ISSN 0146-4116, Automatic Control and Computer Sciences, 2015, Vol. 49, No. 3, pp. 153–158. © Allerton Press, Inc., 2015.
Original Russian Text © N.A. Balonin, A.A. Vostrikov, M.B. Sergeev, 2015, published in Avtomatika i Vychislitel'naya Tekhnika, 2015, No. 3, pp. 42–48.

On Two Predictors of Calculable Chains of Quasi-Orthogonal Matrices

N. A. Balonin[a], A. A. Vostrikov[a], and M. B. Sergeev[b]

[a]*Saint Petersburg State University of Aerospace Instrumentation, ul. Bolshaya Morskaya 67, St. Petersburg, 190000 Russia*

[b]*Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, pr. Kronverkskii 49, St. Petersburg, 197101 Russia*

e-mail: korbendfs@mail.ru, vostrikov.anton@ask-lab.com, mbse@mail.ru

Received July 14, 2014; in final form, March 24, 2015

Abstract—The general definition of quasi-orthogonal matrices, the definition of low-level matrices, and partial definitions of quasi-orthogonal Mersenne and Euler matrices are considered. New quasi-orthogonal symmetric Seidel matrices that exist on odd orders and three-level Legendre symbols used to calculate elements of these matrices are defined. A method to calculate Euler matrices via Mersenne matrices is given. A relation between asymmetric and symmetric odd-order Mersenne and Seidel matrices is shown to exist. A new, modified Sylvester method for calculating Euler matrices using symmetric circulant Seidel matrices is proposed.

Keywords: quasi-orthogonal matrices, Hadamard matrices, Belevitch matrices, Mersenne matrices, Euler matrices, Seidel matrices, three-level Legendre symbols, two-circulant matrices

DOI: 10.3103/S0146411615030025

1. INTRODUCTION

The practical interest in orthogonal matrices, with Hadamard [1] matrices belonging to this class, results from their principal properties, which make them widely used in digital information processing systems [2].

A Hadamard matrix is a square matrix $\mathbf{H}_n$ of an order n that consists of numbers $\{1, -1\}$, and its columns are orthogonal $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}$, where $\mathbf{I}$ is the unity matrix.

First, as little as two integer values of elements of these matrices ensure the efficiency of matrix operations, both for hardware and software implementations. Second, the orthogonality of matrices makes it possible to create symmetric technical systems, since one can simply transpose ($\mathbf{H}_n^{-1} = \mathbf{H}_n^{\mathrm{T}}$) with the matrix $\mathbf{H}_n$ used in the direct transform to find the inverse transform matrix. Third, the existing orthogonal bases include symmetric, circulant, two-circulant, and other matrices, which make the choice of the optimal matrix for a particular information transformation significantly wider.

In coding theory, for instance, columns of orthogonal Hadamard matrices are the basis for constructing codes with a large code distance [3]. The special order of numeration of columns of Hadamard matrices in digital signal processing, image compression, and masking is interpreted as a two-level representation of the widely used Walsh functions [4].

Orthogonal Hadamard matrices exist on orders $n = 4k$, where k is a natural number, and can be calculated as chains based on matrices of previous orders $n/2$ by the Sylvester rule [5] and by the Paley [6] and Scarpis [7] algorithms.

In [8], which describes and classifies matrices of the Hadamard family, the problem is formulated as the finding of two closely related families of quasi-orthogonal Mersenne [9] and Euler [10] matrices that are similar in properties to Hadamard matrices yet differ by their orders and value of elements.

In [8], a quasi-orthogonal matrix is defined as a square matrix $\mathbf{A}_n$ of order n with the maximums of modules of elements in each column reduced to the unity; the matrix satisfies the quadratic relation condition

$$\mathbf{A}_n^{\mathrm{T}}\mathbf{A}_n = \omega(n)\mathbf{I}_n,$$

where $\mathbf{I}_n$ is the identity matrix and $\omega(n)$ is the weight of the matrix.

The weight $\omega(n) = 1$ is characteristic of orthogonal matrices, quasi-orthogonal matrices, and, in particular Hadamard matrices (apart from the trivial first-order matrix, which has nothing to do with the latter) [1]. Along with it, these matrices are very close to the orthogonal ones obtained from $\mathbf{A}_n$ by normalization of their columns, followed by a reduction of the maximal modulo element (m-norm) to $m < 1$ for the orders $n > 1$.

