Инженерный вестник Дона, №1 (2023)
ivdon.ru/ru/magazine/archive/n1y2023/8155

Обогащение набора последовательностей в задаче поиска блоков симметричных матриц Адамара

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

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Аннотация: Поиск ортогональных и квазиортогональных матриц рассматривается как последовательность задания начальных условий, выбора метода реализации, фильтрации набора сгенерированных последовательностей. Предлагается ускорение поиска матриц за счет предварительных фиксации их структуры и фильтрация сгенерированных последовательностей с использованием спектра Фурье. Фиксация структуры предполагает использование свойств симметрии искомых матриц. Фильтрация позволяет исключить последовательности с явными выбросами спектра при формировании блоков симметричных матриц.

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

Введение

Ортогональные [1, 2] и квазиортогональные [3] матрицы широко используются в системах передачи и хранения данных, в таких задачах, как обработка сигналов и изображений [4], кодирование [5], помехоустойчивое кодирование изображений [6] и получение из строк матриц кодов сигналов [7, 8] и многие др. [9].

Возрастающие размеры задач, увеличение длины кодов порождают потребность поиска матриц все более высоких порядков, а перечисленные области применения – их структурных ограничений. Одними из наиболее известных и востребованных являются матрицы симметричных структур [7].

Процесс поиска рассматриваемых матриц является в общем случае трудоемким, требующим огромного количества компьютерных вычислений, несмотря на выбранный для этого метод. Каждая новая матрица с учетом структуры и порядка [10] часто является результатом разработки специального алгоритма [11], длительных вычислений с промежуточными проверками ортогональности [12]. А результат – предметом обсуждения научной общественностью.

Время вычислений некоторых матриц на современных компьютерах составляет месяцы. Поскольку суперкомпьютеры сегодня еще не стали общедоступными в использовании, что позволило бы значительно ускорить процесс вычисления матриц Адамара даже классическими методами, при их поиске важное значение имеет применяемый метод вычислений и приемы, ускоряющие основные трудоемкие процедуры.

Цель настоящей работы – показать возможность сокращения времени поиска симметричных матриц Адамара высоких порядков и прочих похожих на них матриц с малым числом значений элементов [1, 3].

Матрицы Адамара

Ортогональная матрица Адамара $\mathbf{H}_n$ [3] с элементами 1 и -1 порядка n, удовлетворяет условию $\mathbf{H}_n{}^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}_n$. Здесь $\mathbf{I}_n$ – единичная матрица, а порядки $n = 4t$, где t – натуральное число.

Проблемы поиска таких матриц симметричных структур заключаются в следующем. Не существует универсального метода, одинаково эффективно обеспечивающего поиск таких матриц $\mathbf{H}_n$ на всех порядках $4t$, на которых они существуют. Методы Сильвестра, Пэли, Вильямсона, Скарпи и их многочисленные модификации, ставшие классическими, не покрывают все возможные порядки матриц Адамара – имеется большое количество пропусков порядков, характерных для указанных методов. А с учетом того, что количество матриц Адамара бесконечно, то с ростом порядков их поиск становиться все сложнее.

Важную роль в вычислении (поиске) матриц Адамара играет разработка эффективных алгоритмов на основе использования новых подходов и приемов программирования. К таким методам можно отнести оптимизационные методы [13], а к приемам – генерацию и фильтрацию последовательностей из 1 и -1 как основы формирования матриц Адамара [14].

Фиксация симметричной структуры как способ повышения эффективности поиска матриц

Накопленный опыт в области поиска матриц Адамара позволяет сформулировать эффективный подход, заключающийся во введении ограничений на их симметричные структуры. Такая фиксация ограничений, несмотря на, казалось бы, усложнение задачи, тем не менее позволяет значительно повысить эффективность поиска матриц за счет упрощения или сокращения вычислительных затрат. В целом результаты исследований показали способность указанных подходов при разработке алгоритмов давать значительный результат в поиске матриц.

