Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2018) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

Use of symmetric Hadamard and Mersenne matrices in digital image processing

Anton Vostrikov[a,*], Mikhail Sergeev[a], Nikolaj Balonin[a], Alexander Sergeev[a]

[a] *Department of Computer Systems and Networks, Saint-Petersburg State University of Aerospace Instrumentation, 67 Bolshaya Morskaya street, Saint-Petersburg, 190000 Russian Federation*

Abstract

Matrices with orthogonal columns (rows) are extensively used in data processing. One of the pressing challenges for developers of image processing systems is the ability to choose easily the optimal types of structured orthogonal matrices for their specific tasks. The purpose of this study is to systemize the main types of structured symmetric Hadamard matrices, such as the cyclic, negacyclic, bicyclic, four-block and Propus-form three-block ones, which can be used in image processing for compression, filtering, antinoise coding, and masking. The basis of Hadamard matrices is extended with quasi-orthogonal Mersenne matrices of odd orders with previously unknown symmetry properties. It was found that Mersenne matrices and Hadamard matrices built using Mersenne matrices are directly associated with numeric sequences, for some of which the cyclic, bicyclic matrices, and Propus-shaped matrices exist. The paper demonstrates that the use of Mersenne matrices as a "core" produces Haramard matrices with new symmetric structures. This fact expands the classification of orthogonal matrices. Images of previously unknown symmetric Hadamard matrices are provided. The practical value of the paper is that the obtained results provide wide opportunities to facilitate the selection of matrices, which best fit for processing of certain images, including images of non-standard sizes. The number of matrix fragments sufficient for reconstruction of the whole matrix is defined for all matrices under consideration. This way of representation of Hadamard symmetric matrices allows us to increase the efficiency of the image processing using lesser the computer memory.

Keywords: orthogonal matrices; quasi-orthogonal matrices; bicyclic matrices; Propus matrices; Hadamard matrices; Mersenne matrices; image processing; antinoise coding; masking

* Corresponding author. Tel.: +7-921-943-0422 ; fax: +7-812-710-6510 .
E-mail address: vostricov@mail.ru

1877-0509

1. Introduction

Matrices with orthogonal columns (rows) are extensively used in data processing, for example, Hadamard matrices (**H**) [1] of orders 1, 2 and $n = 4k$, where k is the positive integers with two element values 1 and –1. The $\mathbf{H}_n^{\mathrm{T}}\,\mathbf{H}_n = n\mathbf{I}$ equation is true for them, where **I** is the unity matrix. The attractiveness of Hadamard matrices lies in the fact that they have only two integer element values and the computational algorithms with them are easy to implement.

The tasks related to digital image processing using orthogonal matrices include the filtering, compression, anti-noise coding, and masking of images and video sequences [2-7]. The practice of application of orthogonal matrices requires them to be of simple structures. This defines, in many ways, the size of memory required to store pre-defined matrices or the time required to generate matrices by the image processing system. The symmetric structures of Hadamard matrices involve the cyclic, negacyclic, block-symmetric, of "core with bordering" shape, and others.

The current paper considers the structured Hadamard matrices with the purpose of providing the developers of image processing systems with an easy way to select optimal matrices for mentioned above tasks.

2. Structures of Symmetric Orthogonal Matrices

There is no unified algorithm for direct construction of Hadamard matrices with symmetric structures on orders $n = 4k$, where k is a positive integer. Among the simplest structures, the most interesting are ***symmetric matrices,*** which have a number of useful features. They are called symmetric because similar elements of such matrices are arranged symmetrically relative to the main diagonal. Multiplying by symmetric matrices implies less operational costs, that is why the symmetry, in general, is efficient for both storing matrices in memory and image processing. Elements $(n^2 + n)/2$ of such matrices are required for their storage and reconstruction.

Cyclic symmetric orthogonal matrices have an even simpler structure, which is defined by the first row n of their elements. All subsequent rows can be found by successively shifting previous rows to the right and adding the pushed out elements to the left. The advantage of cyclic matrices is evident. Only n elements of the first row need to be stored regarding to $(n^2 + n)/2$ elements for a symmetric matrix. This results in the saving of memory and faster multiplication operations.

