# On Good Matrices and Skew Hadamard Matrices

Gene Awyzio and Jennifer Seberry

**Dedicated to Hadi Kharighani on his 70th Birthday**

n her PhD thesis (Seberry) Wallis described a method using a variation of the Williamson array to find suitable matrices, which we will call good matrices, to construct skew Hadamard matrices. Good matrices were designed to plug into the Seberry-Williamson array to give skew-Hadamard matrices. We investigate the properties of good matrices in an effort to find a new, efficient, method to compute these matrices. We give the parameters of the supplementary difference sets (sds) which give good matrices for use in the Seberry-Williamson array.

## 1 Introduction

Many constructions for $\pm 1$ matrices and similar matrices such as Hadamard matrices, weighing matrices, conference matrices and $D$-optimal designs use skew Hadamard matrices in their construction. For more details see Seberry and Yamada [23].

An Hadamard matrix is a square matrix with elements of $\pm 1$ and mutually orthogonal rows. Thus a $4w \times 4w$ Hadamard matrix must have $2w(4w-1)$ entries of $-1$ and $2w(4w+1)$ entries of $+1$ for a normalized Hadamard matrix, that is one where the first row and first column are all $+1$. For any Hadamard matrix $H$ of size $4w \times 4w$ $HH^\top = 4wI_{4w} = H^\top H$. In all our examples minus ("$-$") is used to denote minus one ("$-1$").

Gene Awyzio
Faculty of Engineering and Information Sciences, University of Wollongong, NSW, 2522 Australia, e-mail: gene_awyzio@uow.edu.au

Jennifer Seberry
Centre for Computer and Information Security Research,
Faculty of Engineering and Information Sciences, University of Wollongong, NSW, 2522 Australia
e-mail: jennifer_seberry@uow.edu.au

Hadamard matrices of order $4w$ are conjectured to exist for all orders $4w \equiv 0 \pmod 4$. A weighing matrix, $W = W(4w,k)$, of order $4w$ and weight $k$ has elements $0,\ \pm 1$ and satisfies $WW^\top = kI_{4w}$. These are conjectured to exist for all $k = 1 \cdots 4w$ for each order $4w$. If an Hadamard matrix $M$, can be written in the form $M = I + S$ where $S^\top = -S$, then $M$ is said to be a *skew-Hadamard matrix*. Skew-Hadamard matrices are also conjectured to exist for all orders $4w \equiv 0 \pmod 4$. The first unresolved case for Hadamard matrices is currently $4 \times 167$.

*Example 1.* **Hadamard matrices**

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix} \quad H_{4_{symmetric}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{bmatrix} \quad H_{4_{skew-type}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ - & 1 & 1 & - \\ - & - & 1 & 1 \\ - & 1 & - & 1 \end{bmatrix}.$$

## *1.1 Circulant and Type 1 Matrix Basics*

Because it is so important for the rest of our work we now spend a little effort to establish why the properties required for Williamson matrices are so important.

We define the *shift matrix, T* of order $n$ by

$$T = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}.$$

So any circulant matrix, of order $n$ and first row $x_1,\ x_2, \cdots, x_n$, that is,

$$\begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_n & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_n & x_1 & \cdots & x_{n-2} \\ \vdots & & & & \vdots \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{bmatrix} \tag{1}$$

can be written as the polynomial

$$x_1T^n + x_2T + x_3T^2 \cdots x_nT^{n-1}.$$

We now note that polynomials commute, so any two circulant matrices of the same order $n$ commute.

We define the *back-diagonal matrix, R* of order $n$ by

$$R = \begin{bmatrix} 0\,0\cdots 1 \\ 0\,0\cdots 0 \\ \vdots \quad\quad \vdots \\ 1\,0\cdots 0 \end{bmatrix}.$$

Since $T^m R$ is the polynomial for any integer $m \geq 0$, we have that, similarly, any back-circulant matrix, of order $n$ and first row $x_1,\ x_2, \cdots, x_n$, that is,

$$\begin{bmatrix} x_1\ x_2\ x_3\ \cdots\ x_n \\ x_2\ x_3\ x_4\ \cdots\ x_1 \\ x_3\ x_4\ x_5\ \cdots\ x_2 \\ \vdots \quad\quad\quad\quad \vdots \\ x_n\ x_1\ x_2\ \cdots\ x_{n-1} \end{bmatrix}$$

can be written as the polynomial

$$x_1 T^n R + x_2 TR + x_3 T^2 R \cdots x_n T^{n-1} R.$$

Mathematically we have that:

A *circulant matrix* $C = (c_{ij})$ of order $n$ is a matrix which satisfies the condition that $c_{ij} = c_{1,j-i+1}$, where $j-i+1$ is reduced modulo $n$ [26]. A *back circulant* matrix $B = (b_{ij})$ order $n$ is a matrix with property that $b_{ij} = b_{1,i+j-1}$, where $i+j-1$ is reduced modulo $n$ [26].

