UDC 004.438

TWO LEVEL CRETAN MATRICES CONSTRUCTED VIA SINGER DIFFERENCE SETS

N. A. Balonin[a], *Dr. Sc., Tech., Professor, korbendfs@mail.ru*
Jennifer Seberry[b], *PhD, Professor of Computer Science, jennifer_seberry@uow.edu.au*
[a]*Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation*
[b]*School of Computer Science and Software Engineering, Faculty of Engineering and Information Science, University of Wollongong, NSW, 2522, Australia*

Purpose: *This note discusses two level quasi-orthogonal matrices which were first highlighted by J. J. Sylvester; 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 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* ***B*** *is the incidence matrix of a (v, k, λ) difference set, then there exists a two-level quasi-orthogonal matrix,* ***S****, a Cretan(v) matrix. We apply this result to the Singer family of difference sets obtaining a new infinite family of Cretan matrices.* ***Practical relevance:*** *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, Quasi-Orthogonal Matrices, Cretan Matrices, Difference Sets, Singer Difference Sets, Hadamard Difference Sets.*

AMS Subject Classification: *05B20; 20B20.*

Introduction

Difference sets are of considerable use and interest to image processing (compression, masking) to statisticians undertaking medical or agricultural research, to position smaller telescopes to make very large deep space telescopes and to spacing the tread on rubber tyres for vehicles.

In this and further papers we use some names, definitions, notation differently than we have in the past [1]. This, we hope, will cause less confusion, bring our nomenclature closer to common usage and conform for mathematical purists. We have chosen the use of the word level, instead of value for the entries of a matrix, to conform to earlier writings. We note that the strict definition of an orthogonal matrix, $\mathbf{X}$, of order n, is that $\mathbf{X}^T\mathbf{X} = \mathbf{X}\mathbf{X}^T = \mathbf{I}_n$ where $\mathbf{I}_n$ is the identity matrix of order n. In this paper we consider $\mathbf{S}^T\mathbf{S} = \mathbf{S}\mathbf{S}^T = \omega\mathbf{I}_n$ where ω is a constant. We call these quasi-orthogonal matrices [2, 3].

Definition 1. A real square matrix $\mathbf{S}$ of order n is called *quasi-orthogonal* if it satisfies $\mathbf{S}^T\mathbf{S} = \mathbf{S}\mathbf{S}^T = \omega\mathbf{I}_n$, where $\mathbf{I}_n$ is the $n\times n$ identity matrix, and ω is a constant real number. The values of the entries of a matrix are called *levels*.

There is a trivial one-level matrix for every order n; it is the zero matrix of order n. Hadamard matrices are two-level matrices and symmetric conference matrices and weighing matrices are three-level matrices. Quasi-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 Cretan matrices as a, $-b$; for positive $0 \le b \le a = 1$.

In this and future work we will only use quasi-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 [4], symmetric conference matrices [5], and weighing matrices [6] are the best known of these matrices with entries from the unit disk [7]. We refer to [2] for definitions of these matrices.

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: $g(a, b) = \omega$, there are n such equations, and $f(a, b) = 0$, there are $n^2 - n$ such equations. We concentrate on two of them: $g(a, b) = \omega$, $f(a, b) = 0$.

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

The maximal weight $\omega = n$ arises from Hadamard matrices, symmetric conference matrices have $\omega = n - 1$. *Quasi-orthogonal* matrices can have also irrational values for the weight.

The second equation $f(a, b) = 0$ we name the *characteristic equation*, as it allows us to find a formulae for level b $\le a$.

Definition 2. A *Cretan*(n) matrix, *CM*, is a quasi-orthogonal matrix of order n with 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. A τ-level *Cretan*(n; τ; ω) matrix, *CM*(n; τ; ω), has τ levels or values for its entries. Level $a = 1$ is pre-determined for all Cretan matrices.

Cretan(n), or *CM*(n) quasi-orthogonal matrices are studied in [2, 3]. In more general notation these are can be *CM*(*order*), *CM*(*order*; *number of levels* = τ), *CM*(*order*; *number of levels* = τ; *occurrences of levels* = $L_1, L_2, \ldots, L_\tau$), *CM*(*order*; *number of levels* = τ; *weight* = ω), *and CM*(*order*; *number of levels* = τ; *weight*; *occurrences of levels in whole matrix*), etc. etc. etc.

The definition of Cretan is not that each variable occurs some number of times per row and column but $L_1, L_2, \ldots, L_\tau$ times in the whole matrix. So we have $CM(n; \tau; \omega; L_1, L_2, \ldots, L_\tau)$ 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 absolute or relative (local) maximal determinants as they have many applications in image processing and masking [3].

