УДК 519.614
doi:10.31799/1684-8853-2025-1-2-8
EDN: JYHOIX

Научные статьи
Articles

Метод вычисления двухуровневых циклических квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов

Е. К. Григорьев[a], *старший преподаватель, orcid.org/0000-0001-5981-4074*
А. М. Сергеев[a], *канд. техн. наук, доцент, orcid.org/0000-0002-4788-9869, aleks.asklab@gmail.com*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *структурированные ортогональные и квазиортогональные матрицы с двумя значениями элементов как математические объекты получили широкое распространение в решении технических задач обработки и передачи информации. При этом поиск и вычисление квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов, являются трудоемкими задачами, которые требуют особого подхода.* ***Цель:*** *разработать метод вычисления циклических квазиортогональных матриц, существующих на порядках произведений простых чисел-близнецов.* ***Результаты:*** *анализ известных методов поиска и вычисления квазиортогональных матриц циклической структуры с двумя значениями элементов {1, –b}, существующих на порядках произведений простых чисел-близнецов, выявил их ограничения либо при вычислении элемента b, либо при поиске первой строки матрицы. Предложен метод вычисления матриц, основанный на аналитических зависимостях значения элемента b от порядка матрицы, что в сравнении с известными методами заметно снижает время расчета и открывает возможности эффективного вычисления матриц высоких порядков. Полученные при помощи предлагаемого метода матрицы при сохранении циклической структуры отличны от найденных ранее матриц целочисленным значением весовой функции, а также значениями элемента b, что открывает возможность дальнейших исследований по поиску подобных матриц на уже известных порядках существования матриц Мерсенна.* ***Практическая значимость:*** *полученные при помощи предлагаемого метода матрицы, являясь ядром матриц Адамара, позволяют пополнить базу матриц с двумя значениями элементов для задач обработки информации и получения кодовых последовательностей с хорошими корреляционными свойствами.*

Ключевые слова *— ортогональные преобразования, матрицы Адамара, матрицы Мерсенна, симметрии матриц, циклические матрицы, простые числа-близнецы.*

Для цитирования: Григорьев Е. К., Сергеев А. М. Метод вычисления двухуровневых циклических квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов. *Информационно-управляющие системы*, 2025, № 1, с. 2–8. doi:10.31799/1684-8853-2025-1-2-8, EDN: JYHOIX
For citation: Grigoriev E. K., Sergeev A. M. Method for calculating two-level cyclic quasi-orthogonal matrices on orders equal to the product of twin primes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 1, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2025-1-2-8, EDN: JYHOIX

Введение

Ортогональные (квазиортогональные) матрицы как математические объекты получили широкое распространение при решении технических задач обработки и передачи информации [1–12], среди которых задачи помехоустойчивого кодирования [2–4], обеспечения конфиденциальности данных в незащищенных коммуникациях [3, 4], синтеза кодовых последовательностей [5–9] и др.

Наибольший интерес для практического применения представляют матрицы симметричной или циклической структуры с двумя значениями элементов (уровнями), позволяющие оптимизировать объем памяти, используемый для генерации и хранения, а также структурировать вычисления с ними [13–15].

Это матрицы Адамара $\mathbf{H}_n$ [1] и Мерсенна $\mathbf{M}_n$ [16] с двумя значениями уровней {1, –1} и {1, –b} соответственно, для которых справедливы следующие квадратичные условия связи:

$$\mathbf{H}_n\mathbf{H}_n^{\mathrm{T}} = n\mathbf{I}; \quad (1)$$

$$\mathbf{M}_n\mathbf{M}_n^{\mathrm{T}} = \omega(n)\mathbf{I}, \quad (2)$$

где n — порядок матрицы, а $\omega(n)$ — ее вес [16].

Сегодня матрицы Адамара и Мерсенна являются не просто объектом теоретических исследований, как существующие на соседних порядках $n = 4t$ и $n = 4t - 1$ соответственно, где t — натуральное число, но и основой пополнения библиотеки матриц, способствующей расширению круга и размера задач с ортогональными преобразованиями.

Взаимосвязи матриц Мерсенна и Адамара позволяют легко получать различные конструкции последних, например симметричную [16, 17] или в форме циклического «ядра» с окаймлением [18].

