Методы формирования квазиортогональных матриц на основе псевдослучайных последовательностей максимальной длины

Е.К. Григорьев

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: В данной работе исследованы методы формирования квазиортогональных матриц на основе псевдослучайных последовательностей максимальной длины (m-последовательностей). Проведен анализ существующего метода, основанного на циклическом сдвиге m-последовательности и дополнении получившейся циклической матрицы каймой. Предложен альтернативный метод, основанный на связи псевдослучайных последовательностей максимальной длины, а также квазиортогональных матриц Мерсенна и Адамара, позволяющий генерировать циклические квазиортогональные матрицы симметричной структуры без каймы. Проведен сравнительный анализ корреляционных свойств матриц, полученных обоими методами, и исходных m-последовательностей. Показано, что предлагаемый метод наследует корреляционные свойства m-последовательностей, обеспечивает более эффективное хранение матрицы и имеет потенциал при решении задач обеспечения конфиденциальности цифровой информации.
Ключевые слова: ортогональная матрица, квазиортогональная матрица, матрица Адамара, матрица Мерсенна, m-последовательность.

Введение

Регистры сдвига с линейной обратной связью (LFSR) и порождаемые ими псевдослучайные последовательности максимальной длины (m-последовательности) получили широкое распространение при решении задач математического моделирования [1,2], криптографии [3,4], радиолокации и связи [5,6]. Широта распространения обуславливается их особыми свойствами, например корреляционными [1,2].

Интересным, но редко обсуждаемым в научной литературе последних лет, свойством данных последовательностей является возможность формирования на их основе квазиортогональных матриц. Поясним квазиортогональность на примере квадратной матрицы $\mathbf{P}$ порядка n. Обозначим как $\mathbf{P}_i$ ее i-ую строку, а ее j-й элемент как $\mathbf{P}_i(j)$, тогда для строк квазиортогональной матрицы $\mathbf{P}$ выполняется следующее равенство:

$$\sum_{j=1}^{n}\mathbf{P}_i(j)\mathbf{P}_k(j)=\begin{cases}0, i\neq k;\\ \omega(n), i=k.\end{cases} \quad (1)$$

Под $\omega(n)$ будем понимать вес матрицы. Данные матрицы не ортогональны в строгом смысле этого слова, но близки к ортогональным [7], у которых в равенстве (1) $\omega(n)=1$.

В дальнейшем изложении под квазиортогональной матрицей будем понимать квадратную матрицу, результат умножения которой на саму себя транспонированную будет давать единичную матрицу, умноженную на некоторый весовой коэффициент [7]. Для произвольной квазиортогональной матрицы **P** порядка n, это можно записать, как:

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

где, **I** – единичная матрица. Как отмечается в монографии [7], данные матрицы будут «… строго ортогональны после нормирования их столбцов».

Ортогональные и квазиортогональные матрицы и преобразования на их основе широко используются при решении задач сжатия [8], помехоустойчивого кодирования [9,10] и маскирования цифровой информации [11,12], что делает актуальными задачи их поиска, вычисления и формирования.

Целью настоящей работы является исследование методов формирования квазиортогональных матриц на основе m-последовательностей.

Методы формирования квазиортогональных матриц

В работе [6] коллективом авторов перечислены основные свойства m-последовательностей, а также предложен метод формирования квазиортогональной матрицы на их основе, включающий в себя:

1. Формирование m-последовательности длины N по заданному примитивному полиному и начальным условиям.

2. Генерацию циклической матрицы размера NxN путем левостороннего циклического сдвига на один элемент.

3. Замену элементов со значением «0» на «-1».

4. Выравнивание количества элементов со значением «1» и «-1» по строкам и по столбцам. Это достигается путем добавления в матрицу сгенерированную в пунктах 1-3 каймы в виде строки и столбца состоящих из элементов «-1».