It should be noted that even if a cyclic matrix is not symmetric, it is still symmetric relative to its second diagonal in the way it is built, and it can be brought to symmetry by mirroring the elements relative to the vertical or horizontal center line (such matrices are known as reverse cyclic matrices). However, the matrices' orthogonal and cyclic properties are contradictory, which was first noticed by Ryser [8], who formulated his well-known hypothesis that there are no cyclic Hadamard matrices of orders above 4. Evidently, the area of application of such matrices is limited, while their storage and calculation for such orders is nonessential.

For this reason, symmetric Hadamard matrices in the form of ***block-symmetric*** structures – matrices with complex symmetries consisting of some sets of blocks (matrices of smaller order), not necessarily symmetric and orthogonal, are the most interesting. It is a wide class of orthogonal Hadamard matrices[1], which can be computed using algorithms based on the Sylvester method [9,10], Paley constructions [11], four-block Williamson arrays [12], Scarpis method [13], etc.

The aforementioned algorithms allow to compute Hadamard matrices of orders of the common sequence $4k$, but different in their appearance. This difference can be seen on their "portraits" [5,6], on which two element values 1 and –1 are represented by cells of different colors. Below we provide some of the most commonly used or new block structures that allowed to find new Hadamard matrices.

Bicyclic form is characteristic for Hadamard matrices derived from two cyclic blocks (matrices) **A** and **B** as

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^{\mathrm{T}} & -\mathbf{A}^{\mathrm{T}} \end{pmatrix}, \tag{1}$$

where $\mathbf{B}^{\mathrm{T}}$ is the transposed **B** matrix and $-\mathbf{A}^{\mathrm{T}}$ is the transposed **A** matrix with inversed signs of its elements. Only blocks **A** and **B** are required to obtain symmetric matrices in the bicyclic form, which amounts to half of the number of its elements $2(n/2)^2$. The bicyclic form, without taking symmetry into account, requires only n elements. Such matrices, being of block-symmetric structure, can be symmetric at the same time, as shown in Fig. 1.

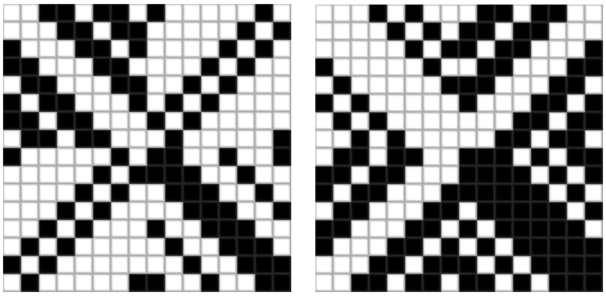

Fig. 1. Hadamard matrices H16 with symmetric blocks.

Paradoxically, the resolution threshold of a bicyclic structure by symmetric matrices was not verified by anyone for a long time, although it is logical to assume that the Raiser constraint applies to this structure. Even, existence of a solution in such a simple form would be satisfactory. According to our evaluations [14], which were pre-verified in a large-scale computer experiment held in a specialized computer center in Canada [15], the bound of symmetric *bicyclic* Hadamard matrices of orders does not exceed the 32nd order (lower bound 8 follows from the Ryser hypothesis and the Sylvester method).

A double-block structure is generalized by a four-block one, which is a combination of two bicyclic matrices with blocks **A**, **B** and **C**, **D** in the form of Williamson array:

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \mathbf{B} & \mathbf{C} & \mathbf{D} \\ -\mathbf{B} & \mathbf{A} & -\mathbf{D} & \mathbf{C} \\ -\mathbf{C} & \mathbf{D} & \mathbf{A} & -\mathbf{B} \\ -\mathbf{D} & -\mathbf{C} & \mathbf{B} & \mathbf{A} \end{pmatrix} \tag{2}$$

Williamson's idea, limiting the use of this array, is that this array is skew-symmetric but with symmetric blocks, which allows to cover the Hadamard matrices of orders below 140. As it was found out in the same computer center by Dragomir Djokovic [16], the cell size equaled 35 is a limit. After this limit there are areas, where Williamson arrays may or may not exist, so the existence of such matrices cannot be guaranteed and is difficult to verify.

