УДК 519.61 DOI:10.47813/dnit-nto.2021.104-110

Анализ реализаций метода Скарпи при вычислении матриц Адамара высоких порядков симметричных структур

А.М. Сергеев

Санкт-Петербургский государственный университет аэрокосмического приборостроения, ул. Большая Морская, 67, Санкт-Петербург, 190000, Россия

E-mail: aleks.asklab@gmail.com

Аннотация. Приводится анализ трех модификаций метода Скарпи с целью оценки их применимости для вычисления матриц Адамара высоких порядков со структурными симметриями. Представлены описания модификаций, демонстрируются результаты вычисления матриц Адамара, подтверждающие вывод о значимости модификации Балонина-Себерри. Вычислительный эксперимент показывает, что нет результатов, опровергающих существование матриц симметричной структуры, вычисленных модификацией Балонина-Себерри.

Ключевые слова: ортогональные матрицы, матрицы Адамара, матрицы Мерсенна, метод Скарпи

Analysis of implementations of the Scarpi method for calculating high orders Hadamard matrices of symmetric structures

A.M. Sergeev

Sankt-Petersburg State University of Aerospace Instrumentation, 67, Bolshaya Morskaya str., Saint Petersburg, 190000, Russia

E-mail: aleks.asklab@gmail.com

Abstract. An analysis of three modifications of the Scarpi method is given in order to assess their applicability to calculating Hadamard matrices of high orders with structural symmetries. Descriptions of modifications are presented, the results of Hadamard matrix calculation are demonstrated, confirming the conclusion about the significance of the Balonin-Seberry modification. The computational experiment shows that there are no results refuting the existence of matrices symmetric structures calculated by the Balonin-Seberry modification.

Keywords: orthogonal matrices, Hadamard matrices, Mersenne matrices, Scarpi method

1. Введение

Ортогональные матрицы Адамара **H** – квадратные матрицы порядков n с элементами {1, –1} и ортогональными столбцами $\mathbf{H}^T\mathbf{H} = n\mathbf{I}$, где **I** – единичная матрица, являются основой преобразования и обработки изображений, их помехозащищенного кодирования, организации систем защиты информации в коммуникациях [1 – 4]. К настоящему времени известны различные методы их вычисления [5], различающихся структурой и порядками вычисляемых матриц. Наиболее востребованными в перечисленных применениях являются матрицы Адамара высоких порядков со структурными симметриями [6].

Одним из первых и оригинальных методов нахождения матриц Адамара высоких порядков на основе матриц более низких порядков является метод Скарпи [7]. Проблемными для метода являются матрицы Адамара очень высоких порядков, для которых производительность современных компьютеров не позволяет пока их вычислить. Даже реализация одной из модификаций метода Скарпи – схемы Вильямсона [8], основанного на использовании блочно-составной конструкции из четырех базовых матриц, не позволяет вычислить хорошо известные проблемные порядки матриц Адамара: 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964 и т.п.

Тем не менее, в отношении некоторых матриц высоких порядков результат вычисления методом Скарпи оказался непревзойденным даже при использовании более позднего метода Пэли, нашедшего применение теории конечных полей Галуа для построения матриц Адамара с помощью символов Лежандра.

2. Постановка задачи

Суть метода Скарпи состоит в реализации операции матричной вставки: каждая следующая матрица получается вставкой на место каждого элемента исходной матрицы самой этой матрицы с учетом знаков заменяемых элементов.

Операция вставки аналогична кронекерову произведению матриц **A** и **B** вида

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \ldots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}\mathbf{B} & a_{n2}\mathbf{B} & \ldots & a_{nn}\mathbf{B} \end{pmatrix},$$

при котором знаки элементов первого сомножителя влияют на всю матрицу второго сомножителя.

Напрямую реализация метода Скарпи позволяет вычислять матрицы больших порядков, однако их симметрия или блочная симметрия, желаемые для большинства применений, не гарантированы.

