УДК 519.614
doi:10.31799/1684-8853-2022-1-2-7

Критские матрицы Одина и Тени, сопровождающие простые числа и их степени

***Н. А. Балонин[a]**, доктор техн. наук, профессор, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru*
***М. Б. Сергеев[a]**, доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277*
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

***Введение:** критские матрицы — ортогональные матрицы, состоящие из элементов 1 и $-b$ (вещественное число), представляют собой идеальный объект для наглядного приложения конечномерной математики. К ним относятся, в частности, матрицы Адамара и, при расширении числа элементов, конференц-матрицы. Наиболее удобный аппарат исследования состоит в привлечении теории полей и мультипликативных групп Галуа, что особенно актуально для новых типов критских матриц. **Цель:** изучить симметрии критских матриц и исследовать два выделенных симметриями новых типа матриц нечетного и четного порядков соответственно, существенно отличающихся от ранее известных матриц Мерсенна, Эйлера и Ферма. **Результаты:** приведены формулы для значений элементов и описаны симметрии новых критских матриц: бициклов Одина (с каймой) порядков $4t-1$ и $4t-3$ и матриц Тени порядков $4t-2$ и $4t-4$. Для нечетных порядков матриц, равных простым числам и степеням простых чисел характеристических размеров, доказано существование симметрий особых типов этих матриц, двоякосимметричных, состоящих из кососимметричного (по знакам элементов) и симметричного циклических блоков. Показано, что ранее выделенные критские матрицы Мерсенна порядков $4t-1$ и Эйлера порядков $4t-2$ являются их частным случаем, существующим при отсутствии симметрии для всех выделенных порядков без исключения. **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, матрицы Белевича, критские матрицы, конечные поля, симметрии матриц.*

Для цитирования: Балонин Н. А., Сергеев М. Б. Критские матрицы Одина и Тени, сопровождающие простые числа и их степени. *Информационно-управляющие системы*, 2022, № 1, с. 2–7. doi:10.31799/1684-8853-2022-1-2-7
For citation: Balonin N. A., Sergeev M. B. Odin and Shadow Cretan matrices accompanying primes and their powers. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 2–7 (In Russian). doi:10.31799/1684-8853-2022-1-2-7

Введение

Впервые наследование порядками n матриц со значениями элементов (уровнями) 1 и –1 и ортогональных в смысле $\mathbf{H}^\mathrm{T}\mathbf{H} = n\mathbf{I}$, где $\mathbf{I}$ — единичная матрица, значений числовых последовательностей заметил еще основоположник теории матриц Дж. Сильвестр [1, 2]. Адамар [3] дополнил это наблюдение вложением ряда степеней простого числа 2^k в более широкую числовую последовательность вида $n = 4t$, где t — натуральное число, самостоятельно найдя матрицы порядков 12 и 20.

С тех пор в теории матриц Адамара достигнуты большие успехи [4, 5]. Вычисление матрицы размера 428 [6] подняло планку нижнего неизвестного пока порядка матриц Адамара до 668. Обобщающие их критские матрицы [7, 8] были введены в рамках композиционного построения теории экстремальных по детерминанту матриц [9], сопровождающих другие известные в теории числовые последовательности.

Изучению свойств симметрии критских матриц, а также двух новых видов симметричных матриц нечетного и четного порядков, существенно отличающихся от ранее известных матриц, посвящена настоящая работа.

Критские матрицы

Критские матрицы $\mathbf{K}$ во многом похожи на матрицы Адамара [10] (даже больше, чем взвешенные матрицы [11] с тремя уровнями на порядках, кратных двум). Это столь же малоуровневые матрицы с элементами 1 и $-b$, не превосходящими по модулю единицы, для которых справедливо $\mathbf{K}^\mathrm{T}\mathbf{K} = \omega\mathbf{I}$, где $\omega \le 1$ — некоторый весовой коэффициент [7, 11]. Число уровней в критских матрицах расширяемо, например, элементом d на диагонали. Фиксировать семейства критских матриц можно, как у матриц Адамара, указывая характер экстремума или предложением формулы для уровней $b = b(n)$ и $d = d(n)$.