Матрицы Адамара $\mathbf{H}_n$ на высоких порядках могут представлять собой разновидности [15, 16] четырехблочного массива Вильямсона [17] с блоками $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$, $\mathbf{C}_{n/4}$ и $\mathbf{D}_{n/4}$ называемыми матрицами Вильямсона. Они являются, как правило, циклическими и обязательно симметричными. В этом ранее ученые видели ключ к упрощению поиска, поскольку, найдя такие блоки, можно получить матрицу Адамара, но не обязательно симметричную.

Однако, в результате предложения, сформулированного в работе [16], матрица $\mathbf{H}_n$ может быть построена в виде симметричной конструкции, ранее названной Пропус [18], на основе всего трех блоков $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$ и $\mathbf{D}_{n/4}$, где только блок $\mathbf{A}_{n/4}$ симметричен, остальные блоки не симметричны. При этом в конструкции $\mathbf{C}_{n/4} = \mathbf{B}_{n/4}$.

Обе конструкции матрицы Адамара приведены для сравнения ниже. Здесь $\mathbf{H}_n^{\mathbf{V}}$ – матрица конструкции Вильямсона, $\mathbf{H}_n^{\mathbf{P}}$ – Пропус.

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

При использовании конструкции Пропус не теряется количество возможных решений, так как есть доказательства, что все матрицы Адамара либо симметричны, либо кососимметричны в целом, а не по блокам. Это предложение способствовало получению большого количества новых матриц, поскольку кососимметричные массивы гарантируют получение матрицы Адамара независимо от порядка [18].

Однако основная задача при выборе начальных строк для циклических блоков состоит в работе с генерируемыми случайным образом последовательностями. А поскольку совокупная матрица должна быть ортогональной, то этот выбор осуществляется только через проверку совместимости выбранных последовательностей для блоков $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$ и $\mathbf{D}_{n/4}$.

Работа с каталогами последовательностей для вычисления блоков

Как правило, в качестве первых строк циклических блоков $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$ и $\mathbf{D}_{n/4}$ используются случайным образом сгенерированные последовательности и в работе [19] для этих целей рассматривается генерация сверхбольших каталогов последовательностей. Они образуются и накапливаются в ходе работы различных алгоритмов их генерации при использовании специальных архитектур вычислителей [20] для ускоренной генерации.

Общий алгоритм работы с большими и сверхбольшими каталогами последовательностей можно разделить на этапы: генерации, фильтрации и поиска совместимости последовательностей [14].

С ростом порядка искомой матрицы $\mathbf{H}_n$ скорость поиска резко падает из-за увеличения объема каталогов. Они не удерживают вместе все три пары последовательностей, нужных для построения блоков $\mathbf{A}_{n/4}$, $\mathbf{B}_{n/4}$ и $\mathbf{D}_{n/4}$.

В случае простейшей реализации генератора количество случайно сгенерированных комбинаций последовательностей из 1 и –1 растет настолько быстро, что компьютер добирается до нужной комбинации неделями. Часто все эти сверхбольшие данные теряются ввиду крайне малой

вероятности встретить все три подходящие последовательности. Ведь достаточно не быть одной из них, и огромная таблица сравнений будет перекрестно проверена зря [14].

Для сокращения вычислительных издержек на сравнения предлагается каталоги «обогащать» фильтрацией сгенерированных последовательностей.

Способы обогащения исходных последовательностей

Одной из задач фильтрации является выявление совместимости последовательностей для построения блоков матрицы Адамара по Вильямсону и близких к ним. Ведь одна последовательность из трех для формирования циклических блоков матрицы Пропус сравнивается с двумя другими, она не может быть уже произвольной. Фильтр совместимости при этом сокращает поле поиска.

Оказывается, фильтрацию можно осуществить такой простой и хорошо известной инженерам процедурой, как преобразование Фурье [21]. Ненужная последовательность имеет всплеск спектра, свидетельствующего о наличии в ней гармонической составляющей, входящей в противоречие с потенциальным решением [22].

