УДК: 519.683 DOI: 10.47813/nto.2.2022.5.92-100 EDN: NEQEED

Повышение эффективности майнинга матриц Адамара для методов цифрового преобразования

Ю.Н. Балонин, А.А. Востриков, Д.В. Куртяник*, А.М. Сергеев

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

* E-mail: dvk88@yandex.ru

Аннотация. Рассматривается задача поиска матриц Адамара как майнинг, включающий в себя задание начальных условий, выбор конструкций матриц, «обогащение» набора последовательностей через фильтрацию Фурье-спектров последовательностей. Анализируются трудности майнинга и рассматривается способ их преодоления. Приводятся примеры выбора конструкции Пропус, предварительной фильтрации сгенерированных последовательностей для ускорения вычислений.

Ключевые слова: майнинг матриц, матрицы Адамара, конструкция Пропус, фильтрация последовательностей

Improving the efficiency of Hadamard matrix mining for digital conversion methods

Iu.N. Balonin, A.A. Vostrikov, D.V. Kurtianik*, A.M. Sergeev

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

* E-mail: dvk88@yandex.ru

Abstract. The problem of searching for Hadamard matrices is considered as mining, which includes setting initial conditions, choosing matrix designs, and "enriching" a set of sequences through filtering the Fourier spectra of sequences. Mining difficulties are analyzed and a way to overcome them is considered. Examples of the choice of the Propus design, pre-filtering of the generated sequences to speed up calculations are given.

Keywords: mining of matrices, Hadamard matrices, Propus construction, sequence filtering

1. Введение

Слово «mining» имеет устоявшееся значение, которое включает в себя добычу полезных ископаемых и их обогащение, связанные с большими трудозатратами. Сегодня, в области цифровизации различных процессов, слово «майнинг» неразрывно связано с трудоемкими и энергоемкими процессами создания блоков в блокчейне для обеспечения функционирования криптовалютных платформ.

Поиск матриц Адамара $\mathbf{H}_n$ [14] порядка n с элементами 1 и -1, удовлетворяющих соотношению $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}_n$, можно также охарактеризовать как трудоемкий в вычислительном смысле процесс. Здесь $\mathbf{I}_n$ – единичная матрица, а порядки $n = 4t$, где t – натуральное число.

Каждая новая матрица с учетом ее структуры и порядка, являясь результатом разработки специального алгоритма, длительных вычислений, проверки ортогональности – имеет не меньшую стоимость, выраженную в трудозатратах, чем биткоин или каменный уголь из шахты.

Время вычислений некоторых матриц нередко составляет недели и месяцы. Поэтому очень важным результатом в майнинге матриц является сокращение времени вычислений. Сегодня использование суперкомпьютеров еще не стало общедоступным, хотя это значимый инструментарий, но не определяющий. Наибольшее значение имеет эффективность применяемого метода вычислений, его лучшие модификации, приемы ускорения рутинных вычислений.

Цель настоящей работы – показать возможности повышения эффективности майнинга матриц Адамара высоких порядков и симметричных структур, как и прочих похожих на них матриц с жестко ограниченным числом значений элементов [6, 17].

2. Матрицы Адамара и области их применения

Ортогональные матрицы широко используются в системах передачи и хранения данных, для которых характерны симметричные ортогональные преобразования. Матрицы Адамара и подобные им квазиортогональные матрицы применяются в обработке сигналов и изображений [13,16,23], помехоустойчивом кодировании изображений [18], в кодировании [9] и многих других технических задачах.

Перечисленные применения порождают сегодня потребность поиска матриц все более высоких порядков, поскольку увеличиваются размеры изображений и возрастают требования к длине кодовых последовательностей, а также структурированных,

гарантированно существующих и вычислимых. Наиболее известными структурами матриц являются симметричные.

Проблемы майнинга матриц Адамара при указанных требованиях заключаются, во-первых, в том, что не существует универсального метода, способного одинаково эффективно искать матрицы Адамара возможных структур на всех порядках их существования. Классические методы Сильвестра, Пэли, Вильямсона, Скарпи и их модификации не позволяют покрыть все возможные порядки матриц Адамара – имеется большое количество их пропусков.

