УДК 519.61:511-33
DOI

Н. А. Балонин, д-р техн. наук, **Ю. Н. Балонин, А. А. Востриков,** канд. техн. наук (Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»), **М. Б. Сергеев,** д-р техн. наук (Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения»; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»);
e-mail: korbendfs@mail.ru

ВЫЧИСЛЕНИЕ МАТРИЦ МЕРСЕННА–УОЛША

Приводится модифицированный метод Пэли вычисления матриц Мерсенна при значениях порядка, равных нечетным простым числам. Рассматриваются примеры сортировок матриц Мерсенна, позволяющих вычислить полную систему функций. Приводится сравнение систем функций Уолша и Мерсенна–Уолша по их особенностям и области применения. Отмечается эффективность развиваемого направления для построения полосовых фильтров.

Ключевые слова: ортогональные матрицы; квазиортогональные матрицы; функции Уолша; матрицы Адамара; модифицированный метод Пэли; матрицы Мерсенна; мирицы Мерсенна–Уолша.

N. A. Balonin, Y. N. Balonin, A. A. Vostrikov (Saint-Petersburg University of Aerospase Instrumentation), **M. B. Sergeev** (Saint-Petersburg University of Aerospase Instrumentation; Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics)

COMPUTATION OF MERSENNE–WALSH MATRICES

***Purpose*:** *The paper deals with the problem of basic generalizations of Hadamard matrices associated with maximum determinant matrices or not optimal by determinant matrices with orthogonal columns* (*weighing matrices*, *Mersenne and Euler matrices*, *ets.*); *quasi-orthogonal local maximum determinant Mersenne matrices studied not enough sufficiently. The goal of this paper is to develop theory of Mersenne matrices on the research results of generalized Walsh functions.* ***Methods*:** *Extreme solutions have been established by minimization of maximum of absolute values of the elements of the matrices followed its subsequent classification according to the quantity of levels and its values depending on orders.* ***Results*:** *Computation of Mersenne matrices of odd prime orders by modified method of Paley have been proposed. The conjecture accordingly existence of all Mersenne matrices of odd order have been formulated. The examples of sorted Mersenne matrices allowing to calculate the whole system of basis functions have been observed. The two systems of Walsh and Mersenne–Walsh basis functions have been compared by their characteristics and applications.* ***Practical relevance*:** *The efficiency of developing directions to construct the bandpass filters have been commented. Algorithms to construct the Mersenne–Walsh matrices have been implemented in developing software of the research program-complex. Mersenne and Fermat Filters based on the suboptimal by determinant matrices have been used for the masking and image compression.*

Keywords: Orthogonal matrices; Quasi-orthogonal matrices; Walsh functions; Hadamard matrices; Paley method; Mersenne matrices; Mersenne–Walsh matrices.

Введение

В [1] раскрыты результаты применения программного комплекса «MMatrix-2» для генерации и изучения свойств специализированных ортогональных (квазиортогональных) базисов, предназначенных для обработки изображений. Алгоритмическая составляющая комплекса и теоретические основы **M**-матриц (матриц локального максимума детерминанта) подробно рассмотрены в [2] и [3, 4] соответственно.

Характеризуя актуальность рассматриваемой в статье задачи, отметим следующее: функции Мерсенна–Уолша и их обобщения не относятся к числу широко известных функций, что делает интересным их применение для задач коммуникаций, помехоустойчивого и защитного кодирования, обработки сигналов, сжатия и (или) маскирования изображений [5, 6]. Теория квазиортогональных матриц, начавшая формироваться в [3, 4, 7], сегодня подкреплена алгоритмами, программами и опытом применения поисковых вычислительных комплексов вида «MMatrix-2» [1].

Для многих приложений вычислительной математики, теории кодирования, цифровой обработки сигналов и т.д. важным требованием является простота, т.е. конечность множества значений функций ортонормированных систем. Первая из таких систем – система Радемахера [8] – была построена в 1922 г. как существенно упрощенный аналог тригонометрической системы функций.

Функции Радемахера (меандры) имеют всего два значения {1, –1}. Их недостаток – система неполна и, следовательно, не является базисом в гильбертовом пространстве L_2. Полная система впервые была введена Дж. Уолшем в 1923 г. [9]. В отличие от функций Радемахера функции Уолша можно разделить на четные и нечетные, этим они аналогичны синусам и косинусам. В 1932 г. Р. Пэли предложил иной порядок их нумерации [10], оказавшийся удобным для вычисления. Помимо этого существует упорядочение по Адамару, также важное при рассмотрении данной темы.