Введение порога, выше которого гармоника делает последовательность непригодной, является простейшим пороговым фильтром, убирающим основную часть ненужных последовательностей.

Например, при синтезе матрицы из 200 парных последовательностей, вместо 20 000 их перекрестных сравнений следует выполнить всего одно. Приятная особенность фильтрации состоит в том, что количество перекрестных проверок растет квадратично, тогда как количество фильтраций (и их аналогов, фильтров совместимости) – линейно. Это оправдывает такое обогащение сверхбольших каталогов поиска.

Простая, но эффективная процедура обогащения последовательностей отсечкой выбросов по спектру Фурье предложена в работе [22]. На рис. 1

просматривается типичная ситуация, характерная практически для всех генерируемых случайных последовательностей. Здесь по горизонтали расположены отсчеты номеров последовательностей, а по вертикали – значения результатов преобразования по Фурье.

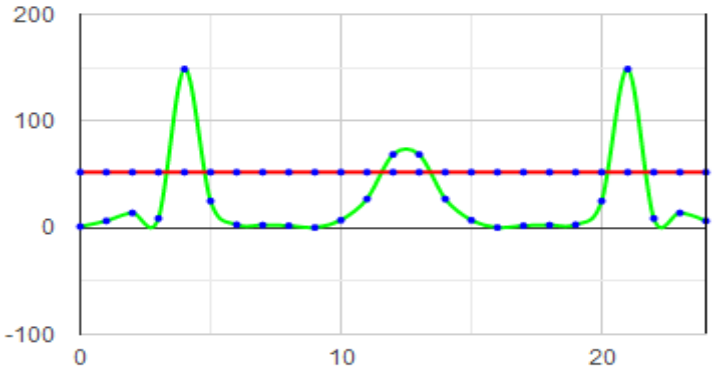

Рис. 1. – Отсечка по выбросам Фурье-спектра последовательностей для построения блока матрицы Пропус порядка 48 (авторская разработка)

Горизонтальная прямая красного цвета на рис.1 (пороговая линия) соответствует значению порядка искомой матрицы. Уровень пороговой линии зависит от типа матриц. Как правило, порог следует задавать пропорциональным размеру матрицы Адамара.

Наличие пика на амплитудном спектре на рис.1 свидетельствует о том, что соответствующая последовательность входит в противоречие с потребностью строить из нее ортогональный массив [19].

Для примера на рис.2 и рис.3 приведены амплитудные Фурье-спектры последовательностей для формирования блоков $\mathbf{A}_{n/4}$ (красный), $\mathbf{B}_{n/4}$ (зеленый), $\mathbf{D}_{n/4}$ (синий) матриц Пропус порядков 28 и 212 соответственно.

Из приведенных рисунков видно, что каждая из последовательностей имеет спектр, меньший n. На рис.3 Фурье-спектры красного и синего цветов идут в некоторой противофазе, а зеленый – в противофазе к их сумме. Это выявленное обстоятельство можно использовать для раннего отсева "неподходящих" последовательностей.

Рис. 2. – Амплитудные Фурье-спектры последовательностей для формирования блоков $\mathbf{A}_{n/4}$ (красный), $\mathbf{B}_{n/4}$ (зеленый), $\mathbf{D}_{n/4}$ (синий) матрицы Пропус порядка 28 (авторская разработка)