Definition 1. We call the values of the matrix elements its levels. For instance, a Hadamard matrix with the elements $\{1, -1\}$ has two levels (is two-level), and a Belevitch matrix [11] with the elements $\{0, 1, -1\}$ is three-level.

Given the above *definition*, we call quasi-orthogonal Mersenne matrices $\mathbf{M}_n$ two-level matrices of orders $n = 4k - 1$ with the values of elements $\{1, -b\}$, where $|b| < 1$, that satisfy the quadratic relation condition

$$\mathbf{M}_n^{\mathrm{T}}\mathbf{M}_n = \omega(n)\mathbf{I}_n$$

with the variable weight $\omega(n) = \frac{(n+1)+(n-1)b^2}{2}$ [8, 9]. For $n = 3$, the coefficient $b = 1/2$; in other cases $b = \frac{q+\sqrt{4q}}{q-4}$, where $q = n + 1$ is the order of the respective Hadamard matrix.

The name of these matrices is associated with the fact that they generalize the calculation of quasi-orthogonal Sylvester matrices [5] of even orders $n = 2^k$ to include odd values of orders that equal the Mersenne numbers $n = 2^k - 1$ [9].

Modular two-level matrices of orders $n = 4k - 2$ [8, 10] with the elements $\{1, -1, b, -b\}$, where $|b| < 1$, that satisfy the quadratic relation condition

$$\mathbf{E}_n^{\mathrm{T}}\mathbf{E}_n = \omega(n)\mathbf{I}_n$$

are called quasi-orthogonal Euler matrices $\mathbf{E}_n$ such that $\omega(n) = \frac{(n+2)+(n-2)b^2}{2}$. The modular level $b = 1/2$ for $n = 6$, in the general case $b = \frac{q-\sqrt{8q}}{q-8}$, where $q = n + 2$ is the order of the respective Hadamard matrix.

Four-level Euler matrices emerged as a compromise substitution for the lacking three-level Belevitch matrices that do not exist for orders n for which the number $n - 1$ cannot be expanded into the sum of two squares of integer numbers [12]. The expandability criterion of numbers is based on the respective Euler theorem, which is the reason the matrices were named as they were.

In this work, we consider the rule for calculating Mersenne and Euler matrices via each other, which generates chains with their interconnected orders. Such chains make the family of Hadamard matrices significantly wider and help simplify the calculation and storage of quasi-orthogonal matrices in symmetric digital information processing systems. The number of chains depends on the start matrices, viz. predictors, with Seidel matrices being those predictors for two unique chains of Mersenne and Euler matrices.

2. CHAINS OF QUASI-ORTHOGONAL MATRICES

The peculiarity of the interconnection of quasi-orthogonal matrices is that each Mersenne matrix of odd order can be used to construct an Euler matrix of double even order. On the orders $n = 1$ and $n = 2$, forms of these two types of matrices do not have any developed distinctions and hence one cannot tell whether the Mersenne or Euler matrix is the primary one. We cannot state that Mersenne matrices are predictors of Euler matrices, since there is a transition rule from any Euler matrix $\mathbf{E}_n$ to the Mersenne matrix $\mathbf{M}_{n+1}$ of an order one unity higher.

A typical chain of Mersenne and Euler matrices looks like $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$. A chain of such successively calculated matrices can also start with a Euler matrix. In [9, 10], the order of Euler matrices is proven to be even and equal $n = 4k - 2$; here k is a natural number as before. Therefore, Mersenne matrices of the orders $n = 4k - 1$ that take values 3, 7, 11, 15... and differ by 4 (the typical period for all types of matrices in the Hadamard family) are the basis for constructing Euler matrices of orders 6, 14, 30....

Thus, there is uncertainty about finding Euler matrices when half of the value of their order is not the order of Mersenne matrices. This is typical, for instance, for the existing matrix $\mathbf{E}_{10}$ [13]. So far, the literature has not defined the generating matrix for such a case when describing the interconnection between Mersenne and Euler matrices.

3. SEIDEL MATRICES

In addition to asymmetric circulant Mersenne matrices of orders $n = 4k - 1$, we introduce symmetric circulant Seidel matrices $\mathbf{S}_n$ of the orders $n = -4k + 1$, which are similar to them to a large extent.

