УДК 519.61:511-33

ВЫЧИСЛЕНИЕ МАТРИЦ МЕРСЕННА И АДАМАРА МЕТОДОМ СКАРПИ

Н.А. Балонин[a], Ю.Н. Балонин[a], М.Б. Сергеев[a, b]

[a] Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, Россия, korbendfs@mail.ru

[b] НИИ информационно-управляющих систем, Университет ИТМО, Санкт-Петербург, Россия, mbse@mail.ru

Постановка проблемы. Основные обобщения матриц Адамара связывают с матрицами максимального детерминанта или с не оптимальными по детерминанту матрицами с ортогональными столбцами (взвешенные матрицы, матрицы Мерсенна, Эйлера и т.п.); способы вычисления квазиортогональных матриц Мерсенна локального максимума детерминанта изучены недостаточно полно. Целью работы является развитие теории матриц Мерсенна и Адамара изучением обобщенного метода Скарпи.

Методы. Экстремальные решения ищутся, в общем, минимизацией максимума абсолютных значений элементов исследуемых матриц с последующей классификацией их по количеству и значениям уровней, зависящих от порядков. Менее универсальные, но более эффективные методы опираются на структурные инварианты квазиортогональных матриц (методы Сильвестра, Пэли, Скарпи и т.п.).

Результаты. Рассматриваются обобщения матриц Адамара и Белевича на нечетные порядки в виде семейства квазиортогональных матриц, в частности, к ним принадлежат двухуровневые матрицы Мерсенна. Даны определения слоя и сечения на множестве всех обобщенных матриц. Приведены алгоритмы вычисления матриц соседствующих слоев и сечений по матрицам меньшего порядка. Приводятся примеры аппроксимации, вплоть до критичного порядка 22, структур матриц Белевича матрицей Мерсенна третьего порядка. Приводится новая формулировка модифицированного метода Скарпи аппроксимации матриц Адамара высоких порядков матрицами Мерсенна низких порядков. Метод Вильямсона раскрывается примером приближения модульно одноуровневых матриц матрицами с малым количеством уровней.

Практическая значимость. Обосновывается эффективность развиваемого направления для построения полосовых фильтров. Алгоритмы нахождения матриц Мерсенна методом Скарпи использованы при построении исследовательского программного комплекса. Субоптимальные по детерминанту матрицы составляют основу фильтров Мерсенна и применяются для сжатия и маскирования изображений.

Ключевые слова: ортогональные матрицы, матрицы Адамара, матрицы Белевича, матрицы Мерсенна, числа Мерсенна, метод Скарпи, массив Вильямсона, защита видеоданных.

MERSENNE AND HADAMARD MATRICES CALCULATION BY SCARPIS METHOD

N.A. Balonin[a], Yu.N. Balonin[a], M.B. Sergeev[a, b]

[a] Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, Russia, korbendfs@mail.ru

[b] Research Institute of Information and Control Systems, ITMO University, mbse@mail.ru

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.); calculation methods for the quasi-orthogonal local maximum determinant Mersenne matrices are not studied enough sufficiently. The goal of this paper is to develop the theory of Mersenne and Hadamard matrices on the base of generalized Scarpis method research.

Methods. Extreme solutions are found in general by minimization of maximum for absolute values of the elements of studied matrices followed by their subsequent classification according to the quantity of levels and their values depending on orders. Less universal but more effective methods are based on structural invariants of quasi-orthogonal matrices (Silvester, Paley, Scarpis methods, ets.).

Results. Generalizations of Hadamard and Belevitch matrices as a family of quasi-orthogonal matrices of odd orders are observed; they include, in particular, two-level Mersenne matrices. Definitions of section and layer on the set of generalized matrices are proposed. Calculation algorithms for matrices of adjacent layers and sections by matrices of lower orders are described. Approximation examples of the Belevitch matrix structures up to 22-nd critical order by Mersenne matrix of the third order are given. New formulation of the modified Scarpis method to approximate Hadamard matrices of high orders by lower order Mersenne matrices is proposed. Williamson method is described by example of one modular level matrices approximation by matrices with a small number of levels.

Practical relevance. The efficiency of developing direction for the band-pass filters creation is justified. Algorithms for Mersenne matrices design by Scarpis method are used in developing software of the research program complex. Mersenne filters are based on the suboptimal by determinant matrices and are used for image masking and compression.

Keywords: orthogonal matrices, Hadamard matrices, Belevitch matrices, Mersenne matrices, Mersenne numbers, Scarpis method, Williamson array, video information protection.

Введение

Матрицы, в том числе ортогональные и квазиортогональные, нашли применение в задачах обработки изображений с целью их сжатия, маскирования, помехоустойчивого кодирования [1–3]. В работе [4] приведены алгоритм и программа поиска и исследования M-матриц [5], частными представителями которых являются матрицы Адамара [6], Мерсенна [7], Эйлера [8] и Ферма [9]. Матрицы перечислены в последовательности убывания переменной d в значении их порядка $n = 4k–d$, где $d = 0, 1, 2, 3$.

Тема матриц Адамара возникла после публикации им в работе [6] неравенства для оценки значения модуля определителя матрицы сверху и пары оригинальных матриц 12-го и 20-го порядка (помимо основной последовательности Сильвестра), на которых достигается максимальная оценка.