Definitions

This paper studies the construction of some Cretan matrices made here using Singer difference sets.

Definition 3. Let D = $\{d_1, d_2, \ldots, d_k\}$ be a subset of the integers 0, 1, 2, ... , $\nu - 1$. If the collection $\Delta = \{d_i - d_j: i, j, 1\ldots k, i \neq j\}$ contains each element 1, 2, ..., $\nu - 1$ exactly λ times, D will be called a (ν, k, λ) *difference set*.

This is said to be additive notation. Equivalently, (ν, k, λ) difference set in a multiplicative group G of order ν is k-subset D of G such, that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with d_1, d_2 from G. The parameter ν is called the order of the difference set.

Difference sets due to James Singer (1938, [8]) appeared first. Marshall Hall [9] wrote an extensive survey in 1956. Difference sets of regular Hadamard matrices were discussed in [10, 11].

We note that for every (ν, k, λ) difference set there is a complementary $(\nu, \nu - k, \nu - 2k + \lambda)$ difference set made by choosing the subset of 1, 2, ..., ν not in D.

Definition 4. Let D = $\{d_1, d_2, \ldots, d_k\}$ be a difference set. Then the $\nu \times \nu$, matrix $\mathbf{B} = (b_{ij})$ is said to be the *incidence matrix* of D if $b_{ij} = 1$ for $j - i$ in D and 0 if $j - i$ is not in D.

Example 1. Let D be the subset {1, 3, 4, 5, 9} of the integers 0, 1, 2, ..., 10. Hence we take all the differences modulo 11. Then Δ contains $1 - 3 = -2 = 9$; $1 - 4 = -3 = 8$; $1 - 5 = -4 = 7$; $1 - 9 = -8 = 3$; $3 - 1 = 2$; $3 - 4 = -1 = 10$; $3 - 5 = -2 = 9$; $3 - 9 = -6 = 5$; $4 - 1 = 3$; $4 - 3 = 1$; $4 - 5 = -1 = 10$; $4 - 9 = -5 = 6$; $5 - 1 = 4$; $5 - 3 = 2$; $5 - 4 = 1$; $9 - 1 = 8$; $9 - 3 = 6 = 5$; $9 - 4 = 5$; $9 - 5 = 4$; which is each non-zero integer 0, 1, 2, ..., 10 exactly twice.

The incidence matrix of D is $\mathbf{B}$ = circ(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0).

Definition 5. The parameters of a *PG*(q, m) projective geometry or Singer difference set are

$$(\nu, k, \lambda) = \left(\frac{q^{m+1} - 1}{q - 1}, \frac{q^m - 1}{q - 1}, \frac{q^{m-1} - 1}{q - 1} \right),$$

q a prime power.

Examples of matrices with these parameters are given in the survey of Marshall Hall [9], they were generalized in [11, 12].

Construction for Two-Level Cretan Matrices

We now use difference sets to construct two-level Cretan (quasi-orthogonal) matrices. We use the notation $\gamma = \dfrac{q^{m-1} - 1}{q^{m-1}(q - 1)}$.

Construction 1. *Consider the* Singer difference sets *with parameters*

$$(\nu, k, \lambda) = \left(\frac{q^{m+1} - 1}{q - 1}, \frac{q^m - 1}{q - 1}, \frac{q^{m-1} - 1}{q - 1} \right),$$

q a prime power.

Then, when its incidence matrix has its ones replaced by a and zeros with $-b$, *we obtain a two-level quasi-orthogonal matrix* $\mathbf{S}$ *satisfying* the orthogonality *equation*

$$\mathbf{S}^{\mathrm{T}}\mathbf{S} = \mathbf{S}\mathbf{S}^{\mathrm{T}} = \omega \mathbf{I}_n, \tag{1}$$

giving the radius equation $k\, a^2 + (\nu - k) b^2 = \omega$ or

$$\frac{q^m - 1}{q - 1} a^2 + q^m b^2 = \omega, \tag{2}$$

and the characteristic equation $\lambda a^2 - 2(k - \lambda) ab + (\nu - 2k + \lambda) b^2 = 0$ or

$$\gamma a^2 - 2ab + (q - 1) b^2 = 0, \tag{3}$$

thus so we have solutions

$$b = \frac{\gamma}{1 \pm \sqrt{1 - \gamma(q - 1)}}. \tag{4}$$

The level a=1 *is pre-determined for all quasi-orthogonal matrices*; *if* b>a *we have to choose the second level to be* 1/b *for the complementary difference set, to ensure entries are from the unit disk.*

The determinant of Cretan matrices $\det(\mathbf{S}) = \omega^{\frac{\nu}{2}}$.

