Стратегии формирования моноциклических квазиортогональных матриц с симметрией

Е.К. Григорьев

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В статье рассматриваются стратегии формирования моноциклических двухуровневых квазиортогональных матриц с симметрией, ориентированные на расширение класса структурированных матриц, применимых в задачах обработки информации. Актуальность исследования обусловлена возрастающими требованиями к вычислительной эффективности современных информационных и телекоммуникационных систем. Цель работы заключается в систематизации и расширении совокупности стратегий формирования моноциклических квазиортогональных матриц Мерсенна, являющихся ядром матриц Адамара. Предложенный подход основан на установлении связи теории квазиортогональных матриц с теорией бинарных кодовых последовательностей, обладающих двухуровневой периодической автокорреляционной функцией, и использовании циклических разностных множеств Адамара. В работе выделены десять стратегий формирования первых строк матриц, различающихся типом базовых последовательностей и охватывающих порядки, связанные с простыми числами, произведениями простых чисел-близнецов и числами Мерсенна. На конкретных примерах матриц 31-го и 63-го порядков экспериментально продемонстрирована возможность получения как симметричных, так и персимметричных конструкций. Полученные результаты создают основу для увеличения разнообразия квазиортогональных матриц заданного порядка и расширяют возможности их практического применения в системах связи, кодирования и маскирования цифровой информации.

Ключевые слова: ортогональные матрицы, квазиортогональные матрицы, матрицы Адамара, матрицы Мерсенна, матричные преобразования.

Введение

В современной научной и инженерной практике повсеместно используются вычислительные методы, основанные на операциях с матрицами. Наибольшее распространение получили ортогональные и квазиортогональные матрицы, в виду удобства и симметричности преобразований с их использованием.

В рамках работы для квазиортогональных матриц будем использовать следующее определение, взятое из работы [1] – «квазиортогональная матрица $\mathbf{A}$ порядка n это матрица, удовлетворяющая уравнению $\mathbf{A}^{\mathrm{T}}\mathbf{A}=\omega(n)\mathbf{I}$». При этом, $\omega(n)$ – функция, определяющая вес матрицы, **I** – единичная матрица. Наиболее известными квазиортогональными матрицами являются матрицы Адамара существующие на порядках $4t$, где t-натуральное число, с двумя значениями уровней {1;-1}, у которых вес матрицы равен её порядку. Другим примером двухуровневых квазиортогональных матриц являются матрицы Мерсенна со значениями уровней $\{1,-b\}$ существующие на нечетных порядках 4t – 1, тесно связанные с матрицами Адамара [1].

Анализ применения ортогональных и квазиортогональных матриц в помехоустойчивом кодировании [1, 2], обеспечении конфиденциальности [3-5] и сжатии [6, 7] цифровой информации, модуляции и манипуляции сигналов [8 – 10], а также постоянный рост требований к системам обработки информации позволяет сделать вывод о том, что для практического использования недостаточно обеспечить только ортогональность/квазиортогональность матрицы. Например, в помехоустойчивом кодировании обеспечение минимума модуля максимального элемента матрицы позволяет снизить влияние помех при декодировании, что активно применялось при передаче изображений поверхности Марса аппаратом «Маринер 9» [1]. Другим примером может служить маскирование цифровой информации [4, 5], где использование матриц с симметриями позволяет оптимизировать вычисления с их использованием. При этом следует учитывать то, что поиск малоуровневых ортогональных и квазиортогональных структурированных матриц с симметриями является задачей трудоемкой [11, 12] и требует особых подходов отличных от традиционных комбинаторных. Обзор некоторых из них был приведен в работе [13]. В той же работе [13] были сформулированы стратегии формирования двухуровневых циклических персимметричных квазиортогональных матриц – симметричных относительно побочной диагонали, однако анализ более поздних работ [14 – 16] показал, что, вопервых, формируемые на основе известных стратегий матрицы могут быть как персимметричными так и симметричным [14, 15], а во-вторых сам набор стратегий может быть расширен [16].