Семейство критских матриц шире семейства матриц Адамара и включает его. Например, критские матрицы при $b = 1$ — это классические матрицы Адамара $\mathbf{H}$, при $b = 1$ и $d = 0$ (на диагонали) — это матрицы Белевича, для которых справедливо иное условие ортогональности $\mathbf{C}^\mathrm{T}\mathbf{C} = (n-1)\mathbf{I}$. Уровни и условие ортогональности вполне однозначно идентифицируют матрицы, однако сами по себе формулы для уровней можно получить не априори, а апостериори, анализируя частные экстремумы детерминантов на серии задаваемых анализируемыми последовательностями (прямо или косвенно) порядков [9].

Матрицы Адамара сопровождают порядки $n = 2^k$ и четные числа $4t$, в которые степени двойки вложены (гипотеза Адамара), а матрицы Белевича (взвешенные матрицы, конференц-матрицы [11]) варьированием их диагонального уровня в 0 охватывают дополнительные порядки, равные числам вида $4t - 2$, разложимым на сумму двух квадратов. Последнее утверждение тоже является гипотезой [1], поскольку вид экстремальных матриц усложняется с ростом порядка настолько, что первые неразрешенные теорией случаи охватывают числа 66 и 86 (а не 668, как у матриц Адамара).

Матрицы Мерсенна $\mathbf{M}$ [12], относящиеся к критским, сопровождают порядки, равные числам последовательности Мерсенна $n = 2^k - 1$ и нечетным числам вида $4t - 1$, в которые отмеченная последовательность вложена, и отличаются иррациональным уровнем $b = \dfrac{t}{t+\sqrt{t}}$.

На настоящее время не известно, ограничено ли множество простых чисел Мерсенна или их количество конечно (как и у чисел Ферма). Следующая задача, которая нас интересует, состоит в выделении критских матриц порядков, сопровождающих простые числа и степени простых чисел вида $4t - 1$ и $4t - 3$.

Случай $4t - 1$ наиболее прост тем, что существование конечного поля $GF(n)$ гарантирует наличие кососимметичных (по знакам элементов, не уровням) матриц Мерсенна [13]. Здесь существенно то обстоятельство, что, как и у матриц Адамара, диагональ этих матриц варьируется по уровню от 0 до 1 без потери ортогональности при условии изменения уровня b. Собственно, матрицы Белевича $\mathbf{C}$ трансформируются в матрицы Адамара $\mathbf{C} = \mathbf{H} + \mathbf{I}$ ровно по такому же принципу — предварительно нужно добиться кососимметрии $\mathbf{C}$, однако взаимные переходы в этом частном случае не изменяют отрицательный уровень.

В общем случае фиксация диагонали уменьшает количество возможных порядков с $4t - 1$ или $4t - 3$ до желаемого множества степеней простых чисел, причем отличаться матрицы будут симметриями. Такие критские матрицы ранее не рассматривались, поэтому мы их опишем максимально общо, не апеллируя к бициклической форме.

Матрицы Одина и матрицы Тени

Рассматриваемые матрицы могут получаться из хаотических матриц (оптимизация детерминанта не накладывает требований поддерживать структуру) или из матриц Адамара или Белевича, с основами (core) которых они тесно связаны при доказательствах теорем существования [12].

Определение 1. Матрица Одина порядка $4t - 1$, являющегося простым числом или его степенью, — это критская матрица с уровнями 1, $-b$, $d = 0$ (на диагонали), где $b = \dfrac{v-1}{v+\sqrt{2v-1}}$, $v = (n - 1)/2$ — половинный размер матрицы, за исключением ее каймы d.

Определение 2. Матрица Одина порядка $4t - 3$, являющегося простым числом или его степенью, — это критская матрица с уровнями 1, $-b$, $d = \dfrac{1}{1+\sqrt{n}}$ (на диагонали), где $b = 1 - 2d$.

Инвариантом матрицы Одина является равное число внедиагональных уровней. Такая структура позволяет с легкостью выделить в качестве первой строки и столбца кайму из элементов векторов $\mathbf{e}$ и $-b\mathbf{e}$, где $\mathbf{e}$ — вектор из 1 длины v. Структуры обеих матриц описываются кососимметричной (по знакам элементов) и симметричной формами соответственно:

$$\mathbf{O}_{4t-1} = \begin{pmatrix} d & \mathbf{e} & -b\mathbf{e} \\ -b\mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & [-\mathbf{B}^{\mathrm{T}}] & \mathbf{D}^{\mathrm{T}} \end{pmatrix};$$

$$\mathbf{O}_{4t-3} = \begin{pmatrix} d & -b\mathbf{e} & \mathbf{e} \\ -b\mathbf{e} & \mathbf{A} & \mathbf{B} \\ \mathbf{e} & \mathbf{B}^{\mathrm{T}} & [-\mathbf{D}^{\mathrm{T}}] \end{pmatrix}.$$

