УДК 519.614
doi:10.31799/1684-8853-2024-2-2-8
EDN: YOXUBL

Научные статьи
Articles

Опыт получения матриц максимума детерминанта бициклических структур на основе случайных последовательностей квантовой генерации

А. А. Востриков[a], *канд. техн. наук, доцент, orcid.org/0000-0002-8513-3683, vostricov@mail.ru*
А. М. Сергеев[a], *канд. техн. наук, доцент, orcid.org/ 0000-0002-4788-9869*
Ю. Н. Балонин[a], *научный сотрудник, orcid.org/0000-0002-5102-4139*
Д. В. Куртяник[a], *старший преподаватель, orcid.org/0000-0002-2895-6990*
К. Ю. Рыжов[a], *аспирант, orcid.org/0000-0002-8809-3218*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *поиск матриц максимума детерминанта с двумя значениями элементов 1 и –1, являясь задачей трудоемкой, может быть упрощен внесением ограничений на их структуру. Поиск матриц на основе бициклических структур требует больших трудозатрат при подборе пар случайных последовательностей, порождающих блоки бицикла.* ***Цель:*** *показать развитие теории и обобщение семейств матриц максимума детерминанта при фиксации их структурных инвариантов. Проверить возможность получения максимальных размеров ортогональных последовательностей, которые можно извлечь при квантовой генерации для построения матрицы максимума детерминанта. Сопоставить случайные последовательности, получаемые из транспозонов в ДНК и с выхода квантового генератора.* ***Результаты:*** *предложено развитие теории и обобщение семейств матриц максимума детерминанта при фиксации их структурных инвариантов. Даны расширенные определения матриц оптимального дизайна, адамаридов, мерсеннидов и экстремальных бициклических структур. Введены определения плеча матрицы бициклической структуры и его размера. Описаны результаты проведенных компьютерных экспериментов с одним миллионом случайных последовательностей длины 100, сгенерированных на квантовом генераторе и позволивших получить ранее неизвестные матрицы максимума детерминанта на порядках, отличных от адамаровых.* ***Практическая значимость:*** *ортогональные матрицы и матрицы максимума детерминанта, являясь срезами ортогонального гиперобъекта, значительно расширяют семейство матриц Адамара, которые имеют большое практическое значение для задач ортогональных преобразований информации в телекоммуникациях.*

Ключевые слова *— квантовая генерация, случайные числа, случайные последовательности, матрицы максимума детерминанта, конструкции матриц, бициклические матрицы.*

Для цитирования: Востриков А. А., Сергеев А. М., Балонин Ю. Н., Куртяник Д. В., Рыжов К. Ю. Опыт получения матриц максимума детерминанта бициклических структур на основе случайных последовательностей квантовой генерации. *Информационно-управляющие системы*, 2024, № 2, с. 2–8. doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL
For citation: Vostrikov A. A., Sergeev A. M., Balonin Yu. N., Kurtyanik D. V., Ryzhov K. Yu. The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL

Введение

Матрицы максимального детерминанта, являясь математическим объектом многих научных исследований [1–5], сегодня уже не только представляют значительный научный или соревновательный интерес [6–9], но и широко используются при цифровой обработке информации в задачах помехозащищенного обмена по коммуникационным каналам, устойчивого корреляционного приема сигналов в системах связи и др. [10, 11]. Поэтому развитие теории и обобщение семейств матриц максимума детерминанта, в том числе при фиксации их структурных инвариантов, является задачей актуальной.

Матрицы максимального детерминанта — квадратные матрицы произвольных порядков n с элементами 1 и –1 — сходны с матрицами Адамара.

Матрицы Адамара [12, 13] $\mathbf{H}_n$ порядка n — матрицы с элементами 1 и –1, удовлетворяющие условию ортогональности $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}_n$. Здесь $\mathbf{I}_n$ — единичная матрица того же порядка $n = 4t$, где t — натуральное число.