Целью настоящей работы является расширение набора стратегий формирования моноциклических двухуровневых квазиортогональных матриц Мерсенна являющихся «ядром» матриц Адамара, а также иллюстрация возможности формирования на их основе матриц с различным типом симметриии.

Стратегии формирования квазиортогональных матриц на основе разностных множеств Адамара

Как отмечается в работе [13] – «В настоящее время для поиска квазиортогональных матриц применяются различные подходы, отличные от традиционных комбинаторных и основанные на связях:

–особенностей структур матриц с решением диофантовых уравнений и расположением точек Гаусса на решетках;

–строк матриц с теорией групп и полей, в которых определяются положения элементов со значениями 1 и -b или -1;

–структур матриц с результатами оптимизационного процесса.»

Однако, можно выделить и альтернативный подход, основанный на связи теории матриц и одной из задач радиолокации и связи, а именно – поиска бинарных кодовых последовательностей (КП) с двухуровневой периодической автокорреляционной функцией [17]. В данном подходе предлагается осуществлять поиск циклических матриц на основе КП, представляющих собой циклические разностные множества Адамара. На основе обзора известных в настоящее время циклических разностных множеств Адамара в рамках настоящей работы предлагаются следующие стратегии формирования первых строк моноциклических двухуровневых квазиортогональных матриц Мерсенна являющихся «ядром» матриц Адамара, представленные в таблице 1. В таблице 1 k – натуральное число.

Таблица № 1

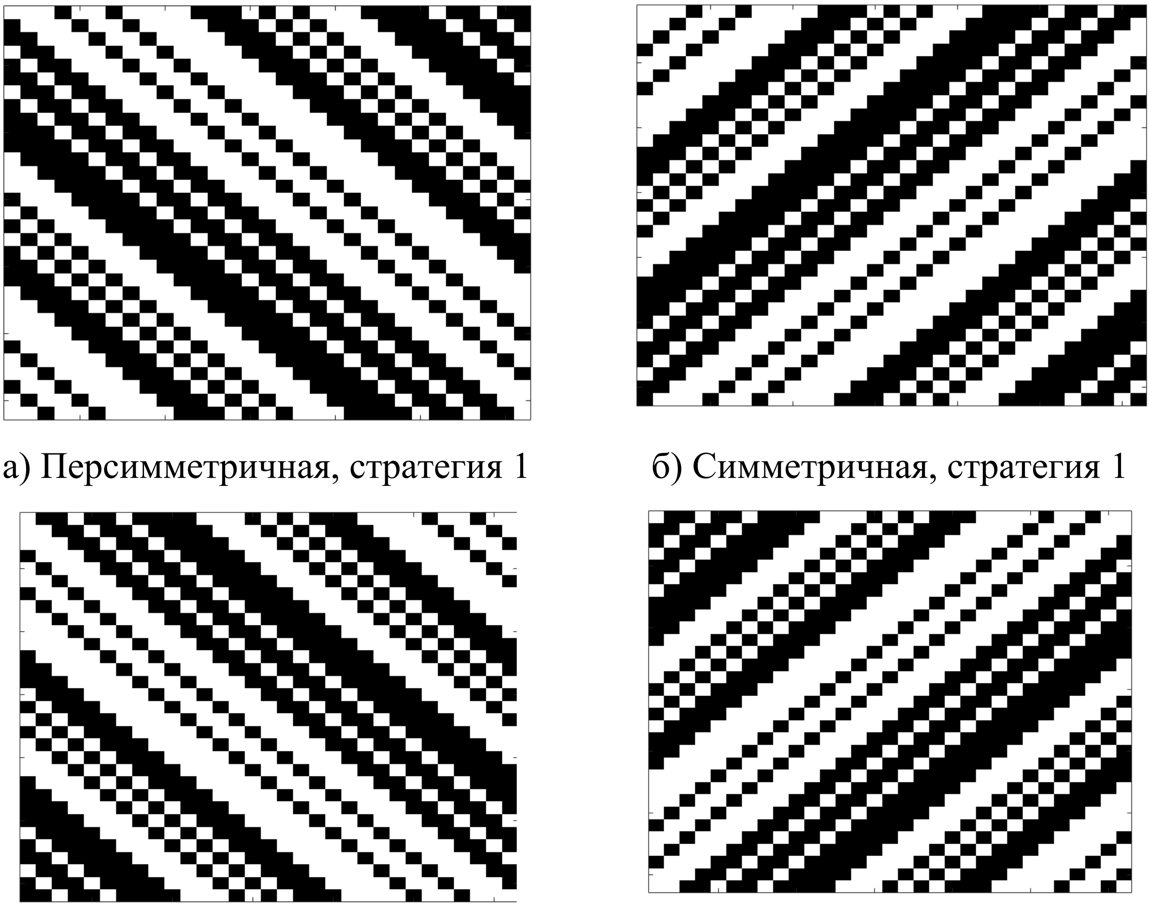
Стратегии формирования моноциклических квазиортогональных матриц