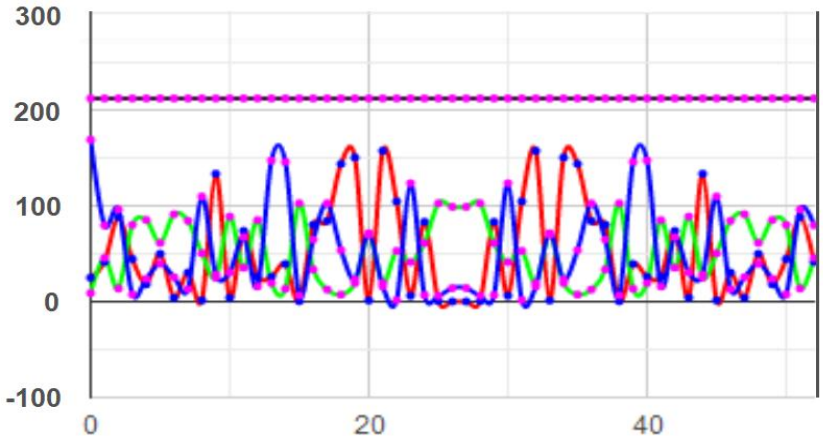

Рис. 3. – Амплитудные Фурье-спектры последовательностей для формирования блоков $\mathbf{A}_{n/4}$ (красный), $\mathbf{B}_{n/4}$ (зеленый), $\mathbf{D}_{n/4}$ (синий) матрицы Пропус порядка 212 (авторская разработка)

Преимущество рассмотренного подхода состоит еще и в том, что такие графики можно строить и изучать статистику частоты появления нужных последовательностей для еще не найденных матриц.

Стабильность воспроизводства условий поиска матриц на компьютерах разного поколения и разной производительности подтверждена равным процентным составом отбираемых последовательностей для построения матриц ряда порядков, полученных экспериментально.

Использование спектра Фурье не единственный прием для отсева ненужных последовательностей. Матрица Фурье – ортогональная матрица, задающая частоты, аналогом которой в дискретной форме являются матрицы Уолша, а в континуальной – матрицы Адамара-Уолша и Мерсенна-Уолша [23]. Иными словами, контролировать поиск матриц Адамара можно и при помощи ранее найденных матриц Адамара или производных от них структурированных матриц.

Поиск редких последовательностей по-настоящему труден, поэтому пренебрегать любой дополнительной информацией не стоит – это тоже культура поиска. Так, например, возможно использовать при поиске корреляционные и автокорреляционные функции. Эти любопытные возможности не указаны в работе [22].

Заключение

В работе рассмотрен современный подход к поиску матриц Адамара высоких порядков – важного математического объекта для методов цифровых ортогональных преобразований информации.

Научная новизна работы, состоящая в развитии ранее не используемого обогащения каталогов последовательностей, как основы построения симметричных матриц Адамара, показывает качественное решение тех же задач, но более высоких порядков.

Сегодня поиск симметричных матриц Адамара переходит в стадию получения гарантированных результатов за приемлемое время за счет применения контроля поиска при помощи амплитудных Фурье-спектров последовательностей.

Благодарность

Авторы выражают благодарность профессорам Н. А. Балонину и М. Б. Сергееву за творческие рекомендации и участие в семинарах, которые

способствовали появлению рассмотренного подхода для повышения эффективности поиска матриц Адамара высоких порядков.

Финансирование

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

Литература

1. Hedayat A., Wallis W.D. Hadamard matrices and their applications // Annals of Statistics. 1978. Vol. 6. pp. 1184-1238. doi:10.1214/aos/1176344370

2. Yarlagadda R.K.R., Hershey J.E. Hadamard Matrix Analysis and Synthesis. New York: Springer, 1997. 123 p.

3. Балонин Н.А., Сергеев М.Б. Специальные матрицы: псевдообратные, ортогональные, адамаровы и критские. СПб.: Политехника, 2019. 196 с. DOI: 10.25960/7325-1155-0

4. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge: Cambridge University Press, 2010. 504 p.

5. Briji J.C. Hadamard Matrix and its Application in Coding Theory and Combinatorial Design Theory // International Journal of Mathematics Trends and Technology. 2018. Vol. 59. pp. 218-227.