Для иллюстрации указанных взаимосвязей будет удобно воспользоваться графическим представлением матриц в виде так называемых «портретов». Установим, что на всех рисунках в рамках настоящей статьи, где будут представлены портреты, черным квадратам будут соответствовать уровни матрицы –1 или $-b$, а белым квадратам — уровень 1.

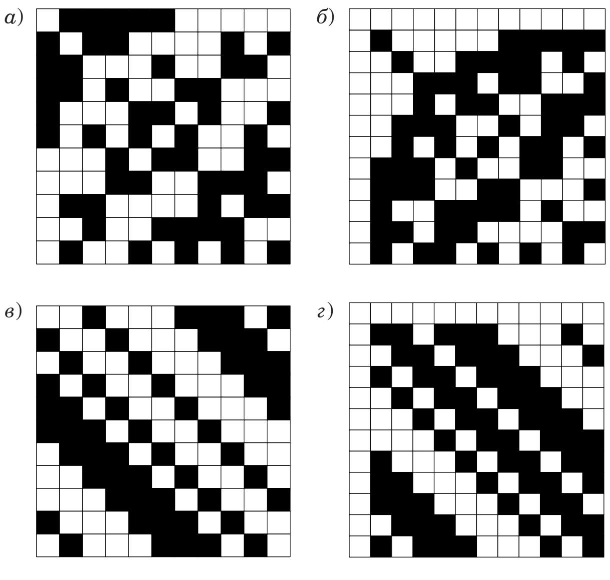
В качестве примера рассмотрим рис. 1, на котором изображены две матрицы Мерсенна одиннадцатого порядка симметричной (рис. 1, *а*) и циклической (рис. 1, *в*) структуры. Связанные с ними нормализованные матрицы Адамара двенадцатого порядка (рис. 1, *б* и *г* соответственно) получаются путем округления уровня $-b$ до –1, инверсией элементов матрицы и добавлением «каймы» в виде первой строки и первого столбца, состоящей из единиц.

Выполнение данной цепочки действий в обратном порядке позволяет получить исходные матрицы Мерсенна [16].

Таким образом, нахождение новых матриц, существующих на соседних порядках, открывает возможность расширить набор матриц для использования в ортогональных преобразованиях [19].

Для поиска квазиортогональных матриц в настоящее время применяются различные методы, например модифицированные методы Сильвестра, Пэли или Скарпи, методы, использующие вычисления в полях Галуа, метод Секереша или классические комбинаторные методы [16].

Однако обособленно стоит случай, при котором порядок матрицы равен произведению простых чисел-близнецов $n = p(p + 2)$, поскольку итерационный алгоритм в данном случае неприменим, а поля Галуа такого размера нет [16]. Целью настоящей работы является разработка метода вычисления циклических квазиортогональных матриц, существующих на порядках произведений простых чисел-близнецов.



■ ***Рис. 1.*** Иллюстрация взаимосвязей между матрицами на соседних порядках: *а* — портрет матрицы $\mathbf{M}_{11}$ симметричной конструкции; *б* — портрет матрицы $\mathbf{H}_{12}$ симметричной конструкции; *в* — портрет матрицы $\mathbf{M}_{11}$ циклической конструкции; *г* — портрет матрицы $\mathbf{H}_{12}$ конструкции «ядро» с окаймлением

■ ***Fig. 1.*** Illustration of relationships between matrices on neighboring orders: *а* — portrait of symmetric matrix $\mathbf{M}_{11}$; *б* — portrait of symmetric matrix $\mathbf{H}_{12}$; *в* — portrait of circulant matrix $\mathbf{M}_{11}$; *г* — portrait of "core" with border design matrix $\mathbf{H}_{12}$

Методы вычисления квазиортогональных матриц

Известен метод вычисления матриц Мерсенна на основе использования динамических систем, описанный в работе [16, с. 179]. Авторами отмечается: «Можно вычислить p значений $x^k \bmod(n)$ и $q - p$ значений $y^k \bmod(n)$ с основаниями $x = y \bmod(p)$, $x = 0 \bmod(p + 2)$, где y — примитивный элемент групп $\mathrm{GF}(p)$ и $\mathrm{GF}(p + 2)$, $q = (n - 1)/2$. Примитивный элемент — это любой элемент, показательная функция от которого обходит всю группу…» Элемент b в данном случае вычисляется как $t/\left(t+\sqrt{t}\right)$.

В более поздней работе [18] предложен альтернативный метод, при котором генерация первой строки циклической квазиортогональной матрицы с элементами $\{1, -b\}$ осуществляется на основе последовательностей Якоби — одного из известных циклических разностных множеств Адамара.