Ставится задача анализа модификаций метода Скарпи, позволяющих получать в результате симметричные матрицы или блочные симметрии в них.

ISBN 978-5-6045165-2-2

3. Реализации метода Скарпи

3.1. Схема Вильямсона

Разновидность метода Скарпи – схема Вильямсона, также, как и сам метод, основана на вставках, но использует ограниченное число вставляемых базовых матриц, которые не обязательно ортогональны, но симметричны. Таких матриц всего четыре: **A**, **B**, **C** и **D** и вставляются они в исходную матрицу в виде

$$\mathbf{W} = \begin{array}{|c|c|c|c|} \hline \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ \hline -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ \hline -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ \hline -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \\ \hline \end{array}$$

Использование квадратных симметричных матриц **A**, **B**, **C** и **D,** называемых матрицами Вильямсона (или базовыми матрицами), позволяет найти перебором их элементов нужный для вставки в **W** вид. К сожалению, количество операций перестановок элементов в матрицах Вильямсона при поиске подходящих для конструирования ортогональной **W** слишком велико даже при упрощении структур до некоторых циклических, связанных с задающими их векторами (первыми строками матриц). Однако использование такой схемы вычислений позволило найти большое число проблемных матриц Адамара.

Тем не менее, следует отметить, что вычисление матриц Адамара высоких порядков по схеме Вильямсона не может иметь серьезной перспективы, поскольку ее реализация не дает принципиального решения. Ведь вычисление очередной матрицы высокого порядка лишь отодвигает проблемный порядок, приводя к значительно возрастающим вычислительным затратам.

Анализ показал, что хотя матрицы Вильямсона симметричны и в **W** располагаются симметрично относительно главной диагонали, но результирующая матрица не обязательно будет симметрична ввиду различий знаков базовых матриц **B**, **C** и **D** при вставке в **W**.

3.2. Модификация с использованием матриц Мерсенна

В работе [9] предложена модификация метода Скарпи с использованием матрицы Адамара в виде $\mathbf{H} = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{M} \end{pmatrix}$, где **e** – вектор единичных элементов каймы, а «ядром» матрицы Адамара является квадратная матрица Мерсенна **M** [10] циклической структуры порядка $n = 4k$

ISBN 978-5-6045165-2-2

– 1 с элементами {1, –*b*}. Матрица **M** такая, что $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\,\mathbf{I}_n$, где $\mathbf{I}_n$ – единичная матрица, $\mu = \frac{(n+1)+(n-1)b^2}{2}$. $b = \frac{1}{2}$ 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 [11]. На портретах матриц Мерсенна (рисунок 1) элементы со значением –*b* представлены черным полем, со значением 1 – белым.

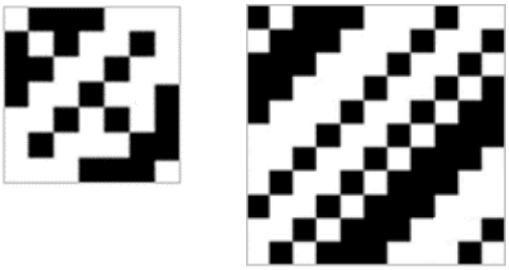

Рисунок 1. Примеры портретов симметричных матриц Мерсенна простых порядков 7 и 11 симметричной структуры.

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 определяется произведением индексов элементов расширяемой матрицы, но отсчет их начинается с 0. Стартовый элемент каймы вставляемой матрицы (пересечение его первых 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 $n^2 + n - 1$. Элемент матрицы –*b* рассчитывается заново, согласно определению.

В качестве примеров используем матрицы Мерсенна **M** порядка 7, вставляя их сами в себя согласно методу Скарпи. После нормализации и усечения общей каймы получим матрицу Мерсенна **M** порядка 55. Побочный продукт этого алгоритма –матрица Адамара порядка 56.