Здесь операция, обозначенная как $[\cdot]$, означает характерную для трехуровневых матриц замену всех положительных элементов транспонированной матрицы на 1 и всех отрицательных на $-b$. Добавление каймы из 1 и –1 в строке и столбце (с учетом симметрий) порождает матрицу Белевича $\mathbf{C}$ с уровнями $-b = -1$, $d = 0$. Отделение каймы у матриц Одина ведет к критским матрицам Тени $\mathbf{T}$ (shadow matrices) вида $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ -\mathbf{B}^{\mathrm{T}} & \mathbf{D}^{\mathrm{T}} \end{pmatrix}$ и $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{D}^{\mathrm{T}} \end{pmatrix}$.

Определение 3. Матрица $\mathbf{T}$ порядка $n = 4t - 2$, где $n + 1$ — простое число или его степень, — это критская матрица с уровнями блоков 1, $-b$, $d = 0$ (на диагонали), где $b = \dfrac{v-1}{v+\sqrt{4v-3}}$, $v = n/2 = 2t - 1$ — размер блока.

Определение 4. Матрица $\mathbf{T}$ порядка $n = 4t - 4$, где $n + 1$ — простое число или его степень, — это критская матрица с уровнями блоков 1, $-b$, $d = \dfrac{2}{3+\sqrt{2n+1}}$ (на диагонали), где $b = 1 - 2d$.

Значения уровней элементов во всех четырех отмеченных определениями случаях следует непосредственно из условия ортогональности и инварианта узора.

Матрицы **H** и **C** порядков $p^m + 1$, где p — простое число, связаны взаимно однозначными преобразованиями с матрицами **O** и **T**. При вычислении их в поле $GF(p^m)$ циклические блоки $\mathbf{A} = \mathbf{D}$, **B** предстают в наиболее экономном виде.

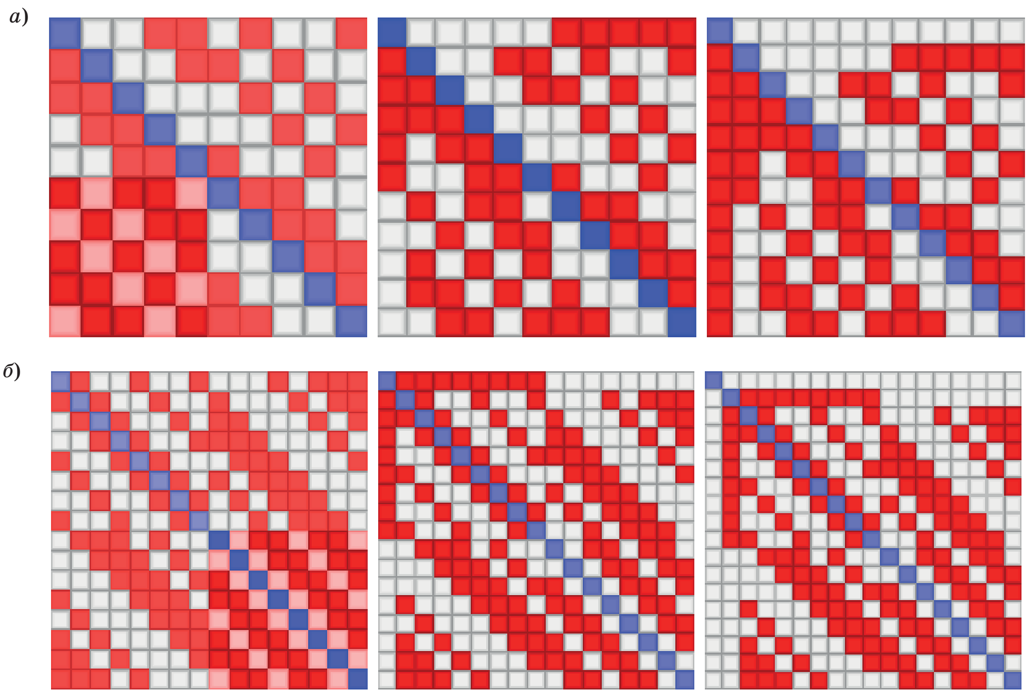
Взаимные переходы дизайнов (узоров) критских матриц показаны для кососимметричного (по знакам) и симметричного случаев на рис. 1, *а* и *б* соответственно. Здесь приведены их портреты — графические представления в цвете.

