UDC 004.67
doi:10.15217/issn1684-8853.2018.3.2

TWO-CIRCULANT HADAMARD MATRICES, WEIGHING MATRICES, AND RYSER'S CONJECTURE

Yu. N. Balonin[a], *Research Fellow, tomaball@mail.ru*
A. M. Sergeev[a], *Senior Lecturer, asklab@mail.ru*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*

Introduction: *Hadamard matrices and weighing matrices share the same family. The latter can fill up voids in the matrix space by setting some elements to zero, but this feature has not been properly studied yet.* ***Purpose:*** *To study how the orders of orthogonal matrices used in information processing can affect their structure.* ***Results:*** *For Ryser's conjecture about orders critical for cyclic Hadamard matrices, an extension has been suggested, covering Hadamard matrices and weighing matrices which consist of two cyclic blocks. We give examples of Hadamard matrices extended to the newly revealed critical order equal to 32, with symmetrical blocks or, on higher orders, with unsymmetrical blocks. We also present two-circulant weighing matrices which replace Hadamard matrices and alternate with them. There is an exceptional case related to the order 24 on which two-circulant Hadamard matrices or weighing matrices do not exist, forcing you to search for a solution among four-block constructions. A special set of Hadamard matrices of 20- and 52-fold orders is pointed out, as their blocks are asymmetric. A new assumption about the critical order 64 is discussed.*

Keywords *— Information Processing, Noise-Immune Coding, Masking Images, Orthogonal Matrices, Quasi-Orthogonal Hadamard Matrices, Belevitch Matrices, Weighing Matrices, Two-Circulant Matrices, Ryser's Conjecture.*

Citation: Balonin Yu. N., Sergeev A. M. Two-Circulant Hadamard Matrices, Weighing Matrices, and Ryser's Conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 2–9. doi:10.15217/issn1684-8853.2018.3.2

Introduction

The practical interest to orthogonal (quasi-orthogonal) matrices is attributable to their features which make them highly popular in digital processing and data conversion systems. Orthogonal matrices, including Fourier matrices, Hadamard matrices, and their most close even-order interpretations which are Belevitch matrices and weighing matrices, are used in noise-proof coding, spectral expansion, image processing, code division of communication channels, security masking, etc.

The orthogonality of these matrices enables their congruent transformation. The possible orthogonal bases, including symmetrical, circulant, two-circulant and other matrix constructions, considerably expand the ways of optimization for certain data conversion problems [1, 2]. In coding theory, Hadamard matrix columns are used to build codes with large code distances [3, 4]. The special way to number the columns of such matrices in digital signal processing, image compression and masking is interpreted as a two-level representation of Walsh function.

The features of such matrices assume special importance when these conversions are implemented in specialized processors at hardware or firmware level. Since the form of the matrices, their orders and values of their elements significantly affect the choice of the corresponding filters, cost of hardware and speed of conversion, it is especially important to properly choose orthogonal matrices out of their vast variety when developing a processor.

Some modern practical applications of orthogonal matrices in genetics, biomechanics, medical technology, crystallography, video data conversion, etc. [5–7] require the fundamentals of the current digital methods to be reconsidered. From this point of view, integer values of matrix elements are not as important as the extremal properties of the matrices and their existence for all possible orders.

The theory of Hadamard matrices $\mathbf{H}_n$ with orthogonal columns of elements 1 and –1 was developed from simple manual calculation methods supplementing the initial sequence of Silvester matrices towards more sophisticated ones with the use of nested matrices by Scarpis method or finite fields used by Paley [8–10].

As time elapsed, the researchers' interest moved from unstructured or semi-structured matrices to those with a clearly pronounced structure [11, 12].

Ryser was the first who noticed that the existence of orthogonal circulant matrices had a limitation. He formulated a conjecture that there were no circulant Hadamard matrices of orders $n > 4$. Turin proved in his work [2] that the conjecture was true for matrices of 8-fold orders. The trials to prove this statement for a more general case are still a subject of profound theoretical research in the area of high-order matrices, though far from any practical application. More practically essential were the suggestions to go beyond the accepted limitation at

the cost of some minor concessions. For example, Barker introduced so called Barker codes which are a source for circulant matrices of orders not higher than 13. When the order is higher than 4, they are not orthogonal but close to that in a strict sense pointed out by Barker himself: he noted that their autocorrelation function has a spike at the beginning but then deviates from zero by no more than 1, oscillating with the values 1 and –1.