The transpose of a back circulant matrix is the same as itself, so it is also a symmetric matrix. In this paper we will not need to study back-circulant matrices further but define them here for completeness only.

In all our definitions of circulant and back-circulant matrices we have assumed that the rows and columns have been indexed by the order, that is for order $n$, the rows are named after the integers $1,\ 2, \cdots,\ n$ and similarly for the columns. The internal entries are then defined by the first row using a 1:1 and onto mapping $f : G \to G$. However we could have indexed the rows and columns using the elements of a group $G$, with elements $g_1$, $g_2$, $\cdots$, $g_n$. Loosely a *type one matrix* will then be defined so the $(ij)$ element depends on a 1:1 and onto mapping of $f(g_j - g_i)$ for type 1 matrices and of $f(g_j + g_i)$ for *type two matrices*. We use additive notation, but that is not necessary. Seberry-Wallis and Whiteman [32] have shown that circulant and type 1 can be used interchangeably in the enunciations of theorems as can the terms back-circulant and type 2. This can be used to explore similar theorems in more structured groups.

## 2 Historical Background

Hadamard matrices first appeared in the literature in an 1867 paper written by J. J. Sylvester [24]. In 1892 Hadamard matrices first appear. They were called matrices

on the unit circle as they satisfied Hadamard's inequality for the determinant of matrices with entries within the unit circle [13].

Later Scarpis [20] found many Hadamard matrices using primes. In 1933 Paley [19] conjectured that Hadamard matrices existed for all positive integer orders divisible by 4. This has become known as the Hadamard conjecture:

*Conjecture 1 (**Paley**).* Hadamard matrices exist for all orders 1, 2, $4w$, where $w$ is a positive integer.

Paley's work [19, 27] left many orders for Hadamard matrices unresolved. Later Williamson [33] gave a method that many researchers hoped would give results for all orders of Hadamard matrices. Many results are given in [1, 2, 3, 4]. That the Williamson method would give results for all orders of Hadamard matrices was first disproved by Djoković in 1993 [7].

Schmidt's review [21] of Holzmann, Kharaghani and Tayfeh-Rezaie [15] points out that there are none of order 47, 53 or 59. Unfortunately the startling paper of Holzmann, Kharaghani and Tayfeh-Rezaie [16] showed that we have no Williamson constructions for some other small orders. They give the following table:

| Order: | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number: | 1 | 1 | 1 | 2 | 3 | 1 | 4 | 4 | 4 | 6 | 7 | 1 | 10 | 6 | 1 |
| Order: | 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 | 47 | 49 | 51 | 53 | 55 | 57 | 59 |
| Number: | 2 | 5 | 0 | 4 | 1 | 1 | 2 | 1 | 0 | 1 | 2 | 0 | 1 | 1 | 0 |

**Table 1** Number of Williamson Matrices of Order 1-59

Good matrices first appeared in the PhD Thesis of Jennifer (Seberry) Wallis [27]. There the matrices, which were given no name, were given for $w = 1, \cdots 15, 19$. In 1971 she gave good matrices for $w = 23$ [30]. The array and construction using the Seberry-Williamson array to construct skew-Hadamard matrices was also given there, but not named. Good matrices were first used by name in [29]. Hunt [17] gave the matrices for $w = 1, \cdots, 25$. Later Szekeres [25] gave a list for order $w = 1, \cdots, 31$. Djoković [8, 7] provided orders $w = 33$, 35 and 127. Then Georgiou, Koukouvinos and Stylianou [12] provided 37, 39. Djoković [11] says that only one set of supplementary difference sets, (41;20,20,16,16;31), for 41 remains to be searched.

We note that while there are no Williamson matrices of order 35 there are good matrices of order 35.

(Seberry) Wallis [27] gave a construction for $w = 19$ and Djoković [8] for $w = 33$, 35, and 127. The remainder were found by computer search.

Other relevant publications are: [10], [6], [5],[9], [11], [22], [31].

# 3 Williamson Type Constructions

## *3.1 Williamson Array*

In 1944 [33] Williamson proposed using what has come to be known as the *Williamson array*. If we can calculate suitable matrices of order $w$ they can be plugged-in to his array to give Hadamard matrices of order $4w$.