№ стратегии	Основа	n
1	Последовательность Лежандра [8, 12, 13]	$4t$-1=p
2	Последовательность Якоби [13, 15]	$4t$-1=$p(p+2)$
3	m-последовательность [13, 15]	$4t$-1=2^k-1
4	GMW-последовательность [16, 18]	$4t$-1=2^k-1
5	3-term последовательность [18]	$4t$-1=2^k-1 k нечетное, k=2m+1, $k \geq 5$
6	5-term последовательность [18]	$4t$-1=2^k-1, 5mod3 $\neq$ 0, $k \geq 7$
7	WG последовательность [18]	$4t$-1=2^k-1, $k \geq 7$
8	Последовательность на основе гиперовалов Segre [18]	$4t$-1=2^k-1; k нечетное, $k \geq 5$
9	Последовательность на основе гиперовалов Glynn 1 типа [18]	$4t$-1=2^k-1; k нечетное, $k \geq 7$
10	Последовательность на основе гиперовалов Glynn 2 типа [18]	$4t$-1=2^k-1; k нечетное, $k \geq 11$

Приведенные в таблице 1 стратегии позволяют формировать моноциклические квазиортогональные матрицы Мерсенна с элементами {1,-b} разной симметрии, как персимметричной, при циклическом сдвиге на один элемент вправо каждой строки, так и симметричной, при аналогичном сдвиге, но влево. При этом, элемент b квазиортогональных матриц может быть найден с использованием универсального алгоритма, представленного в работе [17].

Подтвердим вышесказанное несколькими примерами. Сформируем две симметричные и две персимметричные матрицы по стратегиям 1 и 8 соответственно. Для определенности установим порядок матриц равным 31.

Воспользуемся портретным представлением матриц. Черному квадрату будет соответствовать элемент со значением «-*b*», а, белому квадрату элемент со значением «1». Сформированные на основе стратегий 1 и 8 матрицы представлены на рис. 1.



