УДК 519.61:511-33

ДВУЦИКЛИЧЕСКАЯ М-МАТРИЦА 22-го ПОРЯДКА

Н. А. Балонин[а], *доктор техн. наук, профессор*
М. Б. Сергеев[а, б], *доктор техн. наук, профессор*
[а]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, РФ*

Постановка проблемы: *на классе квазиортогональных матриц четных порядков, отличных от порядков матриц Адамара, характер оптимального по детерминанту решения зависит от количества нулей в столбцах взвешенной матрицы. Двуциклические формы оптимальных или субоптимальных матриц служат источниками парных комплементарных последовательностей, обобщающих коды Голея и Баркера. Целью работы является пример построения субоптимальной двуциклической матрицы на критическом для конференц-матриц 22-м порядке.* ***Методы:*** *экстремальные решения ищутся минимизацией максимума абсолютных значений элементов исследуемых матриц с последующей классификацией их по количеству и значениям уровней, зависящих от порядков.* ***Результаты:*** *выделена и описана матричным портретом и значениями уровней модульно шестиуровневая двуциклическая квазиортогональная матрица локального максимума детерминанта (М-матрица) 22-го порядка. Сформулировано предположение о замещении не существующих (по известным критериям) матриц Белевича М-матрицами четных порядков. В качестве иллюстрации приводится сравнение двуциклической М-матрицы 22-го порядка и взвешенной матрицы* ***W****(22,20) по структуре и по детерминанту.* ***Практическая значимость:*** *алгоритмы нахождения двуциклических М-матриц использованы при построении исследовательского программного комплекса. Обобщенные парные комплементарные последовательности составляют основу фильтров, применяемых для сжатия и маскирования изображений.*

Ключевые слова *— ортогональные матрицы, матрицы Адамара, конференц-матрицы, матрицы Белевича, взвешенные матрицы, детерминант матрицы, двуциклические матрицы, коды Голея, коды Баркера.*

В работе [1] определен класс матриц Белевича (конференц-матриц, или С-матриц), известный своей ролью в построении матриц Адамара. Это квадратные матрицы порядка n, кратного 2, с нулевой диагональю и остальными элементами $\{1, -1\}$, обладающие свойством $\mathbf{C}^{\mathrm{T}}\mathbf{C} = (n - 1)\mathbf{I}$, где $\mathbf{I}$ — единичная матрица.

Необходимое условие существования упомянутых целочисленных матриц — разложимость числа $n - k$ на сумму квадратов двух целых чисел [2]. При $k = 1$ порядки, для которых не существуют конференц-матрицы, таковы: 22, 34, 58, 70, 78, 94 ... . Порядок 22 является первым исключением, поэтому принципиально важно знать матрицы, которые на нем могут замещать матрицу Белевича.

К числу обобщений С-матриц относятся взвешенные конференц-матрицы $\mathbf{W}(n, n - k)$ [3, 4], отличающиеся от них количеством $k \ge 1$ нулевых элементов каждой строки или столбца и уравнением $\mathbf{W}^{\mathrm{T}}\mathbf{W} = (n - k)\mathbf{I}$.

Наиболее известное правило построения взвешенных конференц-матриц четных порядков, отличных от порядков матриц Адамара [5], сводится к построению двуциклических структур

$$\mathbf{W}(n,\ n-k)=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}}\end{pmatrix},$$

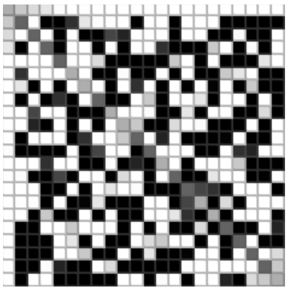
где $\mathbf{A}$, $\mathbf{B}$ — циклические матрицы, построенные на базе парных комплементарных последовательностей Голея добавлением к ним нулей [3].

В работах [6, 7] был описан новый, более общий класс М-матриц, отличающихся от взвешенных конференц-матриц допущением большего, чем $\{0, 1, -1\}$, числа значений элементов (уровней) и удовлетворяющих уравнению $\mathbf{M}^{\mathrm{T}}\mathbf{M} = \mu(n)\mathbf{I}$, где $\mu(n)$ — зависящая от порядка весовая функция.