Генерация происходит в соответствии со следующим правилом:

$$z_N = \begin{cases} 1, \text{ если } N = 0 \pmod{pq} \\ 1, \text{ если } N = 0 \pmod{q},\ N \neq 0 \pmod{p} \\ -1, \text{ если } N = 0 \pmod{p},\ N \neq 0 \pmod{q} \\ \left(\dfrac{n}{pq}\right), \text{ если } N \neq 0 \pmod{q},\ N \neq 0 \pmod{p} \end{cases}, \quad (3)$$

где z_N — элемент первой строки; $q = (p + 2)$; $\left(\dfrac{N}{p}\right)$ и $\left(\dfrac{N}{q}\right)$ — символы Лежандра, а $\left(\dfrac{N}{pq}\right) = \left(\dfrac{N}{p}\right)\left(\dfrac{N}{q}\right)$ — символ Якоби [18].

Пример. Рассмотрим данный метод на примере вычисления матрицы порядка 15 для $p = 3$ и $q = 5$. После проведения несложных вычислений для каждого элемента получим, что квадратичными вычетами являются следующие элементы:

$$\left(\frac{0}{15}\right)=\left(\frac{1}{15}\right)=\left(\frac{2}{15}\right)=\left(\frac{4}{15}\right)==\left(\frac{5}{15}\right)=\left(\frac{8}{15}\right)=\left(\frac{10}{15}\right)=1,$$

а квадратичными невычетами —

$$\left(\frac{3}{15}\right)=\left(\frac{6}{15}\right)=\left(\frac{7}{15}\right)=\left(\frac{9}{15}\right)=\left(\frac{11}{15}\right)=$$
$$=\left(\frac{12}{15}\right)=\left(\frac{13}{15}\right)=\left(\frac{14}{15}\right)=-1.$$

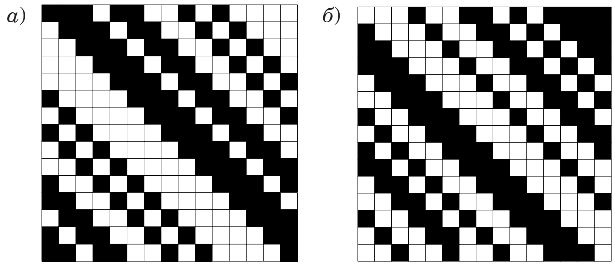
Соответственно, последовательность Якоби будет записана как $z = \{1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1\}$.

Вычисление элемента b квазиортогональной матрицы для замены элементов со значением –1 в полученной последовательности происходит в соответствии с алгоритмом [18], структурная схема которого представлена на рис. 2.

В качестве примера на рис. 3 приведены портреты вычисленных с использованием методов из работ [16] и [18] циклических квазиортогональных матриц порядка 15.

Декомпозиция двух представленных методов показывает, что процесс получения квазиортогональных матриц можно разделить на два этапа: на первом этапе задается структура циклической матрицы путем генерации первой строки, а на втором вычисляется значение элемента b.

Таким образом, первый из рассмотренных методов вычисления матриц [16] имеет сложный этап генерации первой строки, что компенсируется простотой вычисления элемента b. Во втором методе [18], наоборот, при простоте методики генерации первой строки значительно возрастает сложность вычисления элемента b в символьном виде. Таким образом, можно сказать, что при невозможности модифицировать процесс генерации первой строки для достижения поставленной цели целесообразно проанализировать способы ускорения вычисления элемента b.