Матрицы Адамара – квазиортогональные матрицы с элементами {1, –1} [11]. Они ортогональны при условии нормирования их столбцов. Так как векторы-столбцы образуют базис, они порождают полную систему функций, которую называют системой функций Уолша, если столбцы нумеруются по количеству смены знаков их элементов (аналог частоты). Работа Хармута 1969 г. [12] свидетельствует о начале применения изначально сугубо теоретических функций Уолша в прикладных задачах коммуникаций. Примерно в это же время матрицы Адамара нашли непосредственное применение в помехоустойчивом кодировании информации в каналах радиосвязи для обеспечения полетов космических автоматизированных станций к Марсу [13]. Эти и другие применения стимулировали интерес к обобщенным теориям ортогональных базисов на их основе и новым системам функций.

Система функций Мерсенна–Уолша

Обобщенным матрицам Адамара посвящено огромное число работ. Обзор важных обобщений таких матриц на нечетные порядки впервые представлен в [4]. В [14] определен класс квазиортогональных матриц Адамара–Мерсенна порядков, равных числам Мерсенна $n = 2^k - 1$. Позднее теория построения таких матриц изучалась подробно в [15]. В [16] высказана гипотеза их существования для всех значений нечетных порядков $n = 4k - 1$, исследованная в [17].

Определение 1. Матрицу Мерсенна, порождаемую упорядоченными по частоте столбцами, будем называть матрицей Мерсенна–Уолша, а систему ортогональных функций, генерируемых на основе упорядоченной матрицы, – системой функций Мерсенна–Уолша, в отличие от классических функций Уолша.

Для большей наглядности на рис. 1 в виде сигналов (меандров) представлены, например, столбцы матрицы Мерсенна седьмого порядка. Ортогональные функции принимают два значения $\{1, -b\}$, $b < 1$.

Перечислим отличительные особенности такой системы ортогональных функций и назовем причины, по которым этот базис сигналов может быть интересным.

Система функций Мерсенна–Уолша – двухуровневая, такая же, как и классическая система. Она отличается от функций Уолша пониженным по амплитуде нижним значением $-b$, которое с ростом размерности системы стремится к –1. В этом смысле она отличается от системы функций Уолша, но является достаточно близкой аппроксимацией ее на нечетных значениях порядка. Систему функций Мерсенна–Уолша отличает также пониженное

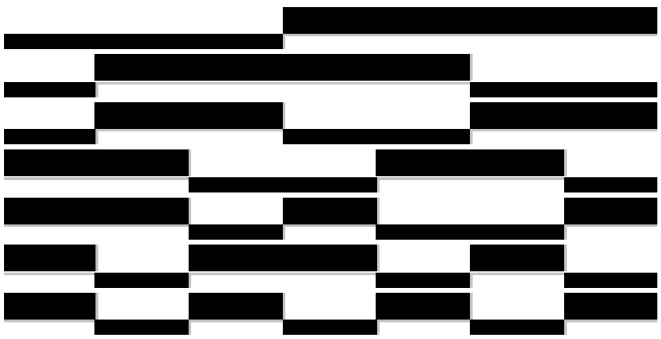


Рис. 1. Столбцы матрицы M_7 в виде сигналов (меандров)

на единицу число порождающих ее элементов столбцов матрицы Мерсенна, т.е. она проще классической для вычисления.

Любой базис отличает предпочтительная область его применения. Система функций Мерсенна–Уолша более высокочастотная, чем система функций Уолша, в ее составе нет функции нулевой частоты (константы). Таким образом, для построения полосовых фильтров изображений первая предпочтительнее.

Первые единичные столбец и строка нормализованных матриц Адамара представляют собой ненужную составляющую, которая у полосовых фильтров никакой нагрузки не несет, поскольку отвечает фильтрующейся ими частоте и означает лишние затраты процессорного времени. Однако простое удаление канвы матрицы Адамара отбрасыванием ее первых строки и столбца нарушает ортогональность столбцов усеченной матрицы.