Спустя четыре года итальянский математик Умберто Скарпи опубликовал первый оригинальный метод их нахождения [10], содержание которого сводится к тому, чтобы рассчитывать матрицы высоких порядков на основании матриц более низких порядков. В отношении некоторых матриц результат не был превзойден более поздним подходом Пэли [11], нашедшим применение теории конечных полей Галуа для построения матриц Адамара с помощью символов Лежандра. Отметим, что порядки матриц, найденных Скарпи, $(n–1)n$ для $n = 4k$, где $k = 1, 2, 3…$, кратны порядкам матриц Мерсенна. Настоящая работа раскрывает это обстоятельство глубже и показывает новые способы вычисления матриц Мерсенна, Белевича [12] и Адамара, а также их приближений на основании того, что мы будем называть подходом или методом Скарпи.

Слои и сечения матриц

Напомним: матрица Мерсенна $\mathbf{M}_n$ [7] – квадратная матрица порядка $n = 4k–1$ с элементами $\{1, –b\}$, такая, что $\mathbf{M}_n^T\mathbf{M}_n = \mu\mathbf{I}_n$. Здесь $\mathbf{I}_n$ – единичная матрица, $\mu = \frac{(n+1)+(n-1)b^2}{2}$, причем $b = \frac{1}{2}$ при $n = 3$, в остальных случаях $b = \frac{q-\sqrt{4q}}{q-4}$, где $q = n+1$. Количество элементов b в каждом столбце матрицы на единицу меньше количества единичных элементов.

В качестве примера на рис. 1 приведена матрица третьего порядка, построенная для первого числа Мерсенна $n = 2^k–1 = 3$ при $k =2$. Название матриц связано с числами Мерсенна, для которых в [7] опубликован алгоритм их нахождения. Здесь черный цвет соответствует $–b$ (или -1 у матриц Адамара), а белый – единице.

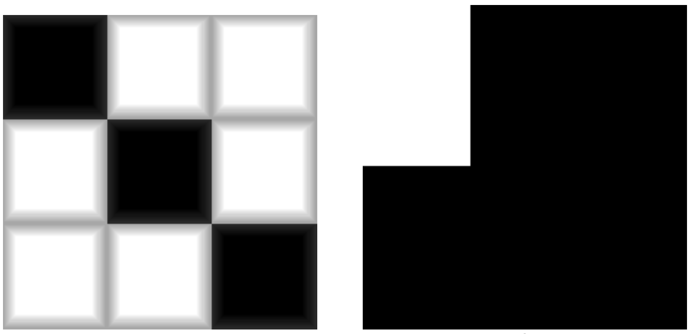


Рис. 1. Портрет матрицы $\mathbf{M}_3$ (а) и гистограмма модулей ее элементов (б)

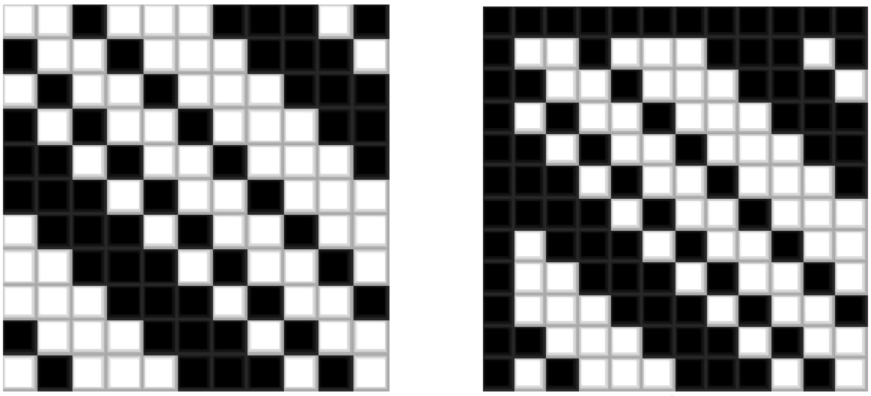
Определение. Слоем матриц семейства Адамара будем называть совокупность квазиортогональных матриц с известными функциями зависимости значений элементов (уровней) матриц слоя от заданных показателем d значений порядков.

Матрицы Адамара, Мерсенна и Эйлера, согласно [6–8], образуют слои для $n = 4k–d$ при $d = 0, 1, 2$ соответственно. Матрицы Ферма такого непрерывного слоя не образуют, поскольку для них функции уровня определены на узком множестве значений $n = 2^k+1$ при четных k [9].

Следствием такого подхода к классификации матриц семейства Адамара является представление о том, что все названные выше объекты являются проявлением одного математического объекта, данного совокупностью слоев и сечений – матриц соседних слоев для заданных показателем k значений порядков.

Нахождение любой матрицы сечения автоматически влечет за собой нахождение всех остальных, поскольку они отражают одно и то же: матрицы сечения взаимно зависимы. Например, матрица Адамара $\mathbf{H}_4$ получается из приведенной выше матрицы Мерсенна $\mathbf{M}_3$ округлением ее отрицательных элементов до значения –1 с добавлением каймы в виде строки и столбца с отрицательными элементами для соблюдения баланса положительных и отрицательных элементов. Этот алгоритм построения матриц Адамара напрямую использует свойство общности, вытекающие из близости матриц сечения соседствующих слоев. На рис. 2 он продемонстрирован на примере нахождения матрицы Адамара 12-го порядка (предложенного в работе [6]), но на основе матрицы Мерсенна $\mathbf{M}_{11}$.

