ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

УДК 519.61:511-33

Н. А. Балонин, М. Б. Сергеев

ВЫЧИСЛЕНИЕ МАТРИЦ МЕРСЕННА МЕТОДОМ ПЭЛИ

Приводится модифицированный метод Пэли вычисления матриц Мерсенна при значениях порядка, равных простым числам. Рассматривается пример вычисления матрицы Мерсенна. Приводится сравнение матриц, находимых модифицированными методами Сильвестра и Пэли. Отмечается эффективность развиваемого метода относительно универсальной процедуры поиска *M*-матриц, определяющая сферу приложения метода.

Ключевые слова: *помехоустойчивое кодирование, обработка информации, ортогональные матрицы, квазиортогональные матрицы, матрицы Адамара, матрицы Мерсенна, метод Сильвестра, метод Скарпи, метод Пэли.*

В работе [1] предложено применять квазиортогональные матрицы Адамара—Мерсенна в качестве базиса ортогональных преобразований при маскировании видеоизображений. Матричные преобразования составляют основу так называемого стрип-метода работы с изображениями, рассмотренного в монографии [2].

Ортогональные матрицы, включающие матрицы Фурье и дополняющие их при нормировании столбцов квазиортогональные матрицы Адамара, а также их наиболее близкие интерпретации для четных порядков — матрицы Белевича (конференц-матрицы) и взвешенные матрицы — используются в помехоустойчивом кодировании, спектральном разложении и обработке изображений [3], кодовом разделении каналов связи и защитном маскировании [4] и т.п. Особое значение свойства таких матриц приобретают при аппаратной или микропрограммной реализации указанных преобразований в специализированных процессорах. Поскольку вид матриц, их порядки, значения коэффициентов существенно влияют на выбор соответствующих фильтров, аппаратные затраты и скорость преобразования, то на этапе проектирования процессоров остро стоит задача правильного выбора ортогональных (квазиортогональных) матриц.

В работе [5] определен класс квазиортогональных матриц Адамара—Мерсенна нечетных порядков, равных числам Мерсенна $n=2^k-1$. В работе [6] этот класс расширен квазиортогональными матрицами Мерсенна, была высказана гипотеза их существования для всех значений нечетных порядков $n=4k-1$, исследованная в работе [7]. Настоящая работа развивает положения работы [1] — предложены эффективные (более быстродействующие) алгоритмы генерации квазиортогональных матриц, — раскрывая прикладную сторону употребления асимметричных символов Лежандра.

Уточним определение квазиортогональной матрицы.

Определение 1. Квазиортогональная матрица **A** — квадратная матрица порядка n, максимальное значение модуля элементов каждого столбца которой равно 1, удовлетворяющая условию связи столбцов вида

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

где **I** — единичная диагональная матрица, ω — вес матрицы.

Вес ω = 1 характерен для ортогональных матриц, к которым квазиортогональные матрицы, в том числе и матрицы Адамара, не относятся ввиду ограничения на значения их элементов. Вместе с тем эти матрицы весьма близки к ортогональным, получаемым из **A** элементарным нормированием их строк и столбцов, в результате чего их максимальный элемент (*m*-норма) уменьшается до $m < 1$, для порядков $n > 1$.

Определение 2. M-матрицами (минимаксными квазиортогональными) назовем матрицы (1), обладающие минимумом *m*-нормы (глобальным или локальным) на классе квазиортогональных матриц порядка *n*. Несложно заметить, что $|\det(\mathbf{A})| = \omega^{n/2}$, 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 ω=*n*.

Согласно исследованиям, между матрицами Мерсенна [7] и Адамара [8] нечетных и четных порядков соответственно существует взаимно-однозначное соответствие, предполагающее общность алгоритмов их вычисления. Оставаясь двухуровневыми, они различаются лишь величинами элементов: для матриц Адамара — {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).

В работах [1, 5] приведен модифицированный алгоритм Сильвестра [8] построения матриц Мерсенна, используемых как базис ортогональных преобразований в маскировании изображений. Для повышения порядка матриц Мерсенна служит алгоритм Скарпи [9]. В отличие от алгоритма Сильвестра, он имеет значительно более простую формулировку в приложении к матрицам нечетных порядков, чем к матрицам Адамара четных порядков. Его основу составляет процедура подстановки матрицы Мерсенна с каймой, определяемой значениями вытесняемых элементов (некоторое обобщение операции кронекерова произведения).