Матрицы Адамара имеют максимальный детерминант на указанных порядках $4t$. На порядках, открытых Голеем [14] и кратных, кроме 2, простым числам 5 и 13, матрицы Адамара представимы в виде бициклической конструкции

$$\mathbf{T}_n = \begin{pmatrix} \mathbf{A}_{n/2} & \mathbf{B}_{n/2} \\ \mathbf{B}_{n/2}^{\mathrm{T}} & -\mathbf{A}_{n/2}^{\mathrm{T}} \end{pmatrix},$$

где $\mathbf{A}_{n/2}$ и $\mathbf{B}_{n/2}$ — циклические матрицы, образуемые из последовательностей a и b длины $n/2$, размещаемых на месте их первых строк, последующим их сдвигом в каждой следующей строке вправо и переносом последнего элемента на первую позицию в этой строке.

Матрицы Адамара сходны с матрицами максимального детерминанта с элементами 1 и –1 тем, что они также имеют максимальный детерминант. Однако порядки, на которых существуют матрицы максимального детерминанта, отличны от адамаровых, и эти матрицы могут быть не ортогональными [13, 14].

В задаче получения (построения) матриц Адамара и матриц максимума детерминанта большую роль играет способ получения последовательностей из 1 и –1, для чего используются случайная генерация, теория полей и групп, точки Гаусса на объектах вращения и др. [15, 16].

Первая матрица бициклической конструкции, отличная от голеевских, имеет порядок 68 (4×17), вторая — порядок 100 [17]. Внешне порядок 68 отличается увеличенным размером основы матрицы — 17.

Только для голеевских пар существует алгоритм перемножения их между собой [18, 19]. Отсюда следует, что находить не голеевские пары надо экспериментально, а это сводится к генерации случайных последовательностей.

Цель настоящей работы — показать влияние квантовой генерации случайных последовательностей на результативность поиска матриц максимума детерминанта с бициклическими структурами в основе.

Способы генерации случайных последовательностей

Получаемые с помощью программ на классическом компьютере случайные последовательности являются на самом деле псевдослучайными, имеющими ряд таких недостатков, как [20, 21]:

— ограниченный период, определяемый количеством последовательностей до начала воспроизводства одной и той же последовательности;

— зависимость последовательных значений, поскольку, как правило, вычисляются с использованием предыдущего значения генератора;

— обратимость — периодичность воспроизведения одной и той же последовательности и др.

Физические генераторы случайных чисел генерируют случайные последовательности за счет измерения параметров протекающих физических процессов [22–25]. В квантовой технике эти процессы, связанные с такими системами, как атомы, молекулы, элементарные частицы и т. п., являются идеальными источниками случайности.

Современные простые и недорогие генераторы случайных последовательностей (ГСП) построены, например, на использовании квантового оптического процесса. Такие квантовые генераторы формируют выходной случайный поток, в котором не наблюдается корреляций и выполняются все статистические тесты со скоростью до 10–16 Мбит/с [26]. ГСП на основе полупроводникового лазера с короткими и резкими пиками интенсивности [27] обеспечивают на выходе случайную последовательность со скоростью до 12,5 Гбит/с.

Более сложными и дорогими ГСП могут служить квантовые компьютеры (процессоры), такие как Advantage компании D-Wave (Канада) или Eagle компании USTC (Китай), в которых генерация случайных последовательностей реализуется за счет определения состояния множества кубитов при разрушении квантовой суперпозиции.

Семейства матриц Адамара

Элементарным обобщением матриц Адамара являются квазиортогональные матрицы со значениями пары элементов 1 и $-b$, удовлетворяющие условию $\mathbf{A}_n^{\mathrm{T}}\mathbf{A}_n = \omega\mathbf{I}_n$, где ω — целое или вещественное (рациональное, иррациональное) число.

Приведенное обобщение порождает семейство матриц Адамара, для которого бициклическая форма является универсальной [28]. Для матриц Адамара повышение порядка сказывается не на разрешимости, а на возможности поддерживать специфическую симметрию не самой матрицы, а операций с матрицами.