That is why the new idea was to neglect the skew-symmetry of the Williamson array, bringing it to the Balonin Seberri block-symmetric form by way of permutations [17] with **B**=**C**. This new form for brevity is called Propus. Matrices can be of two configurations $\mathbf{P}_1$ and $\mathbf{P}_2$. The second one is connected with the generalization of the Williamson array by the Getchals-Seidel form, which uses the reverse symmetry of non-symmetric cyclic blocks **B**, **C**, **D**, mirrored using the reverse unit matrix **R**:

$$\mathbf{P}_1 = \begin{pmatrix} \mathbf{A} & \mathbf{B}=\mathbf{C} & \mathbf{C}=\mathbf{B} & \mathbf{D} \\ \mathbf{C} & \mathbf{D} & -\mathbf{A} & -\mathbf{B} \\ \mathbf{B} & -\mathbf{A} & -\mathbf{D} & \mathbf{C} \\ \mathbf{D} & -\mathbf{C} & \mathbf{B} & -\mathbf{A} \end{pmatrix}, \quad \mathbf{P}_2 = \begin{pmatrix} \mathbf{A} & \mathbf{BR} & \mathbf{CR} & \mathbf{DR} \\ \mathbf{CR} & \mathbf{D}^{\mathrm{T}}\mathbf{R} & -\mathbf{A} & -\mathbf{B}^{\mathrm{T}}\mathbf{R} \\ \mathbf{BR} & -\mathbf{A} & -\mathbf{D}^{\mathrm{T}}\mathbf{R} & \mathbf{C}^{\mathrm{T}}\mathbf{R} \\ \mathbf{DR} & -\mathbf{C}^{\mathrm{T}}\mathbf{R} & \mathbf{B}^{\mathrm{T}}\mathbf{R} & -\mathbf{A} \end{pmatrix}. \tag{3}$$

In order to store symmetric matrices of the n order (not taking cyclicity into account) we need $n^2/4$ elements.

The minimum number of $n^2/8$ cells is required to build a matrix based on all four symmetric blocks. To create Hadamard matrices in the Propus form, we need to store only one row from each of the **A**, **B**, and **D** blocks, since they are cyclic. In this case, only $3n/4$ cells are required to reconstruct a Hadamard matrix. Fig. 2 depicts two symmetric Hadamard matrices in the Propus form.

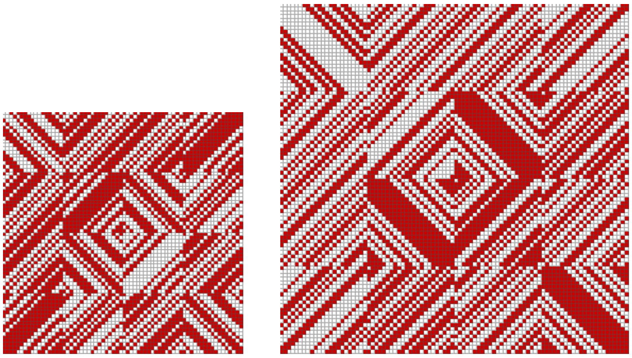

Fig. 2. Symmetric matrices H68 and H92 in the Propus form.

The idea of new matrices, of course, is not limited to permutation only. After careful consideration it becomes evident that the visible sacrifice in the form of restriction **B**=**C** provides a play to find combinations. The classical Paley structure does not allow to find the symmetric and non-symmetric matrices of orders 92, 116, 156, 172, 184, 188, 232, ... Furthermore, the reference document[18] lists these orders as unlikely to have symmetric solutions on them. Note that 92 and 116 were the first matrices analyzed by computer. The early checks found symmetric Propuses [19] on them and on order 172. A more carefully prepared computer experiment conducted in two stages [20, 21] gave all possible symmetric matrices up to order 204.

Subsequent studies using the orbits method cover one by one all difficult orders allowing to claim that Propuses, despite the mentioned sacrifice of material, are a universal and always solvable symmetric structure. A matrix image of order 140, which is unsolvable for the Williamson form, is depicted in Fig. 3.

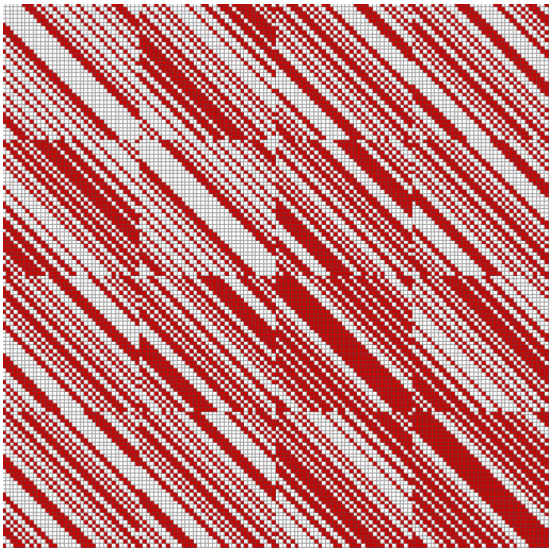

Fig. 3. Symmetric matrix H140.