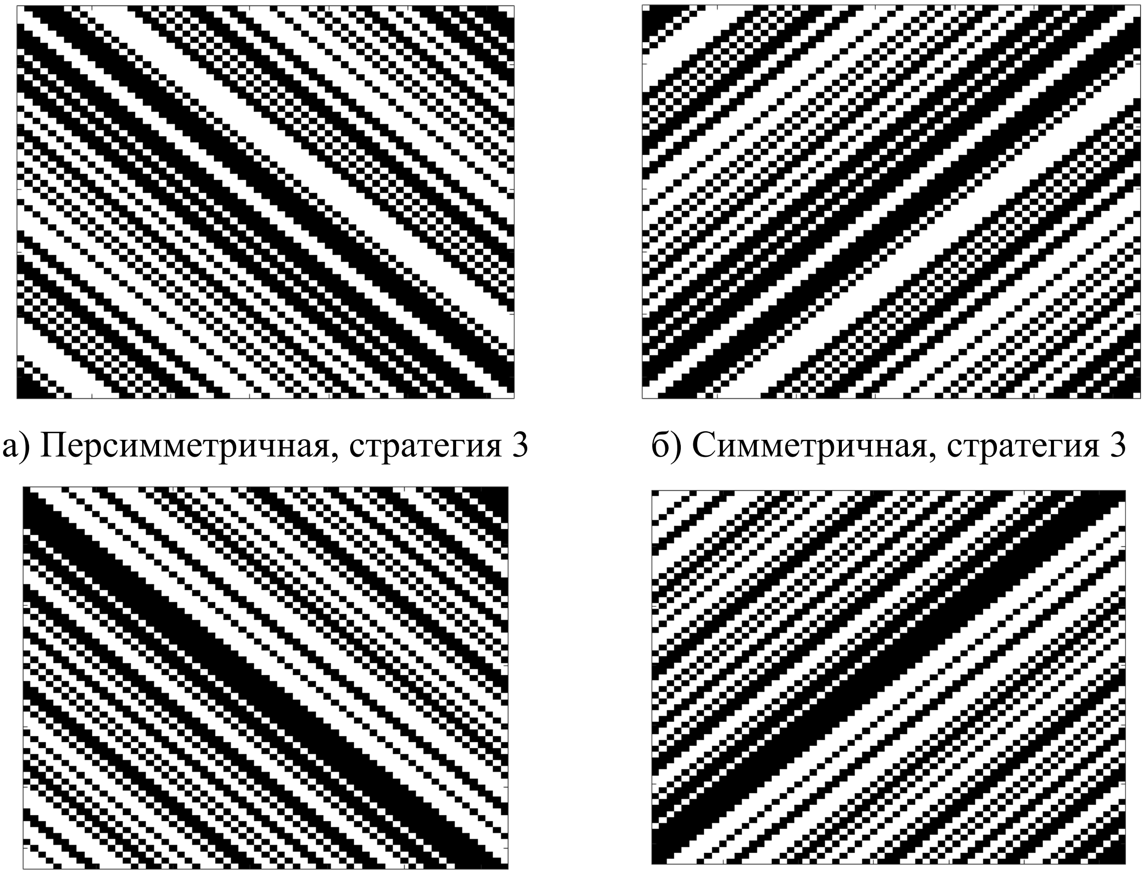
а) Персимметричная, стратегия 1 б) Симметричная, стратегия 1

в) Персимметричная, стратегия 8 г) Симметричная, стратегия 8

Рис. 1. – Портреты матриц 31 порядка сформированные на основе стратегий 1 и 8

Для стратегии 1 требуется определить квадратичные вычеты и невычеты по модулю 31. Квадратичными невычетами по модулю 31 будут являться элементы последовательности 4,7,12,13,14,16,18,22,23,24,25,27,28,30,31, а остальные элементы последовательности будут являться вычетами. Для стратегии 8 оставим за рамками работы вопросы формирования гиперовальных последовательностей, которые подробно изложены в [18], и возьмем готовую последовательность, которая приведена в [18] на стр. 285. Элемент b для данных матриц будет равен 0.7388, а вес $\omega(n)$=27.1873

Рассмотрим дополнительный пример. Сформируем матрицы по стратегиям 3 и 4. Для определенности установим порядок матриц равным 63. Сформированные на основе стратегий 3 и 4 матрицы представлены на рис. 2.