We are particularly interested in the projective planes $PG(q, 2)$ with $\gamma = \frac{1}{q}$.

Corollary 1 (*Singer Difference Sets and Projective Planes*). *Let q be a prime power.*

Then there exists a projective plane $(q^2+q+1, q+1, 1)$. *Hence we have a two-level quasi-orthogonal matrix*, **S**, *satisfying* (1)–(3) *with* $b = \frac{1}{q \pm \sqrt{q}}$,

$$\omega = \frac{q^2}{(q \pm \sqrt{q})^2} + q + 1, \text{ , and } \det(\mathbf{S}) = \omega^{\frac{q^2+q+1}{2}}.$$

For the "–" sign, choosing a = 1, *we have a* principal solution *with bigger b and bigger determinant of Cretan matrix.*

Corollary 2 (*Singer Difference Sets and PG*(2, *m*) with $\gamma = 1 - 2^{1-m}$). *Let q be a prime power.*

Then there exists a projective plane $(2^{m+1}-1, 2^m-1, 2^{m-1}-1)$. *Hence we have a two-level quasi-orthogonal matrix*, **S**, *satisfying* (1)–(3) *with*

$$b = \frac{\lambda}{\lambda+1 \pm \sqrt{\lambda+1}}, \ \omega = k + (\nu - k)b^2, \text{ and } \det(\mathbf{S}) = \omega^{\frac{2^{m+1}-1}{2}}.$$

For the "–" sign, choosing a = 1, *we have b > a, it leads to a principal solution with the complementary difference set* (ν, ν – *k*, ν – 2*k* + λ) *and modulus of level* 1/*b*.

Example 2. Consider *PG*(7, 2) with parameters (57,8,1) and $\gamma = \frac{\lambda}{q^{m-1}} = \frac{1}{7}$.

From [13] we have difference set {0, 1 , 5, 7, 17, 35, 38, 49} to generate *Cretan matrix CM*(57) with moduli of levels $a = 1$, $b = \frac{\gamma}{1-\sqrt{1-\gamma(q-1)}} = \frac{1}{7-\sqrt{7}} = 0.2297$ and weight $\omega = k + (\nu - k)b^2 = 10.5845$, $\det(\mathbf{S}) = \omega^{\frac{57}{2}} =$ $= 1.6\ 10^{29}$ for the principal solution Figure, *a*. Non principal solution will have the same structure of matrix **S** with smaller $b = \frac{\gamma}{1+\sqrt{1-\gamma(q-1)}} = 0.1037$ and smaller determinant 3.7×10^{26}.

Example 3. Consider *PG*(5, 3) with parameters (156,31,6) and $\gamma = \frac{\lambda}{q^{m-1}} = \frac{6}{25}$.

From [13] we have difference set {0,1,2,4,14,18, 21,22,30,31,37,42,45,49,51,55,56,60,76,82, 85,87,88,93,95,98,108,110,117,134,142} to generate *Cretan matrix CM*(156) with moduli of levels $a = 1$, $b = \frac{\gamma}{1-\sqrt{1-\gamma(q-1)}} = \frac{6}{25-\sqrt{25}} = 0.3$ and weight

■ ***Table 1.*** The *CM* given by *PG*(*q*, 2)

q	(ν, *k*, λ)	*b*	ω	det(**S**)
2	(7,4,2)* (7,3,1)	0.5858* 0.2929	5.0294 3.3431	2.85×10^{2} 68
3	(13,4,1)	0.7887 0.2113	5.8660 4.4019	9.87×10^{4} 1.53×10^{4}
5	(31,6,1)	0.3618 0.1382	6.6545 6.4775	5.73×10^{12} 3.77×10^{12}
7	(57,8,1)	0.2297 0.1037	8.3692 8.5267	1.97×10^{26} 3.36×10^{26}
11	(133,12,1)	0.1302 0.0698	12.1863 12.5903	1.6×10^{72} 1.4×10^{73}
13	(183,14,1)	0.1064 0.0602	14.1473 14.6129	1.9×10^{105} 3.6×10^{106}

Signs "–" or "+" (two solutions for *b*) give two columns.

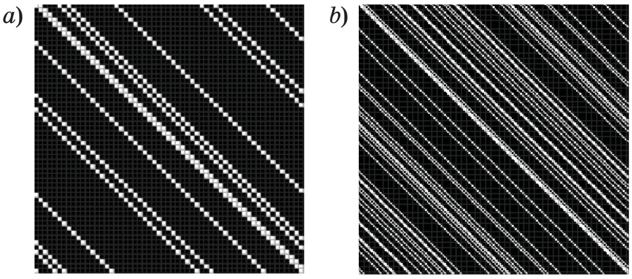
For case, denoted by *, *b* > *a*, it leads to the complementary difference set (ν, ν – *k*, ν – 2*k* + λ) and level 1/*b* = 0.5858 by an analogue of the equivalent version for an Hadamard matrix.

