

УДК 621.391.8

Поиск и модификация кодовых последовательностей на основе персимметричных квазиортогональных циркулянтов^{* **}

Е.К. ГРИГОРЬЕВ¹, В.А. НЕНАШЕВ¹, канд. техн. наук, А.М. СЕРГЕЕВ¹,
Е.В. САМОХИНА², канд. техн. наук

¹Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Санкт-Петербург, 190000, РФ

²Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», Москва, 119454, РФ

E-mail: ev.grig95@gmail.com

Статья поступила в редакцию 20.04.2020

Принята после доработки 22.05.2020

Принята к публикации 21.07.2020

Рассматриваются вопросы поиска и исследования новых помехоустойчивых кодов, построенных на основе персимметричных циркулянтов. Приводится сравнение оценок характеристик полученных новых кодовых последовательностей. Преимущества полученных в работе кодов обсуждаются в аспектах повышения корреляционных характеристик, их обнаружения и помехоустойчивости в радиоканалах распределенных систем.

Ключевые слова: помехоустойчивый код, сжатие кодо-модулированных сигналов, автокорреляционная функция, персимметричный циркулант, квазиортогональная матрица, коды максимальной длины.

The problems of searching and researching new noise-immune codes based on persymmetric circulants are considered. A comparison of characteristic estimates of obtained new code sequences is given. Advantages of the obtained codes are discussed in the aspects of increasing the correlation characteristics, their detection, and noise immunity in radio channels of distributed systems.

Keywords: noise-immune code, compression, code-modulated signal, autocorrelation function, persymmetric circulant, quasi-orthogonal matrix, maximum length code.

* Статья подготовлена при финансовой поддержке Министерства науки и высшего образования, грант FSRF-2020-0004 «Научные основы построения архитектур и систем связи бортовых и информационно-вычислительных комплексов нового поколения для авиационных космических систем и беспилотных транспортных средств».

** Исследование методики вычисления модификаций кодовых последовательностей, основанных на персим-

Введение

Для многих задач обработки информации, в том числе для формирования новых конкурентных кодов и вложенных

метрических квазиортогональных циркулянтах, выполнено за счет гранта Российского научного фонда (проект № 19-79-00303).

кодовых конструкций, используемых в беспроводных коммуникациях для модуляции сигналов [1—3], большое значение имеет поиск и исследование экстремальных матриц. Такими матрицами, например, являются ортогональные и квазиортогональные матрицы симметричных и блочно-симметричных структур [4, 5], матрицы максимума детерминанта [6—8]. В качестве примера можно привести коды Баркера, используемые в наборе стандартов IEEE 802.11. Анализ показал, что, хотя они вычислялись независимо от теории матриц, они являются фрагментами строк матрицы максимума детерминанта, вычисленной Г. Барба [9].

Развитие теории квазиортогональных матриц и новые практические результаты открывают возможность пересмотра методов синтеза помехоустойчивых кодов, разработки новых алгоритмов обработки сигналов и изображений.

Это же способствует пересмотру решений, во-первых, задач локации в части повышения помехоустойчивости в многопозиционных системах, использующих генерацию и обработку кодо-модулированных сигналов [10, 11]; во-вторых, задачи обеспечения надежной передачи информации в радиоканале в условиях сложной электромагнитной обстановки [11, 12].

В настоящей работе рассматривается новый подход к поиску кодовых последовательностей как альтернативы кодам Баркера, m -последовательностям и другим широко известным кодам. Подход основан на построении кодов из строк циклических квазиортогональных матриц, к которым относятся матрицы Мерсенна и Рагхаварао [13, 14].

Циклические квазиортогональные матрицы

В работе [13] квазиортогональной матрицей называется квадратная матрица A порядка n с ограниченными по модулю элементами $|a_{ij}| \leq 1$, такая, что для нее выполняется

$$A^T A = \omega(n) I,$$

где I — единичная матрица, а $\omega(n)$ — весовая функция.