Во-вторых, для широкого круга поисковиков нет доступа к суперкомпьютерам для «добычи» матриц. При таком положении важную роль играет эффективность разрабатываемых алгоритмов как результатов использования новых подходов и приемов программирования.

В-третьих, с ростом порядков матриц Адамара «добыча» значительно усложняется. Каждая новая найденная матрица Адамара порядка выше 428 (который был ранее неразрешен) в известном проблемном сэте порядков является предметом обсуждения научной общественности, занимающейся данной тематикой [15]. Ведь вновь «добытые» матрицы Адамара появляются значительно реже очередной единицы криптовалюты.

3. Основные подходы к разработке эффективных методов майнинга матриц

Многолетний опыт в области поиска и использования матриц Адамара позволяет говорить о возможности повышения эффективности их майнинга.

Во-первых, следует предпринимать усилия к поиску альтернативы известным методам и подходам. Например, совершенно новым является подход, основанный на процедурах оптимизации, не свойственных рассматриваемой области компьютерных вычислений.

Матрицы Адамара всегда считались матрицами, которые нужно находить генерацией последовательностей элементов 1 и –1, после чего выполнять перестановки. В связи с этим область поиска в целом отнесли к развитой в западной литературе ветви комбинаторики. Однако еще Адамар отмечал, что это матрицы максимальные по детерминанту. Оптимизация детерминанта матрицы никак не может быть отнесена к перестановочным алгоритмам, она меняет абсолютные значения всех элементов матрицы от 0 до 1. Есть, хотя и очень малоизвестные, алгоритмы повышения

детерминанта [11, 19, 20], в том числе итерационные [3]. Разумеется, им нужно стартовое начальное приближение, чтобы оптимизатор не остановился в точке локального максимума – это известная болезнь итерационных процедур. Тем не менее, это серьезное предложение для майнинга редких матриц.

У комбинаторных методов нет возможности исправления даже незначительного дефекта начального приближения. Майнинг, построенный на оптимизации, это допускает. Мы отмечаем это как очевидный, но еще мало изученный инструмент развития темы.

Структура матрицы, это, по сути, и есть начальное приближение, необходимое оптимизатору. В качестве подсказки ему можно навязывать любую структуру. В процессе оптимизации структура может разрушаться, но возвращаемый принудительно к ней оптимизатор становится мощным средством поиска.

Во-вторых, разработка эффективных методов поиска матриц Адамара связывается нами с фиксацией ограничений, например, на структуры: циклические, бициклические, трициклические, симметричные и др. и возможные для них порядки. Такая фиксация ограничений, рассматриваемая как усложнение задачи, тем не менее позволяет значительно повысить эффективность поиска за счет упрощения или сокращения вычислительных затрат.

В целом результаты наших поисков показали способность новых подходов при разработке алгоритмов давать значительный результат.

4. Пример работы со структурами матриц

Рассмотрим повышение эффективности процесса майнинга матриц Адамара за счет указанной ранее фиксации их структуры.

Матрицы Адамара $\mathbf{H}_n$ на высоких порядках могут представлять собой разновидность четырехблочного массива Вильямсона [12] вида

$$\mathbf{H}_n = \begin{pmatrix} \mathbf{A}_{n/4} & \mathbf{B}_{n/4} & \mathbf{C}_{n/4} & \mathbf{D}_{n/4} \\ \mathbf{C}_{n/4} & \mathbf{D}_{n/4} & -\mathbf{A}_{n/4} & -\mathbf{B}_{n/4} \\ \mathbf{B}_{n/4} & -\mathbf{A}_{n/4} & -\mathbf{D}_{n/4} & \mathbf{C}_{n/4} \\ \mathbf{D}_{n/4} & -\mathbf{C}_{n/4} & \mathbf{B}_{n/4} & -\mathbf{A}_{n/4} \end{pmatrix}$$

с блоками $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$, $\mathbf{C}_{n/4}$ и $\mathbf{D}_{n/4}$, как правило, циклическими и обязательно симметричными. В этом ранее видели ключ к упрощению поиска. Поясним кратко,

почему это не так. Симметричность влияет, скорее, на размер памяти компьютера, на котором эти матрицы ищутся, т.е. на техническую составляющую поиска.

