умножив обе части ее на множитель $1 - g$, где g — примитивный элемент циклической подгруппы Силова P, вторым слагаемым можно пренебречь: $P(1 - g) = 0$. Смещение составляющих $1, g, g^2, \ldots$ суммы умножением на примитивный элемент не меняет подгруппы. Отсюда имеем $C_0(1 - g) = p^eX_0(1 - g)$, $C_1(1 - g) = p^eX_1(1 - g)$.

Поскольку коэффициенты полиномов C_0 и C_1 не превышают u, то при $u < p^e$ правые части формул придется аннулировать выбором настраиваемых множителей X_0, X_1. Тогда C_0 и C_1 обретают признаки полиномов, описывающих подгруппы, так как выходит, что $C_0 = C_0g$, $C_1 = C_1g$. Это, в свою очередь, невозможно, так как окажется, что характеристики $\chi(C_0) = 0$, $\chi(C_1) = 0$, что противоречит условию, при котором точки решения берутся на окружности, а не в центре. Данный

вывод дает нам в руки желаемый формализм решения задач на существование бициклов. Для матриц Адамара размер $n = 2v$ кратен 4, соответственно, для четного $v = p^{2t}u$ задача неразрешима при $u < 2p$, $p = 3 \bmod 4$.

Пример 6. Перейдем теперь к конкретному порядку. Пусть $n = 2v = 36$, $v = p^{2t}u = 18$, $p = 3$, $t = 1$, $u = 2$, абелева группа G имеет p-подгруппу Силова размера $p^2 = 9$. При $u = 2 < 2p = 2 \times 3 = 6$ задача неразрешима, причем удвоение размера бицикла до порядка 72 с $u = 4$, как видно, тоже ничего не дает. Бицикл порядка 144 реализуем и найден путем компьютерных экспериментов [25].

Заключение

Теоретико-групповой подход позволяет находить матрицы высоких порядков, опираясь на неявно выраженные симметрии, описываемые группами. Это обстоятельство позволяет строить вычислительные алгоритмы, отличные по эффективности от переборных алгоритмов.

Неразрешимость задачи на частном примере не отвергает существование матрицы Адамара. Матричная алгебра не располагает простыми средствами (пока так видится) определять, на каких порядках циклический орнамент блоков матрицы входит в противоречие с условием ортогональности вида $\mathbf{A}^T\mathbf{A} + \mathbf{B}^T\mathbf{B} = n\mathbf{I}$. Однако судить об этом позволяет теоретико-групповой подход.

Благодарности

Авторы выражают искреннюю благодарность профессорам Дж. Себерри и Д. Джоковичу за ценные советы и вспомогательные примеры, облегчившие нашу работу.

Кроме того, мы выражаем признательность Т. В. Балониной за техническую подготовку текста этой статьи.

Финансовая поддержка

Статья подготовлена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004.