Thus, the subject of circulant matrices became exhausted and the interest gradually moved to the area of two-circulant structures which had been poorly studied until recently. Note that a circulant structure is symmetric about the secondary diagonal, therefore Barker's conjecture actually describes a limitation for symmetric matrices.

Two-circulant Hadamard matrices are built on the base of two monocirculant matrices **A** and **B** of twice smaller order. **A** and **B** can be either circulant or backcirculant. Note that when applied to two-circulant Hadamard matrices, an extended interpretation of Ryser's conjecture becomes possible [13–15].

The goal of this work is to describe the structures of two-circulant Hadamard matrices found by the algorithm of search for local determinant maximum [16], different from all the above-listed classical methods, and to study in more details the peculiarities of the extended Ryser's conjecture about Hadamard matrices with two-circulant structure.

Alteration of Hadamard Matrices and Weighing Matrices

For the sake of convenience, we will consider two-circulant matrices built on a circulant **A** and backcirculant **B** matrices. Ryser's limitation is also valid for matrices of orders smaller than the critical order 4. A circulant Hadamard matrix of second order $\mathbf{H}_2$ does not exist [2].

A two-circulant structure considerably expands the opportunities for combining. A circulant Ryser's matrix of order 4 can be treated as a two-circulant matrix built of monocirculant blocks $\mathbf{A} = \mathbf{H}_2$ and $\mathbf{B} = \mathbf{J}$, where **J** is a block of ones.

Fig. 1 shows an additional structure obtained by doubling a circulant diagonal Ryser's matrix $\mathbf{H}_4$ by Silvester's rule. The shown two-circulant Hadamard matrices are symmetric and doubly symmetric by blocks, but so far they just slightly move Ryser's bound from order 4 to 8.

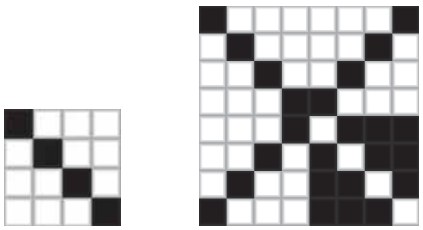
Paired elements 1 and –1 of Hadamard matrices are traditionally depicted on matrix portraits as white and black cells respectively.

The next non-trivial generalization of Ryser's rule is that an order-12 two-circulant matrix, though still doubly symmetric, is "forced" to have zeros on both the diagonals of blocks **A** and **B**. Such matrices were first introduced by professor J. Seberry from Wollongong Science Centre in Australia. She dubbed them "weighing matrices" and denoted as **W** [1]. Later it became common to formally denote such matrices by specifying not only the order but also the number of non-zero elements in the rows. In our case, it is $\mathbf{W}(n, n-2)$. Elements with value 0 are usually depicted on matrix portraits in gray.

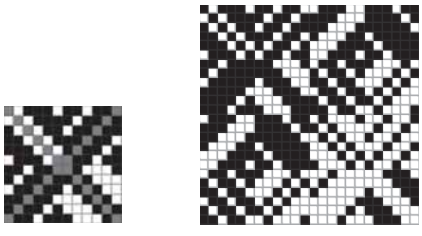
From a weighing matrix $\mathbf{W}(n, n-2)$ you can go to a Hadamard matrix of a twice higher order $\mathbf{H}_{2n}$ whose blocks will coincide with those of the weighing matrix, having the same signs and values of the diagonal elements, which is a generalization of Silvester's order duplication algorithm. Fig. 2 shows both these matrices. The first of them, weighing matrix $\mathbf{W}_{12}$, was found by a determinant optimization program [12, 16].

Hadamard matrices are strictly optimal by determinant. Hence, an order-12 weighing matrix which differs from them and has a simple two-circulant structure exists in the secondary maximum which is the local maximum of the determinant. This means that any sufficiently small change in the matrix elements not making the absolute value of an element higher than 1 decreases the determinant. Therefore, the determinant optimization algorithm can be used to find and analize weighing matrices in the case when two-circulant Hadamard matrices do not exist and the absolute maximum of the determinant belongs to more complex structures.