Такое определение обобщает ортогональные матрицы, к которым относятся известные

матрицы Аламара, Белевича, Хаара, дискретного косинусного преобразования, жакетные матрицы [15] и др.

Введем два ограничения на квазиортогональные матрицы, строки которых будем использовать для получения помехоустойчивых кодов.

Ограничение 1. Количество значений элементов квазиортогональных матриц не должно превышать двух. Будем называть такие матрицы двухуровневыми.

Самыми известными двухуровневыми квазиортогональными матрицами являются матрицы Адамара (Hadamard) H с элементами 1 и -1.

Ограничение 2. Будем рассматривать только структурированные двухуровневые циклические квазиортогональные матрицы — циркулянты [16].

Приведенные ограничения значительно ограничивают класс квазиортогональных матриц, однако такие матрицы существуют и могут быть найдены алгоритмически.

Из теоремы Райзера [17] известно, что единственной циклической симметричной матрицей Адамара является матрица порядка 4. Поэтому основное внимание уделим циклическим персимметричным матрицам — циркулянтам, симметричным относительно побочной диагонали.

В работе [18] показано, что существует множество матриц Адамара, состоящих из $(n-1) \times (n-1)$ циклического сдвигового ядра (core) с добавлением «каймы» из верхней строки и левого столбца, состоящих из единиц. Пример такой матрицы конструкции «циркулант с окаймлением» или «ядро с окаймлением» порядка 8 приведен ниже:

$$H_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & - & - & + & - & + & + \\ + & + & - & - & - & + & - & + \\ + & + & + & - & - & - & + & - \\ + & - & + & + & - & - & - & + \\ + & + & - & + & + & - & - & - \\ + & - & + & - & + & + & - & - \\ + & - & - & + & - & + & + & - \end{bmatrix}.$$

Циркулянты Мерсенна и Рагхаварао

Наиболее важной характеристикой кодов при корреляционном приеме кодированных сигналов является автокорреляционная функция (АКФ). Для получения кодовой последовательности с «хорошой» АКФ рассмотрим способы ее формирования на основе циркулянтов Мерсенна и Рагхаварао.

Первый способ основан на использовании циркулянтов Мерсенна (\mathbf{M}) порядков $2^k - 1$, вложенных в последовательность $n = 4t - 1$ и обладающих локальным максимумом детерминанта [13, 19]. Кодовые последовательности, получаемые из строк такой квазиортогональной матрицы, будут отличаться местами расположения элементов со значением -1 .

Элементу со значением 1 поставим в соответствие a , а элементу со значением -1 , соответственно, $-b$. Тогда циркулянт Мерсенна порядка 3 , вычисленный через квадратичные вычеты, будет представлен как

$$\mathbf{M} = \begin{bmatrix} a & a & -b \\ -b & a & a \\ a & -b & a \end{bmatrix}.$$

Портреты трех циркулянтов Мерсенна приведены на рис. 1. Здесь и далее на рисунках поле черного цвета соответствует значению элемента $-b$ (-1), а поле белого цвета — значению элемента 1 .

Вычислением произведения

$$\mathbf{M} \times \mathbf{M}^T = \begin{bmatrix} a^2 + b^2 & a^2 - b^2 \\ a^2 - b^2 & a^2 + b^2 \end{bmatrix}$$

и решением недиагонального уравнения, при равенстве его нулю, находим значение b . Для каждой i -й строки, $i = 2, 3, \dots$, последовательно вычисляем АКФ для выбора наиболее удачного кода.

В качестве основы получения кодов можно использовать циркулянты Рагхаварао (\mathbf{R})



Рис. 1. Портреты циркулянтов Мерсенна порядков 3, 7 и 11

[14], которые с максимальным детерминантом будут удовлетворять уравнению $\mathbf{R}^T \mathbf{R} = = (n - 1)\mathbf{I} + \mathbf{O}$, где \mathbf{R} — искомая целочисленная матрица из элементов со значениями 1 и -1 , а \mathbf{I} и \mathbf{O} — единичная матрица и матрица, состоящая из всех единиц соответственно. В качестве примера на рис. 2 приведены портреты двух циркулянтов Рагхаварао.