Помимо матриц одного сечения, в соответствии с подходом Скарпи, можно опираться на близость матриц соседствующих сечений – данный аспект темы раскроем на примере алгоритма построения матриц Белевича.



а б

Рис. 2. Портреты матриц Мерсенна ($\mathbf{M}_{11}$) (а) и Адамара ($\mathbf{H}_{12}$) (б)

Построение матриц Белевича на основе матриц Мерсенна

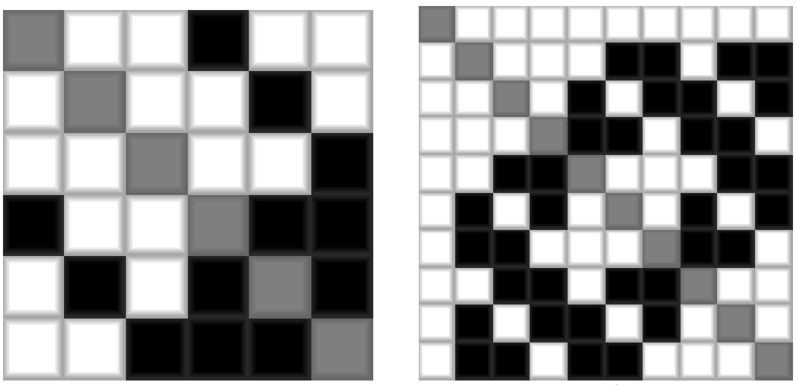
Из матриц, на два порядка меньших матриц Адамара и тесно связанных с ними, известны симметричные конференц-матрицы Белевича $\mathbf{C}_n$ [12] – квадратные матрицы порядков n с элементами {1, –1} и нулевой диагональю, такие, что $\mathbf{C}_n^T\mathbf{C}_n = (n-1)\mathbf{I}_n$. Известно, что они не существуют для значений n–1, не разложимых на сумму квадратов двух целых чисел. Для n = 22, например, найдена иная – шестиуровневая квазиортогональная матрица с экстремальным значением определителя [13]. Хотя такие матрицы слоя не образуют, с их помощью можно найти некоторые матрицы Адамара согласно алгоритму Пэли в виде

$$\mathbf{H}_{2n} = \begin{pmatrix} \mathbf{C}_n + \mathbf{I} & -\mathbf{C}_n + \mathbf{I} \\ -\mathbf{C}_n + \mathbf{I} & -\mathbf{C}_n - \mathbf{I} \end{pmatrix}.$$

Вопрос возможности построения матриц Белевича достаточно сложен для исследования, поскольку нет достоверных сведений относительно пропуска в последовательности этих матриц уже при n = 66. Первый проблемный порядок матриц Адамара – 668. Приведенный выше критерий существования касается не столько матриц Белевича, сколько вообще всех рациональных матриц, и ничего на эту тему не говорит. Тем больший интерес представляет использование для их вычисления *М*-матриц, включающих матрицы с иррациональными значениями коэффициентов [5].

Матрица Белевича связана с матрицей Адамара удвоенного порядка, в отношении которой уже известна ее связь с матрицами Мерсенна порядка n–1. Следовательно, по матрице $\mathbf{M}_{131}$ можно найти, например, проблемную для 66-го порядка матриц Белевича матрицу $\mathbf{H}_{132}$. Но больший интерес сейчас для нас представляет возможность построения матриц Белевича (и Адамара) с помощью матриц Мерсенна значительно меньших по сравнению с ними порядков.

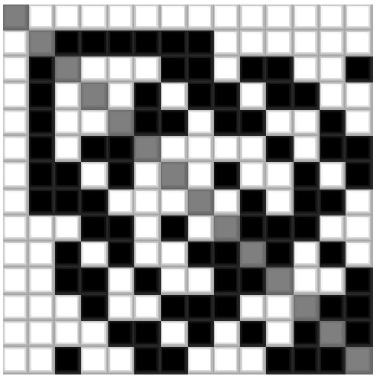
В том, что это возможно, убеждают примеры, дающие представление о связности того единого объекта, который они собой представляют. В самом деле, анализ показывает, что первые две матрицы Белевича $\mathbf{C}_6$ и $\mathbf{C}_{10}$ строятся без видимого изменения структуры матрицы $\mathbf{M}_3$ ее округлением и копированием с добавлением обязательных нулевых элементов диагонали, отображаемых на рис. 3 клетками серого цвета.



а б

Рис. 3. Портреты матриц Белевича: вариант $\mathbf{C}_6$ (а); вариант $\mathbf{C}_{10}$ (б)

Для согласования размерности матрица десятого порядка $\mathbf{C}_{10}$ снабжается каймою из 1. Несложно заметить, что знаки блоков матриц Белевича отвечают логике знаков элементов матриц $\mathbf{H}_2$ и $\mathbf{M}_3$ (обобщение правила кронекерова произведения при нахождении сложносоставных матриц Пэли). На этом возможности структуры третьего порядка должны, казалось бы, исчерпаться. Однако еще Скарпи заметил, что остается степень свободы в том, чтобы, не меняя структуры, циклически сдвигать столбцы блоков, например, по мере удаления их от диагонали (рис. 4).