A weighing matrix $\mathbf{W}_{12}$ replaces a two-circulant Hadamard matrix which does not exist for this order. Weighing matrices alternate with Hadamard matrices in two-circulant form. On order 16, we again



■ ***Fig. 1***. Portraits of a circulant $\mathbf{H}_4$ and two-circulant $\mathbf{H}_8$ matrices



■ ***Fig. 2***. Portraits of matrices $\mathbf{W}_{12}$ and $\mathbf{H}_{24}$

meet a doubly symmetric structure (Fig. 3) which moves Ryser's bound still farther from order 4. This result argues against Ryser's conjecture.

We can presume that this rule is general for all two-circulant matrices of orders 12, 20, 28, 26, etc. On these orders, Hadamard matrices replace weighing matrices which have two zero diagonals. Hadamard matrices of orders $n = 2^k$ have structures belonging to the general sequence of Silvester's orders; however, as we will see later, they do not keep a double-axis or ordinary symmetry. In particular, unsymmetric two-circulant Hadamard matrices produce codes of Mark Golay who used them to continue his search for Barker's monocycles, not orthogonal but close to that. On the other hand, Golay's codes do not support symmetry, so the structure we found for order 16 belongs to a different family, not yet described.

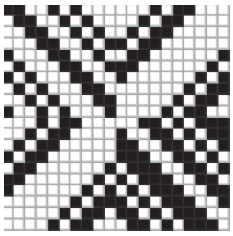
Symmetric order-16 Hadamard and Golay matrices precede the doubly symmetric weighing matrix $\mathbf{W}_{20}$ shown in Fig. 4 along with a Hadamard matrix of a doubled order, according to our presumptions.

Matrix $\mathbf{H}_{40}$ demonstrates a *twister of Seberry* (nearly symmetric Hadamard matrices): the elements of its second subblock form a circulating structure. You can obtain it by unfolding the blocks **A** and **B** of a weighing matrix during the transition to a Hadamard matrix with circulating elements. The twister is a model of standing waves in a square pool with four oscillating areas described by the matrices of nested blocks. Hence, Hadamard matrices are a mathematical interpretation of resonances in a closed cavity (standing waves). Pioneering works in this area belong, among others, to professor J. Seberry. According to Golay's studies [2], on order 20 a main maximum of the determinant exists, producing an unsymmetric matrix $\mathbf{H}_{20}$ (Fig. 5).

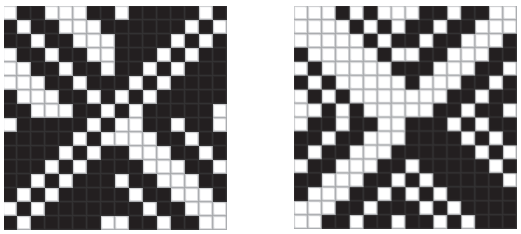
Thus, unsymmetric Golay's sequences for a side branch of orthogonal codes starting on order 20 complement symmetric sequences of weighing matrices. This fact has never been pointed out in scientific literature. Three Golay's side branches are known; the next one starts on order 52. So, order 20 is an order on which symmetry becomes the cost of an attainable absolute maximum. If you focus on symmetric structures, it makes more sense to use open weighing matrices.

Note that the period on which you meet a two-circulant Hadamard matrix grows as the problem size increases. This feature is also shared by weighing matrices. For example, on order 24 we failed to find a weighing two-circulant matrix, which happened for the first time. Instead of it, we found a more complex structure which consisted of not two but four blocks and inherited a pair of blocks from $\mathbf{W}_{12}$. Accordingly, it produces a matrix $\mathbf{H}_{24}$ without the need to double the order, which is demonstrated in Fig. 6.

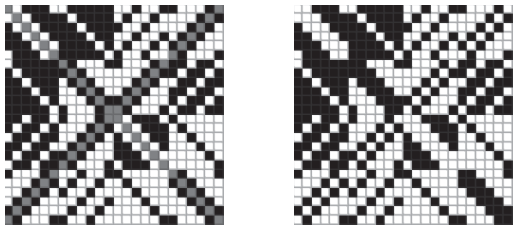
The advantage of complicating is that a four-block weighing matrix, during the transition to a



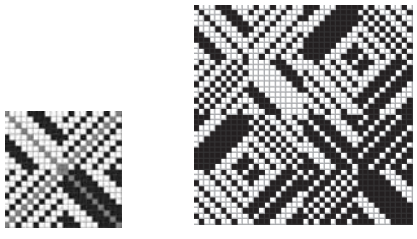
■ ***Fig. 5***. Unsymmetric matrix $\mathbf{H}_{20}$