Матрицы Мерсенна–Уолша

Рассмотрим матрицы Мерсенна–Уолша и способы их эффективного вычисления. Матрицы Мерсенна–Уолша, так же как и матрицы Адамара–Уолша, можно получить сортировкой по частоте столбцов матриц Мерсенна [4, 14] и Адамара [11] соответственно.

Обобщением способов вычисления матриц Адамара занимался еще Р. Пэли. В 1933 г. он нашел алгоритмы [18], существенно повышающие множество вычисляемых квазиортогональных матриц с уровнями $\{1, -1\}$.

Уточним понятие квазиортогональных матриц, к которым искомые матрицы принадлежат.

Определение 2. Квазиортогональной матрицей $\mathbf{A}_n$ будем называть квадратную матрицу порядка n, значения элементов каждого столбца которой ≤ 1 (максимальный элемент равен единице), удовлетворяющую условию связи столбцов вида

$$\mathbf{A}_n^{\mathrm{T}}\mathbf{A}_n = \omega\mathbf{I}, \qquad (1)$$

где $\mathbf{I}$ – единичная диагональная матрица; ω – вес матрицы.

Вес $\omega = 1$ характерен для ортогональных матриц, к которым квазиортогональные матрицы, в том числе и матрицы Адамара, не относятся из-за ограничения на значения их элементов. Эти матрицы весьма близки к ортогональным, получаемым из $\mathbf{A}$ элементарным нормированием их строк и столбцов, после чего их максимальный элемент (m-норма) [4] уменьшается до $m < 1$ для порядков $n > 1$.

Определение 3. M-матрицами (минимаксными квазиортогональными матрицами) будем называть матрицы (1), обладающие минимумом m-нормы (глобальным или локальным) на классе квазиортогональных матриц порядка n

$$|\det(\mathrm{A}_n)| = \omega^{n/2}, \text{ причем } \omega = 1/m^2.$$

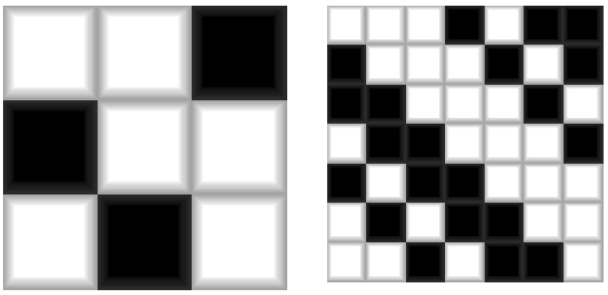
Матрицы Адамара, обладающие глобальным максимумом детерминанта, имеют минимальное значение m-нормы, т.е. являются частным случаем **M**-матриц с весом $\omega = n$.

Матрицы Мерсенна, оставаясь двухуровневыми, отличаются от матриц Адамара лишь величинами их элементов: для матриц Адамара элементы имеют значения $\{1, -1\}$, для матриц Мерсенна – $\{1, -b\}$, где $b = 1/2$ при $n = 3$, а в остальных случаях $b = \dfrac{q - \sqrt{4q}}{q - 4}$ при $q = n + 1$ (порядок сопутствующих матриц Адамара).

Матрицы Мерсенна находятся при помощи универсальных поисковых алгоритмов программного комплекса «MMatrix-2» [1]. Универсальные алгоритмы и соответствующие программы эффективны в широкой области исследования, использующего экстремальные особенности квазиортогональных матриц – локальный максимум детерминанта [4]. Программный комплекс удобен для идентификации систем ортогональных функций, сопоставительного изучения их особенностей, построения необходимых графиков и т.д. Для прикладной области нужны намного более быстродействующие специализированные вычислительные алгоритмы, основанные на иных принципах.

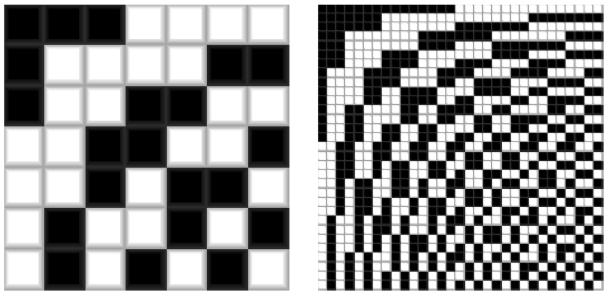
Способы быстрого вычисления матриц Мерсенна и Мерсенна–Уолша опираются на методы теории чисел, впервые замеченные Пэли [11]. Подход Пэли может быть использован для вычисления матриц Мерсенна, но после модификации, состоящей в следующем.