Приведем расширенные определения матриц семейства Адамара, введенные впервые в научный оборот в работе [28].

Определение 1. Матрицами оптимального дизайна (ОД) конструкции $\mathbf{T}_n$ четных порядков $4t - 2$ называют матрицы, сходные с матрицами Адамара тем, что среди матриц с ограниченными по величине элементами (не более единицы) они экстремальны — имеют самый большой детерминант.

Такие матрицы не могут быть ортогональными, это доказал Адамар, но они ортогонализуемы совместным изменением величины элементов одного знака. Иными словами, они не столь далеко отстоят от адамаровых и образуют с ними одно семейство оптимальных матриц.

Определение 2. «Адамаридами» будем называть матрицы порядков $4t + 1$, получаемые из адамаровых бициклов добавлением монотонной каймы из 1 в строке сверху и в столбце слева, первый (угловой) элемент которых равен –1.

Такие матрицы, кроме матриц на порядках, равных первым пяти числам Ферма, не строго оптимальны по детерминанту [29].

Определение 3. «Мерсеннидами» будем называть аналогичные матрицы порядков $4t - 1$, на единицу больших, чем порядки матриц ОД.

Однако следует отметить, что матрицы ОД существуют не всегда, тогда как экстремальные матрицы, построенные на основе бициклической структуры с каймой, существуют для всех порядков $4t - 1$. В них заведомо не входят порядки, равные числам, на единицу меньшим чисел Ферма, поскольку они принадлежат адамаридам.

Экстремальные бициклические матрицы

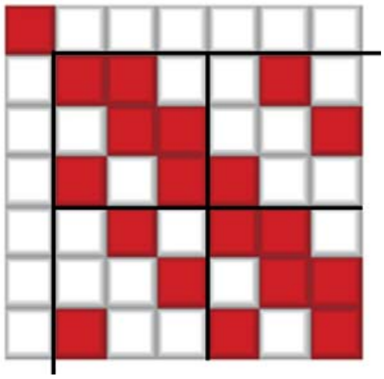
Строго оптимальные по детерминанту матрицы нечетных порядков, отличных от чисел Ферма, неограниченно усложняются с ростом порядков [15].

Определение 4. Плечом бицикла будем называть циклический блок $\mathbf{A}_{n/2}$ или $\mathbf{B}_{n/2}$, размер плеча составляет половину порядка бицикла — $n/2$. В настоящее время достоверно известна и доказана экстремальность матриц, не превышающих критического размера плеча 13.

Вполне ожидаемо, что на порядке 36 предполагаются проблемы поиска основы для наложения каймы, но они есть и для вполне безобидных голеевских порядков 32 и 64, поскольку 33 и 65 — не числа Ферма.

Ввиду резкого роста трудностей оправдан переход к более узкому классу матриц, экстремальных на бициклической структуре с каймой. Пример такой матрицы приведен на рис. 1, где выделены моноциклические блоки и кайма.

Здесь единичные элементы матрицы с положительным знаком представлены белым цветом, элементы с отрицательным знаком — красным цветом.



■ ***Рис. 1.*** Портрет бицикла с каймой
■ ***Fig. 1.*** Portraits of bicycle with border

Определение 5. Матрицу $\mathbf{T}_n$ будем называть экстремальным бициклом [28] в том случае, если она с нормализованной каймой

$$[\mathbf{T}_{n+1}] = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{T}_n \end{pmatrix},$$

где все элементы вектора $\mathbf{e}$ равны единице, имеет максимум детерминанта на множестве матриц с такой структурой.

Уравнение орнамента матриц [15, 16] базируется на точках Гаусса сечения чаши параболоида $x^2 + y^2 = h$ на высотах h, где $h = n$ для матриц Адамара и $h = 2n - 2$ для матриц ОД. Однако ни матриц Адамара, ни матриц ОД бициклической конструкции может и не существовать. Например, нет бициклических матриц Адамара на порядках 36 и 72, хотя точки Гаусса имеются.