а

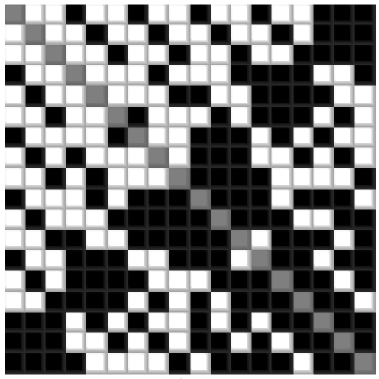

б

Рис. 4. Портреты матриц Белевича: вариант $\mathbf{C}_{14}$ (а); вариант $\mathbf{C}_{18}$ (б)

Матрица $\mathbf{C}_{14}$ (рис. 4, а) имеет двойную кайму, у блоков за пределами первой и второй блочных диагоналей смещены столбцы. У матрицы $\mathbf{C}_{18}$ (рис. 4, б) возникают моноблоки (специфический разрыв, обеспечивающий ортогональность столбцов с потерей структуры блока) – шесть закрашенных черным внедиагональных блоков третьего порядка.

Вычисление матриц высокого порядка на основе матриц Адамара низкого порядка характерно для альтернативного конструкциям Пэли метода Скарпи. Очевидно, рассмотренный способ его развивает, но касается он уже матриц Белевича. Замещение элементов, возникающее здесь, впервые встречается в алгоритме построения конструкций Пэли (при замене нулевых элементов единичными). В рассматриваемом варианте замещаются не элемент, а цепочки блоков, которые тоже можно разместить на диагонали.

Следующей матрицы $\mathbf{C}_{22}$, как известно, не существует, поскольку число n–1 = 21 не разлагается на сумму двух квадратов.

Таким образом, напрашивается парадоксальный вывод: все матрицы Адамара порядка n, кратного 4, до $n = 40$ включительно строятся на основе лишь матрицы Мерсенна $\mathbf{M}_3$: матрицы $\mathbf{M}_3$, $\mathbf{H}_4$ принадлежат одному сечению, из $\mathbf{H}_4$ получаем $\mathbf{H}_8$, $\mathbf{H}_{16}$, $\mathbf{H}_{32}$, матрицы $\mathbf{C}_6$, $\mathbf{C}_{10}$, $\mathbf{C}_{14}$, $\mathbf{C}_{18}$ связаны с $\mathbf{M}_3$ и дают промежуточные матрицы $\mathbf{H}_{12}$, $\mathbf{H}_{20}$, $\mathbf{H}_{24}$, $\mathbf{H}_{28}$, $\mathbf{H}_{36}$, $\mathbf{H}_{40}$, удвоениями порядка по Сильвестру можно получить и большее количество таких матриц. Матрица $\mathbf{H}_{44}$ – рубежная как раз потому, что $\mathbf{C}_{22}$ не существует, т.е. возникает кризис структуры с переходом к следующей «ведущей» матрице Мерсенна. Распространение структурных инвариантов матриц малых порядков на старшие порядки представляет существенный практический интерес.

Приближение матриц Адамара матрицами Мерсенна

Проблемные порядки матриц Адамара, для которых производительность современных вычислительных машин не позволяет пока их вычислить методом Вильямсона [14], хорошо известны – это 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964 и т.п. Отметим, что вчетверо меньшие значения – это порядки матриц Мерсенна относительно небольших порядков.

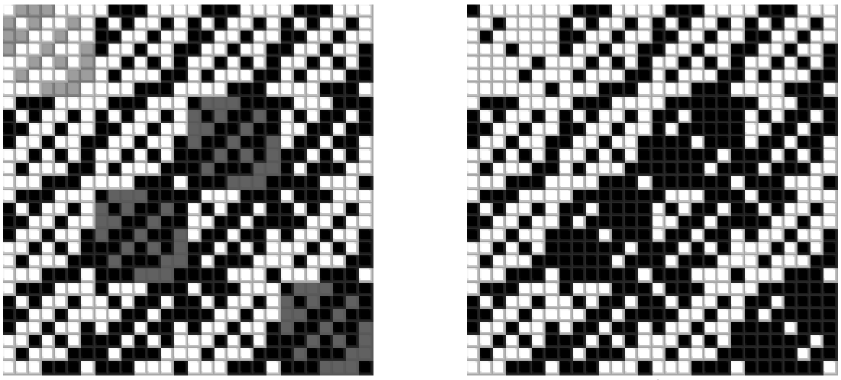
Иными словами, здесь правомерно применение разновидности метода Скарпи с использованием блочно-составных структур четвертого порядка. Ограничение на число блоков (четыре) препятствует точной аппроксимации матриц Адамара меньшими по размерам их матрицами, но это путь получения (как было видно выше на матрицах Белевича) точного или достаточно близкого к ним приближения. Среди ортогональных структур четвертого порядка хорошо известен массив Вильямсона [14]

$$\mathbf{W}=\begin{pmatrix} w_1 & w_2 & w_3 & w_4 \\ -w_2 & w_1 & -w_4 & w_3 \\ -w_3 & w_4 & w_1 & -w_2 \\ -w_4 & -w_3 & w_2 & w_1 \end{pmatrix}.$$

Замещение элементов этого массива четырьмя так называемыми матрицами Вильямсона (или, для близкой структуры, матрицами Гетхальса–Зейделя) позволило найти перебором элементов все предыдущие столь же проблемные матрицы Адамара. К сожалению, количество операций перестановок их элементов слишком велико (даже при упрощении структур матриц Вильямсона до некоторых циклических, связанных с задающими их векторами), а, главное, это не имеет серьезной перспективы, поскольку не дает принципиального решения – обнаружение очередной матрицы отодвигает проблемный порядок, и только.