We use the *Williamson-array* in the form

$$W_{Williamson-array} = \begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}$$

where $A$, $B$, $C$, $D$ are circulant (cyclic) matrices with symmetric first rows which satisfy the *additive property*

$$AA^\top + BB^\top + CC^\top + DD^\top = 4wI_w. \tag{2}$$

These matrices are known as *Williamson matrices*

The Williamson-array is *formally orthogonal*. An Hadamard matrix is made by plugging *Williamson matrices* into the $W_{williamson-array}$.

*Example 2.* **Williamson matrix of order** $4 \times 3$

$$W_{12_{Williamson}} = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & - & - & 1 & - & - & 1 & - & - & 1 & 1 & 1 \\ - & 1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\ - & - & 1 & - & - & 1 & - & - & 1 & 1 & 1 & 1 \\ \hline - & 1 & 1 & 1 & - & - & 1 & 1 & 1 & - & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & 1 & 1 & 1 & - & 1 \\ 1 & 1 & - & - & - & 1 & 1 & 1 & 1 & 1 & 1 & - \\ \hline - & 1 & 1 & - & - & - & 1 & - & - & 1 & - & - \\ 1 & - & 1 & - & - & - & - & 1 & - & - & 1 & - \\ 1 & 1 & - & - & - & - & - & - & 1 & - & - & 1 \\ \hline - & - & - & 1 & - & - & - & 1 & 1 & 1 & - & - \\ - & - & - & - & 1 & - & 1 & - & 1 & - & 1 & - \\ - & - & - & - & - & 1 & 1 & 1 & - & - & - & 1 \end{array}\right]$$

*Remark 1.* An example of the crucial part of proof is: when we look at the terms of $W_{williamson-array}W^\top_{williamson-array}$ for, say the (2,3) element we have

$$BC^\top - AD^\top + DA^\top - CD^\top = BC - AD + DA - CB = 0\,.$$

Noting matrices $A$, $B$, $C$ and $D$ are polynomials, and commute, the (2,3) element will reduce to zero. Similarly the other off diagonal elements are 0. □

### 3.2 Seberry-Williamson Array

In her PhD thesis [27] Seberry Wallis gave a Seberry-Williamson array, a modification of the Williamson array which can be used to make skew Hadamard matrices. Written in terms of circulant and back circulant matrices it is

$$W_{Seberry-Williamson-array} = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & DR & -CR \\ -CR & -DR & A & BR \\ -DR & CR & -BR & A \end{bmatrix}.$$

Where A is a $\pm 1$ skew-type cyclic matrix and $B$, $C$, $D$ are circulant matrices with symmetric first rows which satisfy the additive property given in equation 2. These are called *good* matrices [29]. Thus the first rows each have the form

$$\sigma_A = (1)(S_A)(-S_A*), \sigma_B = (1)(S_B)(S_B*), \sigma_C = (1)(S_C)(S_C*), \sigma_D = (1)(S_D)(S_D*),$$

where $S*$ means the elements of S in reverse order. $S_X*$ are the elements of $S_X$ reversed. (In matrix terms this is $RXR$.) A skew-Hadamard matrix can be made by plugging good matrices into the $W_{Seberry-Williamson-array}$.

*Example 3.* **Seberry-Williamson matrix of order** $4 \times 3$

The Seberry-Williamson matrix for first rows $A = 11-$, $B = 1--$, $C = 1--$, $D = 111$ is:

$$W_{Seberry-Williamson} = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & 1 & - & - & - & 1 & - & - & 1 & 1 & 1 & 1 \\ - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\ 1 & - & 1 & 1 & - & - & 1 & - & - & 1 & 1 & 1 \\ \hline 1 & 1 & - & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 & - \\ 1 & - & 1 & - & 1 & 1 & 1 & 1 & 1 & 1 & - & 1 \\ - & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & - & 1 & 1 \\ \hline 1 & 1 & - & - & - & - & 1 & 1 & - & - & - & 1 \\ 1 & - & 1 & - & - & - & - & 1 & 1 & - & 1 & - \\ - & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - & - \\ \hline - & - & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - \\ - & - & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 \\ - & - & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 \end{array}\right].$$

### 3.3 Structure of First Rows of Williamson and Good Matrices

For the Williamson Hadamard matrix each of the four matrices $A$, $B$, $C$ and $D$, of order $w$, $w$ odd, is symmetric and thus can be written with first row

$$\sigma = 1, \underbrace{x_1,\, x_2, \cdots,\, x_{\frac{w-1}{2}}}_{q \text{ negative elements}}, \quad \underbrace{x_{\frac{w-1}{2}},\, \cdots,\, x_2,\, x_1,}_{q \text{ negative elements}}$$

where each $x_i$, $i = 1, \cdots, \frac{w-1}{2}$ is $\pm 1$.