Definition 2. We call quasi-orthogonal Seidel matrices $\mathbf{S}_n$ three-level matrices of orders $n = 4k + 1$ with the values of elements $\{1, -b, d\}$, where $d < b < 1$, that satisfy the quadratic relation condition

$$\mathbf{S}_n^{\mathrm{T}}\mathbf{S}_n = \omega(n)\mathbf{I}_n.$$

Here, $\omega(n) = d + (n-1)\frac{1+b^2}{2}$ is the variable weight. The diagonal elements of the matrix are $d = \frac{1}{1+\sqrt{n}}$, $b = 1 - 2d$.

What Mersenne and Seidel matrices of odd orders have in common is that they can be treated as the result of orthogonalization of columns of asymmetric and symmetric Jacobsthal matrices [6, 14, 15] obtained from normalized Belevitch matrices by cutting off their edges. In the graph theory, the truncated type of matrices is matched to integer non-orthogonal adjacency matrices of Seidel graphs [16], giving the name for the respective quasi-orthogonal matrices. When what they have in common is taken into account, either a Mersenne and a Seidel matrix can be used to calculate Euler matrices.

Mersenne and Seidel matrices have odd order and can be used to calculate two-circulant even Euler matrices. In the first case, a Euler matrix is constructed based on asymmetric components, while symmetric ones are used in the second case.

4. CALCULATING EULER MATRICES BASED ON MERSENNE AND SEIDEL MATRICES

One can calculate Euler matrices using the Sylvester rule common for all Hadamard matrices [6] using Mersenne matrices [8, 9] in the form

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & -\mathbf{M}_{n/2} \end{pmatrix},$$

where $\mathbf{M}_{n/2}$ is a two-level Mersenne matrix.

At the same time, Mersenne matrices are related to Euler matrices by a row and a column (an edge) added to them in the form [9, 14]

$$\mathbf{M}_{n+1} = \begin{pmatrix} -\lambda & e^{\mathrm{T}} \\ e & \mathbf{E}_n^* \end{pmatrix},$$

where $\lambda = -a$ is an eigenvalue and e is an eigen vector of the "conjugate" matrix $\mathbf{E}_n^* = \begin{pmatrix} \mathbf{M}_{n/2} & \mathbf{M}_{n/2} \\ \mathbf{M}_{n/2} & \mathbf{M}_{n/2}^* \end{pmatrix}$. Block $\mathbf{M}_{n/2}^*$ is obtained from $\mathbf{M}_{n/2}$ by mutual replacement of elements 1 and $-b$ and by recalculation of the level $b = \frac{q - \sqrt{4q}}{q - 4}$, where $q = n + 2$ is the order of the Hadamard matrix.

The informative part of the formulas is that Mersenne and Euler matrices are calculated based on each other, thus forming chains with increasing orders. This generalizes the Sylvester rule, viz. the calculation of Hadamard matrices with their increasing order [1, 5].

Now, suppose n is a prime number that gives the order as $n = 4k + 1$. This is a necessary and sufficient existence condition [12, 14] for three-level quasi-orthogonal circulant Seidel matrices $\mathbf{S}_n$ with elements equaling three-level Legendre symbols.

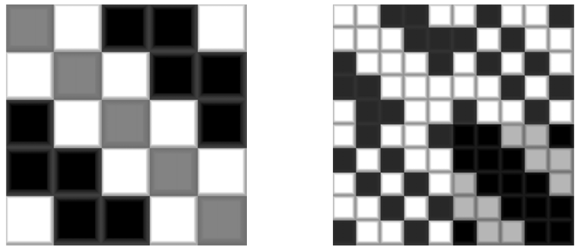

Fig. 1. Portraits of the Seidel $\mathbf{S}_5$ and Euler $\mathbf{E}_{10}$ matrices.

Definition 3. We define three-level Legendre symbols as $\chi\left(\frac{j-i}{n}\right) = \{1, -b, d\}$ calculated via quadratic modulo n residues for differences of indices i and j of their rows and columns in a Seidel matrix of order n. Here, $d < b < 1$.

We recall that the number a is called a quadratic modulo n residue if there exists such $x < n$ that $a = x^2$ (mod n) [17]. Then, for $i = j$ we put $\chi\left(\frac{0}{n}\right) = d = \frac{1}{1+\sqrt{n}}$ and for $i \neq j$ we put $\chi\left(\frac{i-j}{n}\right) = 1$ if $i - j$ is the quadratic modulo n residue and $\chi\left(\frac{i-j}{n}\right) = -b = 2d - 1$, otherwise. The number d is the values of diagonal elements of the Seidel matrix.