В результате предложения, сформулированного в работе [24], матрица $\mathbf{H}_n$ может быть построена в виде симметричной конструкции Пропус на основе трех блоков $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$, и $\mathbf{D}_{n/4}$, где только блок $\mathbf{A}_{n/4}$ симметричен, а остальные – не симметричны и $\mathbf{C}_{n/4}=\mathbf{B}_{n/4}$. Существующее доказательство, что все матрицы Адамара либо симметричны, либо кососимметричны в целом, а не по-блочно, поправило ошибку с матрицами Вильямсона. Это открытие способствовало получению большого количества новых матриц.

Конструкция Пропус [4, 22] и сходные с ним кососимметричные массивы гарантируют получение матрицы Адамара независимо от порядка матрицы.

Сверхбольшие каталоги последовательностей из 1 и –1, рассматриваемые в работе [1], содержат предполагаемые первые строки циркулянтов $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$ и $\mathbf{D}_{n/4}$ матрицы Адамара конструкции Пропус. Такие последовательности генерируются и накапливаются в ходе работы различных алгоритмов [2, 5, 7]. Однако, с ростом порядка искомой матрицы $\mathbf{H}_n$ скорость поиска резко падает из-за увеличения объема каталога.

В случае простейшей реализации генератора [21] количество случайно сгенерированных комбинаций последовательностей растет настолько быстро, что компьютер добирается до нужной комбинации неделями.

5. Способы обогащения исходных последовательностей для построения структурированных матриц Адамара

К разновидности полезной фильтрации последовательностей относятся признаки их совместимости. Когда одна последовательность из трех при конструировании матрицы Адамара конструкции Пропус сравнивается с двумя другими, она не может быть уже вполне произвольной.

Итак, не все последовательности являются источниками блоков-циркулянтов, пригодных для построения матрицы Адамара конструкции Пропус. Введение фильтра совместимости позволяет укоротить поле поиска. Такой фильтр является аналогом обогатительной фабрики на шахте, отделяющей породу от полезного ископаемого.

Исследования показали, что фильтрацию можно осуществить такой простой и хорошо известной инженерам процедурой, как дискретное преобразование Фурье (ДПФ) или его быстрой версией – БДПФ [10]. Всплеск спектра свидетельствует о наличии гармонической составляющей, не позволяющей рассматривать последовательность как

потенциальное решение. Можно установить порог, выше которого гармоника делает рассматриваемую последовательность непригодной.

Простейший пороговый фильтр по выбросам спектра убирает до 99% ненужных последовательностей. Особенность такой фильтрации состоит в том, что рост количества перекрестных проверок описывается квадратичной зависимостью, а количество фильтраций – линейной. И это оправдывает таким образом организованное «обогащение» сверхбольших каталогов последовательностей.

Матрица Фурье, это не единственная ортогональная матрица, используемая для построения фильтров. Парадоксально, но для поиска новых матриц Адамара могут использоваться уже найденные матрицы Адамара в процедурах фильтрации, устроенных сходно с БДПФ. Матрицы могут быть того же порядка, или усеченные.

6. Примеры обогащения последовательностей

В работе [8] обсуждается эффективная процедура обогащения последовательностей отсечкой выбросов по Фурье спектру, как показано на рисунке 1. Здесь по горизонтальной оси располагаются номера элементов спектра сгенерированной последовательности.