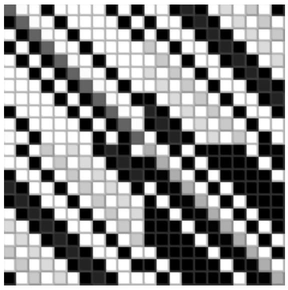
Целочисленные матрицы Белевича и М-матрицы с иррациональными, в общем, уровнями могут обладать как локальным, так и глобальным максимумом детерминанта [7]. Причем на порядках, на которых отсутствуют матрицы Белевича, по критерию максимума детерминанта могут преобладать взвешенные матрицы (порядки 22, 34) или М-матрицы, например, на порядке 58, на котором взвешенная матрица обязана иметь не менее пяти нулей в каждом своем столбце.

Таким образом, М-матрицы полноценно заменяют матрицы Белевича на некоторых значениях порядков, но при этом важным является их строение. В работе [8] предложена шестиуровневая М-матрица 22-го порядка ($\mathbf{M}_{22}$) (рис. 1). Белыми и черными квадратами отмечены элементы 1 и –1 соответственно, а остальные уровни, модули которых имеют значения {0.9802, 0.7846, 0.6924, 0.5299, 0.3076}, переданы оттенками серого цвета. Приведенная структура не позволяет просто описать М-матрицу, кроме того, неясно, почему эта экстремальная по значению детерминанта матрица не симметрична.

Задача поиска парных комплементарных последовательностей, обобщающих бинарные коды Голея на последовательности с большим числом



■ *Рис. 1.* Портрет шестиуровневой матрицы $\mathbf{M}_{22}$ и гистограмма ее элементов



■ *Рис. 2.* Портрет двуциклической шестиуровневой матрицы $\mathbf{M}_{22}$

уровней, в частности, с уровнями М-матриц, может быть решена с помощью опубликованных ранее оптимизационных алгоритмов [9, 10]. Они обладают свойством находить такие комплементарные последовательности кодов при условии, что исходная для итераций матрица представлена не в произвольной, как для приведенной выше М-матрицы, а в двуциклической форме.

Алгоритм, оптимизируя детерминант, сохраняет форму матрицы, приводя к нахождению двуциклической $\mathbf{M}_{22}$ в виде, представленном на рис. 2.

Учитывая, что М-матрицы включают в себя трехуровневые взвешенные матрицы и структурно не отличаются существенно от них, внесем поправку в высказанное в работе [4] предположение о замещениях матриц Белевича.

Предположение. На классе квазиортогональных матриц четного порядка, кратного 2, отличного от значений порядков матриц Адамара, на проблемных для матриц Белевича порядках максимальным значением определителя обладают М-матрицы.

Как видно, полученная структура хорошо поясняет исключительные особенности матриц порядка 22. На диагонали данной структуры, как и у матриц Белевича, сосредоточены самые малые по абсолютной величине элементы (они отмечены серым цветом). Но ортогональности столбцов матрицы не достичь без появления сходных элементов в составе внедиагональных блоков. Компромисс, наблюдаемый у взвешенных матриц, заключается в том, что обе циклические матрицы **A** и **B** имеют нулевые главные диагонали.

Определитель взвешенной матрицы $\det(\mathbf{W}_{22})$ = = 204 800 000 000 000 близок к $\det(\mathbf{M}_{22})$ = = 149 120 095 399 252. В ряде случаев соотношение определителей таких матриц будет меняться на противоположное, особенно для взвешенных матриц малого веса — матриц более чем с двумя нулями в каждом столбце.

Первые строки циклических матриц **A** и **B** дают экономичное описание такой структуры, общей для всех последующих М-матриц четных значений порядков. Парные коды (содержимое строк) обладают экстремальными качествами (обеспечивают оптимальное или субоптимальное значение определителя и т. п.), превосходящими, в том числе, и коды, используемые при построении разряженных взвешенных матриц.

Экстремальные по значению детерминанта квазиортогональные матрицы — предмет пристального внимания исследователей. В этой актуальной для практики помехоустойчивого кодирования области систематически публикуются обзоры, содержащие последние достижения [11, 12].

Приведенный в работе вид двуциклических квазиортогональных матриц нов и связан с новым важным обобщением экстремальных кодов Голея и Баркера [11], применяемых при обработке и защите информации.

Литература

1. **Belevitch V.** Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
2. **Балонин Н. А., Сергеев М. Б.** К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.
3. **Geramita A. V. and Seberry J.** Orthogonal Designs: Quadratic Forms and Hadamard Matrices. — N. Y.: Dekker. 1979. — 460 p.
4. **Балонин Н. А., Сергеев М. Б.** Взвешенная конференц-матрица, обобщающая матрицу Белевича на 22-м порядке // Информационно-управляющие системы. 2013. № 5(66). С. 97–98.
5. **Hadamard J.** Résolution d'une question relative aux determinants//Bulletin des Sciences Mathématiques. 1893. N 17. P. 240–246.
6. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1(50). С. 14–21.