Литература

1. **Davenport H.** *An Introduction to the Theory of Numbers*. Harper & Brothers, New York, 1952.
2. **Manfred Schroeder.** *Number Theory in Science and Communication*. Springer-Verlag, Berlin-Heidelberg, 2009. 431 p.
3. **Манин Ю. И., Панчишкин А. А.** Введение в теорию чисел. *Итоги науки и техники*. Сер. *Современные проблемы математики. Фундаментальные направления*, 1990, т. 49, с. 5–341.
4. **Ball Rouse W. W.** *A Short Account of the History of Mathematics*. NY, Dover Publications, 2001. 439 p.
5. **Балонин Н. А.** *Новый курс теории управления движением*. СПб.: СПбГУ, 2000. 160 с.
6. **Hadamard J.** Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.
7. **Seberry J., Yamada M.** Hadamard matrices, sequences and block designs. In: *Contemporary Design Theory: A Collection of Surveys*. Eds. J. H. Dinitz and D. R. Stinson. J. Wiley, New York, 1992. Pp. 431–560.
8. **Scarpis U.** Sui determinanti di valore Massimo. *Rendiconti della R.* Istituto Lombardo di Scienze e Lettere, 1898, ser. 2, vol. 31, fascicolo 20, pp. 1441–1446.
9. **Singer J.** A Theorem in finite projectie geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 1938, vol. 43, pp. 377–385.
10. **Balonin N. A., Seberry Jennifer.** Two level Cretan matrices constructed via Singer difference sets. *Информационно-управляющие системы*, 2014, № 6, с. 2–5.
11. **Балонин Н. А., Сергеев М. Б.** Матрицы Мерсенна и Адамара, произведения. *Информационно-управляющие системы*, 2016, № 5, с. 2–14, doi.org/10.15217/issn1684-8853.2016.5.2.
12. **Paley R. E. A. C.** On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
13. **Балонин Н. А., Сергеев М. Б.** Нормы обобщенных матриц Адамара. *Вестник СПбГУ.* Сер. 10. *Прикладная математика. Информатика. Процессы управления*, 2014, вып. 2, с. 5–11.
14. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi.org/10.31799/1684-8853-2019-3-2-9
15. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы максимального детерминанта. *Информационно-управляющие системы*, 2020, № 6, с. 2–11. doi.org/10.31799/1684-8853-2020-6-2-11
16. **Szekeres G.** Tournaments and Hadamard matrices. *L'Enseignement Math*, 1969, vol. 15, pp. 269–278.
17. **Szekeres G.** Cyclotomy and complementary difference sets. *Acta Arithmetica*, 1971, vol. 18, pp. 349–353. doi:10.4064/aa-18-1-349-353
18. **Goethals J.-M., Seidel J. J.** Orthogonal matrices with zero diagonal. *Canad. J. Math.*, 1967, vol. 19, pp. 1001–1010. doi:10.4153/CJM-1967-091-8

19. **Ito N.** Note on Hadamard groups of quadratic residue type. *Hokkaido Mathematical Journal*, 1993, vol. 22, pp. 373–378.
20. **Ito N.** On Hadamard groups III. *Kyushu J. Math.*, 1997, no. 51, pp. 369–379.
21. **Horadam K. J.** Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
22. **Arasu K. T., Xiang Q.** On the existence of periodic complementary binary sequences. *Designs, Codes and Cryptography*, 1992, vol. 2, pp. 257–262. doi:10.1007/BF00141970
23. **Egan Ronan.** On equivalence of negaperiodic Golay pairs. *Designs, Codes and Cryptography*, 2017, vol. 85, pp. 523–532. doi:10.1007/s10623-016-0320-6
24. **Ma S. L.** *Polynomial addition sets*. University of Hong Kong, 1985. 120 p. doi:10.5353 / TH_B3123054
25. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея. *Информационно-управляющие системы*, 2015, № 3, с. 2–16. doi.org/10.15217/issn1684-8853.2015.3.2

UDC 519.614
doi:10.31799/1684-8853-2021-4-2-17

Finite field and group algorithms for orthogonal sequence search

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
A. M. Sergeev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-4788-9869
O. I. Sinitsyna[a], Post-Graduate Student, orcid.org/0000-0002-2819-4682
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Hadamard matrices consisting of elements 1 and −1 are an ideal object for a visual application of finite dimensional mathematics operating with a finite number of addresses for −1 elements. The notation systems of abstract algebra methods, in contrast to the conventional matrix algebra, have been changing intensively, without being widely spread, leading to the necessity to revise and systematize the accumulated experience. **Purpose:** To describe the algorithms of finite fields and groups in a uniform notation in order to facilitate the perception of the extensive knowledge necessary for finding orthogonal and suborthogonal sequences. **Results:** Formulas have been proposed for calculating relatively unknown algorithms (or their versions) developed by Scarpis, Singer, Szekeres, Goethal — Seidel, and Noboru Ito, as well as polynomial equations used to prove the theorems about the existence of finite-dimensional solutions. This replenished the significant lack of information both in the domestic literature (most of these issues are published here for the first time) and abroad. **Practical relevance:** Orthogonal sequences and methods for their effective finding via the theory of finite fields and groups are of direct practical importance for noise-immune coding, compression and masking of video data.

Keywords — Hadamard matrices, orthogonal matrices, finite dimensional mathematics, Galois fields, finite groups, Scarpis algorithm, Singer approach, Szekeres method, Goethal — Seidel algorithm, Noboru Ito approach.