Пусть n – простое число, задающее порядок $n = 4k - 1$ матрицы Мерсенна $\mathbf{M}_n$. Тогда это необходимое и достаточное условие существования квазиортогональной кососимметрической циклической матрицы Мерсенна порядка n с элементами, равными символам Лежандра $\chi(j - i/n) = \{1, -b\}$, вычисленным для разностей индексов i, j, их строк и столбцов [16].



а) *б)*

Рис. 2. Портреты циклических матриц $\mathbf{M}_3$ (*а*) и $\mathbf{M}_7$ (*б*)



а) *б)*

Рис. 3. Портреты упорядоченных матриц $\mathbf{M}_7$ (*а*) и $\mathbf{M}_{31}$ (*б*)

Символы Лежандра $\chi(m/n)$ принимают единичное значение, если $m = j - i$ является квадратичным вычетом по модулю n или 0, и значение $-b$, если m – квадратичный невычет по модулю n. Здесь b – абсолютное значение отрицательных элементов матрицы Мерсенна.

Пример. Рассмотрим построение матрицы Мерсенна $\mathbf{M}_7$, связанное с нахождением символов Лежандра для набора чисел {0, 1, 2, 3, 4, 5, 6}, равных разностям индексов элементов первой строки. Их квадраты по модулю 7 равны {0, 1, 4, 2, 2, 4, 1} соответственно. Числа {1, 2, 4}, присутствующие в обоих наборах, представляют собой квадратичные вычеты, а остальные – невычеты.

Портреты циклических матриц Мерсенна $\mathbf{M}_3$ (*а*) и $\mathbf{M}_7$ (*б*) приведены на рис. 2. Белый квадрат на портрете соответствует элементу с единичным значением, а черный – элементу $-b$, где $b = 1/2$ при $n = 3$; $b = 2 - \sqrt{2} \cong 0{,}5857$ при $n = 7$.

Поскольку матрицы Мерсенна двухуровневые (содержат элементы только двух значений $\{1, -b\}$), умножение на –1 для них запрещено. Поэтому сводимость к функциям, близким по смыслу к функциям Уолша, для них не очевидна. Однако матрицы Мерсенна допускают рациональное упорядочивание их строк и столбцов перестановками, результаты которых, например, представлены на рис. 3 портретами упорядоченных матриц $\mathbf{M}_7$ (*а*) и $\mathbf{M}_{31}$ (*б*).

Заключение

Разработана новая система ортогональных функций Мерсенна–Уолша, предназначенная для применения в алгоритмах обработки изображений, в том числе при построении полосовых фильтров, используемых для сжатия информации в методах маскирования [5]. Для вычисления системы ортогональных функций Мерсенна–Уолша использованы глубоко проработанные в теории чисел алгоритмы вычисления символов Лежандра.

В силу вариативности иррационального в общем уровне b матрицы при изменении порядка n, попытки демаскирования защищенного изображения третьими лицами более затруднительны в сравнении с применением целочисленных матриц Адамара [6]. При этом ресурсы на хранение или вычисление варьируемого уровня b невелики, что важно для применения результатов исследования в системах встраиваемого класса [19].

Матрицы Мерсенна и Мерсенна–Уолша вычислялись в программном комплексе [1, 2] универсальными алгоритмами, в основе которых лежат модифицированные методы Пэли и Сильвестра [14]. Рассматриваемый комплекс применим также и для матриц порядков, выражаемых простыми числами.

Библиографический список

1. **Балонин Ю. Н.** Программный комплекс MMatrix-2 и найденные им М-матрицы // Вестник компьютерных и информационных технологий. 2013. № 10. С. 58 – 64.

2. **Балонин Ю. Н., Сергеев М. Б.** Алгоритм и программа поиска и исследования М-матриц // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3. С. 82 – 86.

3. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14 – 21.

4. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1. С. 2 – 15.

5. **Балонин Ю. Н., Востриков А. А., Сергеев М. Б.** О прикладных аспектах применения М-матриц //

Информационно-управляющие системы. 2012. № 1. С. 92 – 93.

6. **Востриков А. А., Чернышев С. А.** Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99 – 103.

7. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара–Ферма // Информационно-управляющие системы. 2012. № 6. С. 90 – 93.