■ ***Fig. 3***. Portraits of two matrices $\mathbf{H}_{16}$ with symmetric blocks



■ ***Fig. 6***. Portraits of matrices $\mathbf{W}_{24}$ and $\mathbf{H}_{24}$



■ ***Fig. 4***. Portraits of matrices $\mathbf{W}_{20}$ and $\mathbf{H}_{40}$

■ ***Fig. 7***. Portraits of matrices $\mathbf{W}_{28}$ and $\mathbf{H}_{56}$

Hadamard matrix, does not require that the order is doubled. Actually, it is a general rule, because when the order is doubled, we go exactly to a four-block structure, found here in a slightly different form with respect to $\mathbf{W}_{12}$. It is followed by a weighing matrix $\mathbf{W}_{28}$ which does not contain anything new or unexpected; by doubling the order, it produces a Hadamard matrix $\mathbf{H}_{56}$. These two matrices are shown in Fig. 7.

Extended Ryser's Bound and its Generalizations

The episode with critical order 24 shows that matrix structures can become more complex. In what follows, we confirm the result obtained in [13] as on order 32 we again meet a doubly symmetric Hadamard matrix of an order of Silvester's sequence. For reference, a structure which is not doubly symmetric is shown next to it in Fig. 8. Remember that the known two-circulant Golay's matrices are not symmetric.

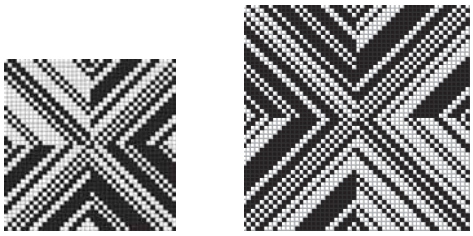
Analysis has shown that order 32 describes the generalization of Ryser's conjecture for two-circulant structures. Beyond this order, it is impossible to obtain a Hadamard matrix in two-circulant form. Nevertheless, our experience with searching for symmetric structures by a determinant optimization program shows that symmetric codes still have some safety margin: a doubly symmetric weighing matrix $\mathbf{W}_{36.}$ By doubling its order, you can turn it into a symmetric Hadamard matrix $\mathbf{H}_{72}$ shown in Fig. 9.

This additional experience supplements the estimation of Ryser's bound for two-circulant orthogonal matrices performed in [13] by new details about weighing matrices.

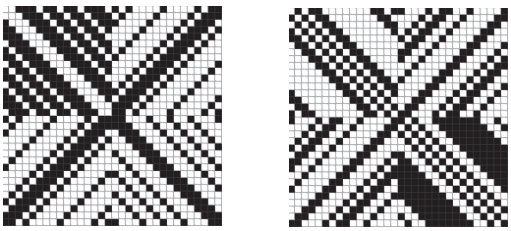
Two-circulant matrices $\mathbf{H}_{40}$ and $\mathbf{H}_{52}$ are not matrices of Silvester's type. They belong to sequences of unsymmetric matrices of 20-fold and 52-fold orders (Fig. 10).

The new doubly symmetric weighing matrix $\mathbf{W}_{52}$ we have found can produce, through doubling its order, a nearly symmetric Hadamard matrix $\mathbf{H}_{104}$ shown in Fig. 11. In other words, from the viewpoint of searching for symmetric matrices, this family is preferable, being considerably different from Mark Golay's two-circulant matrices. Golay's sequences of orders 2, 10 and 26 producing Hadamard matrices of orders 4, 20 and 52 yield unsymmetric codes, so their practical alternative can be symmetric codes of weighing matrices of respective orders.

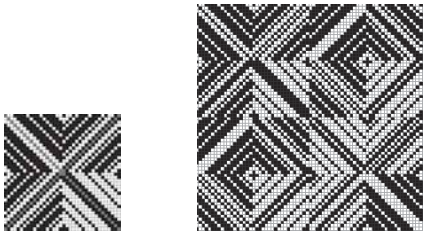
The symmetry of orthogonal matrices on the specified orders and the very fact of their existence is a subject of modern studies. According to a new assumption which resulted from considering a chain of two-circulant Hadamard matrices, order 64 is a key for checking the extended conjecture.