■ ***Table 2.*** The *CM* given by *PG*(2, *m*)

m	(ν, *k*, λ)	*b*	ω	det(**S**)
1	(3,2,1)* (3,1,0)	0.5 0	2.25 1	3.375 1
2	(7,4,2)* (7,3,1)	0.5858* 0.2929	5.0294 3.3431	2.85×10^{2} 68
3	(15,8,4)* (15,7,3)	0.6667* 0.5	11.1111 9	6.97×10^{7} 1.43×10^{7}
4	(31,16,8)* (31,15,7)	0.7388* 0.6464	24.1873 21.6863	2.79×10^{21} 0.51×10^{21}
5	(63,32,16)* (63,31,15)	0.8* 0.75	51.84 49	1.0×10^{54} 1.7×10^{53}
6	(127,64,32)* (127,63,31)	0.8498* 0.8232	109.4938 106.3726	3.2×10^{129} 5.1×10^{128}

Signs "–" or "+" (two solutions for *b*) give two columns.

For case, denoted by *, *b* > *a*, it leads to the complementary difference set (ν, ν – *k*, ν – 2*k* + λ) and level 1/*b* = 0.5858, the same, as we have seen before.



■ Cretan matrix $CM(57)$ for $PG(7, 2)$ (a) and Cretan matrix $CM(156)$ for $PG(5, 3)$ (b) of Singer Family

$\omega = k + (\nu - k)b^2 = 42.25$, $\det(\mathbf{S}) = \omega^{\frac{156}{2}} = 6.5\times10^{126}$ for the principal solution Figure, b. Non principal solution will have the same structure of matrix **S** with smaller $b = \dfrac{\gamma}{1+\sqrt{1-\gamma(q-1)}} = 0.2$ and smaller determinant 2.5×10^{121}.

Acknowledgements

The authors would like to acknowledge Professor Mikhael Sergeev for his advice regarding the content of this paper. The authors also 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

We note that there exist (ν, k, λ) Singer difference sets for $\nu = 4t + 1, 4t, 4t - 1, 4t - 2$.

The La Jolla Difference Set Repository [13] gives many parameter sets which can make circulant incidence matrices from difference sets. It opens new possibilities for image processing (compression, masking) and other areas we mentioned in our introduction.

References

1. **Balonin N. A., Mironovskii L. A.** Hadamard Matrices of Odd Order. *Informatsionno-upravliaiushchie sistemy*, 2006, no. 3(22), pp. 46–50 (In Russian).
2. **Balonin N. A., Seberry Jennifer.** Remarks on Extremal and Maximum Determinant Matrices with Real Entries ≤ 1. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 5(71), pp. 2–4.
3. **Balonin N. A., Sergeev M. B.** Local Maximum Determinant Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1(68), pp. 2–15 (In Russian).
4. **Hadamard J.** Résolution d'une Question Relative aux Déterminants. *Bulletin des Sciences Mathématiques*, 1893, vol. 17, pp. 240–246 (In French).
5. **Balonin N. A., Seberry Jennifer.** A Review and New Symmetric Conference Matrices. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 4(71), pp. 2–7.
6. **Wallis (Seberry) Jennifer.** Orthogonal (0, 1, –1) Matrices. *Proc. of First Australian Conf. on Combinatorial Mathematics*, TUNRA, Newcastle, 1972, pp. 61–84.
7. **Seberry J., 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, 1992, pp. 431–560.
8. **Singer J.** A Theorem in Finite Projectie Geometry and Some Applications to Number Theory. *Transactions of the American Mathematical Society*, 1938, vol. 43, pp. 377–385.
9. **Hall Jr. M.** A Survey of Difference Sets. *Proc. American Mathematical Society*, 1956, vol. 7, pp. 975–986.
10. **Seberry Jennifer.** *Regular Hadamard Matrices of Order 36*. Available at: http://www.uow.edu.au/ jennie/matrices/H36/36R.html (accessed 1 December 2014).
11. **Jonathan Jedwab, James Davis.** *A Survey of Hadamard Difference Sets*. Hewlett Packard Technical Reports. Richmond, University of Richmond, 1994. 16 p.
12. **McFarland, Robert L.** A Family of Difference Sets in Non-cyclic Groups. *Journal of Combinatorial Theory. Ser. A15*, 1973, no. 1, pp. 1–10.
13. *La Jolla Difference Set Repository*. Available at: www.ccrwest.org/ds.html (accessed 1 December 2014).