Построение таких матриц основано на том, что если произведение $\mathbf{R}^T \mathbf{R}$ имеет квазидиагональную форму с элементами на диагонали d и вне ее $s < d$, то определитель будет $\det(\mathbf{R}^T \mathbf{R}) = \det(\mathbf{R})^2 = (d - s)^{n-1}(d + s(n - 1))$. Из условия положительности квадрата детерминанта следует $s = -1$ и $d = n$ или $s > 0$. При этом максимум значения детерминанта приходится на случаи $s = 1$ и $d = n$ (для нечетного n).

Циркулянты максимальной длины

Циркулянты находятся в соответствии с разностными множествами Пэли—Адамара. Для всех таких известных циклических матриц порядка $n = 4t - 1$, где t — натуральное число, значение $(n - 1)$ принадлежит одному из видов последовательностей, связанных с возможностью получения соответствующих кодов:

- $4t - 1 = 2k - 1$, где $k \sim 1$ (m -последовательности),
- $4t - 1 = p$, где p — простое число (коды Мерсенна),
- $4t - 1 = p(p + 2)$, где p и $p + 2$ формируют двойное простое число (коды, сформированные на основе символов Якоби).

Циркулянты первого вида могут быть получены для всех k , если в качестве их верхней строки, задающей циклическую структуру, использовать m -последовательность — последовательность линейного сдвигового регистра максимальной длины с периодом $2k - 1$. Для

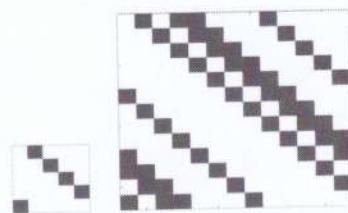


Рис. 2. Портреты циркулянтов Рагхаварао порядков 5 и 13

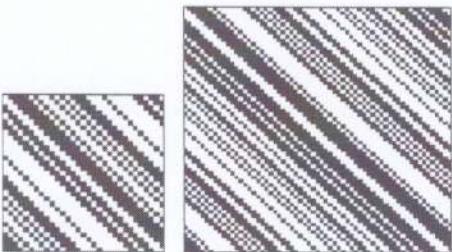


Рис. 3. Портреты циркулянтов порядков 31 и 61

этого необходимо заменить в ней все значения 0 на +1, а 1 на -1.

Портреты таких персимметричных циркулянтов приведены на рис. 3.

Циркулянты второго вида могут быть получены для всех простых чисел $p = 4t - 1$ на основе вычисления квадратичных вычетов, если верхняя строка будет сформирована в виде последовательности:

$$-1, \left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right),$$

где $\left(\frac{a}{p}\right)$ — символ Лежандра. Если a является квадратичным вычетом по модулю p , то символ равен +1, если невычетом — то 1.

Портреты циркулянтов мерсеннова типа, сформированных на основе вычисления символов Лежандра, приведены на рис. 4.

Циркулянты третьего вида могут быть построены на основе вычисления символов Якоби. Если p и q являются разными нечетными простыми числами, то символ Якоби $\left(\frac{a}{pq}\right)$ определяется как произведение символов Лежандра $\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$. Для построения циклических матриц третьего вида при $n - 1 = p(p + 2) = pq$ будем использовать строку, задающую циклическую конструкцию как модификацию последовательности символов Якоби вида $\left\{\left(\frac{0}{pq}\right), \left(\frac{1}{pq}\right), \left(\frac{2}{pq}\right), \dots, \left(\frac{pq-1}{pq}\right)\right\}$.

Здесь символ Якоби используется при ненулевом значении. Для получения строки матрицы следует провести их замену на +1, а для $a \in \{p, 2p, 3p, \dots, (p - 1)p\}$ провести замену на -1.