В том случае, когда нет точек Гаусса для заданного порядка, они определяются на высоте h, на которой существуют. Тогда задача сводится к выяснению: является ли это кольцо среза параболоида ближайшим или оно отстоит подальше.

Экстремальные бициклы и получаемые из них матрицы больших детерминантов нечетных порядков хорошо вписываются в общий контекст задачи на оптимальность и дополняют собой матрицы Адамара и ОД, отличаясь от них инвариантами $k_1 = (v - x)/2$, $k_2 = (v - y)/2$, задающими количество элементов со значением –1 в строках его плеч $\mathbf{A}_{n/2}$ и $\mathbf{B}_{n/2}$ размера v.

Для серий бициклических матриц на порядках Адамара в качестве опорных высот берутся размеры тех самых избранных семейств, куда вложены числа Ферма (минус единица, которая отвечает размеру каймы: 17 – 1 = 16 и т. п.). Отсутствие бицикла порядка 36 само по себе не мешает использовать этот порядок, на котором есть регулярные матрицы Адамара, но сложной структуры для расчета инвариантов серии бициклов. Инвариантами являются числа, а не матрицы. Невозможность ортогонализовать бицикл с такими параметрами для них не критична, поскольку ищутся заведомо неортогональные матрицы больших детерминантов.

Вслед за числом 36 для смещенных семейств такую же роль опорной высоты для расчета координат точек Гаусса играет порядок 64, хотя голеевская пара уступает блочной составной структуре с каймой. Тем самым для вычисления орнаментальных инвариантов используются ровно те же самые формулы, что и для матриц Адамара и ОД, но высота h в них соответствует влиятельному порядку, существенно отличному от порядка матрицы.

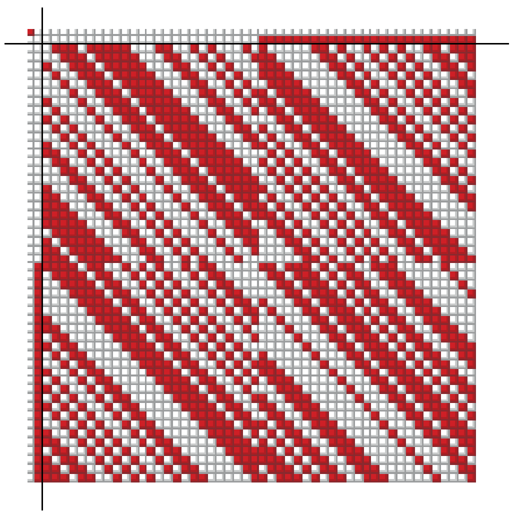
Установление величин инвариантов, характеризующих экстремальное решение, значительно сокращает алгоритмы поиска, поэтому приводимые здесь сведения являются новыми и важными.

Тест последовательности регулируемой длины

Использование случайных последовательностей для формирования ортогональных массивов или их блоков дает возможность судить по разрешимому порядку на выборке заданного объема о емкости массива случайных чисел из 1 и –1. На сегодня не известно о каких-либо работах по измерению емкости последовательностей в матрицах.

Кроме случайных последовательностей, полученных с квантового генератора, например на эффекте интерференции лазерных импульсов со случайной фазой [27], эксперименты для сравнения проводились и с биологическими последовательностями — с выборками из последовательностей Alu ДНК [30]. Длина таких последовательностей составляет всего 300 точек. Известно, что они формируют до 90 % генетического кода, играя специфическую роль скобок при переносах генетического материала. Скобка должна быть узнаваемой, поэтому от Alu получен высокий показатель «емкости» в матрицах.

Взяв сгенерированную квантовым способом 41 000 точек из чисел 1 и –1 и увеличивая в этом пределе выборку длины $W = 1000$, 2000 и т. п., можно наблюдать разрешимость данных бициклом Эйлера $\mathbf{T}_n$, являющимся основой матриц Адамара с двойной каймой (рис. 2). Симметрия бициклических структур [17] пока не учитывается.