Рассмотрим работу данного метода на примере, взятом из работы [6], где используется примитивный полином $M(x)=x^3+x^2+1$, с начальными условиями [1,0,0]. Сам этап формирования m-последовательности в рамках настоящей работы пропустим, в виду достаточного освещения в литературе – например [1-2]. В результате получается m-последовательность – (0,0,1,0,1,1,1). В результате выполнения пунктов 1-2 предлагаемого метода получается матрица $\mathbf{M}_7$ не являющаяся квазиортогональной, что нетрудно проверить:

$$\mathbf{M}_7=\begin{bmatrix}0&0&1&0&1&1&1\\0&1&0&1&1&1&0\\1&0&1&1&1&0&0\\0&1&1&1&0&0&1\\1&1&1&0&0&1&0\\1&1&0&0&1&0&1\\1&0&0&1&0&1&1\end{bmatrix};\mathbf{M}_7\mathbf{M}_7^{\mathrm{T}}=\begin{bmatrix}7&-1&-1&-1&-1&-1&-1\\-1&7&-1&-1&-1&-1&-1\\-1&-1&7&-1&-1&-1&-1\\-1&-1&-1&7&-1&-1&-1\\-1&-1&-1&-1&7&-1&-1\\-1&-1&-1&-1&-1&7&-1\\-1&-1&-1&-1&-1&-1&7\end{bmatrix}.$$

В результате выполнения пунктов 3-4 предлагаемого авторами метода получается матрица $\mathbf{M}_8$ удовлетворяющая условию квазиортогональности, а не ортогональности как утверждают авторы работы [6], поскольку вес матрицы в данном случае становится равным ее порядку $\omega(n)=n=8$.

Что осталось без внимания авторов работы [6], так это то, что их метод восходит к работам Соломона Голомба, который еще в первой редакции монографии [1] опубликованной в 1967 году отмечал связь m-

последовательностей и матриц Адамара, обладающих глобальным максимумом детерминанта (см. главу 3).

$$\mathbf{M}_8=\begin{bmatrix}-1&-1&1&-1&1&1&1&-1\\-1&1&-1&1&1&1&-1&-1\\1&-1&1&1&1&-1&-1&-1\\-1&1&1&1&-1&-1&1&-1\\1&1&1&-1&-1&1&-1&-1\\1&1&-1&-1&1&-1&1&-1\\1&-1&1&1&-1&1&1&-1\\-1&-1&-1&-1&-1&-1&-1&-1\end{bmatrix};\mathbf{M}_8\mathbf{M}_8^{\mathrm{T}}=\begin{bmatrix}8&0&0&0&0&0&0&0\\0&8&0&0&0&0&0&0\\0&0&8&0&0&0&0&0\\0&0&0&8&0&0&0&0\\0&0&0&0&8&0&0&0\\0&0&0&0&0&8&0&0\\0&0&0&0&0&0&8&0\\0&0&0&0&0&0&0&8\end{bmatrix}.$$

И действительно, матрица, получаемая авторами есть ни что иное, как матрица Адамара, но в ненормализованном виде. Чтобы получать матрицы Адамара в нормализованном виде достаточно после выполнения пункта 3 предлагаемого авторами [6] метода инвертировать полученную матрицу и добавить кайму в виде первой строки и первого столбца состоящих из элементов «1».

На связи матриц Адамара с другим семейством квазиортогональных матриц локального максимума детерминанта – матриц Мерсенна [7], можно выделить и другой метод формирования квазиортогональных матриц на основе m-последовательностей, которые удовлетворяют (1) с весом:

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

где a и b – уровни матрицы. Для достижения локального максимума детерминанта a – принимается равным единице, однако если отойти от требований максимума детерминанта, a можно выбрать произвольным.

Действительно матрицы Мерсенна, как отмечено в монографии [7] впервые были обнаружены на порядках существования m-последовательностей – 2^z-1, где z – натуральное число, и являются «ядром» матриц Адамара конструкции ядро с окаймлением.

На основании вышесказанного можно изложить суть метода:

1. Формируется m-последовательность длины N по заданному примитивному полиному и начальным условиям.

2. Элементы m-последовательности со значением «0» заменяются на «-b», а элементы со значением «1» на «a».

3. Выбирается фиксированное значение «a», и рассчитывается значение b по формуле:

$$b = \frac{at}{t + \sqrt{t}},$$

где t вычисляется из соотношения $N=2^z-1=4t-1$. Последнее обусловлено тем, что порядки существования m-последовательностей вложены в порядки существования матриц Мерсенна $4t-1$, где t-натуральное число.

4. Генерируется циклическая матрица размера NxN путем левостороннего циклического сдвига на один элемент.

