

UDC 004.438

doi:10.15217/issn1684-8853.2015.2.4

THREE-LEVEL CRETAN MATRICES CONSTRUCTED VIA CONFERENCE MATRICES

N. A. Balonin^a, Dr. Sc., Tech., Professor, korbendfs@mail.ru

M. B. Sergeev^a, Dr. Sc., Tech., Professor, mbse@mail.ru

Ofer Hadar^b, PhD, Professor, hadar@cse.bgu.ac.il

Jennifer Seberry^c, PhD, Professor of Computer Science, jennifer_seberry@uow.edu.au

^aSaint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

^bBen-Gurion University of the Negev, POB 653, 1, Ben Gurion St., Beer Sheva, 74105, Israel

^cCentre for Computer and Information Security Research, School of Computer Science and Software Engineering, EIS, University of Wollongong, NSW 2522, Australia

Purpose: Orthogonal matrices with many applications introduced by J. J. Sylvester have been become famous: Hadamard matrices, symmetric conference matrices, and weighing matrices are the best known of these matrices with entries from the unit disk. The goal of this note is to develop a theory of such orthogonal matrices based on preliminary research results. **Methods:** Extreme solutions (using the determinant) have been established by minimization of the maximum of the absolute values of the elements of the matrices followed by their subsequent classification. **Results:** We show that if **S** is a core of a symmetric conference weighing matrix, then there exists a three-level orthogonal matrix, **X**. We apply this result to the three-level matrices given by Paley using Legendre symbols to give a new infinite family of Cretan orthogonal matrices. An algorithmic optimization procedure is known which raises the value of the determinant. Our example is for Cretan matrices upto, say four decimal places (but could be made more). **Practical relevance:** The over-riding aim is to seek Cretan matrices as they have many applications in image processing (compression, masking) to statisticians undertaking medical or agricultural research, and to obtain lossless circuits for telecommunications conference networking. Web addresses are given for other illustrations and other matrices with similar properties. Algorithms to construct Cretan matrices have been implemented in developing software of the research program-complex.

Keywords – Hadamard Matrices, Cretan Matrices, Conference Weighing Matrices, Orthogonal Matrices, Legendre Symbols.

AMS Subject Classification: 05B20; 20B20.

Introduction

A Cretan(n) matrix, (CM), is a orthogonal matrix of order n with moduli of entries ≤ 1 , where there must be at least one 1 per row and column. The inner product of a row of $CM(n)$ with itself is the weight ω . The inner product of distinct rows of $CM(n)$ is zero. An τ -level Cretan(n ; τ ; ω) matrix, $CM(n$; τ ; ω), has τ levels or values for its entries.

The definition of Cretan is not that each variable occurs same number of times per row and column but L_1, L_2, \dots, L_τ times in the whole matrix. So we have $CM(n$; τ ; ω ; L_1, L_2, \dots, L_τ) so

$$\begin{pmatrix} -0.5 & 1 & 1 \\ 1 & -0.5 & 1 \\ 1 & 1 & -0.5 \end{pmatrix}$$

is a $CM(3)$, a $CM(3;2)$, a $CM(3;2;2,1)$, a $CM(3;2;2.25)$, a $CM(3;2;2.25;6,3)$ depending on which numbers (in brackets) are currently of interest. We call them Cretan matrices because they were first discussed in this generality at a conference in Crete in July, 2014.

The over-riding aim is to seek $CM(n)$ with maximal determinants as they have many applications

in image processing (compression, masking) to statisticians undertaking medical or agricultural research, and to obtain lossless circuits for telecommunications conference networking.

Definitions

This paper studies the construction of some Cretan matrices [1–3] with three levels constructed via weighing matrices

Definition 1. A weighing matrix, **W**, of order n is an $n \times n$ matrix with elements 0, 1, -1 , such that $\mathbf{W}^T \mathbf{W} = \mathbf{W} \mathbf{W}^T = \omega \mathbf{I}_n$ where \mathbf{I}_n is the identity matrix, ω is the weight.

Weighing matrices of order $2n$, n odd, are conjectured to exist for all $\mathbf{W}(2n; \omega)$ where ω is the sum of two squares [4]. A $\mathbf{W}(2n; 2n - 1)$, for which $2n - 1$ must be the sum of two squares is called a conference matrix or sometimes a Belevitch matrix [5].

A normalized conference matrix has zero diagonal and otherwise first row and column = 1. The most famous of these are from the Paley construction for $2n - 1$ a prime power congruent to 1 modulo 4 [6]. Many other normalized conference matrices are known. For additional details see the books and surveys in the bibliography, for example, [5, 7].

Definition 2. The values of the entries of a matrix are called *levels* [1, 2].

There is a trivial one-level matrix for every order n ; it is the zero matrix of order n .

Hadamard matrices [5, 8, 9] are two-level matrices; symmetric conference matrices [7] and weighing matrices [4] are three-level matrices.

Example 1. For $n = 4t - 2 = 10$, we have a three-level symmetric conference matrix (Fig. 1).

Orthogonal matrices with maximal determinant of odd orders have been discovered with a larger number of levels [1].