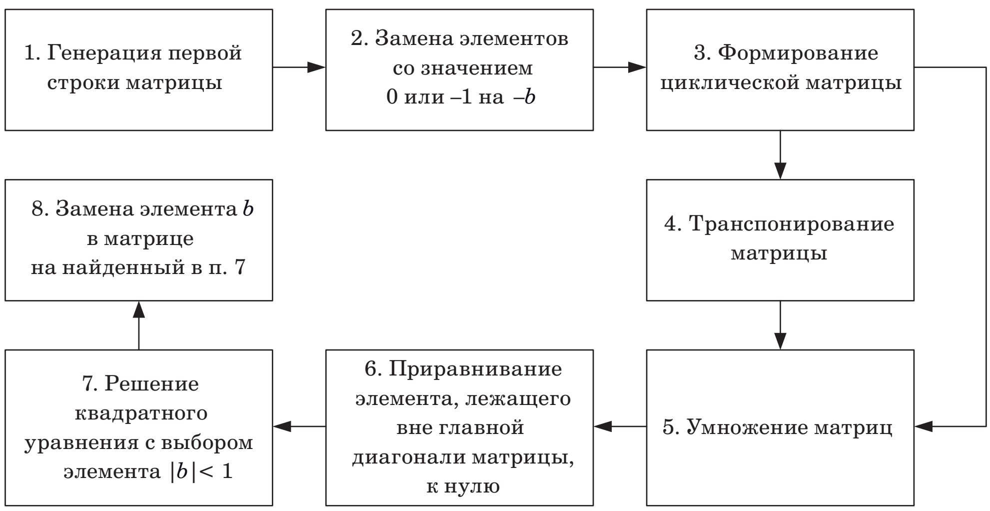


■ ***Рис. 3.*** Портреты циклических квазиортогональных матриц порядка 15, вычисленных на основе метода из работы [16] (*а*) и [18] (*б*)

■ ***Fig. 3.*** Portraits of cyclic quasi-orthogonal matrices of order 15, calculated based on the method from [16] (*а*) and [18] (*б*)

Метод вычисления квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов

В работе [18] анализировались корреляционные свойства модифицированных кодовых последовательностей, основанных на строках циклических квазиортогональных матриц. Следует отметить, что именно длинные кодовые последовательности обеспечивают повышение помехоустойчивости и улучшение энергетических характеристик при их использовании, например, в системах радиолокации и связи [20, 21]. Таким образом, необходимо вычислять ма-



■ ***Рис. 2.*** Структурная схема метода вычисления элемента b

■ ***Fig. 2.*** Structural diagram of the way for calculating element b

трицы высоких порядков, обязательность вычислений в символьном виде значительно замедляет этот процесс.

Например, для пары $p = 29$ и $q = 31$ вычисление элемента b на ПК с Intel Core I7-10510U и 16 ГБ оперативной памяти заняло более часа.

Напомним, что уравнение связи для квазиортогональных матриц Мерсенна записывается как (2) и вес $\omega(n)$ является функцией от порядка матрицы. Ниже приводится впервые выявленная взаимосвязь, позволяющая существенно ускорить получение матриц. Она состоит в том, что значение веса для нескольких первых порядков, найденных при помощи метода вычисления матриц из [18], равно квадрату меньшего простого числа-близнеца:

$$p = 3,\ q = 5 : \mathbf{M}_n\mathbf{M}_n^{\mathrm{T}} = 9\mathbf{I};$$
$$p = 5,\ q = 7 : \mathbf{M}_n\mathbf{M}_n^{\mathrm{T}} = 25\mathbf{I};$$
$$p = 11,\ q = 13 : \mathbf{M}_n\mathbf{M}_n^{\mathrm{T}} = 121\mathbf{I}.$$

Таким образом, можно предположить, что для указанных циклических квазиортогональных матриц вес $\omega(n) = p^2$. Тогда, используя данный вес, можно вывести аналитическое выражение для элемента b через порядок и значение положительного элемента a, не всегда равного 1, а именно:

$$p^2 = \frac{(n-1)a^2 + (n+1)b^2}{2},$$

где в числителе учтен тот факт, что количество отрицательных элементов на единицу больше числа положительных элементов в строке матрицы [16].

Обозначив порядок ближайшей матрицы Адамара как $h = n + 1$, получим аналитическое выражение для расчета элемента b:

$$p^2 = \frac{(n+1-1-1)a^2 + (n+1)b^2}{2};$$
$$p^2 = \frac{(h-2)a^2 + hb^2}{2};$$
$$b = \sqrt{\frac{2p^2 - (h-2)a^2}{h}}. \qquad (4)$$

Для демонстрации возможности вычисления элемента b по выражению (4) сравним предлагаемый метод решения с изложенным в работе [18] (см. рис. 2).

Значения вычисленных и округленных до четвертого знака после запятой элементов b при $a = 1$ для различных порядков, а также затраченное время τ представлены в табл. 1.

Таким образом, предлагаемый метод вычисления двухуровневых квазиортогональных матриц, существующих на порядках простых чисел-близнецов, предполагает генерацию первой строки матрицы по правилу (3) с последующей заменой элементов со значением –1 на значение $-b$, где b вычисляется по выражению (4).