We will refer to these first rows as

$$\sigma = \{1,\ S,\ S*\}.$$

where, for example the first row of $A$,

$$\sigma_A = \{1,\ S_A,\ S_A*\}$$

contains

$$S_A = x_1,\, x_2, \cdots,\, x_{\frac{w-1}{2}}$$

and $S_A*$, the reverse of this sequence, is:

$$S_A* = x_{\frac{w-1}{2}}, \cdots,\, x_2,\, x_1\,.$$

Similarly we obtain $S_B$, $S_B*$, $S_C$, $S_C*$, $S_D$ and $S_D*$. The number of such matrices, in each case, $2^{\frac{w-1}{2}}$. We see that the congruence class of $S_A*$ is given by the two little endian entries of $S_A$.

These properties will allow us to impose constraints on the search space (and time) to find these matrices.

**Lemma 1.** *Suppose $A$ is a circulant matrix with first row written as $\sigma_A = (1)(S_A)(-S_A*)$. Then the matrix $A'$ with first row $\sigma'_A = (1)(-S_A)(S_A*)$, that is, it has all the 2nd to wth elements of the first row written in the reverse order, has exactly the same inner products of its rows as $A$.*

From Marshall Hall [14, lemma 14.2.1] we have a lemma for Williamson matrices:

**Lemma 2.** *If $w$ is odd, and if the Williamson matrices $A$, $B$, $C$, $D$, are chosen so the first element of their first rows is $+1$, then for each $i = 2, \cdots, w$ exactly three of the $i$th elements of the first rows have the same sign.*

## *3.4 Structure of First Rows of Good Matrices*

We now consider further the good matrices, $A$, $B$, $C$, $D$ of order $m$ which satisfy the additive property 2.

Write, using the shift matrix $T$,

$$A = P_1 - N_1 \tag{3}$$

with $P_1$ the sum of the terms with positive coefficient in $A$ and $-N_1$ the sum of the terms with negative coefficient in $A$, whence

$$P_1 = \sum_j a_{1j} T^{j-1}, \qquad a_{1j} = +1, \qquad -N = \sum_j a_{1j} T^{j-1}, \qquad a_{1j} = -1 \tag{4}$$

In the same way write

$$B = P_2 - N_2, \qquad C = P_3 - N_3, \qquad D = P_4 - N_4. \tag{5}$$

Since $a_{11} = +1$ and $A$ is circulant and skew-type, $a_{1j} = -a_{1,m+2-j}$, $2 \le j \le m$. Hence there are

$$\frac{m+1}{2} = p_1 \tag{6}$$

positive terms in the first row of $A$, so the number of terms in the first row of $P_1$ is an odd number if $m \equiv 1 \pmod 4$ and an even number if $m \equiv 3 \pmod 4$.

Since $B$ is circulant and symmetric we may choose $b_{11} = +1$ and $b_{1j} = b_{1,m+2-j}$, $2 \le j \le m$. The positive terms occur in pairs, so $p_2$ the number of positive terms in the first row of $P_2$, is an odd number. Similarly $p_3$ and $p_4$ are odd numbers.

We now write

$$J = I + T + T^2 + \ldots T^{m-1} = \left(I + T + T^2 \ldots T^{m-1}\right) R. \tag{7}$$

Then

$$P_i + N_i = J, \quad i = 1,2,3,4 \tag{8}$$

so the additive property 2 becomes

$$AA^T + B^2 + C^2 + D^2 = 4mI_m$$

and by (3), (4) and (5) this becomes

$$(2P_1 - J)(2P_1 - J)^T + (2P_2 - J)^2 + (2P_3 - J)^2 + (2P_4 - J)^2 = 4mI_m,$$

that is

$$(2P_1 - J)(-2P_1 + J + 2I) + (2P_2 - J)^2 + (2P_3 - J)^2 + (2P_4 - J)^2 = 4mI_m,$$

since $A$ is skew-type. So we have since $P_i J = p_i J$ and $J^2 = mJ$

$$4\left(-P_1^2 + P_2^2 + P_3^2 + P_4^2 + P_1\right) + 4(p_1 - p_2 - p_3 - p_4)J + (2m-2)J = 4mI_m. \tag{9}$$

Now from (6)

$$4p_1 + 2m - 2 = 4m$$

so (9) becomes

$$\left(-P_1^2 + P_2^2 + P_3^2 + P_4^2 + P_1\right) = -(m - p_2 - p_3 - p_4)J + mI_m. \tag{10}$$

If $m$ is odd, then since $P_2$, $P_3$ and $P_4$ all have an odd number of positive elements in their first rows, the coefficients of $J$ are all even.