Работоспособность метода предлагается проверить на примере уже рассмотренной m-последовательности - (0,0,1,0,1,1,1). Зафиксируем значение a=1, тогда значение b=0.5858. Тогда сформированная квазиортогональная матрица $\mathbf{M}_{7,b}$ будет выглядеть следующим образом:

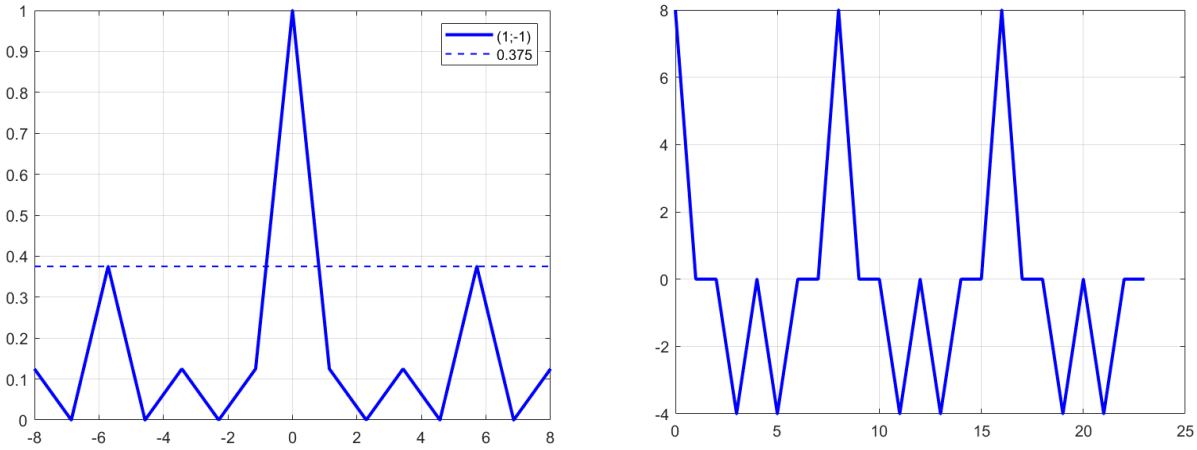
$$\mathbf{M}_{7,b} = \begin{bmatrix} -0.5858 & -0.5858 & 1 & -0.5858 & 1 & 1 & 1 \\ -0.5858 & 1 & -0.5858 & 1 & 1 & 1 & -0.5858 \\ 1 & -0.5858 & 1 & 1 & 1 & -0.5858 & -0.5858 \\ -0.5858 & 1 & 1 & 1 & -0.5858 & -0.5858 & 1 \\ 1 & 1 & 1 & -0.5858 & -0.5858 & 1 & -0.5858 \\ 1 & 1 & -0.5858 & -0.5858 & 1 & -0.5858 & 1 \\ 1 & -0.5858 & -0.5858 & 1 & -0.5858 & 1 & 1 \end{bmatrix},$$

Нетрудно проверить, что она удовлетворяет условию (1), при этом значение $\omega(n)$=5.7574

Второй метод обладает рядом достоинств по сравнению с первым. Во-первых, это структура матрицы. Первый метод формирует симметричные

матрицы, а второй метод формирует циклические матрицы при сохранении симметрии, что снижает вычислительные затраты на хранение матрицы, сохраняя при этом скорость вычислений [13]. Во-вторых, отсутствие каймы из единиц в матрице снижает вероятность переполнения разрядной сетки при умножении матриц. В-третьих, матрицы, формируемые вторым методом, имеют преимущество при решении задач обеспечения конфиденциальности [11,12] в виду сложности подбора третьей стороной как расположения элементов матрицы – вследствие возможности случайного выбора полинома и начальных условий m-последовательности, так и возможности случайного выбора значения *a,* что напрямую влияет на результаты умножения. В-четвертых, строки матриц, формируемых вторым методом, наследуют корреляционные свойства прототипа – m-последовательностей [14], в отличии от первого метода, где формируются матрицы Адамара, корреляционные свойства которых известны и не являются удовлетворительными [2].

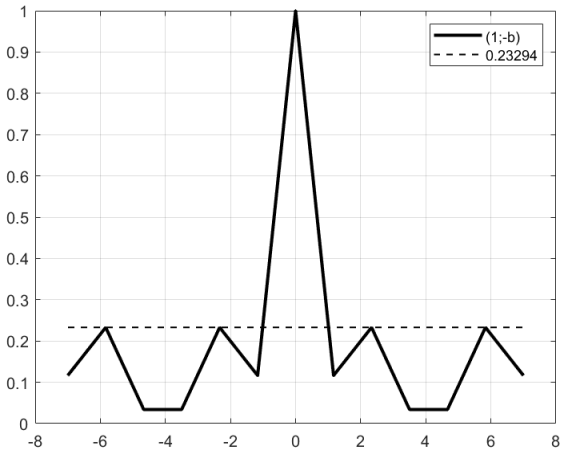
Продемонстрируем примеры, подтверждающие последнее утверждение. Рисунками 1-3.