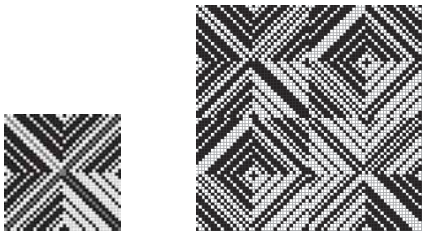
■ ***Fig. 10.*** Portraits of matrices $\mathbf{H}_{40}$ and $\mathbf{H}_{52}$



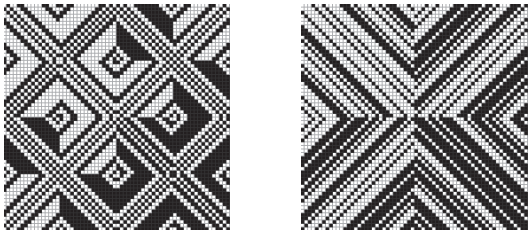
■ ***Fig. 8.*** Two matrices $\mathbf{H}_{32}$



■ ***Fig. 11.*** Portraits of matrices $\mathbf{W}_{52}$ and $\mathbf{H}_{104}$



■ ***Fig. 9.*** Portraits of matrices $\mathbf{W}_{36}$ и $\mathbf{H}_{72}$



■ ***Fig. 12.*** Symmetric and unsymmetric matrices $\mathbf{H}_{64}$

Order 64 is the simplest one for search and symmetry check of Hadamard matrices from Silvester's sequence. For this order, we have identified the symmetric four-circulant matrix shown in Fig. 12.

If a symmetric two-circulant matrix $\mathbf{H}_{64}$ does not exist (which is confirmed by our experiment on searching, with a formal algorithm, for matrices optimal by determinant), then on higher orders there are no symmetric two-circulant matrices.

Chains of Golay's matrices $\mathbf{H}_{20} — \mathbf{H}_{40} —$... and $\mathbf{H}_{52} — \mathbf{H}_{104} —$... of 20-fold and 52-fold orders are apparently unsymmetric.

Algorithm Scheme

Fig. 13 shows a simplified scheme of the algorithm developed by the authors. It consists of three sequentially performed blocks (from left to right):

— two-circulant matrix generator;

— cross-accumulator which provides the possibility for the matrices to swap their parts **A** and **B**;

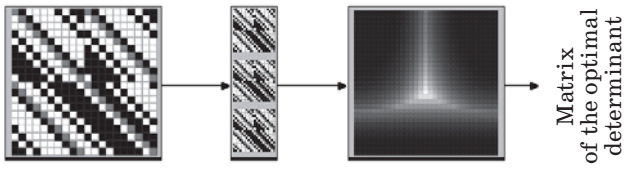
— two-circulant matrix determinant optimizer.

With software implementing the proposed algorithm, you can control the optimized determinant and visually control the structure of the resulting matrix.

The determinant optimizer is fully considered in [16] and will not be discussed here. We will only note that it is a novel scheme, not like any other one widely known from the numerical analysis literature. It optimizes not the determinant calculation algorithm, but a matrix with n^2 elements.

A matrix with a two-circulant structure has a stable local determinant, because to let the iterations go to the absolute maximum, you would have to rebuild the rigidly specified initial structure. It is much easier to convert the matrix elements 1 to 0 or –1, providing that the result is fixed in the form of a Hadamard matrix or weighing matrix if they exist. This scheme can easily be transformed for tetracycle search.

The cross-accumulator is a block which significantly reduces the time cost of generating the necessary initial matrices. At this stage, the blocks **A** and **B** can be relatively random, and the combinational circuit which allows the initial matrices to swap their already generated parts saves the computing resources. Besides, the matrices accumulated in the database can be cached, being spread over buffer zones according to the value of a certain cache function. Blocks which considerably differ from each other are filtered and never come to the cross-accumulator input together.



■ ***Fig. 13.*** Algorithm scheme

These preliminary measures enrich the output of the cross-accumulator, giving the optimizer the material it needs. Such an algorithm can be implemented in several languages. We have developed software versions in C++, Pascal and Javascript. Each of these versions has its advantages.

The implementation in C++ is the fastest one but needs a heavy compiler and is not suitable for all computers. The Pascal implementation is slower but more universal; it can be run under any version of Windows starting from XP. The Javascript implementation within mathscinet.ru international mathematical network is available for wide circles of scientists and researchers from different countries, as well as for students studying orthogonal transformations.

Javascript software has another implicit advantage: it provides the opportunity for a wide circle of users to modify the underlying algorithm. This is very valuable in a research when you need to modify both the algorithm and the construction of the calculated matrix.