For citation: Balonin N. A., Sergeev A. M., Sinitsyna O. I. Finite field and group algorithms for orthogonal sequence search. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 4, pp. 2–17 (In Russian). doi:10.31799/1684-8853-2021-4-2-17

References

1. Davenport H. *An Introduction to the Theory of Numbers*. Harper & Brothers, New York, 1952.
2. Manfred Schroeder. *Number Theory in Science and Communication*. Springer-Verlag, Berlin-Heidelberg, 2009. 431 p.
3. Manin Yu. I., Panchishkin A. A. Introduction to number theory, *Itogi Nauki i Tekhniki*. Ser. *Sovrem. Probl. Mat. Fund. Napr.*, 1990, vol. 49, pp. 5–341.
4. Ball Rouse W. W. *A Short Account of the History of Mathematics*. NY, Dover Publications, 2001. 439 p.
5. Balonin N. A. *Novyj kurs teorii upravleniya dvizheniem*. [New Course in Motion Control Theory]. Saint-Petersburg, SPbGU Publ., 2000. 160 p. (In Russian).
6. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
7. Seberry J., Yamada M. *Hadamard matrices, sequences and block designs*. In: *Contemporary Design Theory: A Collection of Surveys*. Eds. J. H. Dinitz and D. R. Stinson. J. Wiley, New York, 1992. Pp. 431–560.
8. Scarpis U. Sui determinanti di valore Massimo. *Rendiconti della R.* Istituto Lombardo di Scienze e Lettere, 1898, ser. 2, vol. 31, fascicolo 20, pp. 1441–1446 (In Italian).
9. Singer J. A theorem in finite projectie geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 1938, vol. 43, pp. 377–385.
10. Balonin N. A., Seberry Jennifer. Two level Cretan matrices constructed via Singer difference sets. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 6, pp. 2–5.
11. Balonin N. A., Sergeev M. B. Mersenne and Hadamard Matrices, Products. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 5, pp. 2–14 (In Russian). doi.org/10.15217/issn1684-8853.2016.5.2
12. Paley R. E. A. C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
13. Balonin N. A., Sergeev M. B. The generalized Hadamard matrix norms. *Vestnik S.-Petersburg Univ.* Ser. 10. *Prikl. Mat. Inform*, 2014, iss. 2, pp. 5–11 (In Russian).
14. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 2–9 (In Russian). doi.org/10.31799/1684-8853-2019-3-2-9
15. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 6, pp. 2–11 (In Russian). doi.org/10.31799/1684-8853-2020-6-2-11
16. Szekeres G. Tournaments and Hadamard matrices. *L'Enseignement Math*, 1969, vol. 15, pp. 269–278.

17. Szekeres G. Cyclotomy and complementary difference sets. *Acta Arithmetica*, 1971, vol. 18, pp. 349–353. doi:10.4064/aa-18-1-349-353
18. Goethals J.-M., Seidel J. J. Orthogonal matrices with zero diagonal. *Canad. J. Math.*, 1967, vol. 19, pp. 1001–1010. doi:10.4153/CJM-1967-091-8
19. Ito N. Note on Hadamard groups of quadratic residue type. *Hokkaido Mathematical Journal*, 1993, vol. 22, pp. 373–378.
20. Ito N. On Hadamard groups III. *Kyushu J. Math.*, 1997, no. 51, pp. 369–379.
21. Horadam K. J. Hadamard matrices and their applications: Progress 2007–2010. *Cryptography and Communications*, 2010, no. 2, iss. 2, pp. 129–154.
22. Arasu K. T., Xiang Q. On the existence of periodic complementary binary sequences. *Designs, Codes and Cryptography*, 1992, vol. 2, pp. 257–262. doi:10.1007/BF00141970
23. Egan Ronan. On equivalence of negaperiodic Golay pairs. *Designs, Codes and Cryptography*, 2017, vol. 85, pp. 523–532. doi:10.1007/s10623-016-0320-6
24. Ma S. L. *Polynomial Addition Sets*. University of Hong Kong, 1985. 120 p. doi:10.5353 / TH_B3123054
25. Balonin N. A., Djokovic D. Z. Symmetry of two-circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 2–16. doi.org/10.15217/issn1684-8853.2015.3.2