а) Персимметричная, стратегия 3 б) Симметричная, стратегия 3

в) Персимметричная, стратегия 4 г) Симметричная, стратегия 4

Рис. 2. – Портреты матриц 63 порядка сформированные на основе стратегий 3 и 4

Для формирования матрицы по стратегии 3 требуется задать примитивный полином. Выберем $x^6+x^4+x^3+x+1$ с начальными условиями [0,0,0,0,0,1]. Для стратегии 4 аналогичным образом оставим за рамками работы вопросы формирования последовательностей Гордона-Миллса-Велча (GMW), которые подробно изложены в [18], и возьмем готовую последовательность, которая приведена в [18] на стр. 240. Элемент b для данных матриц будет равен 0.8, а вес $\omega(n)$=51.84.

Заключение

Предложенные в настоящей работе стратегии позволяют формировать моноциклические квазиортогональные матрицы Мерсенна с элементами {1,-b} как персимметричной, так и симметричной конструкции, что позволит увеличить представительство подобных матриц по порядкам, а также расширить возможности использования в различных сферах их применения.

Выделенные стратегии формирования матриц позволяют формировать различные матрицы оставаясь в рамках одной структуры и одного порядка, что может быть использовано, например в маскировании цифровой информации при формировании матриц-ключей.

Благодарность

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. Хвощ С. Т. Матрицы Адамара в космической связи. Инженерный вестник Дона. 2024. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8973

2. Мироновский Л. А., Слаев В. А. Стрип-метод преобразования изображений и сигналов. СПб.: Политехника. 2006. 163с.

3. Kulchytska K., Semeniv M., Kovalskyi B., Pysanchyn N., Selmenska Z. Influence of Hadamard Matrices Canonicity on Image Processing. Lecture Notes in Networks and Systems. 2022. V. 463. P. 329-338

4. Костров Б. В., Гринченко Н. Н., Баранова С. Н., Трушина Е. А., Вьюгина А. А. Ортогональное кодирование бинарных изображений. Вестник Ярославского высшего военного училища противовоздушной обороны. 2023. № 2. С. 82-87.

5. Хвощ С. Т. Об особенности реализации помехозащищенного кодирования изображений. Вопросы радиоэлектроники. Серия: Техника телевидения. 2024. № 4. С. 60-65.

6. Костров Б. В., Баранова С. Н., Лобачев М. А., Трушина Е. А., Вьюгина А. А. Сжатие изображений в пространственно-спектральном представлении. Вестник Ярославского высшего военного училища противовоздушной обороны. 2024. № 2 . С. 93-100.

7. Костров Б. В., Бастрычкин А. С. Сжатие изображений на основе ортогональных преобразований. Известия Тульского государственного университета. Технические науки. 2016. № 9. С. 113-119.

8. Жук А. П., Стогний К. В., Копытов В. В., Макаров И. В. Методика получения ансамблей дискретных ортогональных кодовых последовательностей с улучшенными автокорреляционными функциями. Системы управления, связи и безопасности. 2025. № 1. С. 48-78.

9. Жук А. П., Студеникин А. В., Макаров И. В., Беседин А. А. Оценка структурной скрытности ансамблей многофазных ортогональных кодовых последовательностей. Телекоммуникации. 2024. № 3. С. 13-21.

10. Светлов Г. В., Суменков Н. А., Костров Б. В., Гринченко Н. Н., Трушина Е. А. Построение ортогонального базиса на основе

псевдослучайных последовательностей. Вестник Концерна ВКО "Алмаз – Антей". 2020. № 4. С. 95-100.

11. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley. 2020. 384 p.

12. Dokovic D. Z. Some new symmetric Hadamard matrices. Information and Control Systems.. 2022. № 2. P. 2-10.

13. Ненашев В. А., Григорьев Е. К., Сергеев А. М., Самохина Е. В. Стратегии вычисления персимметричных циклических квазиортогональных матриц как основы кодов. Электросвязь. 2020. № 10. С. 58-61.

14. Григорьев Е. К. Методы формирования квазиортогональных матриц на основе псевдослучайных последовательностей максимальной длины. Инженерный вестник Дона. 2025. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9796

15. 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.