Now notice $B$, $C$, $D$, are polynomials in $T$ and $R$ so

$$P_i = \left(\sum_j e_{1j} T^{j-1}\right) R$$

for $i = 2,3,4$ and $e_{1j} = b_{1j}$, $c_{1j}$, $d_{1j}$ respectively, also $P_i = P_i^T$ so

$$P_i^2 = P_i P_i^T = \left(\sum_j e_{1j} T^{j-1}\right) RR^T \left(\sum_k e_{1k} T^{k-1}\right) = \sum_n f_n T^n,$$

that is $P_1^2$, $P_2^2$, $P_3^2$, and $P_4^2$ may all be regarded as polynomials in $T$.

For each $t = 1,\ldots,m-1$, there is a unique $s$ such that $(T^s)^2 = T^t$. In $P_j^2 = \left(\sum T^k\right)^2$, $k$ is a subset of $1,2,\ldots,m$, we have

$$P_j^2 \equiv \sum T^k \pmod 2.$$

Then since the coefficient of $J$ in (10) is always even, we have shown:

**Theorem 1.** *If $m$ is odd, $T$ the shift matrix, and $P_1$, $P_2$, $P_3$, $P_4$ are the terms with positive coefficients of $A$, $B$, $C$, $D$ as defined by* (8)*, respectively, and if*

$$AA^T + BB^T + CC^T + DD^T = 4mI$$

*then writing*

$$P_1 + P_1^2 = \sum_{\substack{i \\ i \neq 0}} f_i T^i \quad \textit{and} \quad P_2^2 + P_3^2 + P_4^2 = \sum_{\substack{i \\ i \neq 0}} g_i T^i$$

*we have $g_i = f_i \pmod 2$ when $i \neq 0$.*

Marshall Hall's lemma [14] allowed considerable improvements in algorithms to find Williamson matrices. Theorem 1 allows for improvements in algorithms to find good matrices.

## *3.5 Sums of Squares of First Rows for Arrays*

We notice that for the arrays, of Williamson and Seberry-Williamson, which have $\pm 1$ matrices, $A$, $B$, $C$, $D$ of order $w$ plugged into them, these must satisfy the additive property 2.

$$AA^\top + BB^\top + CC^\top + DD^\top = 4wI_w.$$

Then if $\mathbf{e}$ is the $1 \times w$ matrix of all ones and the row sums of $A$, $B$, $C$, $D$ are $a$, $b$, $c$, and $d$ respectively. Then

$$\mathbf{e}A = a\mathbf{e}, \quad \mathbf{e}B = b\mathbf{e}, \quad \mathbf{e}C = c\mathbf{e}, \quad \mathbf{e}D = d\mathbf{e},$$

and

$$\mathbf{e}(AA^\top + BB^\top + CC^\top + DD^\top) = a^2\mathbf{e} + b^2\mathbf{e} + c^2\mathbf{e} + d^2\mathbf{e} = 4w\mathbf{e}.$$

For Williamson and good matrices we have

$$4w = a^2 + b^2 + c^2 + d^2.$$

**Lemma 3.** *For the a, b, c, d, and w just defined for Williamson matrices*

$$a \equiv b \equiv c \equiv d \equiv w \pmod 4.$$

*For good matrices*

$$b \equiv c \equiv d \equiv w \pmod 4. \square$$

## 4 Implications for Seberry-Williamson Arrays and Good Matrices

Note if

$$4w = a^2 + b^2 + c^2 + d^2, \tag{11}$$

$b$, $c$, $d$ and $w$ are all of the same congruence class modulo 4. $a$ is always 1 within a good matrix.

| Length | Order | Pattern of Four Squares | $b$, $c$, $d$ | $b+c+d+w$ | $\lvert b\rvert+\lvert c\rvert+\lvert d\rvert+w$ |
|---|---|---|---|---|---|
| 21 | 84 | $1^2+1^2+1^2+d^2$ | 1, 1, 9 | 32 | 32 |
| 5 | 20 | $1^2+1^2+(-c)^2+(-c)^2$ | 1, -3, -3 | 0 | 12 |
| 13 | 52 | $1^2+1^2+c^2+c^2$ | 1, 5, 5 | 24 | 24 |
| 9 | 36 | $1^2+1^2+c^2+d^2$ | 1, -3, 5 | 12 | 18 |
| 7 | 28 | $1^2+b^2+b^2+b^2$ | 3, 3, 3 | 16 | 16 |
| 19 | 76 | $1^2+(-b^2)+(-b^2)+(-b^2)$ | -5, -5, -5 | 4 | 34 |
| 17 | 68 | $1^2+b^2+b^2+c^2$ | -3, -3, -7 | 4 | 30 |
| 21 | 84 | $1^2+b^2+c^2+d^2$ | -3, 5, -7 | 16 | 36 |
| 39 | 156 | $1^2+b^2+c^2+d^2$ | -5, 7, -9 | 32 | 60 |