■ ***Рис. 2.*** Портрет матрицы Адамара с бициклом Эйлера в качестве основы и с двойной каймой

■ ***Fig. 2.*** Portrait of Hadamard matrix with Euler bicycle and two borders

Из первых же экспериментов со случайными последовательностями стало ясно, что порядок 22 при заданных параметрах найти легко. Попытка подняться через четыре порядка выше по n приводит к критическому порядку 46, когда решение единственно и найти его можно увеличением объема данных. Это позволяет строить зависимость $n = f(\max(W))$ и следом прогнозировать нужные объемы данных.

Мерсенниды, описанные ранее, удобны тем, что их бицикл имеет такой же порядок, что и матрицы Эйлера, но они не ортогональны, и это гарантирует экстремальный детерминант для бицикла с каймой.

Если матрицы Эйлера — это типичный ортогональный базис при понижении уровня элемента со значением –1, то мерсенниды — базис из неортогональных векторов. Для них уже порядок 42 оказывается критичным. Ведут себя эти матрицы иначе: они имеют высокий эксцесс — бóльший разброс необходимых количеств 1 и –1. На порядке 42 этот разброс определяется значениями $k_1 = 11$ и $k_2 = 8$.

Обсуждение

Поскольку число паттернов (узоров) внутри ограниченной последовательности тоже ограничено, рано или поздно любая последовательность генератора исчерпывается. Кроме того, при равномерном выходе 1 и –1 с генератора случайных чисел возникает нарастающий с ростом порядка искомых матриц конфликт в различии эксцессов при поиске мерсеннидов, которого нет у биологических генераторов на основе ДНК.

Выход из этой ситуации видится в сложении двух последовательностей, получаемых с генератора случайных чисел и из последовательностей Alu ДНК. Получаемые при этом три уровня позволяют за единицу принимать один из них, меняя тем самым вероятность появления 1 и –1.

Использование такого способа позволило в частном эксперименте поднять разрешимый порядок мерсеннидов с 42 до 58, что ранее являлось недостижимым результатом при многочисленных поисках.

Однако такой способ сложения случайных последовательностей нельзя признать лучшим решением, хотелось бы иметь обратную связь на генератор случайных чисел. Это входит в общий вывод исследования.

Заключение

Использование квантовых ГСП и последовательностей Alu ДНК [30] как источников последовательностей с большим периодом и независимостью их фрагментов создает условия для продвижения в решении задач поиска новых ортогональных матриц и матриц максимума детерминанта.

Формирование широкого предложения таких матриц на различных порядках обеспечивает возможность лучшего выбора для задач обработки информации в телекоммуникационных системах и связи.

Описанный прием сложения двух случайных последовательностей позволяет менять как вероятность, так и разнообразие паттернов, искусственно расширяя выборку за счет времени работы генератора.

Анонсируя результаты выполненных исследований, мы не спешим с окончательными выводами, поскольку область нова и требует более тщательного исследования способов генерации случайных последовательностей и их влияния на результативность поиска матриц максимума детерминанта высоких порядков.

Благодарность

Авторы выражают благодарность сотруднику МИСиС Шаховому Роману за предоставленные для проведенных экспериментов случайные последовательности, сгенерированные в МИСиС в бинарном виде на квантовом генераторе «КуРэйт».

Финансирование

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003 «Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга».