We construct, for instance, a quasi-orthogonal Seidel matrix of the fifth order $\mathbf{S}_5$ based on Legendre symbols for the set of numbers {0, 1, 2, 3, 4}, which are the differences of indices of the elements in the first row of the matrix. Their mod5 squares are {0, 1, 4, 4, 1}. This set include numbers 1 and 4, which are quadratic residues. Numbers 2 and 3 are not quadratic residues. The values of the diagonal elements are $d = \frac{1}{1+\sqrt{5}} \cong 0.309$ and $b = 1 - 2d \cong 0.382$.

The circulant Seidel matrix $\mathbf{S}_5$ is constructed using the sequence $\{d, 1, -b, -b, 1\}$ and its conjugate matrix $\mathbf{S}_5^*$ is constructed using the sequence $\{d, -b, 1, 1, -b\}$ of paired Legendre symbols with 1 and $-b$ replaced by $-b$ and 1, respectively. Hence,

$$\mathbf{S}_5 = \begin{pmatrix} d & 1 & -b & -b & 1 \\ 1 & d & 1 & -b & -b \\ -b & 1 & d & 1 & -b \\ -b & -b & 1 & d & 1 \\ 1 & -b & -b & 1 & d \end{pmatrix}, \quad \mathbf{S}_5^* = \begin{pmatrix} d & -b & 1 & 1 & -b \\ -b & d & -b & 1 & 1 \\ 1 & -b & d & -b & 1 \\ 1 & 1 & -b & d & -b \\ -b & 1 & 1 & -b & d \end{pmatrix}.$$

Note that the diagonal of both matrices have numbers d are two times lower as the values of the golden ratio $2d = 1/\psi = 0.618$, where $\psi = 1.618$. The difference between the maximum of the element (the unity) and b is exactly the golden ratio. Therefore, the Seidel matrix $\mathbf{S}_5$ can be attributed to a sort of quasi-orthogonal golden ratio matrices [13].

The two-circulant Euler matrix is calculated with a pair of the original and conjugate Seidel matrices by the modified Sylvester rule [14]

$$\mathbf{E}_n = \begin{pmatrix} \mathbf{S}_{n/2} & \mathbf{S}_{n/2}^* \\ \mathbf{S}_{n/2}^* & -\mathbf{S}_{n/2} \end{pmatrix},$$

with consideration that their elements are corrected up to the values of their respective elements in the Euler matrix: $b = 1/2$ for $n = 6$, otherwise $b = \frac{q - \sqrt{8q}}{q-8}$, where $q = n + 2$ is the order of the neighboring Hadamard matrix. Modules of diagonal elements of mutually conjugate blocks are 1. Figure 1 shows portraits of a fifth-order Seidel matrix and tenth-order Euler matrix that were calculated with it. Here and in what follows, the white square in the matrix portrait is for 1 and the black square is for -1 (or $-b$ in the Seidel matrix). Other elements that are intermediate in terms of their values are shown in shades of grey.

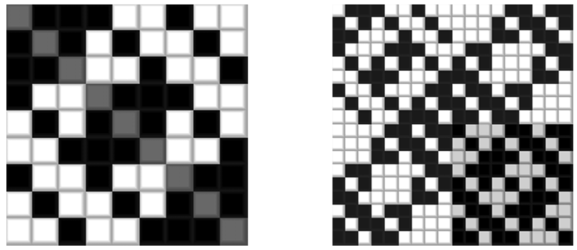

Fig. 2. Portraits of the block Seidel $\mathbf{S}_9$ and Euler $\mathbf{E}_{18}$ matrices.

This modified Sylvester rule generalizes the Paley rule for calculating Hadamard matrices with Belevitch matrices and relies on one-to-one relation between Hadamard, Mersenne, and Euler matrices.

The circulant kernel of normalized Belevitch matrices and the adjacency table of Seidel graphs [16] are constructed based on rounded integer sequence {0, 1, –1, –1, 1}; such arrays do not have orthogonality of their own and do not relate to irrational numbers, though they include them indirectly. Hence, we can state a formal transition rule from Belevitch matrices to quasi-orthogonal Seidel matrices by cutting off the edge and recalculating the diagonal and negative elements of the matrix; this is done to orthogonalize it. One can apply this rule to calculate block circulant matrices.

Moreover, the block circulant matrix $\mathbf{S}_9$ can be calculated with the Kronecker product of two matrices $\mathbf{M}_3$ and is the basis for calculating the block Euler matrix $\mathbf{E}_{18}$ (Fig. 2).