We will denote the level/values of two-level matrices as $a, -b$; for positive $0 \leq b \leq a = 1$.

Definition 3. A real square matrix \mathbf{X} of order n is called *orthogonal* if it satisfies $\mathbf{X}^T\mathbf{X} = \mathbf{X}\mathbf{X}^T = \omega\mathbf{I}_n$, where \mathbf{I}_n is the $n \times n$ identity matrix, and ω is a constant real number.

In this and future work we will only use orthogonal to refer to matrices with moduli of real elements ≤ 1 [2], where at least one entry in each row and column must be 1.

Hadamard matrices [5], symmetric conference matrices [7], and weighing matrices [4] are the best known of these matrices with entries from the unit disk [2, 8].

Definition 4. A *Cretan matrix*, \mathbf{S} , order n , is an orthogonal matrix which has indeterminate entries, $x_1, x_2, x_3, x_4, \dots, x_\tau$. It is said to have τ levels.

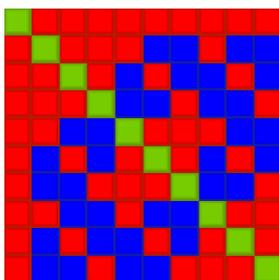
The $\mathbf{S}^T\mathbf{S} = \mathbf{S}\mathbf{S}^T$ have diagonal entries the weight $\omega(n)$ and off diagonal entries 0.

CM-matrices can be defined by a function $\omega(n)$ or functions $x_1(n), x_2(n), x_3(n), x_4(n), \dots, x_\tau(n)$. We write $CM(n; x_1(n), x_2(n), x_3(n), x_4(n), \dots, x_\tau(n); \omega(n); \text{determinant})$ as shorthand.

Notation: When the variable (indeterminate) entries, $x_1, x_2, x_3, \dots, x_\tau$ occur $s_1, s_2, s_3, \dots, s_\tau$ times in each row and column, we write $CM(n; s_1, s_2, s_3, \dots, s_\tau; x_1(n), x_2(n), x_3(n), \dots, x_\tau(n); \omega(n); \text{determinant})$ as shorthand.

Review and questions of existence are discussed in [2, 3, 10, 11].

Balonin N. and Sergeev M. [3] and Sergeev A. [12] conjectured that the resolution of the question



■ **Fig. 1.** Symmetric conference matrix of order 10 (entries 1 and -1 given as red and blue squares, level 0 given by green squares)

of the existence of orthogonal matrices and their generalizations discussed here depends on the order:

— for $n = 4t$, t an integer, at least 2 levels, $a, -b, a = b$, are needed;

— for $n = 4t - 1$, at least 2 levels, $a = 1, -b, b < a$, are needed;

— for $n = 4t - 2$, at least 2 levels, $a = 1, -b, b < a$, are needed for a two blocks construction;

— for $n = 4t - 3$, at least 3 levels, $a = 1, -b, c, b < a, c < a$, are needed.

Normalized Weighing Matrix Core Construction

We now use Paley's famous Legendre symbol construction [6] for $(0,1,-1)$ orthogonal matrices of order p congruent 1 modulo 4 ($p = 4t - 3$), for prime powers p , to obtain three-level Cretan matrix.

Suppose there exists a normalized conference matrix, \mathbf{C} , of order $4t - 2$, that is a $\mathbf{W}(4t - 2; 4t - 3)$. Then \mathbf{C} may be written as

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & & & & \\ 1 & & \mathbf{S} & & \\ \vdots & & & & \\ 1 & & & & \end{pmatrix}.$$

Removing the first row and column, this gives the core of the conference matrix, and replacing the ones of \mathbf{S} by $a, a = 1$, the -1 s of \mathbf{S} by $-b$, and the zeros of \mathbf{S} by c gives a three-level $CM(4t - 3; a = 1; -b; c)$ satisfying equation $\mathbf{S}^T\mathbf{S} = \mathbf{S}\mathbf{S}^T = \omega\mathbf{I}_{4t-3}$.

The matrix orthogonality equation $\mathbf{S}^T\mathbf{S} = \mathbf{S}\mathbf{S}^T = \omega\mathbf{I}_n$, is a set of n^2 scalar equations, giving two kinds of formulae: $g(a, b, c) = \omega$, there are n such equations, and $f(a, b, c) = 0$, there are $n^2 - n$ such equations. We concentrate on two of them: $g(a, b, c) = \omega, f(a, b, c) = 0$.

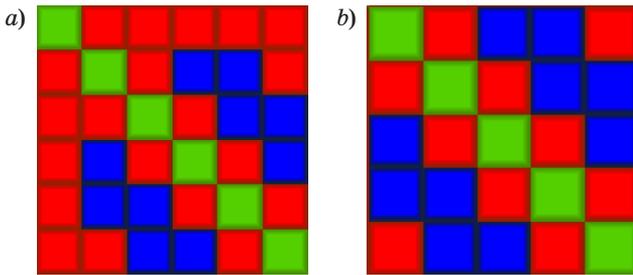
The entries in $\omega\mathbf{I}_n$ which are on the diagonal, are given by the *radius equation* $\omega = g(a, b, c)$, they depend on the choice of a, b, c . If $a = 1$, then $\omega \leq n$.