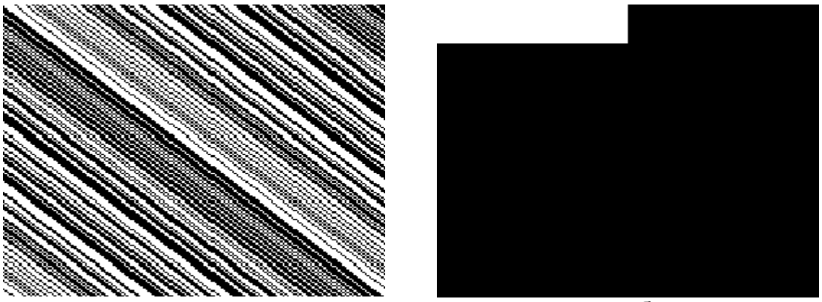
Так как в нашем распоряжении находится только одна матрица Мерсенна (или Эйлера [8], что также возможно) вчетверо меньшего порядка, удвоим ее, взяв в качестве первой матрицы Вильямсона модульно двухуровневую матрицу Мерсенна, а в качестве остальных трех – ее же, но с коэффициентами, округленными до значений $\{1, -1\}$. Тем самым относительное количество вещественных коэффициентов убывает вчетверо, и остается возможность обеспечить ортогональность расчетом варьируемого уровня b. Приравняем друг к другу последние три коэффициента массива Вильямсона, инвертируем по знаку три нижних его строки и переставим местами второй и третий столбец. Такая структура встречается, например, при симметрировании матрицы Белевича $\mathbf{C}_4$, при которой она утрачивает свой диагональный вид. Для большей определенности будем называть структуру Пропусом (Propuses, Близнец), поскольку матрицы Эйлера и Мерсенна всегда идут парами и дают парные матрицы.

Работоспособность подхода Скарпи подтверждается тем, что стартовые матрицы Мерсенна $\mathbf{M}_3$ и Эйлера $\mathbf{E}_6$ сразу переходят в матрицы Адамара $\mathbf{H}_{12} = \mathbf{W}_{12}$ и $\mathbf{H}_{24} = \mathbf{W}_{24}$. Отрыв от аппроксимируемой таким способом структуры матриц Адамара начинается только с применения матрицы $\mathbf{M}_7$. Не меняя существенно матрицу $\mathbf{W}_{28}$, предложенный в работе [4] алгоритм сжатия ее адамаровой нормы позволяет свести итог к матрице Адамара $\mathbf{H}_{28}$, что демонстрируется на рис. 5.



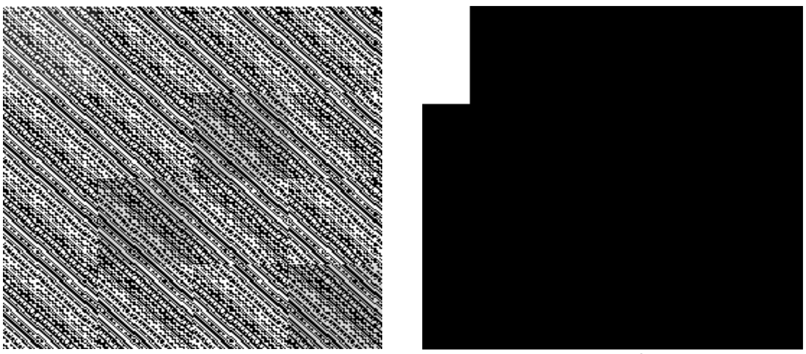
а б

Рис. 5. Портреты матриц Вильямсона $\mathbf{W}_{28}$ (а) и Адамара $\mathbf{H}_{28}$ (б)



а б

Рис. 6. Портрет матрицы $\mathbf{M}_{167}$ (а) и гистограмма модулей ее элементов (б)



а б

Рис. 7. Портрет матрицы приближения к $\mathbf{H}_{668}$ (а) и гистограмма модулей ее элементов (б)

Задача нахождения матрицы Адамара $\mathbf{H}_{28}$ решается редукцией структуры: измененная сжатием одна из четырех матриц Вильямсона содержит в явном виде не $\mathbf{M}_7$, а уже встречавшиеся при построении матриц Белевича моноблоки и матрицу Мерсенна $\mathbf{M}_3$. То, что за матрицами Вильямсона стоят матрицы Мерсенна, ранее в литературе не обсуждалось. Заметим, что и сами по себе матрицы Мерсенна стремятся с ростом порядка к матрицам Адамара, поскольку их коэффициент b приближается к 1. Например, матрица Мерсенна относительно малого 167-го порядка, судя по гистограмме ее уровней, уже немногим отличается от матрицы Адамара (рис. 6).

Даже без сжатия (адаптации структуры) коэффициент b, характеризующий приближение массива Вильямсона с этой матрицей Мерсенна к матрице H_{668}, составляет около 70% от максимально возможного уровня (рис. 7).