Сама матрица формируется циклическим сдвигом вправо первой строки. Отметим, что процесс формирования первой строки можно заменить на операцию чтения из памяти, поскольку первые строки матриц представляют собой известные кодовые последовательности Якоби.

Следует отметить, что предлагаемый метод вычисления не ограничивается порядком 3599. Авторами последовательно были вычислены матрицы до пары $p = 179$, $q = 181$ включительно, что соответствует порядку 32 399, однако предлагаемый метод позволяет вычислить матрицы на всех остальных порядках, равных произведению простых чисел-близнецов. Последнее утверждение обосновывается детерминированностью процедур нахождения первой строки матрицы и вычисления элемента b.

Сравнив получаемые при помощи двух разных методов матрицы порядка 15, представленные на рис. 3, можно заметить, что их структуры схожи. Однако у матриц, формируемых методом из работы [16], количество отрицательных элементов на единицу меньше количества положительных элементов. У матриц, вычисляемых предлагаемым методом, отрицательных элементов на единицу больше числа положительных элементов. Сравнение матриц приведено в табл. 2.

Сравнение параметров матриц из табл. 2 показывает, что, хотя матрицы, формируемые предлагаемым методом, не достигают локального максимума детерминанта, они также являются

■ ***Таблица 1.*** Сравнение скорости вычисления матриц
■ ***Table 1.*** Comparison of matrix calculation speed

Простые числа-близнецы	Порядок матрицы	Параметр	Подход из [18]	Предлагаемый метод
$p = 17$, $q = 19$	323	b	0,8889	0,8889
		τ, с	256,56	0,02
$p = 29$, $q = 31$	899	b	0,9333	0,9333
		τ, с	4535,77	0,02
$p = 41$, $q = 43$	1763	b	0,9524	0,9524
		τ, с	25 140,86	0,02
$p = 59$, $q = 61$	3599	b	0,9667	0,9667
		τ, с	219 600,57	0,06

■ ***Таблица 2.*** Сравнение вычисленных квазиортогональных матриц
■ ***Table 2.*** Comparison of computed quasi-orthogonal matrices

Предмет сравнения	Подход из [16]	Предлагаемый метод
Структура матрицы	Циклическая	Циклическая
Выражение для расчета b	$b = t\Big/\left(t+\sqrt{t}\right)$	$b=\sqrt{\dfrac{2p^2-(h-2)a^2}{h}}$
Весовая функция $\omega(n)$	$\dfrac{(n+1)a^2+(n-1)b^2}{2}$	p^2
Ядро матрицы Адамара	Да	Да
Локальный максимум детерминанта	+	–

ядром матриц Адамара и у них значение весовой функции $\omega(n) = p^2$ или $\omega(n) = n - 2p$ также целочисленное, как и у матриц Адамара с $\omega(n) = n$.

Заключение

Поиск квазиортогональных матриц на порядках, равных произведению простых чисел-близнецов, не может быть осуществлен распространенными методами и требует особого подхода. Проведенный анализ известных методов вычисления подобных матриц показал ограниченную применимость метода с использованием динамических систем.

Предложенный в работе метод по сравнению с прототипом имеет лучшие показатели не только по времени, но и по возможности вычисления матриц высоких порядков. Дополнительно открывается возможность находить матрицы не только с элементами $\{1, -b\}$, но и с элементами $\{a, -b\}$, что позволит значительно пополнить базу двухуровневых матриц для задач обработки информации и получения кодовых последовательностей.

Значимым результатом является то, что получаемые при помощи предлагаемого метода матрицы при сохранении циклической структуры отличаются от известных матриц Мерсенна целочисленным значением весовой функции и значением элемента b. Этот результат открывает возможность дальнейших исследований результатов поиска подобных матриц на уже известных порядках Мерсенна.

Благодарность

Авторы выражают благодарность профессорам М. Б. Сергееву и Н. А. Балонину за конструктивные замечания и помощь в подготовке статьи.

Финансовая поддержка

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003 «Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга».