Therefore, Propuses seem to solve the well-known problem of Hadamard concerning the solvability of orders $4k$ by orthogonal matrices with elements 1 and –1 in a symmetrical form. The reason for this is that orthogonal bicyclic and tetracyclic matrices are specific graphic illustrations of Fermat-Euler and Lagrange theorems about solvability of integers by the sums of two and four squares. Integers of the $4k$ form are not just even numbers, but they also can be divided by 4. Therefore, the graphic illustration allows to simplify only in the form of symmetric three-cycles – Propuses. Four blocks, as it turns out, are simply not necessary to solve the decomposition problem. This somewhat unexpected result is little known. Note that in addition to the cyclic and bicyclic forms of blocks of symmetric matrices, there is a *negacyclic* form, which is different from the cyclic form only in the inversion of signs of elements located below its entries diagonal.

3. Expansion of the Symmetric Orthogonal Matrices Basis

The requirements for quality of video information and its resolution are constantly increasing. This is a trend promoted by manufacturers of image sensors and displays. Recently, the processed images were of PAL, SECAM and NTSC formats, whereas today the UHD (Ultra High Definition) digital format implies the processing of 3840×2160 (4K) and 7680×4320 (8K) video resolutions. The Quality Box technology of selection of image areas (on an image in a video sequence) requires the processing of images of arbitrary size.

These circumstances lead the necessity in image processing to have a wide basis of orthogonal matrices including not only previously unknown matrices of large sizes, but also matrices of various orders including odd ones [5,6]. Thus, the requirements for the matrix basis can be briefly formulated as follows:

- Matrices should be orthogonal in order to provide the symmetry of image processing procedures
- The orders of the matrices must correspond to as many natural numbers as possible providing a wide selection of matrices (or use the same ones) for different image sizes
- There should be more than one orthogonal matrix for each order
- The number of possible entry values (levels) should not exceed 2 to optimize the memory size required for storage of matrices and simplify the computations

As noted before, the existence of Hadamard matrices is limited by $4k$ orders, which significantly limits their application for processing of images of arbitrary resolution. A number of limitations exists in application of Sylvester and Scarpis methods, especially for computing matrices of large orders. Relatively recent concepts [22], which provided some exotic orders in a simple form, only confirm this general rule. It should be noted that floating-point calculations take virtually the same time as integer calculations on modern computers. That is why, stepping away from the requirement for entries to have integer values, which is typical for Hadamard matrices, allows the significant expansion of the basis of orthogonal matrices with two values of elements.

The aforementioned requirements are met in full by the basis of *quasi-orthogonal* matrices, which is a natural generalization of orthogonal matrices. The paper [23] introduced a classification of quasi-orthogonal matrices, which prominent representatives are Mersenne matrices (**M**) of odd orders, having, just like Hadamard matrices, two element values $\{1, -b\}$. In our previous papers, we formulated a hypothesis about the existence of such matrices for all orders $n = 4k - 1$, adjacent to $4k$ orders. The paper [24] described the found interconnections of such quasiorthogonal matrices and their structures. For example, the $\mathbf{H}_{4t}$ matrix can be calculated by bordering a rounded to integers Mersenne matrix:

$$\mathbf{H}_{4t} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{M}_{4t-1} \end{pmatrix} \tag{4}$$

with substitution of $-b$ elements to -1 in the $\mathbf{M}_{4t-1}$ matrix. Here λ and e are the eigen value and eigen vector of the rounded integer matrix $\mathbf{M}_{4t-1}$, respectively.

The reverse of such calculation of Mersenne matrix by truncation of the normalized Hadamard matrix with the changing its sign and the negative values of its entries to the calculated value of level $-b$, calculated for $\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \mu\mathbf{I}$ using the formulas:

$$b = \frac{t}{t+\sqrt{t}}, \quad \mu = \frac{p+qb^2}{2}, \tag{5}$$

where $p = n - 1$, $q = n + 1$ and n is the order of Hadamard matrix. This interrelation shows that up to the sign, the rounded Mersenne matrix is the core of a normalized Hadamard matrix.