5. CONCLUSIONS

With the described way of calculating quasi-orthogonal Euler matrices based on Seidel matrices, we can add a chain of matrices of the form $\mathbf{M}_3 - \mathbf{E}_6 - \mathbf{M}_7 - \mathbf{E}_{14} - \mathbf{M}_{15} - \ldots$ with the exclusion chain $\mathbf{S}_5 - \mathbf{E}_{10} - \mathbf{M}_{11} - \mathbf{E}_{22} - \mathbf{M}_{21} - \ldots$ with the matrices $\mathbf{E}_{10}$ and then $\mathbf{E}_{22}$ calculated, the latter replacing the nonexistant three-level Belevitch matrix, as well as the chain $\mathbf{S}_9 - \mathbf{E}_{18} - \mathbf{M}_{19} - \mathbf{E}_{38} - \mathbf{M}_{39} - \ldots$ based on the above mentioned block matrix $\mathbf{S}_9$, although 9 is not prime and is the even power of 3. Hence, the block matrices Jacobsthal, Belevitch, and Seidel exist and can be constructed on generalized Legendre symbols for size 3 blocks.

Scientifically, what we considered here allows significant expansion of the direction of study of solvability conditions for circulant structures to include one- and two-circulant structures with two allowed values of modular levels of elements of matrices from the Hadamard family. Practically, it allows significant simplification of the way matrices of various orders are calculated, stored, and chosen for digital data processing algorithms.

REFERENCES

1. Hadamard, J., Resolution d'une question relative aux determinants, *Bull. Sci. Mathem.,* 1893, vol. 17, pp. 240–246.
2. Horadam, K.J., *Hadamard Matrices and Their Applications*. New York: Princeton University Press, 2007.
3. Shalom, E., *La conjecture de Hadamard. I. Image des Mathématique,* 2015. http://images.math.cnrs.fr/html.
4. Walsh, J.L., A closed set of normal orthogonal functions, *Amer. J. Math.,* 1923, vol. 45, pp. 5–24.
5. Silvester, J.J., Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile–work, and the theory of numbers, *Philos.l Mag.*, 1867, vol. 34, pp. 461–475.
6. Paley, R.E.A.C., On orthogonal matrices, *J. Mathem. Phys.,* 1933, vol. 12, pp. 311–320.
7. Scarpis, U., Sui determinanti di valore massimo, *Rendiconti della R. Istituto Lombardo di Scienze e Lettere,* 1898, vol. 31, pp. 1441–1446.
8. Sergeev, A.M., Generalized Mersenne's matrices and Balonin's Hypothesis, *Avtom. Vychisl. Tekhn.,* 2014, no. 4, pp. 35–43.
9. Balonin, N.A., Sergeev, M.B., and Mironovskii, L.A., Calculation of Hadamard-Mersenne matrices, *Inform.-Upravl. Sistemy*, 2012, no. 5, pp. 92–94.
10. Balonin, N.A. and Sergeev, M.B., Two ways to construct Hadamard–Euler matrices, *Inform.-Upravl. Sistemy*, 2013, no. 1, pp. 7–10.
11. Belevitch, V., Theorem of 2n-terminal networks with application to conference telephony, *Electr. Commun,* 1950, vol. 26, pp. 231–244.

12. Balonin, N.A. and Sergeev, M.B., On the issue of existence of Hadamard and Mersenne matrices, *Inform.-Upravl. Sistemy,* 2013, no. 5, pp. 2–8.
13. Balonin, N.A. and Sergeev, M.B., Matrix of golden ratio G_{10}, *Inform.-Upravl. Sistemy,* 2013, no. 6, pp. 2–5.
14. Balonin, N.A. and Sergeev, M.B., Quasi-orthogonal local maximum determinant matrices. *Appl. Mathem. Sci.,* 2015, vol. 9, no. 6. pp. 285–293. DOI:10.12988/ams.2015.4111000
15. Gilman, R.E., On the Hadamard determinant theorem and orthogonal determinants, *Bull. Amer. Math. Soc.,* 1931, vol. 37, pp. 30–31.
16. Seidel, J.J., Strongly regular graphs with (–1, 1, 0) adjacency matrix having eigenvalue 3, *Lin. Alg. Appl.,* 1968, vol. 1, pp. 281–298.
17. Bukhshtab, A.A., *Teoriya chisel* (Theory of Numbers), Moscow: Prosveshchenie, 1966.

Translated by M. Talacheva