На рисунке 2 показаны портреты двух симметричных исходных матриц **M** порядка $v = 7$ (ядро матрицы Адамара **H** порядка $n = 8$) и портреты вычисленных на их основе матриц Адамара **H** порядка $vn = 56$, что позволяет наблюдать структуру и характер сдвигов столбцов вставляемых матриц.

ISBN 978-5-6045165-2-2

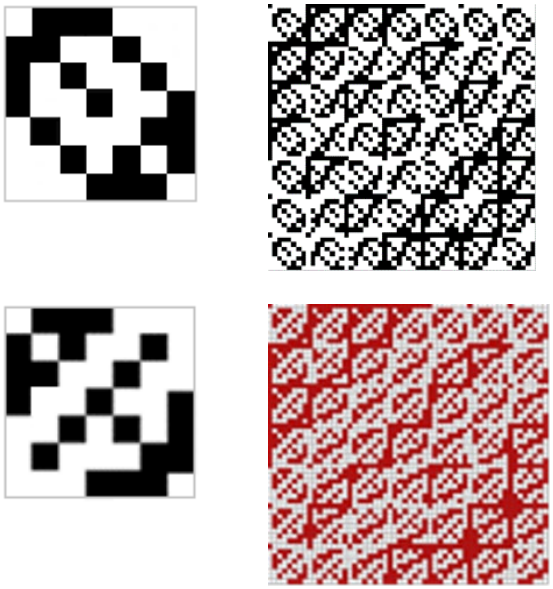

Рисунок 2. Портреты матриц Мерсенна порядка 7 и матриц Адамара порядка 56, вычисленных методом Скарпи.

Матрицы Адамара, вычисляемые такой модификацией метода Скарпи при этом, не являются симметричными, но обладают локальными симметриями отдельных выделяемых в них блоков.

3.3. Схема Балонина-Себерри

Схема предложена профессорами Балониным Н. А. и Дж. Себерри (J. Seberry) [12]. Ее первое принципиальное отличие от схемы Вильямсона заключается в том, что одна из вставляемых матриц заменяется уже выбранной ранее. Таким образом, при построении шестнадцатиблочной структуры используются не четыре базовых матрицы, а только три: **A**, **B** (**C = B**) и **D**. Это существенно сокращает время поиска матриц Адамара в такой конструкции, поскольку необходим компьютерный подбор только трех циклических базовых матриц.

Второе отличие состоит в схеме расположения базовых матриц в результирующей матрице [13], называемой Пропус (**P**), приведенной ниже.

$$\mathbf{P} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{B} & \mathbf{D} \\ \mathbf{B} & \mathbf{D} & -\mathbf{A} & -\mathbf{B} \\ \mathbf{B} & -\mathbf{A} & -\mathbf{D} & \mathbf{B} \\ \mathbf{D} & -\mathbf{B} & \mathbf{B} & -\mathbf{A} \end{bmatrix}$$

В работе [12] авторами высказывается предположение, что в такой конструкции получаемые ортогональные матрицы на всех возможных порядках Адамара $n = 4t$, где t – натуральное число, будут симметричными относительно главной диагонали. Пока такое предположение теоретически не доказано, однако в результате проведенных компьютерных поисков оказалось, что в его подтверждение все результаты вычислений завершились нахождением симметричных матриц Адамара.

ISBN 978-5-6045165-2-2

Ниже на рисунке 3 в качестве примера приведены две новые симметричные матрицы Адамара порядков 120 и 364 соответственно, полученные на основе циклических базовых матриц.