Литература

1. **Ehlich H.** Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, no. 83, pp. 123–132.
2. **Wojtas W.** On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloquium Mathematicum*, 1964, vol. 12, pp. 73–83.
3. **Seberry J., Xia T., Koukouvinos C., Mitrouli M.** The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra and its Applications*, 2003, vol. 373, pp. 297–310. doi:10.1016/S0024-3795(03)00584-6
4. **Cohn J. H. E.** On determinants with elements ±1, II. *Bulletin of the London Mathematical Society*, 1989, no. 21, pp. 36–42.
5. **Neubauer M. G., Radcliffe A. J.** The maximum determinant of ±1 matrices. *Linear Algebra and its Applications*, 1997, no. 257, pp. 289–306.
6. **Brent R. R., Osborn J. H.** General lower bounds of maximal determinants of binary matrices: preprint, 2012. 15 p. arXiv:1208.1805
7. **Osborn J. H.** *The Hadamard Maximal Determinant Problem*: Honours thesis. University of Melbourne. http://maths-people.anu.edu.au/~osborn/publications/pubsall.html (дата обращения: 28.07.2023).
8. **Orrick W. P.** The maximal {−1, 1}-determinant of order 15. *Metrika*, 2005, no. 62, pp. 195–219.
9. **Orrick W. P., Solomon B.** Large determinant sign matrices of order 4k+1. *Discrete Mathematics*, 2007, no. 307, pp. 226–236.
10. **Wang R.** *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis*. Cambridge University Press, 2010. 504 p.
11. **Ahmed N., Rao K. R.** *Orthogonal Transforms for Digital Signal Processing*. Springer-Verlag Berlin Heidelberg, 2012. 264 p.
12. **Hadamard J.** Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathematiques*, 1893, vol. 17, pp. 240–246.
13. **Jennifer S., Yamada M.** *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Wiley, 2020. 384 p.
14. **Colbourn C. J., Dinitz J. H.** *Handbook of Combinatorial Designs*. Second Ed. Chapman and Hall/CRC, 2007. 967 p.
15. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi:10.31799/1684-8853-2019-3-2-9
16. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы максимального детерминанта. *Информационно-управляющие системы*, 2020, № 6, с. 2–11. doi:10.31799/1684-8853-2020-6-2-11
17. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея. *Информационно-управляющие системы*, 2015, № 3, с. 2–16. doi:10.15217/issn1684-8853.2015.3.2
18. **Balonin N. A., Djocovich D. Z.** Negaperiodic Golay pairs and Hadamard matrices. *Информационно-*

управляющие системы, 2015, № 5, с. 2–17. doi:10.15217/issn1684-8853.2015.5.2
19. **Turyn R. J.** Hadamard matrices, Baumert — Hall units, four symbol sequences. pulse compression and surface wave encodings. *Journal of Combinatorial Theory*, 1974, no. 16, pp. 313–333.
20. **Иванов М. А., Чугунков И. В.** *Теория, применение и оценка качества генераторов псевдослучайных последовательностей.* М., Кудиц-образ, 2003. 240 с.
21. **Абросимов Д., Абросимова Е.** *Развитие графического способа тестирования псевдослучайной последовательности чисел.* Концепты хаоса и порядка в естественных и гуманитарных науках: монография. Нижний Новгород, Деком, 2011. С. 67–71.
22. **Манин Ю. И.** *Вычислимое и невычислимое.* М., Сов. радио, 1980. 128 с.
23. **Feyman R.** Simulating physics with computers. *International Journal of Theoretical Physics*, 1982, vol. 21, iss. 6–7, pp. 467–488.
24. **Benioff P.** Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 1982, vol. 29, no. 3, pp. 515–546.
25. **Хвощ С. Т.** Матрицы Адамара как источник тестов квантовых компьютеров. *Инженерный вестник Дона*, 2023, № 3. www.ivdon.ru/ru/magazine/archive/n3y2023/8265 (дата обращения: 28.07.2023).
26. **Балыгин К. А., Зайцев В. И., Климов А. Н., Кулик С. П., Молотков С. Н.** Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов. *Письма в ЖЭТФ*, 2017, т. 106, № 7–8, с. 451–458. doi:10.7868/S0370274X17190109
27. **Shakhovoy R., Sych D., Sharoglazova V., Udaltsov A., Fedorov A., Kurochkin Y.** Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. *Optics Express*, 2020, vol. 28. iss. 5, pp. 6209–6224. doi:10.1364/OE.380156
28. **Балонин Н. А., Сергеев М. Б.** Максимум детерминанта бициклических матриц с каймой. *Информационно-управляющие системы*, 2023, № 3, с. 2–15. doi:10.31799/1684-8853-2023-3-2-15, EDN: JQPBFE
29. **Balonin N. A., Sergeev M. B., Vostricov A. A.** Prime Fermat numbers and maximum determinant matrix conjecture. *Информационно-управляющие системы*, 2020, № 2, с. 2–9. doi:10.31799/1684-8853-2020-2-2-9
30. **Хитринская И. Ю., Степанов В. А., Пузырев В. П.** Alu-повторы в геноме человека. *Молекулярная биология*, 2003, т. 37, № 3, с. 382–391.