Apart from the cyclic array form, there is its negacyclic form, when during a shift of a block row its last pushed-out element is carried to the beginning with its sign inverted. Besides, the size of a two-circulant matrix can be reduced by several elements using the matrix border distinctive in its wide variety of implementation. Most commonly, Hadamard and weighing matrices have structures with unary or binary border, leading to a multi-block implementation of the matrix core. Studying the cores can explain on which structure the absolute determinant maximum is attainable and where it goes to from a two-circulant structure with buffer zeros. However, the search for universal cores of orthogonal matrices is beyond the scope of this research.

The Novelty of the Results

Hadamard and weighing matrices are an object of intensive studies because of their application in information processing; in particular, image processing. New facts are regularly discovered: for example, an exhaustive search for rows in weighing matrices with a single zero (Belevitch matrices) showed recently that these matrices do not exist in a two-circulant form on order 66. The same, according to some experimental results, if true for order 86. These orders follow each other with a step of 20.

On order 46, Maton's result is widely known. He found a solution in the form of a five-block matrix:

in two of these five, not elements are shifted but entire sequences of elements. These results are very valuable because forms of matrices with an absolute determinant maximum are not theoretically known, and the discovery of Belevitch matrices of orders 66 and 86 stimulates the research in this field. So far, the question about what Maton's structure turns into when the order increases by 20 has no answer, either.

Studies of weighing matrices have been focused mostly on forms with many zeros. Considering them a natural supplement to two-circulant Hadamard matrices when the latter do not exist is a new approach. Especially new is the idea that they expand symmetric structures, because the extended Ryser's bound as such, up to order 32, was discovered and studied quite recently, with the use of supercomputers in a scientific centre in Canada. Hence, the results of our experiment introduce a significant correction to this knowledge of two-circulant matrices, showing what a symmetric structure turns into when it cannot be embodied in the form of matrices with elements 1 and –1.

The discovery of symmetric two-circulant weighing matrices $\mathbf{W}(n, n-2)$ on orders of Hadamard matrices $n = 4t$ makes them available for practical applications and poses new theoretical problems: in particular, what Ryser's bound is for weighing matrices. Symmetric weighing matrices with two zeros supplement symmetric Belevitch matrices in the sense that in both cases they are a source for Hadamard matrices of a doubled order. Finite field theory receives a new application domain here, as we have to find out how to calculate these new matrices; sometimes, for very high orders.

For video information coding systems, the two-circulant scheme is good because it is relatively simple to implement. Omissions of two-circulant Hadamard matrices caused unnecessary problems for the applications in passing to tetracyclic constructions. In other words, the results of the research in this area seriously affects the efficiency of the applications.

Some Applications for Visual Information Transmission Systems

The transmission of visual information, i.e. images or frame-by-frame video, is an integral feature of territory monitoring systems, multifunctional registration systems, distributed industrial systems, security surveillance systems, and other systems which use open networks to build their infrastructure. The information transmitted in such distributed video systems, even not top-secret information, needs to be protected from unauthorized access, distortion in the communication channels or substitution.

Generally, the process of protecting visual information goes as follows. At the transmitting side of a distributed system, the protected information is shaped. Then it is directed to a communication channel where it may become a target for the above-mentioned threats. At the receiving side, the protected information is recast into the initial form, along with finding out whether it has been distorted by noise or deliberately changed by a third party. Depending on the implementation of the method and circuitry, the visual information can come to the receiving side either with or without losses.

An effective way to protect visual information from unauthorized usage is the method of bilateral matrix masking [17]. According to it, an image (frame) $\mathbf{P}$ at the transmitting side is masked by an orthogonal Hadamard matrix as $\mathbf{Y} = \mathbf{H}^{\mathrm{T}}\mathbf{P}\mathbf{H}$. Such a transformation visually destroys the image down to a level similar to noise, with computing cost much smaller compared to coding methods. This allows you to mask images (video frames) in real time, as fast as they come from the video camera matrix.

The shaped and masked image $\mathbf{Y}$ is passed through the communication channel to the receiving side where it undergoes a reverse bilateral transformation in order to obtain the initial image according to the expression $\mathbf{P} = (\mathbf{H}^{\mathrm{T}})^{-1}\mathbf{Y}\mathbf{H}^{-1}$.