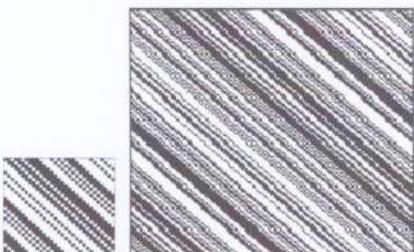


Рис. 4. Портреты персимметричных циркулянтов мерсеннова типа порядков 31 и 127

На рис. 5 для примера приведены портреты двух вычисленных циркулянтов, соответствующих третьему виду для $p = 5$ ($q = 7$) и $p = 11$ ($q = 13$).

Модификация кодовых последовательностей

Приведем пример модификации кодовой последовательности, улучшающей АКФ. Для заранее определенной m -последовательности будем использовать конструкцию матрицы Пэли—Адамара первого вида, которые, как было показано ранее, могут быть получены для всех $n - 1$. Для достижения результата модификации выполним ряд действий.

Шаг 1. На основе m -последовательности с периодом $N = 2k - 1$ сформируем циркулянт, перемещая ее по строкам со сдвигом по фазе в каждой из них.

Для $N = 15$ такой циркулянт представлен ниже:

1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
0	1	0	0	0	1	1	1	1	0	1	0	1	1	0
0	0	1	0	0	0	1	1	1	1	0	1	0	1	1
1	0	0	1	0	0	0	1	1	1	1	0	1	0	1
1	1	0	0	1	0	0	0	1	1	1	1	0	1	0
0	1	1	0	0	1	0	0	0	1	1	1	1	0	1
1	0	1	1	0	0	1	0	0	0	1	1	1	1	0
0	1	0	1	1	0	0	1	0	0	0	1	1	1	1
1	0	1	0	1	1	0	0	1	0	0	0	1	1	1
1	1	0	1	0	1	1	0	0	1	0	0	0	1	1
1	1	1	0	1	0	1	1	0	0	1	0	0	0	1
1	1	1	1	0	1	0	1	1	0	0	1	0	0	0
0	1	1	1	1	0	1	0	1	1	0	0	1	0	0
0	0	1	1	1	1	0	1	0	1	1	0	0	1	0
0	0	0	1	1	1	1	0	1	0	1	1	0	0	1

Шаг 2. Заменой всех элементов со значением 0 на -1 , а со значением 1 — на $+1$ получим матрицу вида:

$$\begin{bmatrix} +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & +1 & -1 & -1 \\ -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & +1 & -1 \\ -1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 \\ -1 & +1 & +1 & -1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 \\ +1 & -1 & +1 & +1 & -1 & -1 & +1 & -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 \\ -1 & +1 & -1 & +1 & +1 & -1 & -1 & +1 & -1 & -1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & +1 & -1 & -1 & +1 & -1 & -1 & +1 & +1 & +1 & +1 \\ +1 & +1 & -1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & +1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & -1 & +1 & -1 \\ -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 & -1 \\ -1 & -1 & +1 & +1 & +1 & +1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ -1 & -1 & -1 & +1 & +1 & +1 & +1 & -1 & -1 & +1 & -1 & +1 & -1 & -1 & +1 \end{bmatrix}$$

Шаг 3. Заменой всех элементов, имеющих значение -1 , на неопределенное значение $-b$, получим матрицу:

$$\begin{bmatrix} +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b \\ -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b \\ -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 \\ +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 \\ +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b \\ -b & +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 \\ +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 & -b \\ -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 & +1 \\ +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 & +1 & +1 \\ +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b & -b & +1 \\ +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b & -b \\ -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b & -b \\ -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 & -b \\ -b & -b & -b & +1 & +1 & +1 & +1 & -b & +1 & -b & +1 & +1 & -b & -b & +1 \end{bmatrix}$$

Шаг 4. Полученную матрицу умножим на ее транспонированную матрицу. В результирующей матрице элементы главной диагонали равны $8 + 7b^2$, а все прочие элементы равны $4 - 8b + 3b^2$.