UDC 519.614
doi:10.31799/1684-8853-2024-2-2-8
EDN: YOXUBL

The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation

A. A. Vostrikov[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-8513-3683, vostricov@mail.ru
A. M. Sergeev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-4788-9869
Yu. N. Balonin[a], Research Fellow, orcid.org/0000-0002-5102-4139
D. V. Kuryatnik[a], Senior Lecturer, orcid.org/0000-0002-2895-6990
K. Yu. Ryzhov[a], Post-Graduate Student, orcid.org/0000-0002-8809-3218
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation

Introduction: The process of finding the maximum determinant matrices with two values of elements 1 and –1 being a laborious task, it can be simplified by introducing restrictions on their structure. Finding the matrices based on binary circulant structures is associated with the laborious selection of pairs of random sequences that generate two circulant blocks. **Purpose:** To show the development of the theory and generalization of families of maximum determinant matrices while fixing their structural invariants. To check the possibility of obtaining the orthogonal sequences of maximum sizes that can be extracted during quantum generation to construct a matrix of the maximum determinant. To compare random sequences obtained from transposons in DNA and from the output of a quantum generator. **Results:** We propose the development of the theory and generalization of families of maximum determinant matrices while fixing their structural invariants. We give extended definitions of optimal design matrices, hadamarides, mersennides and extremal two circulant structures. We introduce the definition for the arm of the matrix of the binary structure and its size. The results of computer experiments with 1 million random sequences of length 100 generated with a quantum generator are described, which allowed us to obtain previously unknown matrices of the maximum determinant on non-Hadamard orders. **Practical relevance:** Orthogonal matrices and matrices of the determinant maximum as the results of slices of an orthogonal hyperobject significantly expand the family of Hadamard matrices, which are of great practical importance for problems of orthogonal transformations of information in telecommunications.

Keywords — quantum generation, random numbers, random sequences, maximum determinant matrices, matrix constructions, two circulant matrices.

For citation: Vostrikov A. A., Sergeev A. M., Balonin Yu. N., Kurtyanik D. V., Ryzhov K. Yu. The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL

Acknowledments

The authors express their gratitude to the MISiS employee Shakhov Roman for providing random sequences generated in binary form on the KuRate quantum generator in MISiS for the experiments carried out.

Financial support

The paper was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, grant agreement No. FSRF-2023-0003.