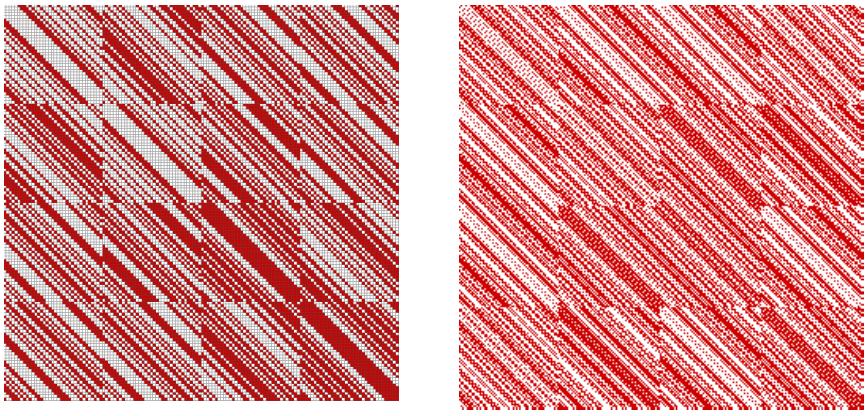

Рисунок 3. Симметричные матрицы Адамара порядков 120 и 364, вычисленные по схеме Балонина-Себерри.

4. Выводы

Метод Скарпи ориентирован на вычисление матриц Адамара высоких порядков.

Схема Балонина-Себерри реализации метода Скарпи обеспечивает сокращение вычислительных затрат за счет необходимости поиска только трех базовых матриц в конструкции Пропус матрицы Адамара.

На сегодня не существует опровержения предположения о симметричности матриц Адамара конструкции Пропус как целиком, так и по-блочно.

Благодарность

Статья подготовлена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004 «Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств».

Список литературы

1. Ахмед, Н. Ортогональные преобразования при обработке цифровых сигналов / Н. Ахмед, К. Р. Рао, пер. с англ. под ред. И. Б. Фоменко. М.: Связь, 1980. –130 –132 с.
2. Мироновский, Л.А. Стрип-метод преобразования изображений и сигналов / Л.А. Мироновский, В.А. Слаев. – СПб: Политехника, 2006. – 163 с.
3. Wang, R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis / R. Wang. New York: Cambridge University Press, 2010. – 504 p.

4. Vostrikov, A. Expansion of the quasi-orthogonal basis to mask images / A. Vostrikov, M. Sergeev // Smart Innovation, Systems and Technologies. – 2015. – 40. – P. 161-168.
5. Сергеев, А.М. Специальные матрицы: вычисление и применение / А.М. Сергеев, А.А. Востриков. – СПб: Политехника, 2018. – 112 с.
6. Сергеев, А.М. Ортогональные матрицы симметричных структур для задач обработки изображений / А.М. Сергеев, Н.Ш. Блаунштейн // Информационно-управляющие системы. – 2017. – № 6(91). – С. 2-8.
7. Scarpis, U. Sui determinanti di valore Massimo / U. Scarpis // Rendiconti della R. Istituto Lombardo di Scienze e Lettere. – 1898. – 31. – P. 1441-1446.
8. Williamson, J. Hadamard's Determinant Theorem and the Sum of Four Squares / J. Williamson // Duke Math. J. – 1944. – № 11. – P. 65-81.
9. Балонин, Н.А. О модификации метода Скарпи вычисления матриц Мерсенна для задач преобразования изображений / Н.А. Балонин, Ю.Н. Балонин, М.Б. Сергеев // Информационные технологии. – 2014. – № 4. – С. 48-51.
10. Sergeev, A. Generalized Mersenne Matrices and Balonin's Conjecture / A. Sergeev // Automatic Control and Computer Sciences. – 2014. – Vol. 48. – No. 4 – P. 214-220.
11. Балонин, Н.А. Вычисление матриц Адамара-Мерсенна / Н.А. Балонин, М. Б. Сергеев, Л. А. Мироновский // Информационно-управляющие системы. – 2012. – № 5(60). – С. 92–94.
12. Seberry, J. Two infinite families of symmetric Hadamard matrices / J. Seberry, N. A. Balonin // Australasian Journal of Combinatorics. – 2017. – 69(3). – P. 349-357.
13. Балонин, Н.А. Матрицы Пропус 92 и 116 / Н.А. Балонин, М.Б. Сергеев // Информационно-управляющие системы. – 2016. – № 2(81). – С. 101-103.

ISBN 978-5-6045165-2-2