Модификация метода Скарпи

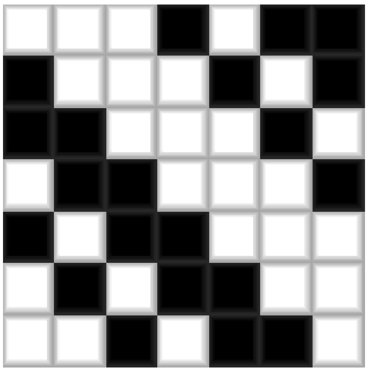
Наиболее интересный результат можно получить, находя при помощи матриц Мерсенна низкого порядка тот же самый сорт матриц порядка более высокого. Для учета условий ортогональности применим циклическую перестановку столбцов блоков, принесшую заметный успех при построении матриц Белевича. Поскольку в оригинале [10] еще отсутствует понятие матриц Мерсенна с их естественным разделением множества всех элементов на целые (1) и вещественные ($-b$), идея прежнего метода Скарпи не может быть выражена в столь простой формулировке, как приводимая ниже.

Модифицированный алгоритм. Любую матрицу Мерсенна порядка n, где n – простое число, можно вставить саму в себя с циклическим сдвигом, пропорциональным ее положению, используя в качестве каймы замещаемый элемент матрицы: после нормализации и усечения каймы получим снова матрицу Мерсенна.

Величина циклического сдвига столбцов равна произведению индексов элементов расширяемой матрицы, отсчет их начинается с 0.

Стартовый элемент каймы блока (пересечение первых его строки и столбца) выбирается отрицательным. Под нормализацией подразумевается выравнивание знаков первого столбца и строки итоговой матрицы так, чтобы они были отрицательными – усечение каймы воспроизводит их количественный дефицит на единицу в матрице Мерсенна, но теперь уже порядка n^2+n-1. Коэффициент $-b$ ее рассчитывается заново согласно определению. Отметим, что полином $n^2+n-1=0$ имеет корни, равные по модулю числам золотого сечения, т.е. известная в математике пропорция, так или иначе, лежит в основе этого построения.

В качестве примера возьмем матрицу Мерсенна $\mathbf{M}_7$, применим ее не для построения матрицы Вильямсона, а увеличим число блоков составной матрицы до значения ее порядка, вставляя матрицу саму в себя согласно алгоритму. После нормализации и усечения общей каймы получим матрицу Мерсенна $\mathbf{M}_{55}$. Побочный продукт этого алгоритма – промежуточная матрица Адамара, поскольку это матрицы одного сечения (рис. 8). Показана матрица Адамара $\mathbf{H}_{56}$ до ее нормализации, что позволяет наблюдать структуру и характер сдвигов столбцов размножаемой матрицы.


а

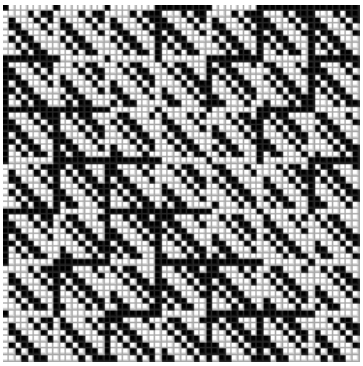

б

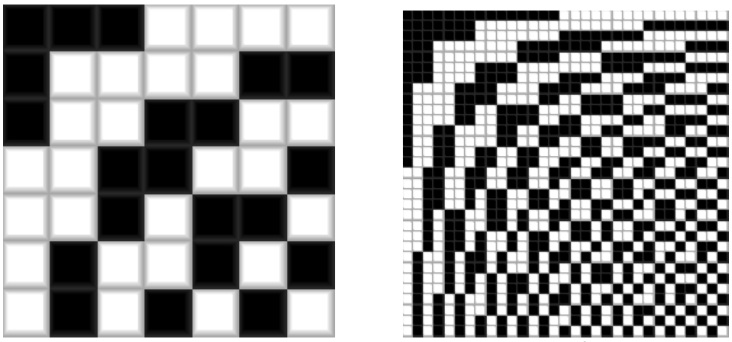
Рис. 8. Портреты матриц Мерсенна ($\mathbf{M}_7$) (а) и Адамара ($\mathbf{H}_{56}$) (б)

Фильтр Мерсенна

Для многих приложений вычислительной математики, теории кодирования, цифровой обработки сигналов и др. важным требованием является простота и конечность множества значений функций ортонормированных систем. Первая из таких систем – система Радемахера – была построена как существенное упрощение аналога тригонометрической системы функций. Функции Радемахера имеют всего два значения $\{1, -1\}$, но их недостаток состоит в том, что система неполна и, следовательно, не является базисом в гильбертовом пространстве L_2. Полная система впервые была введена Дж. Уолшем. В отличие от функций Радемахера, функции Уолша можно разделить на четные и нечетные, этим они аналогичны синусам и косинусам. Такие функции применяются в практике помехоустойчивого сжатия и маскирования изображений, заменяя матрицу дискретного косинусного преобразования матрицей Адамара–Уолша в классическом тракте JPEG-алгоритма сжатия изображения [1, 3, 5].

Фильтр, построенный на матрице Мерсенна, будем называть фильтром Мерсенна.