7. **Балонин Н. А., Сергеев М. Б.** Матрицы локального максимума детерминанта // Информационно-управляющие системы. 2014. № 1(68). С. 2–15.
8. **Балонин Ю. Н., Сергеев М. Б.** М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5(54). С. 87–90.
9. **Балонин Ю. Н., Сергеев М. Б.** Алгоритм и программа поиска и исследования М-матриц // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3. С. 82–86.
10. **Балонин Ю. Н.** Программный комплекс MMatrix-2 и найденные им М-матрицы // Вестник компьютерных и информационных технологий. 2013. № 10(112). С. 58–64.
11. **Colbourn C. J., Dinitz J. H.** Handbook of Combinatorial Designs. Sec. Ed. — Chapman and Hall/CRC, 2007. — 967 p.
12. **Horadam K. J.** Hadamard Matrices and Their Applications. — Princeton: Princeton University Press, 2007. — 280 p.

UDC 519.61:511-33

Two-Circulant M-Matrix of the 22nd Order

Balonin N. A.[a], Dr. Sc., Tech., Professor, korbendfs@mail.ru
Sergeev M. B.[a, b], Dr. Sc., Tech., Professor, mbse@mail.ru
[a] Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[b] Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, 49, Kronverkskiy St., 197101, Saint-Petersburg, Russian Federation

Purpose: Within a class of quasi-orthogonal matrices of even orders different from Hadamard matrices a nature of the optimal by determinant solutions depends on an amount of zeros in columns of weighing matrices. Two-circulant forms of optimal or suboptimal matrices have been used as a source of complementary pair sequences generalizing Golay and Barker codes. The goal of this paper is to construct an example of a suboptimal two-circulant matrix of the 22nd order which is critical for conference matrices. **Methods:** There have been found extreme solutions by minimization of maximum of matrix elements absolute values with their consequent classification according to an amount and values of levels depending on orders. **Results:** There has been identified and described by matrix portrait and meaning of levels a modular two-circulant six-level quasi-orthogonal matrix of the 22nd order (M-matrix) having the local maximum. There has been formulated a conjecture on replacing Belevitch matrices if they are absent (do not exist due to the known criteria) by odd order M-matrices. To demonstrate the abovementioned there has been given a comparison of two-circulant 22nd order M-matrix and a weighing matrix **W**(22,20) by its structures and determinants. **Practical relevance:** The algorithms of constructing two-circulant M-matrices have been applied for development of the research software. Generalized complementary pair sequences have been used as a basis of filers for image masking and compression.

Keywords — Orthogonal Matrices, Hadamard Matrices, Conference Matrices, Belevitch Matrices, Weighing Matrices, Matrix Determinant, Two-Circulant Matrices, Golay Codes, Barker Codes.

References

1. Belevitch V. Theorem of 2n-Terminal Networks with Application to Conference Telephony. *Electrical Communication*, 1950, vol. 26, pp. 231–244.
2. Balonin N. A., Sergeev M. B. On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 5(66), pp. 2–8 (In Russian).
3. Geramita A. V. and Seberry J. Orthogonal Designs: Quadratic Forms and Hadamard Matrices. New York, Dekker, 1979. 460 p.
4. Balonin N. A., Sergeev M. B. Weighted Conference Matrix Generalizing Belevich Matrix at the 22nd Order. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 5(66), pp. 97–98 (In Russian).
5. Hadamard J. *Résolution d'une question relative aux déterminants* [Resolution of one problem related to the determinants]. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
6. Balonin N. A., Sergeev M. B. M-Matrices. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 1(50), pp. 14–21 (In Russian).
7. Balonin N. A., Sergeev M. B. The Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1(68), pp. 2–15 (In Russian).
8. Balonin N. A., Sergeev M. B. M-Matrix of 22nd Order. *Informatsionno-upravliaiushchie sistemy*, 2011, no. 5(54), pp. 87–90 (In Russian).
9. Balonin Yu. N., Sergeev M. B. The Algorithm and Program for Searching and Studying of M-Matrices. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2013, no. 3, pp. 82–86 (In Russian).
10. Balonin Yu. N. Software Complex MMatrix-2 and M-Matrices Found by it. *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, 2013, no. 10(112), pp. 58–64 (In Russian).
11. Colbourn C. J., Dinitz J. H. Handbook of Combinatorial Designs. Sec. Ed. Chapman and Hall/CRC, 2007. 967 p.
12. Horadam K. J. Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ, 2007. 280 p.