В теории матриц Адамара не менее хорошо известны алгоритмы, полученные по методу Пэли [10], модификация которого для поиска матриц Мерсенна, учитывающая особенность их порядка, приведена ниже.

Переопределим значения символов Лежандра $\chi(m/n) = \{1, -b\}$ таким образом, что единичное значение принимается, если *m* — квадратичный вычет по модулю *n* (или 0); −*b*, если *m* — квадратичный невычет по модулю *n*, где *b* — абсолютное значение отрицательных элементов матрицы Мерсенна [5, 6].

Пусть *n* — простое число, задающее порядок *n*=4*k*−1 матрицы Мерсенна. Тогда, как и в случае нахождения матриц Адамара, это необходимое и достаточное условие существования квазиортогональной циклической матрицы Мерсенна порядка *n* ($\mathbf{M}_n$) с элементами, равными символам Лежандра $\chi(j-i/n)$, вычисленным для разностей пар индексов *i*, *j* их строк и столбцов.

Пример. Рассмотрим процедуру построения матрицы Мерсенна $\mathbf{M}_7$, связанного 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}, которые присутствуют в обоих наборах, представляют собой квадратичные вычеты, а остальные — невычеты.

Циклическая матрица Мерсенна $\mathbf{M}_7$ и гистограмма модулей ее элементов приведены на рис. 1 (белый квадрат соответствует элементу с единичным значением, черный — элементу — *b*, где $b = 2 - \sqrt{2} \cong 0{,}5857$).

Отметим, что в случае нечетных порядков *n*=4*k*+1 нахождение подобных двухуровневых матриц методом Пэли невозможно, в этом состоит специфика объекта расчета. Аппроксимировать матрицы Белевича [11] иррациональными матрицами на единицу меньшего

порядка возможно только в рамках трехуровневой структуры, как у матриц Ферма [12], причем, в отличие от матриц Мерсенна и Ферма, результат такой аппроксимации соответствует некоторой седловой точке (которая не всегда существует), а не локальному максимуму детерминанта матрицы.

а) *б)*

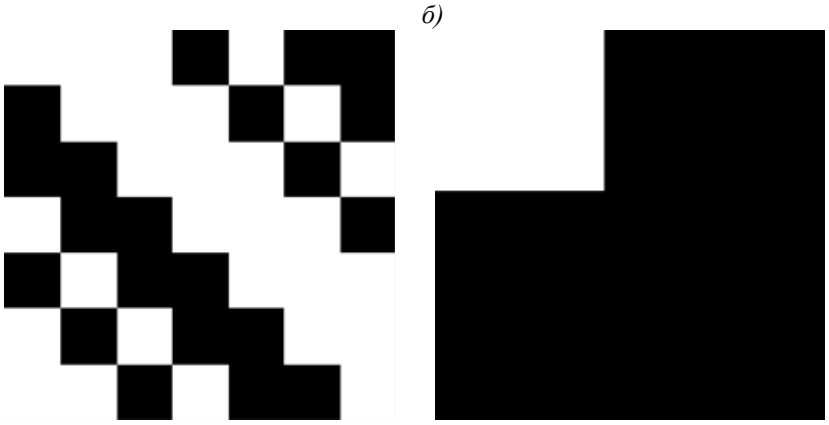

Рис. 1

Модифицированный метод Пэли значительно расширяет возможности вычисления матриц Мерсенна и Эйлера [13] в сравнении с ранее изложенными подходами [1, 5, 14]. В частности, он позволяет вычислить матрицы Мерсенна 11-го и 19-го порядков (порядки — простые числа), найденные в работе [6] методом поиска локального максимума детерминанта [15], соответствующего локальным минимумам *m*-норм этих *M*-матриц [5, 6], при помощи специализированного математического обеспечения [15, 16].

На рис. 2 для сравнения приведены матрицы Мерсенна порядка 31, найденные модифицированными методами Сильвестра и Пэли.