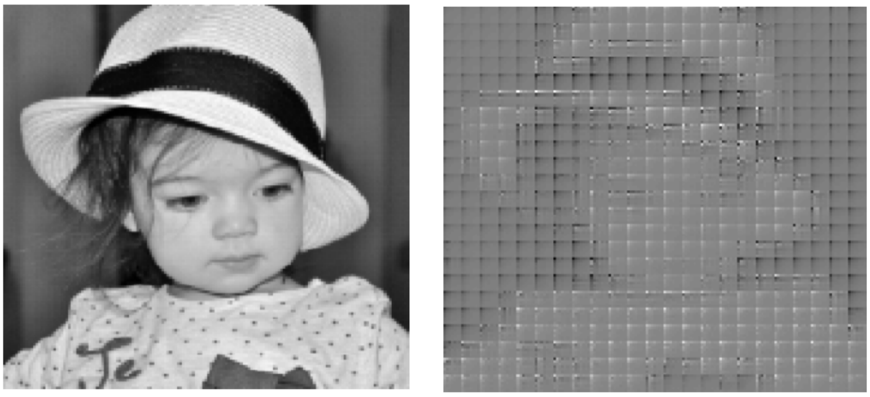
Матрицы Мерсенна − двухуровневые, они содержат только элементы двух значений $\{1, -b\}$ и допускают упорядочивание их строк и столбцов перестановками, результаты которых представлены на рис. 9.



а б

Рис. 9. Портрет матриц Мерсенна-Уолша $\mathbf{M}_7$ (а) и Мерсенна-Уолша $\mathbf{M}_{31}$ (б)

Пример применения фильтра Мерсенна на основе матрицы M_7 к модельному изображению приведен на рис. 10.



а б

Рис. 10. Модельное изображение «Мария» (а) и матрица прореженных фильтром Мерсенна значений ее двухмерного спектра (б)

Исходное и отфильтрованное изображения сравнивались по объемам, достигаемым алгоритмом статистической компрессии PNG (Portable Network Graphics). Исходное изображение перед обработкой имеет объем 37 кБ, обработанное фильтром Мерсенна составляет 32 кБ при малом сжатии, которое уменьшается до 26 кБ и ниже при высоком, более детально технология раскрыта в работах [15, 16].

Систему ортогональных функций, порождаемых упорядоченными по частоте столбцами матриц Мерсенна, будем называть системой функций Мерсенна–Уолша по аналогии с классическими функциями Уолша. Перечислим ее отличительные особенности и назовем причины, по которым такой 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 не совпадает с системой функций Уолша, но является достаточно близкой аппроксимацией ее на нечетных значениях порядка. Систему функций Мерсенна–Уолша характеризует пониженное на единицу количество порождающих ее элементов столбцов матрицы Мерсенна, т.е. она более проста для вычисления, чем классическая.

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, она более предпочтительна для построения полосовых фильтров изображений (для обработки рисунков, где отсутствует монотонный фон). Первые единичные столбец и строка нормализованных матриц Адамара представляют собой ненужную составляющую, которая у полосовых фильтров никакой нагрузки не несет, поскольку отвечает частоте, которую они фильтруют. Иначе говоря, она означает лишние затраты процессорного времени. Однако заметим, что простое удаление канвы матрицы Адамара отбрасыванием ее первых строки и столбца нарушает ортогональность столбцов усеченной матрицы.

Заключение

Для ряда приложений квазиортогональных матриц к помехоустойчивому кодированию информации, маскированию изображений и защите видеоданных целочисленные значения их элементов далеко не столь важны, как высокая размерность решаемой задачи и наличие экстремальных качеств [1, 3–5, 17], которыми обладают матрицы Адамара и все близкие к ним матрицы их семейства. В работе подведены некоторые итоги использования алгоритма и программы исследования *M*-матриц [4].

Построение матриц Белевича при помощи матриц Мерсенна в настоящей работе публикуется впервые. Это означает, что матрицы Адамара и Белевича более высоких порядков достижимы не только при помощи матриц Мерсенна ближайшего к ним среза – имеются и более дальние связи. Приведенный в работе подход показывает вариант замены известного кронекерова произведения матриц Адамара, введенный еще Пэли, операциями с каймой и сдвигами столбцов матриц Мерсенна. Отсутствие некоторых матриц Белевича получило объяснение естественным исчерпанием комбинаторной возможности, сопровождаемой появлением в их составе моноблоков (разрыв структуры).

Матрицы Белевича и Адамара далеко не всегда являются конечной целью таких алгоритмов, поскольку известны приложения, например, при моделировании квазикристаллов [18, 19], в которых содержательная сторона задачи связывается с модульно двухуровневыми матрицами. По простоте и надежности поиска матрицы Мерсенна предпочтительнее матриц Адамара. Они занимают в тетраде матриц Адамара, Мерсенна, Эйлера и Ферма наиболее удаленное положение от матриц порядка $4k$–3, на котором наблюдается отсутствие явно выделенного и проходящего по всем порядкам матриц слоя. Справа и слева (по порядкам) от матриц Мерсенна находятся связанные с ними взаимно-однозначным соответствием матрицы Адамара и Эйлера.

Модификация алгоритма поиска матриц Белевича с циклической перестановкой столбцов позволяет непосредственно вычислять матрицы Мерсенна и Адамара высоких порядков, недостижимых при использовании метода Пэли [11]. Снижение числа блоков и отказ от перестановок элементов матрицы Мерсенна позволяет эффективно находить приближения матриц Адамара высоких проблемных порядков при имеющейся мощности вычислительной техники.