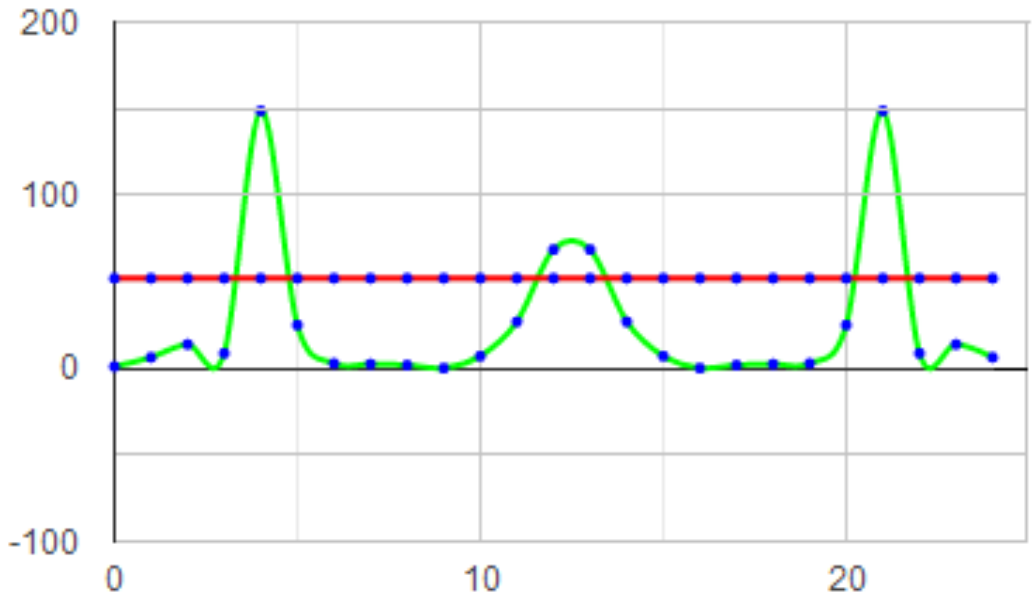

Рисунок 1. Отбраковка последовательностей по выбросам их спектра Фурье.

Наличие ярко выраженных гармоник (пики на спектре) свидетельствует о невозможности использования этой последовательности для построения блочной ортогональной матрицы [21].

Установка уровня пороговой линии зависит от типа искомых матриц. Как правило, он равен порядку матрицы Адамара.

Преимущество использования спектра Фурье последовательностей состоит в возможности изучения статистики частоты появления нужных, получаемых на выходе соответствующего генератора, для еще не найденных матриц.

7. Заключение

Рассмотренные подходы к становлению техники современного майнинга матриц Адамара, крайне важны в своем развитии для получения уникальных матриц, используемых в методах ортогональных преобразований информации.

Научная новизна работы заключается в том, что она развивает направление «обогащения» набора последовательностей как основы построения симметричных матриц Адамара. Все отмеченные нами поисковые процедуры выполнялись по необогащенной выборке.

Сегодня майнинг от находок редких матриц Адамара и «рекордов» на порядках переходит в стадию гарантированных результатов за приемлемое время. Этому способствует ранее не применяемый контроль поиска матриц Адамара при помощи уже найденных матриц Адамара или производных от них матриц.

Благодарность

Авторы выражают благодарность обладателю премии Пирси почетному профессору University of Wollongong (Австралия) Дженнифер Себерри за творческие рекомендации и участие в семинарах, способствовавших становлению технологии майнинга матриц Адамара.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004.

Список литературы

1. Балонин, Н. А. Алгоритмы конечных полей и групп поиска ортогональных последовательностей / Н. А. Балонин, А. М. Сергеев, О. И. Синицына // Информационно-управляющие системы. – 2021. – № 4. – С. 2-17. doi:10.31799/1684-8853-2021-4-2-17
2. Балонин, Ю. Н. Генерация симметричных ортогональных матриц Адамара с тремя блоками (Пропусов) на базе предварительного поиска части последовательностей. /

Ю. Н. Балонин, О. И. Синицына // Свидетельство о государственной регистрации программы для ЭВМ № 2020662383 от 13 октября 2020 г.