16. Григорьев Е. К., Сергеев А. М. Формирование ансамблей квазиортогональных кодовых последовательностей с высокой структурной скрытностью. Известия высших учебных заведений. Приборостроение. 2025. Т. 68, № 5. С. 388-396.

17. Григорьев Е. К. Поиск и применение циклических квазиортогональных матриц в задачах обработки информации: Дис. ... канд. техн. Наук. 2.3.1. СПб. 2025. 129 с.

18. Golomb S.W., Gong G. Signal design for good correlation for wireless communication, cryptography, and radar. Cambridge Univ. Press. 2006.

References

1. Hvosh S. T. Inzhenernyj vestnik Dona, 2024, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8973.

2. Mironovskij L. A., Slaev V. A. Strip-metod preobrazovaniya izobrazhenij i signalov [Strip method for image and signal transformation]. Saint-Peterburg: Politexnika. 2006. 163 p.

3. Kulchytska K., Semeniv M., Kovalskyi B., Pysanchyn N., Selmenska Z. Lecture Notes in Networks and Systems. 2022. V. 463. Pp. 329-338

4. Kostrov B. V., Grinchenko N. N., Baranova S. N., Trushina E. A., V′yugina A. A. Vestnik Yaroslavskogo vysshego voyennogo uchilishcha protivovozdushnoy oborony. 2023. № 2. Pp. 82-87.

5. Hvosh S. T. Voprosy radioelektroniki. Seriya: Tekhnika televideniya. 2024. № 4. Pp. 60-65.

6. Kostrov B. V., Baranova S. N., Lobachev M. A., Trushina E. A., V′yugina A. A. Vestnik Yaroslavskogo vysshego voyennogo uchilishcha protivovozdushnoy oborony. 2024. № 2 . Pp. 93-100.

7. Kostrov B. V., Bastrychkin A. S. Izvestiya Tul′skogo gosudarstvennogo universiteta. Tekhnicheskiye nauki. 2016. № 9. Pp. 113-119.

8. Zhuk A. P., Stogniy K. V., Kopytov V. V., Makarov I. V. Systems of Control, Communication and Security. 2025. № 1. Pp. 48-78.

9. Zhuk A. P., Studenikin A. V., Makarov I. V., Besedin A. A. Telekommunikatsii. 2024. № 3. Pp. 13-21.

10. Svetlov G. V., Sumenkov N. A., Kostrov B. V., Grinchenko N. N., Trushina E. A. Vestnik Kontserna VKO "Almaz – Antey". 2020. № 4. Pp. 95-100.

11. Jennifer S., Yamada M. Hadamard Matrices: Constructions using number theory and linear algebra. Wiley. 2020. 384 p.

12. Dokovic D. Z. Information and Control Systems. 2022. № 2. Pp. 2-10.

13. Nenashev V.A., Grigoriev E.K., Sergeev A. M., Samohina E.V. Electrosvyaz. 2020. № 10. pp. 58-61.

14. Grigoriev E. K. Inzhenernyj vestnik Dona. 2025. № 1 URL: ivdon.ru/ru/magazine/archive/n1y2025/9796

15. Grigoriev E.K., Sergeev A. M. Information and Control Systems. 2025. № 1. P. 2-8.

16. Grigoriev E.K., Sergeev A. M. Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie. 2025. T. 68, № 5. C. 388-396.

17. Grigoriev E.K. Poisk i primeneniye tsiklicheskikh kvaziortogonal′nykh matrits v zadachakh obrabotki informatsii [Search and application of cyclic quasi-orthogonal matrices in information processing problems]: Dis. ... kand. tekhn. Nauk. 2.3.1. Sankt-Peterburg. 2025. 129 p.

18. Golomb S.W., Gong G. Signal design for good correlation for wireless communication, cryptography, and radar. Cambridge Univ. Press. 2006.

Дата поступления: 29.12.2025

Дата публикации: 22.02.2026