The use of orthogonal Hadamard matrices $\mathbf{H}$ $(\mathbf{H}^{-1} = \mathbf{H}^{\mathrm{T}})$ simplifies the computing down to $\mathbf{P} = \mathbf{H}\mathbf{Y}\mathbf{H}^{\mathrm{T}}$. In this case, the reverse transformation repeats the direct one with a precision of transposing the masking matrix; also, there is no need to separately store or calculate the reverse matrix: this saves memory when the method is implemented within the system. The next advantage can be provided by switching to Hadamard matrices with symmetric structures [18] for which the amount of the stored data to produce an order-n Hadamard matrix of circulant or two-circulant structure can be no more than n elements, as many as one row of a matrix.

In a similar way, we can implement the method of noise-proof image coding used in data transmission systems when the ratio signal/noise is low, known as strip transformation [19]. However, for this transformation two different orthogonal matrices are used (those of premultiplication and postmultiplication), and the multiplication itself yields Kronecker product, adding small extra computing cost with software implementation of the method, as compared to masking.

In order to prevent image substitution or changing, the procedure of introducing digital watermarks can be applied, with the use of Hadamard transformation [20].

Conclusion

The principal question of Ryser's theory about two-circulant Hadamard matrices is determining the maximum achievable order of symmetry and the form of symmetric matrices which are exceptions. For example, the conference matrices of Maton's construction found for order 46 already have non-circulant blocks in their structure.

If there are no symmetric two-circulant structures, and Golay's codes produce only unsymmetric blocks, then the source for symmetric Hadamard matrices of orders higher than 32 will be two-circulant and four-circulant weighing Seberry matrices with two zeros on their diagonals.

The extension of Ryser's conjecture can explain the peculiarities of the order alteration followed by Hadamard matrices and weighing matrices. It can also explain the difficulties experienced when searching for matrices of Hadamard family and symmetric conference matrices.

The work has been carried out with the support of Ministry of Education and Science of the Russian Federation for research within the development part of the scientific governmental task #2.2200.2017/4.6

References

1. Seberry J. *Orthogonal Designs. Hadamard Matrices, Quadratic Forms and Algebras*. Springer, International Publishing AG, 2017. 459 p. doi:10.1007/978-3-319-59032-5_1 http://www.springer.com/us/book/9783319590318
2. Craigen R., Kharaghani H. Hadamard Matrices and Hadamard Designs. In: *Handbook of Combinatorial Designs*. 2nd ed. C. J. Colbourn, J. H. Dinitz (eds). Boca Raton, FL, Chapman & Hall/CRC, 2007. Pp. 273–280.
3. Tarannikov Iu. V. *Kombinatornye svoistva diskretnykh struktur i prilozheniia k kriptografii* [Combinatorial Properties of Discrete Structures and Applications to Cryptography]. Moskow, MTsNMO Publ., 201. 152 p. (In Russian).
4. Jongkil Kim, Willy Susilo, Man Ho Au and Jennifer Seberry. Efficient Semi-Static Secure Broadcast Encryption Scheme. *LNCS*, Berlin, Springer Verlag, 2014, vol. 8365, pp. 62–76.
5. Petukhov S. V. *Matrichnaia genetika, algebry geneticheskogo koda, pomekhoustoichivost'* [Matrix Genetics, Algebras of The Genetic Code, Noise Immunity]. Moskow, RKhD Publ., 2008. 316 p. (In Russian).
6. Petoukhov S. V. The Genetic Coding, United-Hypercomplex Numbers and Artificial Intelligence. *Advances in Artificial Systems for Medicine and Education*, 2017, pp. 2–13.
7. Moon Ho Lee, Han Hai, Sung Kook Lee, Petoukhov S. V. A Mathematical Proof of Double Helix DNA to Reverse Transcription RNA for Bioinformatics. *Advances in Artificial Systems for Medicine and Education*, 2017, pp. 23–38.
8. Dragomir Ž. Doković. Generalization of Scarpis' Theorem on Hadamard Matrices. *Linear and Multilinear Algebra*, 2017, vol. 65, iss. 10, pp. 1–3.
9. Dragomir Ž. Doković. Williamson Matrices of Order 4n for n = 33;35;39. *Discrete Math*, 1993, vol. 115, pp. 267–271.
10. Holzmann W. H., Kharaghani H., Tayfeh-Rezaie B. Williamson Matrices up to Order 59. *Designs, Codes and Cryptography*, 2008, no. 46, pp. 343–352.
11. Sergeev A. M. Generalized Mersenne Matrices and Balonin's Conjecture. *Automatic Control and Computer Sciences*, 2014, vol. 48, no. 4, pp. 214–220.
12. Balonin Ju. N., Vostrikov A. A., Sergeev A. M., Egorova I. S. On Relationships Among Quasi-Orthogonal Matrices Constructed on the Known Sequences of Prime Numbers. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2017, iss. (1)50, pp. 209–223. doi:http://dx.doi.org/10.15622/sp.50.9 (In Russian).
13. Balonin N. A., Djokovic D. Symmetry of Two Circulant Hadamard Matrices and Periodic Goley Pairs. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
14. Gene Awyzio and Jennifer Seberry. On Good Matrices and Skew Hadamard Matrices. *Springer Proc. in Mathematics and Statistics: Algebraic Design Theory and Hadamard Matrices*, 2015, pp. 13–28.
15. Olivia Di Matteo, Dragomir Z. Djokovic, Ilias S. Kotsireas. Symmetric Hadamard Matrices of Order 116 and 172 Exist. *Special Matrices*, 2015, no. 3, pp. 227–234.
16. Balonin N. A., Sergeev M. B., Suzdal V. S. Dynamic Generators of the Quasiortogonal Hadamard Matrix Family. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2017, iss. (5)54, pp. 224–243 (In Russian). doi:http://dx.doi.org/10.15622/sp.54.10
17. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images. *Smart Innovation, Systems and Technologies*, 2015, vol. 40, pp. 161–168. doi: 10.1007/978-3-319-19830-9_15
18. Sergeev A. M., Blaunstein N. S. Orthogonal Matrices with Symmetrical Structures for Image Processing. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 6, pp. 2–8 (In Russian). doi:10.15217/issn1684-8853.2017.6.2
19. Mironovskii L. A., Slaev V. A. The Strip Method of Noise-Immune Image Transformation. *Measurement Techniques*, 2006, vol. 49, no. 8, pp. 745–754.
20. Anthony T. S. Ho, Jun Shen, Soon Hie Tan. A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform. *School of Electrical and Electronic Engineering*, 2003, vol. 4793, pp. 76–85.