**Table 2** Table of Good Matrix Observations

## 5 Some Observations

**Lemma 4.** *Squares of odd numbers are* $\equiv 1 \pmod 4$. *Thus* $b+c+d+w \equiv 0 \pmod 4$.

**Lemma 5.** *The only possible sum of four squares with* $4w = 1^2+(\pm 1)^2+c^2+c^2$ *has* $w \equiv c \equiv 1 \pmod 4$) *(c can be negative).*

*Proof.* We note that $c^2$ is always congruent to $\equiv 1 \pmod 4$.

Consider the case where $4w = 1^2+1^2+2c^2$ with $c \equiv 1 \pmod 4$, and $c = 4t+1$, then

$$4w = 1+1+2(4t+1)^2 = 2+2(16t^2+8t+1) = 2+32t^2+16t+2 = 4+32t^2+16t\,.$$

So $w = 1+8t^2+4t$ and $w \equiv 1 \pmod 4$.

In the case where $4w = 1^2+(-1)^2+2c^2$ with $c \equiv 3 \pmod 4$, and $c = 4t+3$, then

$$\begin{aligned} 4w = 1+1+2(4t+3)^2 &= 2+2(16t^2+24t+9) \\ &= 2+32t^2+48t+18 = 20+32t^2+48t\,. \end{aligned}$$

So $w = 5+8t^2+12t$ and $w \equiv 1 \pmod 4$. Thus $c$ cannot be $\equiv 3 \pmod 4$. □

**Lemma 6.** *If* $4w = a^2+b^2+c^2+d^2$ *(where* $a,b,c,d$ *are all in the same congruence class as* $w \pmod 4$*) then the number of ones in the first rows of* $A+B+C+D$ *(where A,B, C, D are good matrices) are respectively* $= \frac{1+w}{2}, \frac{b+w}{2}, \frac{c+w}{2}, \frac{d+w}{2}$ *and so the total number of ones in the first rows of the four good matrices is* $\frac{a+b+c+d+4w}{2}$.

## 6 Good Matrices and Supplementary Difference Sets

Good matrices and any other set of four $\pm 1$ matrices which satisfy the additive property of equation (2) can be used to form supplementary difference sets (see [18]).

*Example 4.* In our example of Seberry-Williamson array we could have used the first rows `1 1 - , 1 - - , 1 - - , 1 1 1` for the good matrices. These correspond to sets $\{1,2\}, \{1\}, \{1\}, \{1,2,3\}$ which are in fact supplementary difference sets as defined below.

**Definition 1.** A $(v,k,\lambda)$ difference set $(d_1,\cdots,d_k)$ is a subset of $v$ such that all the differences $d_i - d_j,\ i,j \in \{1,\cdots,v-1\}$ occur precisely $\lambda$ times. Note that $\lambda(v-1) = k(k-1)$.

*Example 5.* A (13,4,1) difference set is $\{0,1,3,9\}$ because the differences

| - | 0 | 1 | 3 | 9 |
|---|---|---|---|---|
| 0 | ∗ | 1 | 3 | 9 |
| 1 | 12 | ∗ | 2 | 8 |
| 3 | 10 | 11 | ∗ | 6 |
| 9 | 4 | 5 | 7 | ∗ |

$\{1,\cdots,12\}$ each occur once.

We use Wallis' [28] definition for $n-\{v;k_1,k_2,\cdots k_n;\lambda\}$ supplementary differences sets such that all the differences $d_i-d_j \pmod n, i,j\in\{1,\cdots,k_n\}$ occur precisely $\lambda$ times. Note

$$\lambda(v-1)=\sum_{i=1}^{n}k_i(k_i-1). \tag{12}$$

*Example 6.* $4-\{9;5,5,3,7;11\}$ supplementary difference sets (sds) are $\{1,2,3,5\}$, $\{1,3,4,7,8\}$, $\{1,2,9\}$, $\{1,2,3,5,6,8,9\}$.