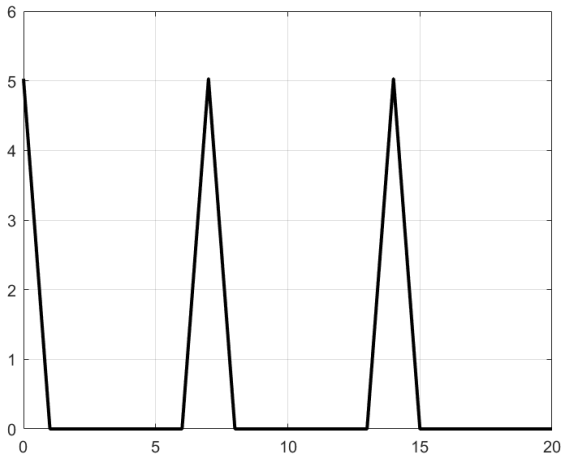
а) Апериодическая АКФ б) Периодическая АКФ

Рис. 1. – Графики корреляционных функций первой строки матрицы, сформированной первым методом

На рис. 1-3 представлены попарно графики нормированных к единице апериодических автокорреляционных функций (а) и ненормированных периодических автокорреляционных функций (б) для первых строк матриц, формируемых по первому (рис. 1) и второму (рис. 2) методу, а также исходной m-последовательности (рис. 3). Значения апериодической автокорреляционной функции взяты по модулю.

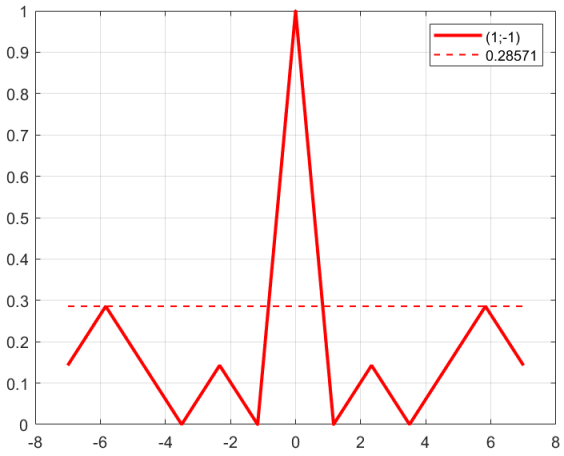


а) Апериодическая АКФ

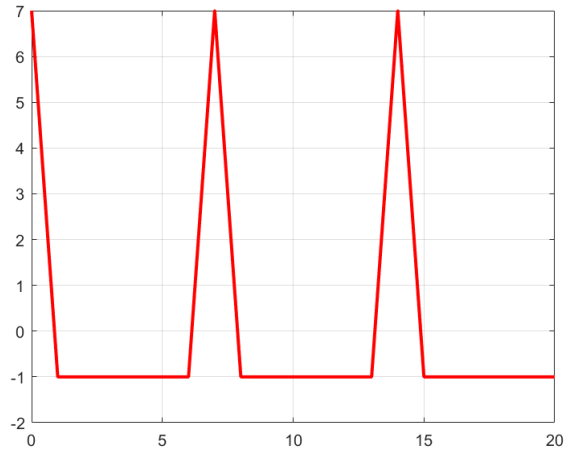


б) Периодическая АКФ

Рис. 2. – Графики корреляционных функций первой строки матрицы, сформированной вторым методом



а) Апериодическая АКФ



б) Периодическая АКФ

Рис. 3. – Графики корреляционных функций исходной m-последовательности

Как видно из рисунков 2 и 3, у строк матриц, формируемых вторым методом, наследуются корреляционные свойства m-последовательностей, а именно - одноуровневость периодической автокорреляционной функции, однако следует отметить, что уровень максимума периодической автокорреляционной функции у строк матриц формируемых вторым методом снижается до $\omega(n)$ против N у m-последовательностей, а величина боковых пиков апериодической автокорреляционной функции становится близка к $1/\sqrt{\omega(n)}$, против $1/\sqrt{N}$.

Заключение

Псевдослучайные последовательности максимальной длины являются простым и доступным инструментом формирования квазиортогональных матриц.