Литература

1. **Dziech A.** New orthogonal transforms for signal and image processing. *Applied Sciences*, 2021, no. 11(16), pp. 7433. doi:10.3390/app11167433
2. **Хвощ С. Т.** Матрицы Адамара в космической связи. *Инженерный вестник Дона*, 2024, № 1, с. 210–222. http://www.ivdon.ru/uploads/article/pdf/IVD_24__1y24_Chvosh.pdf_a054a7270c.pdf (дата обращения: 20.10.2024).
3. **Sergeev A. M., Vostrikov A. A.** Calculating symmetrical Hadamard matrices of Balonin — Seberry construction for coding and masking. *Procedia Computer Science*, 2020, vol. 176, pp. 1722–1728. doi:10.1016/j.procs.2020.09.197
4. **Sergeev M. B., Blaunstein N. S.** *Matrix Approach to Solution of the Inverse Problems for Multimedia Wireless Communication Links*. Computer Vision in Advanced Control Systems-5. Intelligent Systems Reference Library. Springer, 2020, pp. 99–118. doi:10.1007/978-3-030-33795-7_4
5. **Сергеев М. Б., Ненашев В. А., Сергеев А. М.** Вложенные кодовые конструкции Баркера — Мерсенна — Рагхаварао. *Информационно-управляющие*

системы, 2019, № 3, с. 71–81. doi:10.31799/1684-8853-2019-3-71-81
6. **Леухин А. Н.** Построение циклических разностных множества Адамара. *Математические методы распознавания образов*, 2009, т. 14, № 1, с. 395–398.
7. **Manjhi P. K.** Some results on the parameters of the general difference sets correspond to circulant partial Hadamard matrices. *Research in Mathematics*, 2022, no. 9(1). doi:10.1080/27684830.2022.2152961
8. **Dimitrov M., Baitcheva T., Nikolov N.** Efficient generation of low autocorrelation binary sequences. *IEEE Signal Processing Letters*, 2020, vol. 27, pp. 341–345. doi:10.1109/LSP.2020.2972127
9. **Shi M., Li Y., Cheng W., Crnkovis D., Krotov D., Sole P.** Self-dual Hadamard bent sequences. *Journal of Systems Science and Complexity*, 2023, vol. 36, pp. 894–908. doi:10.1007/s11424-023-2276-8
10. **Ягнятинский Д. А., Федосеев В. Н.** Алгоритм последовательной коррекции аберраций волнового фронта по критерию минимизации размера фокального пятна. *Оптический журнал*, 2019, т. 86, № 1, с. 32–39. doi:10.17586/1023-5086-2019-86-01-32-39
11. **Балонин Н. А., Сергеев М. Б., Суздаль В. С.** Матричные модели обобщенной кристаллографии. *Информационно-управляющие системы*, 2016, № 4, с. 26–33. doi:10.15217/issn1684-8853.2016.4.26
12. **Zhang H., Du K., Zhao C., Tang J., Si S., Jia W., Xue L., Li Z.** Optimizing the ordering of the Hadamard masks of ghost imaging suitable for the efficient face reconstruction using the max-projection method. *Scientific Reports*, 2023, vol. 13(22702). doi:10.1038/s41598-023-48453-2
13. **Антонов А. П., Беседин Д. С., Филиппов А. С.** Исследование и сравнительный анализ эффективности программной и аппаратных реализаций операции суммирования транспонированных матриц. *Информатика, телекоммуникации и управление*, 2022, т. 15, № 4, с. 51–63. doi:10.18721/JCSTCS.15404. https://infocom.spbstu.ru/article/2022.75.4/ (дата обращения: 20.10.2024).
14. **Тарасов И. Е., Советов П. Н., Люлява Д. В., Мирзоян Д. И.** Методика проектирования специализированных вычислительных систем на основе совместной оптимизации аппаратного и программного обеспечения. *Russian Technological Journal*, 2024, т. 12, № 3, с. 37–45. doi:10.32362/2500-316X-2024-12-3-37-45, EDN: PXKDKR
15. **Bernasconi A., Berti A., Corso G. M. d., Poggiali A.** Quantum subroutine for efficient matrix multiplication. *IEEE Access*, 2024, vol. 12, pp. 116274–116284. doi:10.1109/ACCESS.2024.3446176
16. **Балонин Н. А., Сергеев М. Б.** *Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские*: монография. СПб., Политехника, 2019. 196 с. doi:10.25960/7325-1155-0
17. **Сергеев А. М.** Обобщенные матрицы Мерсенна и гипотеза Балонина. *Автоматика и вычислительная техника*, 2014, № 4, с. 35–43.
18. **Григорьев Е. К., Ненашев В. А., Сергеев А. М., Самохина Е. В.** Поиск и модификация кодовых последовательностей на основе персимметричных квазиортогональных циркулянтов. *Телекоммуникации*, 2020, № 10, с. 27–33. EDN: EGQMAS
19. **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
20. **Опалихина О. В.** Формирование М-последовательности над полем вычетов Галуа. *Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии*, 2023, № 2, с. 77–90. doi:10.17308/sait/1995-5499/2023/2/77-90, EDN: ZWXTCG
21. **Кукунин Д. С., Березкин А. А., Киричек Р. В.** Многослойные ортогональные структуры на основе последовательностей максимальной длины. *Инфокоммуникационные технологии*, 2022, т. 20, № 2, с. 42–50. doi:10.18469/ikt.2022.20.2.05