6. Mironovsky L.A., Slaev V.A. Strip-Method for Image and Signal Transformation. Berlin, Boston: De Gruyter, 2011. doi.org/10.1515/9783110252569

7. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Use of symmetric Hadamard and Mersenne matrices in digital image processing // Procedia Computer Science. 2018. pp. 1054-1061. DOI: 10.1016/j.procS.2018.08.042

8. Horadam K. J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.

9. Agaian S.S. Hadamard matrices and their application. Berlin: Springer-Verlag, 1986. 227p.

10. Kharaghani H., Tayfeh-Rezaie B. A. Hadamard matrix of order 428 // Journal of Combinatorial Designs. 2005. Vol. 13. pp. 435-440.

11. Doković D.Ž. Generalization of Scarpis' theorem on Hadamard matrices // Linear and Multilinear Algebra. 2017. № 65(10). pp. 1985–1987

12. Hall M. A survey of difference sets // Proceedings of the American Mathematical Society. 1956. Vol. 7. Pp. 975-986.

13. Балонин Н.А., Сергеев М.Б., Суздаль В.С. Динамические генераторы квазиортогональных матриц семейства Адамара // Труды СПИИРАН. 2017. №5 (54). С. 224-243. DOI:10.15622/sp.54.10

14. Сергеев А.М., Балонин Ю.Н. Майнинг Матриц // Обработка, передача и защита информации в компьютерных системах '22. Сборник докладов Второй Международной научной конференции. СПб.: ГУАП, 2022. С. 169-173. DOI: 10.31799/978-5-8088-1701-2-2022-2-169-173

15. Holzmann W.H., Kharaghani H., Tayfeh-Rezaie B. Williamson matrices up to order 59 // Designs, Codes and Cryptography. 2008, № 46 (3), pp. 343-352.

16. Acevedo S., Dietrich H. New infinite families of Williamson Hadamard matrices // Australian Journal of Combinatorics. 2019. Vol. 73(1). pp. 207-219.

17. Turyn R.J. An infinite class of Williamson matrices // Journal of Combinatorial Theory, Series A. 1972. Vol. 12. pp. 319-321.

18. Miyamoto M. A construction for Hadamard matrices // Journal of Combinatorial Theory, Series A. 1991. Vol. 57. pp. 86-108.

19. Абузин Л.В., Балонин Ю.Н., Куртяник Д.В., Сергеев А.М. Генерация, фильтрация и поиск экстремума в сверхбольшом каталоге бинарных последовательностей // Обработка, передача и защита информации в компьютерных системах. Первая Всероссийская научная конференция. СПб.: ГУАП, 2020. С. 121-124. DOI: 10.31799/978-5-8088-1452-3-2020-1-121-124

20. Быков Д.В., Неретин А.Д. Прогнозирование производительности при реализации алгоритмов генерации случайных последовательностей больших размерностей на реконфигурируемых архитектурах с сопроцессорами // Инженерный вестник Дона. 2014. № 2. URL: ivdon.ru/uploads/article/pdf/IVD_90_bykov.pdf_2414.pdf

21. Бахтин Н.И. Применение Фурье-анализа для изучения механизмов формирования электрического потенциала на границе металл-вода // Инженерный вестник Дона. 2008. № 2. URL: ivdon.ru/uploads/article/doc/articles.59.big_image.doc

22. Fletcher R.J., Gysin M., Seberry J. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices // Australasian Journal of Combinatorics. 2001. № 23. pp. 75-86.

23. Балонин Н.А., Балонин Ю.Н., Востриков А.А., Сергеев М.Б. Вычисление матриц Мерсенна-Уолша // Вестник компьютерных и информационных технологий. 2014. №11 (125). С. 51-56. DOI: 10.14489/vkit.2014.011.pp.051-056

References

1. Hedayat A., Wallis W.D. Annals of Statistics. 1978. Vol. 6. pp. 1184-1238. doi:10.1214/aos/1176344370

2. Yarlagadda R.K.R., Hershey J.E. Hadamard Matrix Analysis and Synthesis. New York: Springer, 1997. 123 p.

3. Balonin N.A., Sergeev M.B. Spetsial'nye matritsy: psevdoobratnye, ortogonal'nye, adamarovy i kritskie [Special matrices: pseudo-inverse, orthogonal, Hadamard and Cretan]. SPb.: Politekhnika, 2019. 196 p. DOI: 10.25960/7325-1155-0