| − | 1 | 2 | 3 | 5 |
|---|---|---|---|---|
| 1 | ∗ | 1 | 2 | 4 |
| 2 | 8 | ∗ | 1 | 3 |
| 3 | 7 | 8 | ∗ | 2 |
| 5 | 5 | 6 | 7 | ∗ |

| − | 1 | 3 | 4 | 7 | 8 |
|---|---|---|---|---|---|
| 1 | ∗ | 2 | 3 | 6 | 7 |
| 3 | 7 | ∗ | 1 | 4 | 5 |
| 4 | 6 | 8 | ∗ | 3 | 4 |
| 7 | 3 | 5 | 6 | ∗ | 1 |
| 8 | 2 | 4 | 5 | 8 | ∗ |

| − | 1 | 2 | 9 |
|---|---|---|---|
| 1 | ∗ | 1 | 8 |
| 2 | 8 | ∗ | 7 |
| 9 | 1 | 2 | ∗ |

| − | 1 | 2 | 3 | 5 | 6 | 8 | 9 |
|---|---|---|---|---|---|---|---|
| 1 | ∗ | 1 | 2 | 4 | 5 | 7 | 8 |
| 2 | 8 | ∗ | 1 | 3 | 4 | 6 | 7 |
| 3 | 7 | 8 | ∗ | 2 | 3 | 5 | 6 |
| 5 | 5 | 6 | 7 | ∗ | 1 | 3 | 4 |
| 6 | 4 | 5 | 6 | 8 | ∗ | 2 | 7 |
| 8 | 2 | 3 | 4 | 6 | 7 | ∗ | 1 |
| 9 | 1 | 2 | 3 | 5 | 2 | 8 | ∗ |

We note that (12) becomes

$$11(9-1)=88=20+20+6+42\,.$$

We now give the relationship between the necessary condition for good matrices from (11)

$$4w=a^2(=1^2)+b^2+c^2+d^2$$

and $G=\{w;k,k_2,k_3,k_4;\lambda\}sds$.

**Lemma 7.** *Let w be the order of 4 good matrices. Then, with*

$$4w=a^2+b^2+c^2+d^2$$

*where $a=1$ and $w,\ b,\ c,\ d$ all in the same congruence class modulo 4 the good matrices correspond to*

$$4-\left\{w;\ \frac{a+w}{2},\frac{b+w}{2},\frac{c+w}{2},\frac{d+w}{2};\ w+\frac{a+b+c+d}{2}\right\} \tag{13}$$

*supplementary difference sets.*

*Proof.* We write the positions of 1s in the first rows of the good matrices as subsets of $w$ of size $k_1, k_2, k_3, k_4$ then using $p$ for the number of positive elements and $q$ for the number of negative elements in each sds, $i = 2,\ 3,\ 4$ we have

$$p+q=w \tag{14}$$

and

$$p_2-q_2=b, \quad p_3-q_3=c \quad \text{and} \quad p_4-q_4=d\,. \tag{15}$$

Thus, $2p_2=w+b$, $2p_3=w+c$, $2p_4=w+d$ as $k_2=\frac{1}{2}(w+b),\ k_3=\frac{1}{2}(w+c)$ and $k_4=\frac{1}{2}(w+d)$. Since $a=1$ and the first good matrix is skew-type $k_1=\frac{1}{2}(w+a)$.

Now for sds $4-\{w;\ k_1,\ k_2,\ k_3,\ k_4;\ \lambda\}$ we have

$$\lambda(v-1)=\sum_{i=1}^{n}k_i(k_i-1)$$

and

$$\begin{aligned}\lambda(w-1)=&\left(\frac{a+w}{2}\right)\left(\frac{a+w-2}{2}\right)+\left(\frac{b+w}{2}\right)\left(\frac{b+w-2}{2}\right)\\&+\left(\frac{c+w}{2}\right)\left(\frac{c+w-2}{2}\right)+\left(\frac{d+w}{2}\right)\left(\frac{d+w-2}{2}\right)\end{aligned} \tag{16}$$

$$\begin{aligned}=\frac{1}{4}&\left(a^2+w^2+2aw-2w-2a+b^2+w^2+2bw-2w-2b+c^2+w^2\right)\\&+\left(cbw-2w-2c+d^2+w^2+2dw-2w-2d\right)\end{aligned}$$

$$=\frac{1}{4}\left(a^2+b^2+c^2+d^2-2(w-1)(a+b+c+d)+4w^2-8w\right)$$

$$=\frac{1}{4}(4w^2-4w-2(w-1)(a+b+c+d)$$

$$=w(w-1)+\frac{1}{2}(w-1)(a+b+c+d)$$

and so

$$\lambda=w+\frac{a+b+c+d}{2}. \tag{17}$$

Thus we have the result. □

*Example 7.* For $w=9$, we have seen, above $4-\{9;\ 5,\ 5,\ 3,\ 1;\ 11\}$ sds and $4w=36=a^2(=1^2)+b^2(=1^2)+c^2(=(-3)^2)+d^2(=5^2)$.