В первой кососимметричной по **A** версии узора вторая (парная) матрица **B** симметрична, а в симметричной версии — кососимметричной (по знакам) является ее первая строка, в силу четности размера она состоит из инвертированных по знаку половинок. Вторая половинка реверсирована. Именно этот важный инвариант структуры навязывается арифметикой полей Галуа, именно он отвечает за сопровождение порядков матриц простыми числами и их степенями.

Данное обстоятельство вскрыл еще основоположник использования полей Пэли, но в его время (30-е годы XX века) использовалось приведение матиц Адамара к циклическому блоку с одинарной каймой [13] (матриц Белевича тогда еще не было). Эта форма неустойчива к показателю степени простого числа. Для кратных простых чисел основа (core) матриц разваливается на мультиблоки. Бициклический характер основы освобождает нас от погружения в мультиблочные структуры, значительно упрощая подход Пэли.

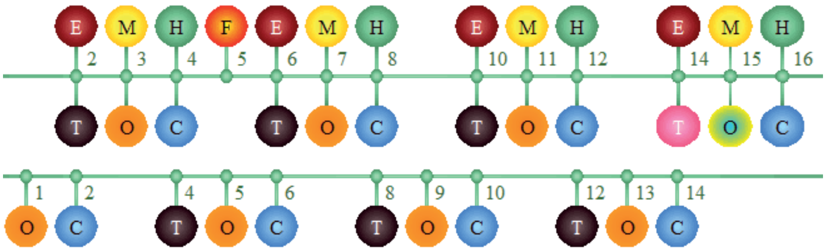
Различие между матрицами Одина и Тени с ранее описанными матрицами Мерсенна и Эйлера [12] фундаментально. Малозначимая на порядках простых чисел замена 0 на 1 на диагонали открывает возможность циклическим смещением блоков **A** и **B** бициклов Эйлера *восстанавливать ортогональность* при отсутствии поля, однозначно связанного с указанными симметриями. Таким образом, помимо матриц, сопровождающих простые числа и их степени, появляются матрицы Эйлера **E** порядков $4t - 2$ и Мерсенна **M** составных порядков $4t - 1$, которые можно найти либо переборами, либо оптимизацией детерминанта [9].

Хорошо известная из литературы невозможность в *рамках комбинаторной теории* [1, 4, 5] доказать наличие матриц Адамара (не встречая принципиальных возражений) не означает, что альтернативная применению техники полей логика поиска экстремумов [9] в чем-либо ущербна. Не менее хорошо известно, что матрицы максимума детерминанта сопровождают все порядки, независимо от их составного характера. На приведенной на рис. 2 диаграмме заметны длинные цепочки матриц **E**-**M**-**H**-(**F**) и короткие вида **T**-**O**-**C**.



■ *Рис. 1*. Взаимные переходы кососимметричных (*а*) и симметричных (*б*) дизайнов матриц **T**, **O**, **C**

■ *Fig. 1*. Mutual transitions of skew-symmetric (*а*) and symmetric (*б*) designs of matrices **T**, **O**, **C**



■ ***Рис. 2.*** Диаграмма цепочек матриц

■ ***Fig. 2.*** Diagram of matrix chains

Матрицы **H** и **C** сосуществуют на порядках $4t$. Некоторые матрицы Адамара сопровождают синхронизированные с последовательностью чисел Ферма критские матрицы **F** порядков $4t + 1$ [9, 12].

Из диаграммы следует, например, что можно находить все четыре разновидности обобщенных критских матриц **E-M** и **T-O** методом сверху (отделением каймы), а не снизу (использованием поля) для составного порядка 15, отвечающего матрицам **H** и **C** порядка 16. В таких случаях критские матрицы будут лишены не существенных для их поиска иным путем инвариантов — у них не будет гарантируемых полем взаимных циклических симметрий их блоков.

Можно показать связь проблемы существования и поиска матриц Адамара с теоремой Гаусса о гарантированном разложении простых и составных чисел на три фигурных числа, отмечаемом еще Ферма. Простое по реализации отделение каймы открывает возможность находить матрицы Одина и Тени (как и матрицы Мерсенна и Эйлера) не снизу, переборами (алгоритмы работы в поле [13, 14] тоже относятся к комбинаторным процедурам) или оптимизацией [8, 9, 15], а сверху, отделением каймы от структур, параметры которых и блочное строение мы здесь описали.