As an example of Hadamard matrices, different from the matrices of the main sequence, Fig. 4 depicts the portraits of Hadamard matrices $\mathbf{H}_{12}$ with sign-reversed core, which ensures the required value – λ and core – Mersenne matrix $\mathbf{M}_{11}$, accordingly.

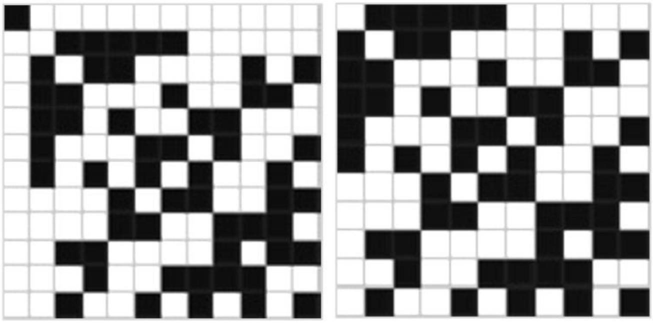

Fig. 4. Matrix $\mathbf{H}_{12}$ based on the core – a symmetric $\mathbf{M}_{11}$ matrix.

Consequently, Mersenne matrices including the orders different from Mersenne numbers can be found using Hadamard matrices (and vise-versa). Moreover, each of such Mersenne matrices is a predictor [24] of a branch of new (in their structure) matrices obtained using the described above and modified for odd orders Sylvester algorithm. Mersenne matrices tend to be fractal, which means that the algorithm for calculation of Hadamard matrices based on them is very simple. Fig. 5 depicts the portraits of four Mersenne matrices as an example. It shows the method for construction of matrix sequences, up to the highest orders.

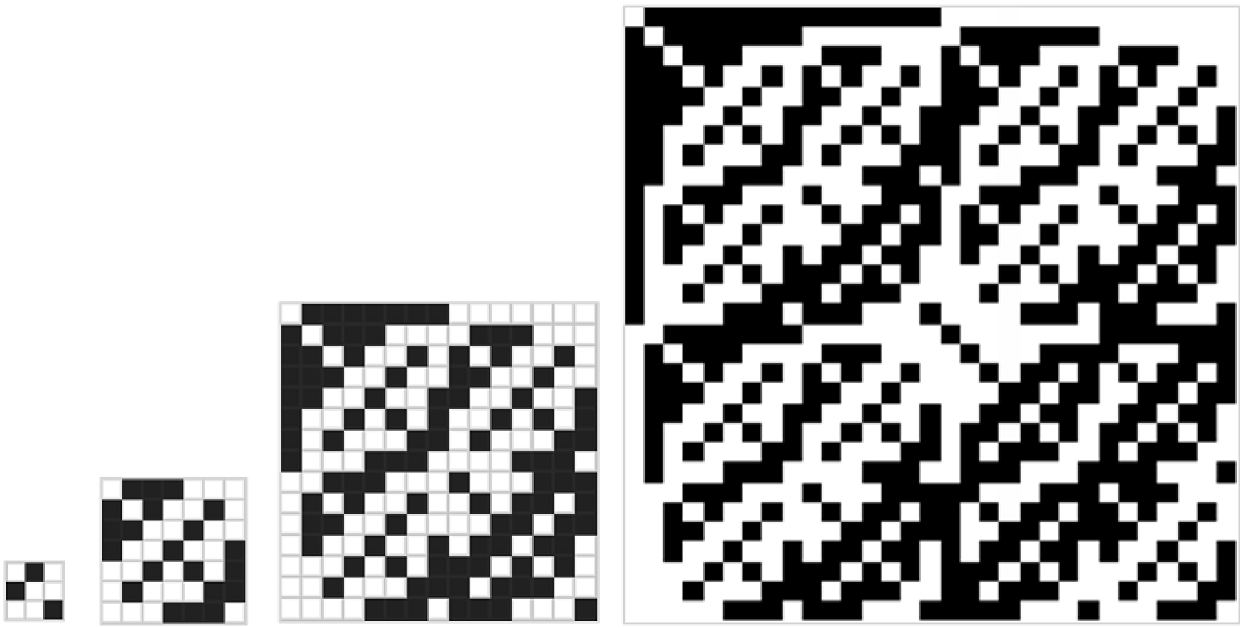

Fig. 5. Matrices $\mathbf{M}_3$, $\mathbf{M}_7$, $\mathbf{M}_{15}$, $\mathbf{M}_{31}$.