UDC 519.614
doi:10.31799/1684-8853-2025-1-2-8
EDN: JYHOIX

Method for calculating two-level cyclic quasi-orthogonal matrices on orders equal to the product of twin primes

E. K. Grigoriev[a], Senoir Lecturer, orcid.org/0000-0001-5981-4074
A. M. Sergeev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-4788-9869, aleks.asklab@gmail.com
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Structured orthogonal and quasi-orthogonal matrices with a small number of levels have become widely used as mathematical objects in solving technical problems of information processing and transmitting. At the same time, the search and calculation of quasi-orthogonal matrices at orders equal to the product of twin primes are a labor-intensive task that cannot be carried out by common methods and requires a special approach. **Purpose:** To develop a method for calculating cyclic quasi-orthogonal matrices that exist on orders of products of twin prime numbers. **Results:** We carry out the analysis of the known methods for the search and calculation of quasi-orthogonal matrices of cyclic structure with two values of levels $\{1, -b\}$, existing on orders equal to the product of twin primes. We reveal their limitations with this analysis. We propose a method for calculating matrices based on analytical dependencies of the value of the element b on the order of the matrix, which, in comparison with the known methods, significantly reduces the calculation time and makes it possible to efficiently calculate high-order matrices. Matrices obtained with the use of the proposed method, while preserving the cyclic structure, differ from the previously found matrices by the integer value of the weight function, as well as by the values of the element *b*, which opens up the possibility of further research on searching for similar matrices on already known orders of existence of Mersenne matrices. **Practical relevance:** The matrices obtained with the use of the proposed method, being the core of the Hadamard matrices, make it possible to replenish the base of two-level matrices for the tasks of data processing and for obtaining code sequences with good correlation properties.

Keywords — orthogonal transformation, Hadamard matrices, Mersenne matrices, matrix symmetries, cyclic matrices, twin primes.

For citation: Grigoriev E. K., Sergeev A. M. Method for calculating two-level cyclic quasi-orthogonal matrices on orders equal to the product of twin primes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 1, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2025-1-2-8, EDN: JYHOIX

Financial support

The work was carried out with financial support from the Ministry of Science and Higher Education of the Russian Federation, agreement No. FSRF-2023-0003 “Fundamentals of structures of noise-protected spacecraft systems communication and satellite communications, relative navigation gation, technical vision and aerospace monitoring”.

