TWO LEVEL CRETAN MATRICES CONSTRUCTED VIA SINGER DIFFERENCE SETS

N. A. Balonin, Dr. Sc., Tech., Professor, korbendfs@mail.ru
Jennifer Seberry, PhD, Professor of Computer Science, jennifer_seberry@uow.edu.au

School of Computer Science and Software Engineering, Faculty of Engineering and Information Science, University of Wollongong, NSW, 2522, Australia

UDC 004.438

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 definitions, notation differently than we have in our past [1]. This, we hope, will cause less confusion, bring our nomenclature closer to common definitions, notation differently than we have in the past [1]. This, we hope, will cause less confusion, bring our nomenclature closer to common

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

In this and future work we will only use quasi-orthogonal to refer to matrices with moduli of real elements $\leq 1$ [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 $STS = SS^T = = \omega I_n$, 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 $\omega I_n$, 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 $\omega \leq n$.

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 formulation for level $b \leq a$.

Definition 2. A Cretan(n) matrix, CM, is a quasi-orthogonal matrix of order $n$ with entries $\leq 1$, 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 $\omega$. The inner product of distinct rows of $CM(n)$ is zero. A $\tau$-level Cretan(n; $\tau$; $\omega$) matrix, $CM(n; \tau; \omega)$, has $\tau$ 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 = \( \tau \), CM(order; number of levels = \( \tau \); occurrences of levels = \( L_1, L_2, \ldots, L_\tau \)), CM(order; number of levels = \( \tau \); weight = \( \omega \)), and CM(order; number of levels = \( \tau \); weight; occurrences of levels in whole matrix), 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 the integers 0, 1, 2, \ldots, 10. Hence we take all the differences modulo 11. Then \( \Delta \) 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 B = circ(0, 1, 0, 1, 1, 0, 0, 0, 1, 0).

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

\[
(v, k, \lambda) = \left( \frac{q^m - 1}{q - 1} - \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} \right),
\]

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 \( \gamma = \frac{q^m - 1}{q - 1} \).

Construction 1. Consider the Singer difference sets with parameters

\[
(v, k, \lambda) = \left( \frac{q^m - 1}{q - 1} - \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} \right),
\]

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 S satisfying the orthogonality equation

\[
S^TS = SS^T = \omega I_n,
\]

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

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

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

\[
\gamma a^2 - 2ab + (q - 1)b^2 = 0,
\]

thus so we have solutions

\[
b = \frac{\gamma}{1 \pm \sqrt{1 - \gamma(q - 1)}}.
\]

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

**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 $b = \frac{1}{q^{\pm 1} + q}$,

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

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 $\gamma = 1 - 2^{1-b}$). Let $q$ be a prime power.

Then there exists a projective plane $(2^{m+1} - 1, 2^{m+1} - 1 - 1)$. Hence we have a two-level quasi-orthogonal matrix, $S$, satisfying (1)-(3) with $b = \frac{\sqrt{q}}{\sqrt{q} + 1} + 1, \omega = k + (v - h)^2$, and $\det(S) = \omega \frac{q^2}{2}$. For the $"-"$ sign, choosing $a = 1$, we have $b > a$, it leads to a principal solution with the complementary difference set $(v, v - k, v - 2k + \lambda)$ and modulus of level $1/b$.

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

From [13] we have difference set $(0,1,5,7,17,35,38,49)$ to generate Cretan matrix $CM(57)$ with moduli of levels $a = 1, b = \frac{\gamma}{1 - \sqrt{1 - \gamma(q-1)}} = a. 1026$ 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 $3.7 \times 10^{26}$.

**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 $(0,1,2,4,14,18,21,22,30,31,37,42,45,49,51,53,56,60,76,82,85,87,88,93,95,98,108,110,117,134,142)$ to generate Cretan matrix $CM(156)$ with moduli of levels $a = 1, b = \frac{\gamma}{1 - \sqrt{1 - \gamma(q-1)}} = 1.6 \times 10^{23}$ and weight $6$.

### Table 1. The CM given by $PG(q, 2)$

<table>
<thead>
<tr>
<th>$q$</th>
<th>$(v, k, \lambda)$</th>
<th>$b$</th>
<th>$\omega$</th>
<th>$\det(S)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(7,4,2)</td>
<td>0.5858*</td>
<td>0.2929</td>
<td>5.0294</td>
</tr>
<tr>
<td>3</td>
<td>(13,4,1)</td>
<td>0.7887</td>
<td>0.2113</td>
<td>5.8660</td>
</tr>
<tr>
<td>5</td>
<td>(31,6,1)</td>
<td>0.3618</td>
<td>0.1382</td>
<td>6.6545</td>
</tr>
<tr>
<td>7</td>
<td>(57,8,1)</td>
<td>0.2297</td>
<td>0.1037</td>
<td>8.3692</td>
</tr>
<tr>
<td>11</td>
<td>(133,12,1)</td>
<td>0.1302</td>
<td>0.0699</td>
<td>12.1863</td>
</tr>
<tr>
<td>13</td>
<td>(183,14,1)</td>
<td>0.1064</td>
<td>0.0602</td>
<td>14.1473</td>
</tr>
</tbody>
</table>

Signs $"-"$ or $"+"$ (two solutions for $b$) give two columns.

For case, denoted by $e$, $b > a$, it leads to the complementary difference set $(v, v - k, v - 2k + \lambda)$ and level $1/b = 0.5858$ by an analogue of the equivalent version for an Hadamard matrix.

### Table 2. The CM given by $PG(2, m)$

<table>
<thead>
<tr>
<th>$m$</th>
<th>$(v, k, \lambda)$</th>
<th>$b$</th>
<th>$\omega$</th>
<th>$\det(S)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(3,2,1)</td>
<td>0.5</td>
<td>0</td>
<td>2.25</td>
</tr>
<tr>
<td>2</td>
<td>(7,4,2)</td>
<td>0.5858*</td>
<td>0.2929</td>
<td>5.0294</td>
</tr>
<tr>
<td>3</td>
<td>(15,8,4)</td>
<td>0.6667*</td>
<td>0.5</td>
<td>11.1111</td>
</tr>
<tr>
<td>4</td>
<td>(31,16,8)</td>
<td>0.7388*</td>
<td>0.6464</td>
<td>24.1873</td>
</tr>
<tr>
<td>5</td>
<td>(63,32,16)</td>
<td>0.8*</td>
<td>0.75</td>
<td>51.84</td>
</tr>
<tr>
<td>6</td>
<td>(127,64,32)</td>
<td>0.8498*</td>
<td>0.8232</td>
<td>109.4938</td>
</tr>
</tbody>
</table>

Signs $"-"$ or $"+"$ (two solutions for $b$) give two columns.

For case, denoted by $e$, $b > a$, it leads to the complementary difference set $(v, v - k, v - 2k + \lambda)$ and level $1/b = 0.5858$, the same, as we have seen before.
ω = k + (v - k)b² = 42.25, \( \det(S) = \omega \frac{156}{2} = 6.5 \times 10^{126} \)

for the principal solution Figure, b. Non principal solution will have the same structure of matrix \( S \) with smaller \( b = \frac{\gamma}{1 + \sqrt{1 - \gamma(q - 1)}} \approx 0.2 \) and smaller
determinant \( 2.5 \times 10^{121} \).

**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 \((v, k, \lambda)\) Singer difference sets for \( v = 4t + 1, 4t, 4t - 1, 4t - 2 \).

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**