Таким образом, уязвимой является лишь цепочка нижних троиц симметричных матриц **T-O-C** (см. рис. 2), связанных с особенностями разложения чисел, соответствующих порядкам матриц **O**, на суммы двух квадратов. Матрицы могут отсутствовать по двум причинам: либо такой порядок неразложим в указанном смысле, либо он является составным числом, приводящим к мультиблочности. Если бы не последнее обстоятельство, матрицы Белевича порядков 66 и 86 и т. п. были бы давно найдены. Но они до сих пор не известны [1]. Отмеченные матрицы пополняют новыми представителями состав ортогональных матриц семейства Адамара с выделенными чертами симметрии или кососимметрии в рамках исследований, которые ведутся в настоящее время [16–18].

Симметрии матриц Адамара

Матрицы Адамара — это матрицы порядков $n = 4v$, которые традиционно делят на 4, выделяя характерный размер блоков **A**, **B**, **C**, **D** в виде $v = n/4$. Условие ортогональности дает квадратичное уравнение связи $w^2 + x^2 + y^2 + z^2 = n$, регламентирующее число -1 в них: $k_1 = (v - w)/2$, $k_2 = (v - x)/2$, $k_3 = (v - y)/2$, $k_4 = (v - z)/2$.

Для матриц порядков, идущих с шагом 8: $n = 4 + 8t = 4(2t + 1)$, размер блока $v = 2t + 1$ — нечетное число. Поэтому у кососимметричных с точностью до диагонали $\mathbf{A} - \mathbf{I} = (\mathbf{I} - \mathbf{A})^{\mathrm{T}}$ матриц **A** число $k_1 = (v - 1)/2$, т. е. $w = 1$, что сразу же дает уравнение сферы $x^2 + y^2 + z^2 = n - 1$. Для симметричного варианта решения $\mathbf{A} = \mathbf{A}^{\mathrm{T}}$ и $\mathbf{B} = \mathbf{C}$, поменяв местами обозначения w и x, связав свободную переменную x с первой матрицей, имеем $w = y$, что приводит к уравнению сфероида $x^2 + 2y^2 + z^2 = n$.

Разрешимостью в целых числах уравнений сферы и сфероида занимались Гаусс и Лиувилль, сводившие заменой $x^2 = 8T_x + 1$, $y^2 = 8T_y + 1$, $z^2 = 8T_z + 1$ уравнения к линейному виду: $T_x + T_y + T_z = t$ и $T_x + 2T_y + T_z = t$, где t, как и ранее, — натуральное число, задающее номер матрицы в отмеченной числовой последовательности. По теореме Гаусса, любое целое число разрешимо не более чем тремя треугольными числами, т. е. числами, взятыми из последовательности сумм чисел 0, 1, 3, 6, 10 и т. п. (аддитивный факториал). Лиувилль распространил это правило на второе линейное уравнение, близкое к уравнению Гаусса по смыслу.

Таким образом, симметричные и кососимметричные матрицы Адамара сосуществуют на всех порядках, идущих с шагом порядка 8. Разновидность правила Сильвестра $\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ \mathbf{H} & -\mathbf{H} \end{pmatrix}$ и $\begin{pmatrix} \mathbf{H} & \mathbf{H} \\ -\mathbf{H}^{\mathrm{T}} & \mathbf{H}^{\mathrm{T}} \end{pmatrix}$ позволяет распространить свойство симметрии и кососимметрии на удвоенные порядки. Следовательно, среди матриц Адамара нет такого порядка, на котором нельзя найти две отмеченные симметрии.

Заключение

В настоящей работе свойство симметрии изучается при делении матрицы Адамара на две каймы и соответствующие делениям каймы большие по размеру блоки. При этом оказывается, что симметричные признаки присущи и критским матрицам, которые образуются ортогонализацией основы (core) матриц Адамара при последовательном отделении первой и второй каймы. Поскольку значения элементов матрицы перестают быть целочисленными, понимание симметрии изменяется — мы отслеживаем знаки, а не плавающие при сечении матрицы значения элементов. Разумеется, симметрии матриц, если они есть, сохраняются при выделении основы сверху для любых порядков.