References

1. Dziech A. New orthogonal transforms for signal and image processing. *Applied Sciences*, 2021, no. 11(16), pp. 7433. doi:10.3390/app11167433
2. Hvoshch S. T. Hadamard matrices in cosmic communication. *Engineering Journal of Don*, 2024, no. 1, pp. 210–222. Available at: http://www.ivdon.ru/uploads/article/pdf/IVD_24__1y24_Chvosh.pdf_a054a7270c.pdf (accessed 20 October 2024) (In Russian).
3. Sergeev A. M., Vostrikov A. A. Calculating symmetrical Hadamard matrices of Balonin — Seberry construction for coding and masking. *Procedia Computer Science*, 2020, vol. 176, pp. 1722–1728. doi:10.1016/j.procs.2020.09.197
4. Sergeev M. B., Blaunstein N. S. *Matrix Approach to Solution of the Inverse Problems for Multimedia Wireless Communication Links*. In. *Computer Vision in Advanced Control Systems-5*. Intelligent Systems Reference Library. Springer, 2020, pp. 99–118. doi:10.1007/978-3-030-33795-7_4
5. Sergeev M. B., Nenashev V. A., Sergeev A. M. Nested code sequences of Barker — Mersenne — Raghavarao. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2019, no. 3, pp. 71–81 (In Russian). doi:10.31799/1684-8853-2019-3-71-81
6. Leuhin A. N. Construction of cyclic difference Hadamard sets. *Matematicheskie metody` raspoznavaniya obrazov* [Mathematical methods of pattern recognition], 2009, vol. 14 no. 1, pp. 395–398 (In Russian).
7. Manjhi P. K. Some results on the parameters of the general difference sets correspond to circulant partial Hadamard matrices. *Research in Mathematics*, 2022, no. 9(1). doi:10.1080/27684830.2022.2152961
8. Dimitrov M., Baitcheva T., Nikolov N. Efficient generation of low autocorrelation binary sequences. *IEEE Signal Processing Letters*, 2020, vol. 27, pp. 341–345. doi:10.1109/LSP.2020.2972127
9. Shi M., Li Y., Cheng W., Crnkovis D., Krotov D., Sole P. Self-dual Hadamard bent sequences. *Journal of Systems Science and Complexity*, 2023, vol. 36, pp. 894–908. doi:10.1007/s11424-023-2276-8
10. Yagnyatinskiy D. A., Fedoseyev V. N. Algorithm for sequential correction of wavefront aberrations with the criterion of focal spot size minimization. *Journal of Optical Technology*, 2019, vol. 86 no. 1, Article 25. doi:10.1364/jot.86.000025
11. Balonin N. A., Sergeev M. B., Suzdal V. S. Matrix models of generalized crystallography. *Information and Control Systems* [Information and Control Systems], 2016, no. 4, pp. 26–33 (In Russian). doi:10.15217/issn1684-8853.2016.4.26
12. Zhang H., Du K., Zhao C., Tang J., Si S., Jia W., Xue L., Li Z. Optimizing the ordering of the Hadamard masks of ghost imaging suitable for the efficient face reconstruction using the max-projection method. *Scientific Reports*, 2023, vol. 13(22702). doi:10.1038/s41598-023-48453-2
13. Antonov A. P., Besedin D. S., Filippov A. S. Research and comparative analysis of the effectiveness of software and hardware implementations of the operation of summing transposed matrices. *Computing, Telecommunications and Control*, 2022, vol. 15, no. 4, pp. 51–63 (In Russian). doi:10.18721/JCSTCS.15404. Available at: https://infocom.spbstu.ru/article/2022.75.4/ (accessed 20 October 2024).
14. Tarasov I. E., Sovietov P. N., Lulyava D. V., Mirzoyan D. I. Method for designing specialized computing systems based on hardware and software co-optimization. *Russian Technological Journal*, 2024, vol. 12, no. 3, pp. 37–45. doi:10.32362/2500-316X-2024-12-3-37-45, EDN: PXKDKR
15. Bernasconi A., Berti A., Corso G. M. d., Poggiali A. Quantum subroutine for efficient matrix multiplication. *IEEE Access*, 2024, vol. 12, pp. 116274–116284. doi:10.1109/ACCESS.2024.3446176
16. Balonin N. A., Sergeev M. B. *Special`ny`e matricy: psevdoobratny`e, ortogonal`ny`e, adamarovy` i kritskie* [Special matrices: pseudo-return, orthogonal, Hadamardian and Cretan]. Saint-Petersburg, Politekhnika Publ., 2019. 196 p. (In Russian) https://doi.org/10.25960/7325-1155-0
17. Sergeev A. M. Generalized Mersenne matrices and Balonin’s conjecture. *Automatic Control and Computer Sciences*, 2014, no. 48, pp. 214–220. doi:10.3103/S0146411614040063
18. Grigoriev E. K., Nenashev V. A., Sergeev A. M., Samohina E. V. Search and modification of code sequences based on persymmetric quasi-orthogonal circulants. *Telekommunikatsii* [Telecommunications], 2020, no. 10, pp. 27–33 (In Russian). EDN: EGQMAS
19. 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
20. Opalikhina O. V. Formation of an M-sequence over the Galois residue field. *Proceedings of Voronezh State University. Series: Systems Analysis and Information Technologies*, 2023, no. 2, pp. 77–90 (In Russian). doi:10.17308/sait/1995-5499/2023/2/77-90, EDN: ZWXTCG
21. Kukunin D. S., Berezkin A. A., Kirichek R. V. Multilayer orthogonal structures based on maximum length sequences. *Infokommunikacionnye tekhnologii* [Infokommunikacionnye Tehnologii], 2022, no. 20(2), pp. 42–50 (In Russian). doi:10.18469/ikt.2022.20.2.05