References

1. Ehlich H. Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, no. 83, pp. 123–132 (In German).
2. Wojtas W. On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloquium Mathematicum*, 1964, vol. 12, pp. 73–83.
3. Seberry J., Xia T., Koukouvinos C., Mitrouli M. The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra and its Applications*, 2003, vol. 373, pp. 297–310. doi:10.1016/S0024-3795(03)00584-6
4. Cohn J. H. E. On determinants with elements ±1, II. *Bulletin of the London Mathematical Society*, 1989, no. 21, pp. 36–42.
5. Neubauer M. G., Radcliffe A. J. The Maximum determinant of ±1 matrices. *Linear Algebra and its Applications*, 1997, no. 257, pp. 289–306.
6. Brent R. R., Osborn J. H. General lower bounds of maximal determinants of binary matrices: preprint, 2012. 15 p. arXiv:1208.1805
7. Osborn J. H. *The Hadamard Maximal Determinant Problem*: Honours thesis. University of Melbourne. Available at: http://maths-people.anu.edu.au/~osborn/publications/pubsall.html (accessed 28 July 2023).
8. Orrick W. P. The maximal {–1, 1}-determinant of order 15. *Metrika*, 2005, no. 62, pp. 195–219.
9. Orrick W. P., Solomon B. Large determinant sign matrices of order 4k+1. *Discrete Mathematics*, 2007, no. 307, pp. 226–236.
10. Wang R. *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis*. Cambridge University Press, 2010. 504 p.
11. Ahmed N., Rao K. R. *Orthogonal Transforms for Digital Signal Processing*. Springer-Verlag Berlin Heidelberg, 2012. 264 p.
12. Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathematiques*, 1893, vol. 17, pp. 240–246 (In French).
13. Jennifer S., Yamada M. *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Wiley, 2020. 384 p.
14. Colbourn C. J., Dinitz J. H. *Handbook of Combinatorial Designs*. Chapman and Hall/CRC, 2007. 967 p.
15. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9
16. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2020, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2020-6-2-11
17. Balonin N. A., Djocovich D. Z. Symmetry of two-circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
18. Balonin N. A., Djocovich D. Z. Negaperiodic Golay pairs and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2015, no. 5, pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2
19. Turyn R. J. Hadamard matrices, Baumert — Hall units, four symbol sequences. pulse compression and surface wave encodings. *Journal of Combinatorial Theory*, 1974, no. 16, pp. 313–333.
20. Ivanov M. A., Chugunkov I. V. *Teoriya, primenenie i ocenka kachestva generatorov psevdosluchajnyh posledovatel'nostej* [Theory, application and quality assessment of pseudorandom sequence generators]. Moscow, Kudic-obraz Publ., 2003. 240 p. (In Russian).
21. Abrosimov D., Abrosimova E. *Razvitie graficheskogo sposoba testirovaniya psevdosluchajnoj posledovatel'nosti chisel*. In: *Koncepty haosa i poryadka v estestvennyh i gumanitarnyh naukah* [Development of a graphical method for testing a pseudorandom sequence of numbers. In: Concepts of chaos and order in natural sciences and humanities]. Nizhnij Novgorod, Dekom Publ., 2011, pp. 67–71 (In Russian).
22. Manin Yu. I. *Vychislimoe i nevychislimoe* [*Computable and non-computable*]. Moscow, Sovetskoe radio Publ., 1980. 128 p. (In Russian).
23. Feyman R. Simulating physics with computers. *International Journal of Theoretical Physics*, 1982, vol. 21, iss. 6–7, pp. 467–488.
24. Benioff P. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 1982, vol. 29, no. 3, pp. 515–546.
25. Khvoshch S. T. Hadamard matrices as a source of quantum computer tests. *Engineering Journal of Don*, 2023, no. 3 (In Russian). Available at: www.ivdon.ru/ru/magazine/archive/n3y2023/8265 (accessed 28 July 2023).
26. Balygin K. A., Zajcev V. I., Klimov A. N., Kulik S. P., Molotkov S. N. Implementation of a quantum random number generator based on optimal grouping of photo reports. *JETP Letters*, 2017, vol. 106, no. 7–8, pp. 451–458 (In Russian). doi:10.7868/S0370274X17190109
27. Shakhovoy R., Sych D., Sharoglazova V., Udaltsov A., Fedorov A., Kurochkin Y. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. *Optics Express*, 2020, vol. 28, iss. 5, pp. 6209–6224. doi:10.1364/OE.380156
28. Balonin N. A., Sergeev M. B. Maximum determinant two circulant matrices with border. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 3, pp. 2–15 (In Russian). doi:10.31799/1684-8853-2023-3-2-15, EDN: JQPBFE
29. Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 2, pp. 2–9. doi:10.31799/1684-8853-2020-2-2-9
30. Khitrinskaya I. Yu., Stepanov V. A., Puzyrev V. P. Alu repeats in the Human Genome. *Molecular Biology*, 2003, vol. 37, no. 3, pp. 325–333.