а) *б)*

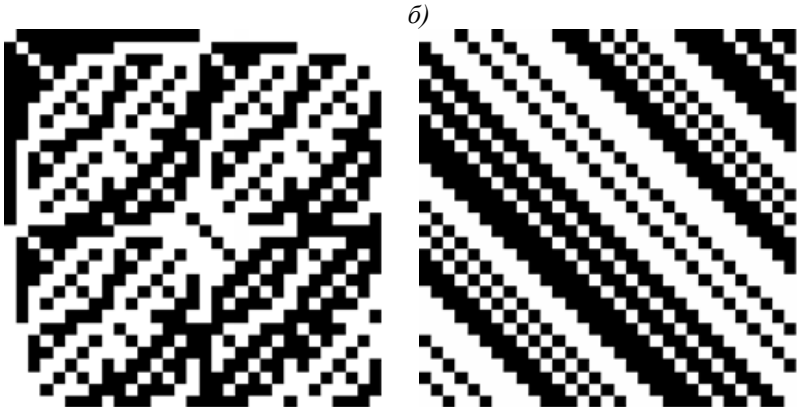

Рис. 2

Стоит обратить внимание на то, что квазиортогональные матрицы глобального и локального максимумов детерминанта не являются, в общем, целочисленными матрицами. На них не распространяются жесткие критерии существования, целиком вытекающие из целочисленности [6, 7].

Неортогональные и не сводимые к ортогональным матрицы абсолютного максимума детерминанта существуют на всех значениях порядков. Квазиортогональные матрицы, особенно матрицы локального максимума детерминанта, обладают сходным свойством. Универсальный метод поиска *M*-матриц [15] вытекает из общего обоснования существования матриц Мерсенна [7] порядков $n=4k-1$ и используется для нахождения редких артефактных *M*-матриц [17—19]. Метод Пэли рассматривается как эффективное средство нахождения матриц Мерсенна при выполнении соответствующего условия — значение порядка матрицы является простым числом.

СПИСОК ЛИТЕРАТУРЫ

1. *Востриков А. А., Балонин Ю. Н.* Матрицы Адамара-Мерсенна как базис ортогональных преобразований в маскировании видеоизображений // Изв. вузов. Приборостроение. 2014. Т. 57, № 1. С. 15—19.

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

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

4. *Ерош И. Л., Сергеев А. М., Филатов Г. П.* О защите цифровых изображений при передаче по каналам связи // Информационно-управляющие системы. 2007. № 5. С. 20—22.

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

6. *Балонин Н. А.* О существовании матриц Мерсенна 11-го и 19-го порядков // Информационно-управляющие системы. 2013. № 2 (63). С. 89—90.

7. *Балонин Н. А., Сергеев М. Б.* К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5 (66). С. 2—8.

8. *Hadamard J.* Résolution d'une question relative aux determinants // Bulletin des Sciences Mathématiques. 1893. N 17. P. 240—246.

9. *Scarpis U.* Sui determinanti di valore Massimo // Rendiconti della R. Istituto Lombardo di Scienze e Lettere 31. 1898. P. 1441—1446.

10. *Paley R. E. A. C.* On orthogonal matrices // J. of Mathematics and Physics. 1933. Vol. 12. P. 311—320.

11. *Belevitch V.* Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. Vol. 26. P. 231—244.

12. *Балонин Н. А., Сергеев М. Б., Мироновский Л. А.* Вычисление матриц Адамара-Ферма // Информационно-управляющие системы. 2012. № 6 (61). С. 90—93.

13. *Балонин Н. А., Сергеев М. Б.* О двух способах построения матриц Адамара-Эйлера // Информационно-управляющие системы. 2013. № 1 (62). С. 7—10.

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

15. *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.

16. *Балонин Ю. Н.* Программный комплекс MMatrix-2 и найденные им М-матрицы // Вестник компьютерных и информационных технологий. 2013. № 10 (112). С. 58—64.

17. *Балонин Ю. Н., Сергеев М. Б.* М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87—90.

18. *Балонин Н. А., Сергеев М. Б.* Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационные управляющие системы. 2013. № 5 (66). С. 97—98.

19. *Балонин Н. А., Сергеев М. Б.* Матрица золотого сечения G_{10} // Информационные управляющие системы. 2013. № 6 (67). С. 2—5.

Сведения об авторах

Николай Алексеевич Балонин — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра вычислительных систем и сетей; E-mail: korbendfs@mail.ru

Михаил Борисович Сергеев — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра вычислительных систем и сетей; заведующий кафедрой; E-mail: mbse@mail.ru

Рекомендована кафедрой вычислительных систем и сетей

Поступила в редакцию 24.02.14 г.