Для нахождения $-b$ из этого произведения решим квадратное уравнение, приравняв произвольный элемент матрицы, не принадлежащий главной диагонали, к нулю. Выберем наименьший корень данного уравнения, который в приведенном примере $b = 2/3$ ($-b = -2/3$). Полученное значение $-b$ проверяем и сравниваем с первоначально заданной m -последовательностью.

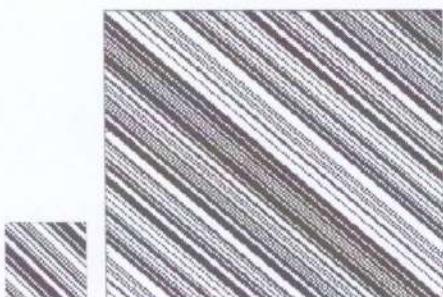


Рис. 5. Портреты персимметричных циркулянтов порядков 35 и 143, сформированных на основе символов Якоби

Сравнение нормированных к единице АКФ обычной и модифицированной m -последовательностей, приведенных на рис. 6, показывает повышение вероятности правильного обнаружения модифицированной последовательности на фоне помех.

Вычислительные эксперименты для модифицированных последовательностей максимальной длины, полученных из циркулянтов мерсеннова типа (см. рис. 4) и сформированных на основе символов Якоби (см. рис. 5), показали аналогичные улучшения АКФ.

Заключение

В работе рассмотрены механизмы формирования циркулянтов — персимметричных циклических квазиортогональных матриц пяти видов. На основе этих циркулянтов осуществлен поиск новых модифицированных кодов.

Приведены особенности нахождения пар значений элементов a и b новой модифицированной кодовой последовательности максимальной длины, применение которых определяет результат маркирования сигнально-кодовых конструкций.

Результат проведенного исследования показывает, что коды, получаемые на основе персимметричных квазиортогональных циркулянтов, обеспечивают большую помехоустойчивость сигналов в радиоканалах, а также повышение вероятности их правильного обнаружения на фоне внешних помех.

Полученные результаты позволяют сделать предположение о целесообразности и эффективности применения рассмотренных новых

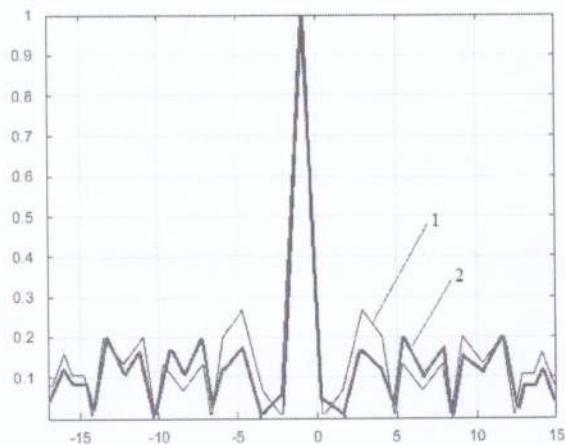


Рис. 6. АКФ для m -последовательности (1) и ее модификации (2) при $N=15$

модифицированных кодов для амплитудной и фазовой модуляции радиосигнала.

Наиболее интересны полученные результаты для синтеза сверхширокополосных сигнально-кодовых конструкций, модулированных полученными модифицированными кодовыми последовательностями. Конечно, для их применения необходима разработка специальных алгоритмов обработки таких сложных сигналов, учитывающих особенности радиолокационных и телеметрических каналов.