УДК 004.67
doi:10.15217/issn1684-8853.2018.3.2

Двуциклические матрицы Адамара, взвешенные матрицы и гипотеза Райзера

Балонин Ю. Н.[a], инженер, tomaball@mail.ru
Сергеев А. М.[a], старший преподаватель, asklab@mail.ru
[a]Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ

Введение: матрицы Адамара и взвешенные матрицы образуют единое семейство, причем свойство последних заполнять пустоты матричного пространства посредством обнуления части элементов изучено недостаточно полно. **Цель:** исследование влияния порядков ортогональных матриц, используемых для обработки информации, на их структуру. **Результаты:** рассмотрено расширение гипотезы Райзера, трактующей критические для циклических матриц Адамара порядки, на матрицы Адамара и взвешенные матрицы, состоящие из двух циклических блоков. Приведены примеры матриц Адамара, расширенных до выявленных на новом критическом порядке, равном 32, с симметричными блоками, и более высоких порядках — с несимметричными блоками. Представлены чередующиеся с матрицами Адамара и заменяющие их двуциклические взвешенные симметричные и несимметричные матрицы. Приведен случай-исключение — порядок 24, на котором нет двуциклических матриц Адамара и взвешенных матриц, что вынужденно переводит решение задачи к четырехблочным конструкциям. Отмечена особая линия матриц Адамара порядков, кратных 20 и 52, выделенных среди остальных матриц асимметрией своих блоков. Сформулировано новое предположение о критическом порядке 64.

Ключевые слова — обработка информации, помехоустойчивое кодирование, маскирование изображений, ортогональные матрицы, квазиортогональные матрицы Адамара, матрицы Белевича, взвешенные матрицы, двуциклические матрицы, гипотеза Райзера.

Цитирование: Balonin Yu. N., Sergeev A. M. Two-Circulant Hadamard Matrices, Weighing Matrices, and Ryser's Conjecture // Информационно-управляющие системы. 2018. № 3. С. 2–9. doi:10.15217/issn1684-8853.2018.3.2
Citation: Balonin Yu. N., Sergeev A. M. Two-Circulant Hadamard Matrices, Weighing Matrices, and Ryser's Conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 2–9. doi:10.15217/issn1684-8853.2018.3.2

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12-ти языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org