4. Wang R. Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis. Cambridge: Cambridge University Press, 2010. 504 p.

5. Briji J.C. International Journal of Mathematics Trends and Technology. 2018. Vol. 59. pp. 218-227.

6. Mironovsky L.A., Slaev V.A. Strip-Method for Image and Signal Transformation. Berlin, Boston: De Gruyter, 2011. doi.org/10.1515/9783110252569

7. Vostrikov A., Sergeev M., Balonin N., Sergeev A. Procedia Computer Science. 2018. pp. 1054-1061. DOI: 10.1016/j.procS.2018.08.042

8. Horadam K. J. Hadamard matrices and their applications. Princeton University Press, 2007. 263 p.

9. Agaian S.S. Hadamard matrices and their application. Berlin: Springer-Verlag, 1986. 227 p.

10. Kharaghani H., Tayfeh-Rezaie B. Journal of Combinatorial Designs. 2005. Vol. 13. pp. 435-440.

11. Doković D.Ž. Linear and Multilinear Algebra. 2017. № 65(10). pp. 1985–1987

12. Hall M. Proceedings of the American Mathematical Society. 1956. № 7. pp. 975-986.

13. Balonin N.A., Sergeev M.B., Suzdal' V.S. Trudy SPIIRAN. 2017. № 5(54). pp. 224-243. DOI:10.15622/sp.54.10

14. Sergeev A.M., Balonin Yu.N. Obrabotka, peredacha i zashchita informatsii v komp'yuternykh sistemakh '22. Sbornik dokladov Vtoroy Mezhdunarodnoy nauchnoy konferentsii (Processing, transmission and protection of information in computer systems '22. Collection of reports of the Second International Scientific Conference). Sankt-Peterburg. 2022. pp. 169-173. DOI: 10.31799/978-5-8088-1701-2-2022-2-169-173

15. Holzmann W.H., Kharaghani H., Tayfeh-Rezaie B. Designs, Codes and Cryptography. 2008, № 46 (3). pp. 343-352.

16. Acevedo S., Dietrich H. Australian Journal of Combinatorics. 2019. Vol. 73(1). pp. 207-219.

17. Turyn R.J. Journal of Combinatorial Theory, Series A. 1972. Vol. 12. pp. 319-321.

18. Miyamoto M. Journal of Combinatorial Theory, Series A. 1991. Vol. 57. pp. 86-108.

19. Abuzin L.V., Balonin Yu.N., Kurtyanik D.V., Sergeev A.M. Obrabotka, peredacha i zashchita informatsii v komp'yuternykh sistemakh. Pervaya Vserossiyskaya nauchnaya konferentsiya (Processing, transmission and protection of information in computer systems. The First All-Russian Scientific Conference). Sankt-Peterburg, 2020. pp. 121-124. DOI: 10.31799/978-5-8088-1452-3-2020-1-121-124.

20. Bykov D.V., Neretin A.D. Inzhenernyj vestnik Dona. 2014. №2. URL: ivdon.ru/uploads/article/pdf/IVD_90_bykov.pdf_2414.pdf

21. Bakhtin N.I. Inzhenernyj vestnik Dona. 2008. №2. URL: ivdon.ru/uploads/article/doc/articles.59.big_image.doc

22. Fletcher R.J., Gysin M., Seberry J. Australasian Journal of Combinatorics. 2001. №23. pp. 75-86.

23. Balonin N.A., Balonin Yu.N., Vostrikov A.A., Sergeev M.B. Vestnik komp'iuternykh i informatsionnykh tekhnologii. 2014. №11 (125). pp. 51-56. DOI: 10.14489/vkit.2014.011.pp.051-056