Этим и объясняется наличие матриц Эйлера, не обязательно бициклических, но симметричных или кососимметичных на порядках, на два меньших порядков матриц Адамара. Однако деление может быть тоньше, когда мы обращаем внимание на двоякосимметричные матрицы Одина и Тени, являющиеся основами, в том числе, и конференц-матриц. В этом случае характерные бициклы сопровождают не все порядки, а только равные простым числам и их степеням. Ранее такие критские матрицы не выделялись, и их уровни и симметрии не описывались. Это дает право говорить о новом семействе матриц, позволяющих понять глубже симметрии матриц Адамара и конференц-матриц, основой которых они являются.

Благодарности

Мы выражаем благодарность за многолетнюю помощь и поддержку профессорам Дженнифер Себерри и Драгомиру Джоковичу. За помощь в технической работе с рукописью благодарим Т. В. Балонину.

Финансовая поддержка

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

Литература

1. **Colbourn C. J., Dinitz J. H.** *Handbook of Combinatorial Designs*. Second Ed. Chapman and Hall/CRC, 2007. 967 p.
2. **Silvester J. J.** Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Philosophical Magazine*, 1867, no. 34, pp. 461–475.
3. **Hadamard J.** Résolution d'une question relative aux déterminants. *Bulletin des sciences mathématiques*, 1893, vol. 17, pp. 240–246.
4. **Jennifer S., Yamada M.** *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Wiley, 2020. 384 p.
5. **Craigen R.** Hadamard Matrices and Designs. In: *CRC Handbook of Combinatorial Designs*. C. J. Colbourn and J. H. Dinitz eds. CRC Press, 1996. Pp. 229–516.
6. **Kharaghani H., Tayfeh-Rezaie B. A.** Hadamard matrix of order 428. *Journal of Combinatorial Designs*, 2005, vol. 13, pp. 435–440.
7. **Balonin N. A., and Seberry J.** Remarks on extremal and maximum determinant matrices with real entries ≤ 1. *Информационно-управляющие системы*, 2014, № 5, с. 2–4.
8. **Mohan M. T.** *p*-almost Hadamard matrices and λ-planes. *Journal of Algebraic Combinatorics*, 2020, 20 p. ttps://doi.org/10.1007/s10801-020-00991-y
9. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта. *Информационно-управляющие системы*, 2014, № 1, с. 2–15.
10. **Mohan M. T.** On some *p*-almost Hadamard matrices. *Operators and Matrices*, 2019, vol. 13, no. 1, pp. 253–281. doi:10.7153/oam-2019-13-17
11. Balonin N. A., Đoković D. Ž. Conference matrices from Legendre C-pairs. *Информационно-управляющие системы*, 2020, № 4, с. 2–10. doi:10.31799/1684-8853-2020-4-2-10
12. **Балонин Н. А., Сергеев М. Б.** Как гипотезе Адамара помочь стать теоремой. Ч. 1. *Информационно-управляющие системы*, 2018, № 6, с. 2–13.
13. **Paley R. E. A. C.** On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
14. **Балонин Н. А., Сергеев А. М., Синицына О. А.** Алгоритмы конечных полей и групп поиска ортогональных последовательностей. *Информационно-управляющие системы*, 2021, № 4, с. 2–16.
15. **Wen Z., Yin W.** A feasible method for optimization with orthogonality constraints. *Mathematical Programming*, Ser. A, 2013, vol. 142, pp. 397–434. https://doi.org/10.1007/s10107-012-0584-1
16. **Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B.** Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, vol. 46, iss. 3, pp. 343–352.
17. **Awyzio G., Seberry J.** *On Good Matrices and Skew Hadamard Matrices*. 2015. 15 p. https://www.researchgate.net/publication/285233232_On_Good_Matrices_and_Skew_Hadamard_Matrices (дата обращения: 12.11.2021).
18. **Acevedo S., Dietrich H.** New infinite families of Williamson Hadamard matrices. *Australian Journal of Combinatorics*, 2019, vol. 73, iss. 1, pp. 207–219.