If a matrix order is a power of a prime number, then Mersenne matrix consists of cyclic blocks, which sizes equal the prime number. The paper [24] provides a structural exception, which confirms the general rule: if the order $n = 4k - 1$ equals the product of pairs of close prime numbers, then the Mersenne matrix will be cyclic, but not symmetric.

Symmetric constructions of Haramard-Walsh matrices formed by the way of arranging the columns by the frequency of the change in the signs of their entries are of particular interest in image processing tasks. However, ordered Hadamard-Walsh matrices can be obtained from Mersenne-Walsh matrices by inverting the signs of their entry values and adding borders. Fig. 6 depicts a portrait of a Mersenne-Walsh matrix of the 31 order obtained by the way of ordering the $\mathbf{M}_{31}$ matrix.

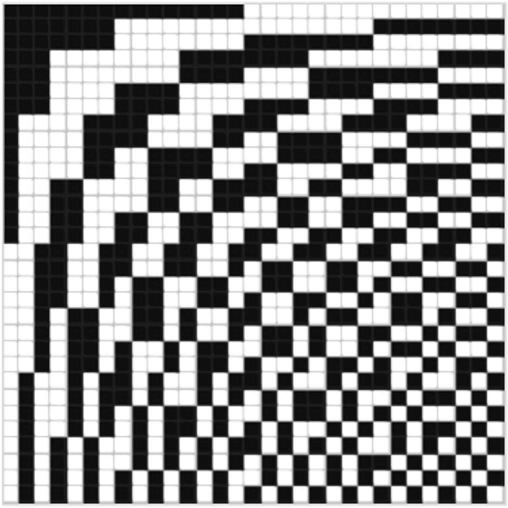

Fig. 6. Mersenne-Walsh Matrix.

The ways to compute Hadamard matrices through chain matrix structures are detailed in papers [23,24], where it was demonstrated that the class of orthogonal matrices with two element values is firmly connected to numbers and numerical sequences.

4. Conclusion

The basis of quasi-orthogonal matrices used for image processing is significantly wider than the orthogonal basis of Hadamard matrices and actually includes it. This provides for wider choice in selecting the best fit matrices for processing of specific images including those of non-standard sizes. The peculiarity of quasi-orthogonal Mersenne matrices with two values of their entries is that $-b$ is irrational. However, the computing power of today's CPUs allow for efficient computations with such matrices, as well as Hadamard matrices.

The symmetric Hadamard matrices considered in this paper are built based on Mersenne matrices and Williamson's three-block array. They are significantly different in type from known sequences of Hadamard matrices obtained by Paley, Sylvester, and Scarpis methods and the Williamson's classic array. Mersenne matrices and Hadamard matrices built on their basis are directly associated with numerical sequences. For a number of such sequences, there exist the cyclic and bicyclic matries and Propus-form matrices, which provide their simple and efficient storage. Mersenne matrices at orders equaled to prime numbers are guaranteed to be of simple structures.

Acknowledgements

Our study of orthogonal symmetric matrices proceeded from the assumption that the limitation formulated by Ryser successively weakens with when the number of cyclic blocks in these matrices increases. At the same time, the complexity of the calculations, of course, remained quite high. Our work was greatly supported by facilities of the Shared Hierarchical Academic Research Computing Network (SHARCNET) and Compute/Calcul Canada, which provided their computing capacities, along with efficient consultations with Jennifer Seberry (Professor Emeritus, University of Wollongong, Australia) and Dragomir Djokovic (Professor Emeritus, Department of Pure Mathematics and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada). Hereby, we express our sincere gratitude to them.

The research leading to these results has received funding from the Ministry of Education and Science of the Russian Federation according to the project part of the state funding assignment No 2.2200.2017/4.6.

References

[1]. Hadamard, Jacques S. (1893) "Resolution d'une question relative aux determinants." *Bulletin des Sciences Mathematiques* **17**: 240–246.

[2]. Horadam, Kathy J. (2007) "Hadamard matrices and their applications." Princeton, NJ: Princeton University Press, Princeton, NJ

[3]. Mironovsky, Leonid A, and Valery A. Slaev. (2011) "Strip-method for image and signal transformation." Berlin: De Gruyter

[4]. Behrooz, Ali, Ali A. Eftekhar, and Ali Adibi. (2014) "Hadamard multiplexed fluorescence tomography." *Biomedical Optics Express* **5 (3)**: 763–777.