The maximal weight $\omega = n$ arises from Hadamard matrices and symmetric conference matrices which have $\omega = n - 1$. Cretan matrices can have also irrational values for the weight.

The second equation $f(a, b, c) = 0$ (or equations, the same type) we name the *characteristic equation*, as it allows us to find a formulae for level $b, c; c \leq b \leq a$.

Level $a = 1$ is pre-determined for all Cretan matrices.

Three-level orthogonal matrices $CM(n = 4t - 3; a = 1; -b; c); -b = 2c - 1; c = \frac{1}{1 + \sqrt{n}}$ are based on cores of symmetric conference matrices with non-zero diagonal elements c .



■ Fig. 2. Orthogonal matrices: *a* — the conference matrix of order 6 (entries 1 and -1 given as red and blue squares, zero level given by green squares); *b* — the Cretan matrix of order 5 (entries $a = 1$ and $-b$ given as red and blue squares, level c given by green squares)

Example 2. For $n = 4t - 3 = 5$, at least 3 levels, $a = 1, -b, c, b < a, c < a$, are needed. The radius equation is $2a^2 + 2b^2 + c^2 = \omega$; the characteristic equations are $b^2 + 2ac - 2ab = 0$ and $a^2 - 2bc - 2ab = 0$.

The normalized conference matrix (Fig. 2, *a*), has a symmetric one circulant core giving three-level Cretan matrix (Fig. 2, *b*), $a = 1$, level $c = 1$ is incompatible, due characteristic equations, with bound $b \leq 1$, the possible $c = \frac{1}{1 + \sqrt{5}} < 1$ gives solution $-b = 2c - 1 = \frac{1 - \sqrt{5}}{1 + \sqrt{5}}$ with $\omega = 2a^2 + 2b^2 + c^2 = \left(\frac{5}{1 + \sqrt{5}}\right)^2 = 2.3873$.

References

1. Balonin N. A., Mironovsky L. A. Hadamard Matrices of Odd Order. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2006, no. 3, pp. 46–50 (In Russian).
2. Balonin N. A., Seberry Jennifer. Remarks on Extremal and Maximum Determinant Matrices with Moduli of Real Entries ≤ 1 . *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5(72), pp. 2–4.
3. Balonin N. A., Sergeev M. B. Quasi-Orthogonal Local Maximum Determinant Matrices. *Applied Mathematical Sciences*, 2015, vol. 9, no. 6, pp. 285–293. doi:10.12988/ams.2015.4111000
4. Wallis (Seberry), Jennifer. Orthogonal (0,1,-1) Matrices. *Proc. of First Australian Conference on Combinatorial Mathematics*, TUNRA, Newcastle, 1972, pp. 61–84. Available at: <http://www.uow.edu.au/> (accessed 16 February 2015).
5. Seberry Jennifer, Yamada M. Hadamard Matrices, Sequences, and Block Designs. *Contemporary Design Theory: A Collection of Surveys*. J. H. Dinitz and D. R. Stinson eds. John Wiley and Sons, Inc., 1992, pp. 431–560.

So we have $CM \left(n = 5; 2, 2, 1; a = 1, -b, c; a = 1, -b = 2c - 1; c = \frac{1}{1 + \sqrt{5}}; \omega = \left(\frac{5}{\sqrt{5} + 1}\right)^2; \det = 8.8057 \right)$.

Acknowledgements

The authors wish to sincerely thank Tamara Balonina for converting this paper into printing format. We acknowledge the use of the <http://www.mathscinet.ru> and <http://www.wolframalpha.com> sites for the number and symbol calculations in this paper.

Conclusion

This paper gives the set of basic definitions used in all works of this area tied with questions of Cretan matrices (orthogonal matrices) usage. It helps us work in a new area with well defined statements. Importantly there is an optimization procedure to raise determinant of the computer generated matrix. Our example is a "computationally-Cretan" matrix, but not "theoretically-Cretan", it is a Cretan matrix if we allow round-off errors to be sufficiently small. This is important because it highlights the difference between an engineering solution, where some tolerance is permitted, and the theoretical solution, which must be exact.

6. Paley, R. E. A. C. On Orthogonal Matrices. *J. Math. Phys.*, 1933, no. 12, pp. 311–320.
7. Balonin N. A., Seberry Jennifer. A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 4(71), pp. 2–7.
8. Hadamard J. Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
9. Seberry Jennifer. *Regular Hadamard Matrices of Order 36*. Available at: <http://www.uow.edu.au/jennie/matrices/H36/36R.html> (accessed 16 February 2015).
10. Balonin N. A. Existence of Mersenne Matrices of 11th and 19th Orders. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 2, pp. 89–90 (In Russian).
11. Balonin N. A., Sergeev M. B. On the Issue of Existence of Hadamard and Mersenne Matrices. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 5(66), pp. 2–8 (In Russian).
12. Sergeev A. M. The Generalized Matrices of Mersenne and Balonin's Conjecture. *Automatic Control and Computer Sciences*, 2014, no. 4, pp. 35–43. doi:10.3103/S0146411614040063