UDC 519.614
doi:10.31799/1684-8853-2022-1-2-7

Odin and Shadow Cretan matrices accompanying primes and their powers

N. A. Balonin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7338-4920, korbendfs@mail.ru
M. B. Sergeev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Cretan matrices — orthogonal matrices, consisting of the elements 1 and $-b$ (real number), are an ideal object for the visual application of finite-dimensional mathematics. These matrices include, in particular, the Hadamard matrices and, with the expansion of the number of elements, the conference matrices. The most convenient research apparatus is to use field theory and multiplicative Galois groups, which is especially important for new types of Cretan matrices. **Purpose:** To study the symmetries of the Cretan matrices and to investigate two new types of matrices of odd and even orders, distinguished by symmetries, respectively, which differ significantly from the previously known Mersenne, Euler and Fermat matrices. **Results:** Formulas for levels are given and symmetries of new Cretan matrices: Odin bicycles (with a border) of orders $4t - 1$ and $4t - 3$ and shadow matrices of orders $4t - 2$ and $4t - 4$ are described. For odd character sizes equal to prime numbers and powers of primes, the existence of matrix symmetries of special types, doubly symmetric, consisting of skew-symmetric (with respect to the signs of elements) and symmetric cyclic blocks, is proved. It is shown that the previously distinguished Cretan matrices are their special case: Mersenne matrices of orders $4t - 1$ and Euler matrices of orders $4t - 2$ existing in the absence of symmetry for all selected orders without exception. **Practical relevance:** Orthogonal sequences and methods of their effective finding by the theory of finite fields and groups are of direct practical importance for the problems of noise-immune coding, compression and masking of video information.
Keywords — Hadamard matrices, Belevich matrices, Cretan matrices, finite fields, matrix symmetries.

For citation: Balonin N. A., Sergeev M. B. Odin and Shadow Cretan matrices accompanying primes and their powers. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 1, pp. 2–7 (In Russian). doi:10.31799/1684-8853-2022-1-2-7

Financial support

The article was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, agreement No. FSRF-2020-0004.

References

1. Colbourn C. J., Dinitz J. H. *Handbook of Combinatorial Designs*. Second Ed. Chapman and Hall/CRC, 2007. 967 p.
2. Silvester J. J. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *Philosophical Magazine*, 1867, no. 34, pp. 461–475.
3. Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des sciences mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
4. Jennifer S., Yamada M. *Hadamard Matrices: Constructions using number theory and linear algebra*. Wiley, 2020. 384 p.
5. Craigen R. *Hadamard matrices and designs*. In: *CRC Handbook of Combinatorial Designs*. C. J. Colbourn and J. H. Dinitz eds. CRC Press, 1996. Pp. 229–516.
6. Kharaghani H., Tayfeh-Rezaie B. A. Hadamard matrix of order 428. *Journal of Combinatorial Designs*, 2005, vol. 13, pp. 435–440.
7. Balonin N. A., and Seberry J. Remarks on extremal and maximum determinant matrices with real entries ≤ 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5, pp. 2–4.
8. Mohan M. T. *p*-almost Hadamard matrices and λ-planes. *Journal of Algebraic Combinatorics*, 2020. 20 p. ttps://doi.org/10.1007/s10801-020-00991-y
9. Balonin N. A., Sergeev M. B. Local maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 1, pp. 2–15 (In Russian).
10. Mohan M. T. On some *p*-almost Hadamard matrices. *Operators and Matrices*, 2019, vol. 13, no. 1, pp. 253–281. doi:10.7153/oam-2019-13-17
11. Balonin N. A., Đoković D. Ž. Conference matrices from Legendre C-pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 4, pp. 2–10. doi:10.31799/1684-8853-2020-4-2-10
12. Balonin N. A., Sergeev M. B. Helping Hadamard conjecture to become a theorem. Part 1. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 6, pp. 2–13 (In Russian). doi:10.31799/1684-8853-2018-6-2-13
13. Paley R. E. A. C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, no. 12, pp. 311–320.
14. 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. 2–16 (In Russian). doi:10.31799/1684-8853-2021-4-2-17
15. Wen Z., Yin W. A feasible method for optimization with orthogonality constraints. *Mathematical Programming*, Ser. A, 2013, vol. 142, pp. 397–434. https://doi.org/10.1007/s10107-012-0584-1
16. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 2008, vol. 46, iss. 3, pp. 343–352.
17. Awyzio G., Seberry J. *On Good Matrices and Skew Hadamard Matrices*. 2015. 15 p. Available at: https://www.researchgate.net/publication/285233232_On_Good_Matrices_and_Skew_Hadamard_Matrices (accessed 12 November 2021).
18. Acevedo S., Dietrich H. New infinite families of Williamson Hadamard matrices. *Australian Journal of Combinatorics*, 2019, vol. 73, iss. 1, pp. 207–219.