[5]. Balonin, Nikolaj, and Mikhail Sergeev. (2014) "Construction of transformation basis for video and image masking procedures." *Frontiers in Artificial Intelligence and Applications* **262:** 462–467.

[6]. Balonin, Nikolaj, and Mikhail Sergeev. (2014) "Expansion of the orthogonal basis in video compression." *Frontiers in artificial intelligence and applications* **262**: 468–474.

[7]. Vostrikov, Anton, and Mikhail Sergeev. (2015) "Expansion of the Quasi-orthogonal Basis to Mask Images." *Smart Innovation, Systems and Technologies* **40:** 161–168.

[8]. Ryser, Herbert J. (1963) "Combinatorial mathematics" *The Carus mathematical monographs* Published by the mathematical association of America. – N. Y.: John Wiley and Sons **14**

[9]. Sylvester, James J. (1867) "Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers." *Philosophical Magazine* **34**: 461–475.

[10]. Eliahou, Shalom. (2012) "La conjecture de Hadamard" *Images des Mathématiques, CNRS*

[11]. Paley, Raymond Edward Alan Christopher. (1933) "On orthogonal matrices." *Journal of Mathematics and Physics* **12**: 311–320.

[12]. Scarpis, Umberto. (1898) "Sui determinanti di valore massimo, Rendiconti della R." *Istituto Lombardo di Scienze e Lettere* **31**: 1441–1446.

[13]. Williamson, John. (1944) "Hadamard's determinant theorem and the sum of four squares." *Duke Math. J.* **11**: 65–81.

[14]. Balonin, Nikolaj A, and Mikhail Sergeev B. (2017) "Ryser's Conjecture Expansion for Bicirculant Strictures and Hadamard Matrix Resolvability by Double-Border Bicycle Ornament." *Informatsionno-upravliaiushchie sistemy [Information and Control Systems]* **1**: 2–10 (In Russian).

[15]. Balonin, Nikolaj A, and Dragomir Z. Djokovic. (2015) "Symmetry of Two Circulant Hadamard Matrices and Periodic Goley Pairs." *Informatsionno-upravliaiushchie sistemy [Information and Control Systems]* **3**: 2–16 (In Russian).

[16]. Djokovic, Dragomir Z. (1993) "Good matrices of orders 33, 35 and 127." *JCMCC* **14**: 145–152.

[17]. Seberry, Jennifer, and Nikolaj A Balonin. (2017) "The propus construction for symmetric Hadamard matrices" *Australasian Journal of Combinatorics* **69 (3)**: 349–357.

[18]. Craigen, Robert, and Hadi Kharaghani. (2007) "Hadamard matrices and Hadamard designs.", in C. J. Colbourn, J. H. Dinitz (eds) *Handbook of Combinatorial Designs, 2nd ed.. Discrete Mathematics and its Applications (Boca Raton).* Chapman & Hall/CRC, Boca Raton

[19]. Matteo, Di O, Dragomir Z. Djokovic, and Ilias S Kotsireas. (2015) "Symmetric Hadamard Matrices of Order 116 and 172 Exist." *Special Matrices* **3.1**: 227–234.

[20]. Balonin, Nikolaj A, Yury N. Balonin, Dragomir Z. Djokovic, Dmitry A Karbovskiy, and Mikhail B Sergeev. (2017) "Construction of symmetric Hadamard matrices." *Informatsionno-upravliaiushchie sistemy [Information and Control Systems]* **5**: 2–11 (In Russian).

[21]. Balonin, Nikolaj A, Dragomir Z. Djokovic, and Dmitry A Karbovskiy. (2018) "Construction of symmetric Hadamard matrices of order 4v for v = 47, 73, 113." *Special matrices* **6**: 11–22.

[22]. Hall, Marshall. (1956) "A survey of difference sets" *Proc. Amer. Math. Soc.* **7**: 975–986.

[23]. Sergeev, Alexander M. (2014) "Generalized Mersenne Matrices and Balonin's Conjecture" *Automatic Control and Computer Sciences* **48 (4)**: 214–220.

[24]. Balonin, Nikolaj A, Anton A Vostrikov, and Mikhail B Sergeev. (2015) "On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices" *Automatic Control and Computer Sciences* **49 (3)**: 153–158.