Проведенная работа выявила достоинства и недостатки обоих методов формирования квазиортогональных матриц, что позволит продолжить исследования, направленные на изучение свойств получаемых матриц и оптимизацию уровней для решения специфических задач в области цифровой обработки сигналов, криптографии и кодирования информации.

Литература

1. Golomb S.W. Shift Register Sequences. Singapore: World Scientific, 2017, 265 p.

2. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.

3. Горбунов А.В., Даюнов Р.С. Использование псевдослучайных последовательностей в системах квантовой связи // Инженерный вестник Дона. 2014. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2014/2364.

4. Кузьмин Е.В., Зограф Ф.Г. Параметризованная модель генератора псевдослучайных последовательностей в OrCAD // Инженерный вестник Дона. 2013. № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1766.

5. 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.

6. 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.

7. Балонин Н.А., Сергеев М.Б. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские. СПб.: Политехника, 2019. 196 с.

8. Ортогональные преобразования при обработке цифровых сигналов / Ахмед Н., Рао К.Р., под ред. Фоменко И.Б. М.: Связь, 1980. 248 с.

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

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

11. Сергеев А.М., Сергеев М.Б. О маскировании изображений, как основе построения схемы визуальной криптографии // Инженерный вестник Дона. 2024. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9039.

12. Сергеев М.Б., Татарникова Т.М., Сергеев А.М., Боженко В.В. Метод обеспечения конфиденциальности данных с применением ортогональных матриц // Инженерный вестник Дона. 2024. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8967.

13. Стройникова Е.Д. Оптимизация цифровой обработки сигналов с использованием структурных алгоритмов для матриц некоторых кодов Якоби // Доклады БГУИР. 2007. №1. С. 5-17.

14. Grigoriev, E.K., V.A. Nenashev, A.M. Sergeev and S.A. Nenashev, 2020. Research and analysis of methods for generating and processing new code structures for the problems of detection, synchronization and noise-resistant coding. Proc. SPIE, Image and Signal Processing for Remote Sensing XXVI (issue 11533), SPIE Date Views 25.12.2024 URL: spiedigitallibrary.org/conference-proceedings-of-spie/11533/2574238/Research-and-analysis-of-methods-for-generating-and-processing-new/10.1117/12.2574238.short.

References

1. S. W. Golomb, Shift Register Sequences, Singapore:World Scientific, 2017. 265 p.

2. Varakin L. E. Sistemy` svyazi s shumopodobny`mi signalami [Noise-like signal communication systems]. M.: Radio i svyaz, 1985. 384 p.

3. Gorbunov A. V. Inzhenernyj vestnik Dona, 2014, № 2. URL: ivdon.ru/ru/magazine/archive/n2y2014/2364.

4. Kuzmin E. V. Inzhenernyj vestnik Dona, 2013, № 3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1766.

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

6. Svetlov G. V., Sumenkov N. A., Kostrov B. V., Grinchenko N.N., Trushina E.A. Journal of «Almaz – Antey» Air and Space Defence Corporation. 2020. № 4. pp. 95-100.

7. Balonin N. A., Sergeev M. B. Special`ny`e matricy: psevdoobratny`e, ortogonal`ny`e, adamarovy` i kritskie [Special matrices: pseudoinverse, orthogonal, Hadamard and Cretan]. Saint-Peterburg: Politexnika, 2019. 196 p

8. Axmed N., Rao K. R. Ortogonal`ny`e preobrazovaniya pri obrabotke cifrovy`x signalov [Orthogonal transforms in digital signal processing]. M.: Svyaz, 1980. 248 p.

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

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

11. Sergeev A. M. Inzhenernyj vestnik Dona, 2024, № 2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9039.

12. Sergeev M. B., Tatarnikova T. M., Sergeev A. M., Bozhenko V.V. Inzhenernyj vestnik Dona, 2024, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2024/8967.

13. Strojnikova E.D. Doklady` BGUIR. 2007 №1. pp. 5-17.

14. Grigoriev E.K., Nenashev V.A., Sergeev A.M., Nenashev S.A. Research and analysis of methods for generating and processing new code structures for the problems of detection, synchronization and noise-resistant coding. Proc. SPIE, Image and Signal Processing for Remote Sensing XXVI (issue 11533), SPIE Date Views 25.12.2024. URL: spiedigitallibrary.org/conference-proceedings-of-spie/11533/2574238/Research-and-analysis-of-methods-for-generating-and-processing-new/10.1117/12.2574238.short.

Дата поступления: 5.12.2024

Дата публикации: 10.01.2025