3. Балонин, Н. А. Динамические генераторы квазиортогональных матриц семейства Адамара / Н. А. Балонин, М. Б. Сергеев, В. С. Суздаль // Труды СПИИРАН. – 2017. – № 5(54). – С. 224-243. doi:10.15622/sp.54.10
4. Балонин, Н. А. Как гипотезе Адамара помочь стать теоремой, часть 1 / Н. А. Балонин, М. Б. Сергеев // Информационно-управляющие системы. – 2018. – № 6. – С. 2-13. doi:10.31799/1684-8853-2018-6-2-13
5. Балонин, Ю. Н. Накопление пар ортогональных последовательностей для поиска симметричных ортогональных матриц Адамара с тремя блоками (Пропусов) / Ю. Н. Балонин, А. М. Сергеев // Свидетельство о государственной регистрации программы для ЭВМ № 2020662384 от 13 октября 2020 г.
6. Балонин, Н. А. Окружности на решетках и матрицы Адамара / Н. А. Балонин, М. Б. Сергеев, Дж. Себерри, О. И. Синицына // Информационно-управляющие системы. – 2019. – № 3. – С. 2-9. doi:10.31799/1684-8853-2019-3-2-9
7. Балонин, Ю. Н. Программный комплекс поиска бициклических матриц на основе таблицы перекрестных ссылок. / Ю. Н. Балонин, А. М. Сергеев // Свидетельство о государственной регистрации программы для ЭВМ № 2018616390 от 01.06.2018 г.
8. Turnerб J. S. A Legendre pair of length 77 using complementary binary matrices with fixed marginal / J. S. Turner, I. S. Kotsireas, D. A. Bulutoglu, A. J. Geyer // Designs, Codes and Cryptography. – 2021. – Vol. 89. – № 6. – P. 1321-1333.
9. Evangelaras, H. Applications of Hadamard matrices / H. Evangelaras, C. Koukouvinos, J. Seberry // Journal of telecommunications and information Technology. – 2003. – № 2. – P. 3-10.
10. Fletcher, R. J. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices / R. J. Fletcher, M. Gysin, J. Seberry // Australasian Journal of Combinatorics. – 2001. – № 23. – P. 75-86.
11. Orrick, W. P. Large determinant sign matrices of order 4k+1 / W. P. Orrick, B. Solomon // Discrete Math. – 2007. – Vol. 307. – P. 226-236.
12. Acevedo, S. New infinite families of Williamson Hadamard matrices / S. Acevedo, H. Dietrich // Australian Journal of Combinatorics. – 2019. – Vol. 73(1). – P. 207-219.
13. Seberry, J. On some applications of Hadamard matrices / J. Seberry, B. Wysocki, T. Wysockiet // Metrika. – 2005. – № 62(2-3). – P. 221-239.

14. Seberry, J. Hadamard Matrices: Constructions using number theory and linear algebra / Seberry J., Yamada M. – Wiley, 2020. – 384 p.
15. Kharaghani, H. Hadamard matrix of order 428 / H. Kharaghani, B. A. Tayfeh-Rezaie // Journal of Combinatorial Designs. – 2005. – Vol. 13. – P. 435-440.
16. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge University Press, 2010. – 504 p.
17. Mohan, M. T. p-almost Hadamard matrices and λ-planes / M. T. Mohan // Journal of Algebraic Combinatorics. – 2020. – P. 20. doi:10.1007/s10801-020-00991-y
18. Mironovsky, L. A. Strip-Method for Image and Signal Transformation. / L. A. Mironovsky, V. A. Slaev. – Berlin, Boston: De Gruyter, 2011. – 166 p. doi:10.1515/9783110252569
19. Seberry, J. The maximal determinant and subdeterminants of ±1 matrices / J. Seberry, T. Xia, C. Koukouvinos, M. Mitrouli // Linear Algebra and its Applications. – 2003. – Vol. 373. – P. 297-310. doi:10.1016/S0024-3795(03)00584-6
20. Orrick, W. P. The maximal {−1,1}-determinant of order 15 / W. P. Orrick // Metrika. – 2005. – № 62. – P. 195-219.
21. Balonin, Y. The Study of Generators of Orthogonal Pseudo-Random Sequences / Y. Balonin, L. Abuzin, A. Sergeev, V. Nenashev // Smart Innovation, Systems and Technologies. – 2019. – Vol. 143. – P.125-133. doi:10.1007/978-981-13-8303-8
22. Seberry, J. Two infinite families of symmetric Hadamard matrices / J. Seberry, N. A. Balonin // Australian Journal of Combinatorics. – 2017. – Vol. 69(3). – P. 349-357.
23. Use of symmetric Hadamard and Mersenne matrices in digital image processing / A. Vostrikov, M. Sergeev, N. Balonin, A. Sergeev // Procedia Computer Science. – 2018. – P. 1054-1061. doi: 10.1016/j.procS.2018.08.042
24. Holzmann, W. H. Williamson matrices up to order 59 / W. H. Holzmann, H. Kharaghani, B. Tayfeh-Rezaie // Designs, Codes and Cryptography. – 2008. – № 46 (3). – P. 343-352.