СПИСОК ЛИТЕРАТУРЫ

1. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge University Press, 2010. 504 p.
2. Levanon N., Mozeson E. Radar Signals. John Wiley & Sons, Inc. 2004. 411 p.
3. Ахмед Н., Рао К.Р. Ортогональные преобразования при обработке цифровых сигналов: Пер. с англ. / Под ред. И.Б. Фоменко. М.: Связь, 1980.
4. Сергеев А.М., Блауиштейн Н.Ш. Ортогональные матрицы симметричных структур для задач обработки изображений // Информационно-управляющие системы. 2017. № 6 (91). С. 2–8. DOI: 10.15217/issn1684-8853.2017.6.2.
5. Сергеев А.М., Востриков А.А. Специальные матрицы: вычисление и применение. СПб: Политехника, 2018. 112 с.
6. Balonin N.A., Sergeev M.B., Vostrikov A.A. Conjecture of maximum determinant matrices with orders equal to prime Fermat numbers // Информационно-управляющие системы. 2020. No 2. P. 2–7. DOI: 10.31799/1684-8853-2020-2-2-7.
7. Neubauer M.G., Radcliffe A.J. The maximum determinant of ± 1 matrices // Linear Algebra and its Applications. 1997. V. 257. No 1–3. P. 289–306.
8. Popescu O., Rose Ch., Popescu D. Maximizing the determinant for a special class of block-partitioned matrices //

- Mathematical Problems in Engineering. 2004. No 1. P. 49—61.
9. Barba G. Intorno al Teorema di Hadamard sui Determinanti a Valore Massimo // Giorn. Mat. Battaglini. 1933. V. 71. P. 70—86.
10. Ненашев В.А., Сергеев А.М., Капранова Е.А. Исследование и анализ автокорреляционных функций кодовых последовательностей, сформированных на основе моноциклических квазиортогональных матриц // Информационно-управляющие системы. 2018. № 3. С. 9—14. <https://doi.org/10.31799/1684-8853-2018-4-9-14>
11. Ненашев В.А., Сергеев А.М., Сергеев М.Б. Вложенные кодовые конструкции Баркера—Мерсенна—Рагхавара // Информационно-управляющие системы. 2019. № 3. С. 63—73. DOI: 10.31799/1684-8853-2019-3-63-73.
12. Востриков А.А., Балонин Ю.Н., Куртянин Д.В., Сергеев А.М., Синицына О.И. О гибридном методе защиты видеоданных в IP-сетях // Телекоммуникации. 2018. № 2. С. 34—39.
13. Raghavarao D. Some optimum weighing designs // Ann. Math. Statist. 1959. V. 30. P. 295—303.
14. Balonin, N., Sergeev M. Quasi-Orthogonal Local Maximum Determinant Matrices // Applied Mathematical Sciences. 2015. V. 9. No 8. P. 285—293.
15. Lee M.H. Jacket Matrices: Constructions and Its Applications for Fast Cooperative Wireless Signal Processing. LAP LAMBERT Publishing, Germany, 2012.
16. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Use of symmetric Hadamard and Mersenne matrices in digital image processing // Procedia Computer Science. 2018. P. 1054—1061. DOI: 10.1016/j.procs.2018.08.042.
17. Ryser H.J. Combinatorial Mathematics. The Carus Mathematical Monographs, Published by the Mathematical Association of America. N. Y.: John Wiley & Sons, 1963. No 14. 162 p.
18. Балонин Н.А., Сергеев М.Б. Расширение гипотезы Райзера на двуциклические структуры и разрешимость матриц Аламара орнаментом в виде бицикла с двойной каймой // Информационно-управляющие системы. 2017. № 1. С. 2—10. DOI: 10.15217/issn1684-8853.2017.1.2.
19. Сергеев А.М. Обобщенные матрицы Мерсенна и гипотеза Балонина // Автоматика и вычислительная техника. 2014. № 4. С. 35—41.

ВНИМАНИЕ!

В связи с участвующими случаями распространения контрафактной продукции и нене выполнения договорных обязательств со стороны некоторых подписных агентств убедительная просьба оформлять подписку только в рекомендованных агентствах (список агентств приведен ниже). Также напоминаем, что все журналы, выпускаемые ООО «Наука и технологии», снабжены голограммой на первой сторонке обложки. При отсутствии голограммы просьба незамедлительно сообщать об этом в издательство по тел. (495)223-09-10 или e-mail: market@nait.ru.

Рекомендованные подписные агентства:

ООО «УРАЛ-ПРЕСС», ООО «АГЕНТСТВО «КНИГА-СЕРВИС», ООО «ИНФОРМ-НАУКА».