Reference

1. Mironovsky L.A., Slaev V.A. *Strip-metod preobrazovaniya izobrazhenii i signalov* [The strip-method for transforming signals and images]. St. Petersburg, Politekhnika Publ., 2006, 163 p.
2. Erosh I.L., Sergeev A.M., Filatov G.P. O zashchite tsifrovykh izobrazhenii pri peredache po kanalam svyazi [Protection of images during transfer via communication channels]. *Informatsionno-Upravlyayushchie Sistemy*, 2007, no. 5, pp. 20–22.
3. Balonin Yu.N., Vostrikov A.A., Sergeev M.B. O prikladnykh aspektakh primeneniya M-matrits [Applied aspects of M-matrix use]. *Informatsionno-Upravlyayushchie Sistemy*, 2012, no. 1, pp. 92–93.
4. Balonin Yu.N., Sergeev M.B. Algoritm i programma poiska i issledovaniya M-matrits [The algorithm and program of M-matrices search and study]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 3 (85), pp. 82–86.
5. Balonin N.A., Sergeev M.B. M-matritsy [M-Matrices]. *Informatsionno-Upravlyayushchie sistemy*, 2011, no. 1, pp. 14–21.
6. Hadamard J. Résolution d'une question relative aux determinants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246.
7. Balonin N.A., Sergeev M.B., Mironovsky L.A. Vychislenie matrits Adamara-Mersenna [Calculation of Hadamard-Mersenne matrices]. *Informatsionno-Upravlyayushchie Sistemy*, 2012, no. 5, pp. 92–94.
8. Balonin N.A., Sergeev M.B. O dvukh sposobakh postroeniya matrits Adamara-Eilera [Two ways to construct Hadamard-Euler matrices]. *Informatsionno-Upravlyayushchie Sistemy*, 2013, no. 1 (62), pp. 7–10.
9. Balonin N.A., Sergeev M.B., Mironovsky L.A. Vychislenie matrits Adamara-Ferma [Calculation of Hadamard-Fermat matrices]. *Informatsionno-Upravlyayushchie Sistemy*, 2012, no. 6 (61), pp. 90–93.
10. Scarpis U. Sui determinanti di valore Massimo. *Rendiconti della R. Istituto Lombardo di Scienze e Lettere*, 1898, vol. 31, pp. 1441–1446.
11. Paley R.E.A.C. On orthogonal matrices. *Journal of Mathematics and Physics*, 1933, vol. 12, pp. 311–320.
12. Belevitch V. Theorem of 2n-terminal networks with application to conference telephony. *Electronic Communications*, 1950, vol. 26, pp. 231–244.
13. Balonin Yu.N., Sergeev M.B. M-matritsa 22-go poryadka [M-matrix of the 22nd order]. *Informatsionno-Upravlyayushchie Sistemy*, 2011, no. 5, pp. 87–90.
14. Williamson J. Hadamard’s determinant theorem and the sum of four squares. *Duke Math. J*, 1944, vol. 11, pp. 65–81.
15. Balonin N.A., Sergeev M.B. O rasshirenii ortogonal'nogo bazisa v zadachakh szhatiya videoizobrazhenii [Expansion of the orthogonal basis in video compression]. *Vestnik Komp’iuternykh i Informatsionnykh Tekhnologii*, 2014, no. 2 (116), pp. 11–15.
16. Vostrikov A.A., Balonin Yu.N. Matritsy Adamara-Mersenna kak bazis ortogonal'nylh preobrazovanii v maskirovanii videoizobrazhenii [Hadamard – Mersenne matrices as a basis of orthogonal transformation for video masking encoding]. *Izv. vuzov. Priborostroenie*, 2014, vol. 57, no. 1, pp. 15–19.
17. Balonin N.A., Sergeev M.B. Matritsy local'nogo maksimuma determinanta [Local maximum determinant matrices]. *Informatsionno-Upravlyayushchie Sistemy*, 2014, no. 1 (68), pp. 2–15.
18. Balonin N.A., Sergeev M.B. Matritsa zolotogo secheniya G_{10} [Matrix of golden ratio G_{10}]. *Informatsionno-Upravlyayushchie Sistemy*, 2013, no. 6 (67), pp. 2–5.

19. Balonin N.A., Sergeev M.B. M-matritsy i kristallicheskie struktury [M-matrices and crystal structures]. *Vestnik of Nosov Magnitogorsk State Technical University*, 2013, no. 3 (43), pp. 58–62.

Балонин Николай Алексеевич – доктор технических наук, доцент, профессор, Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, Россия, korbendfs@mail.ru

Балонин Юрий Николаевич – программист, Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, Россия, tomaball@mail.ru

Сергеев Михаил Борисович – доктор технических наук, профессор, зав. кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, Россия; директор, НИИ информационно-управляющих систем, Университет ИТМО, mbse@mail.ru

Nikolai A. Balonin – Professor, D.Sc., Associate professor, Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, Russia, korbendfs@mail.ru

Yuri N. Balonin – programmer, Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, Russia, tomaball@mail.ru

Mikhail B. Sergeev – D.Sc., Professor, Department head; Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, Russia; Director, Research Institute of Information and Control Systems, ITMO University, mbse@mail.ru

Принято к печати 18.02.2014
Accepted 18.02.2014