8. **Rademacher H.** Einige Sätze über Reihen von allgemeinen Orthogonalfunktionen // Math. Ann. 1922. V. 87, № 1–2. P. 112 – 138.

9. **Walsh J. L.** A Closed Set of Normal Orthogonal Functions // Amer. J. Math. 1923. V. 45. P. 5 – 24.

10. **Paley R. E. A. C.** A Remarkable Series of Orthogonal Functions. I, II // Proc. Lond. Math. Soc. 1932. V. 34. P. 241 – 279.

11. **Hadamard J.** Résolution d'une question relative aux déterminants // Bulletin des Sciences Mathématiques. 1893. № 17. P. 240 – 246.

12. **Harmuth H. F.** Applications of Walsh Functions in Communications // IEEE Spectrum. 1969. № 6. P. 82 – 91.

13. **Eliahou S.** La conjecture de Hadamard (I) – Images des Mathématiques // CNRS. 2012 [Электронный ресурс]. URL: http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (дата обращения: 15.09.2014).

14. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара–Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92 – 94.

15. **Балонин Н. А., Сергеев М. Б.** О двух способах построения матриц Адамара–Эйлера // Информационно-управляющие системы. 2013. № 1. С. 7 – 10.

16. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5. С. 2 – 8.

17. **Балонин Н. А.** О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 89–90.

18. **Paley R. E. A. C.** On orthogonal matrices // Journal of Mathematics and Physics. V. 12. 1933. P. 311 – 320.

19. **Информационно-управляющие** системы на основе INTERNET / А. М. Астапкович и др. // Информационно-управляющие системы. 2002. № 1. С. 12 – 18.

Библиографический список

1. **Балонин Ю. Н.** Программный комплекс MMatrix-2 и найденные им М-матрицы // Вестник компьютерных и информационных технологий. 2013. № 10. С. 58 – 64.

2. **Балонин Ю. Н., Сергеев М. Б.** Алгоритм и программа поиска и исследования М-матриц // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3. С. 82 – 86.

3. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14 – 21.

4. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1. С. 2 – 15.

5. **Балонин Ю. Н., Востриков А. А., Сергеев М. Б.** О прикладных аспектах применения М-матриц // Информационно-управляющие системы. 2012. № 1. С. 92 – 93.

6. **Востриков А. А., Чернышев С. А.** Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5. С. 99 – 103.

7. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара – Ферма // Информационно-управляющие системы. 2012. № 6. С. 90 – 93.

8. **Rademacher H.** Einige Sätze über Reihen von allgemeinen Orthogonalfunktionen // Math. Ann. 1922. V. 87, № 1 – 2. P. 112 – 138.

9. **Walsh J. L.** A Closed Set of Normal Orthogonal Functions // Amer. J. Math. 1923. V. 45. P. 5 – 24.

10. **Paley R. E. A. C.** A Remarkable Series of Orthogonal Functions. I, II // Proc. Lond. Math. Soc. 1932. V. 34. P. 241 – 279.

11. **Hadamard J.** Résolution d'une question relative aux déterminants // Bulletin des Sciences Mathématiques. 1893. № 17: P. 240 – 246.

12. **Harmuth H. F.** Applications of Walsh Functions in Communications // IEEE Spectrum. 1969. № 6. P. 82 – 91.

13. **Eliahou S.** La conjecture de Hadamard (I) – Images des Mathématiques // CNRS. 2012 [Электронный ресурс]. URL: http://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html (дата обращения: 15.09.2014).

14. **Балонин Н. А., Сергеев М. Б., Мироновский Л. А.** Вычисление матриц Адамара – Мерсенна // Информационно-управляющие системы. 2012. № 5. С. 92 – 94.

15. **Балонин Н. А., Сергеев М. Б.** О двух способах построения матриц Адамара – Эйлера // Информационно-управляющие системы. 2013. № 1. С. 7 – 10.

16. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5. С. 2 – 8.

17. **Балонин Н. А.** О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2. С. 89 – 90.

18. **Paley R. E. A. C.** On orthogonal matrices // Journal of Mathematics and Physics. V. 12. 1933. P. 311 – 320.

19. **Информационно-управляющие** системы на основе INTERNET / А. М. Астапкович и др. // Информационно-управляющие системы. 2002. № 1. С. 12 – 18.

Статья поступила в редакцию 03.03.2014 г.