We have for $w=9,\ k_1=\frac{1}{2}(9+1),\ k_2=\frac{1}{2}(9+1),\ k_3=\frac{1}{2}(9-3),\ k_1=\frac{1}{2}(9+5)$

and $\lambda = w + \frac{1}{2}(a+b+c+d) = 9 + \frac{1}{2}(1+1-3+5) = 9+2 = 11$. Thus we have $4-\{9;\ 5,\ 5,\ 3,\ 7;11\}$ sds.

*Remark 2.* Lemma 7 actually applies to any four circulant matrices with elements of $\pm 1$ which have row sums $|a|,|b|,|c|,|d|$ which satisfy the additive property given in equation 2.

## 7 Conclusion

We have given for the first time conditions to improve computer searches for good matrices and hence for skew-Hadamard matrices. Further research will be undertaken to implement this on various platforms.

This survey has not been submitted to any other book or journal.

## References

1. L. D. Baumert, Hadamard matrices of orders 116 and 232, *Bull. Amer. Math. Soc.*, 72 (1966), 237.
2. L. D. Baumert and S. W. Golomb and M. Hall, Jr., Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.*, 68 (1962), 237–238.
3. L. D. Baumert and M. Hall, Jr., Hadamard matrices of Williamson type, *Math. Comp.*, 19 (1965), 442–447.
4. L. D. Baumert and M. Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.*, 71 (1965), 169–170.
5. Dragomir Z. Djoković, Construction of some new Hadamard matrices, *Bulletin of the Australian Mathematical Society*, 45, 2, (1992), 327–332.
6. D. Z. Djoković, Ten new orders for Hadamard matrices of skew type, *Elektrotehnickog Fak*, Ser. Matematika, 3, (1992), 47-59,
7. D. Z. Djoković, Good matrices of order 33, 35 and 127 exist, *J. Combin. Math. Combin. Comput*, 14 (1993), 145-152.
8. D. Z. Djoković, Williamson matrices of order 4n for 33, 35 and 127, *Discrete Mathematics*, 115 (1993), 267-271.
9. D. Z. Djoković, Five new orders for Hadamard matrices of skew type, *Australasian J. Comb.*, 10, (1994), 259-264.
10. Dragomir Z. Djoković, Supplementary difference sets with symmetry for Hadamard matrices, (English summary) *Oper. and Matrices*, 3, 2009, no. 4, 557-569.
11. Dragomir Z. Djoković, Regarding good matrices of order 41, Email communication to author, 23rd July 2014.
12. S. Georgiou, C. Koukouvinos and S. Stylianou, On good matrices, skew Hadamard matrices and optimal designs, *Computational Statistics and Data Analysis*, 41, 1, (2002), 171-184. ISSN 0167-9473,
13. J. Hadamard, Resolution d'une question relative aux determinants, *Bull. des Sciences Mathematiques*, 17 (1893), 240–246.
14. M. Hall, Jr., *Combinatorial Theory*, 2nd ed., John Wiley and Sons, New York, 1986.
15. W. H.(Holzmann, H. Kharaghani, B. Tayfeh-Rezaie, Williamson matrices up to order 59. *Des. Codes Cryptogr.* 46 (2008), no. 3, 343352.

16. Wolf H. Holzmann, Hadi Kharaghani and Behruz Tayfeh-Rezaie, Williamson matrices up to order 59, *Designs, Codes and Cryptography*, 46, 3, (2008), 343–352.
17. D. C. Hunt, Skew-Hadamard matrices of order less than 100, *Combinatorial Mathematics: Proceedings of the First Australian Conference*, eds J. Wallis and W. D. Wallis, TUNRA, Newcastle, NSW, (1971), 55–59.
18. David C. Hunt and Jennifer Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Congr. Numer.*, 7, (1972), 351–382.
19. R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.,* 12 (1933), 311-320.
20. V. Scarpis, Sui determinanti di valoremassimo, *Rend.R. Inst. Lombardo Sci. e Lett.*, 31, 2, (1898), 1441-1446.
21. Bernhard Schmidt, Review MR2372843 (2008i:05025) of W. H. Holzmann, H. Kharaghani, B. Tayfeh-Rezaie, [15]. `http://www.ams.org/mathscinet/search/publdoc.html?b=2372843&batch_title=Selected%%20Matches%20for:%20Title=(Williamson).`
22. Jennifer Seberry, Good matrices online resource, `http://www.uow.edu.au/~jennie/good.html`, 1999.
23. Jennifer Seberry and Mieko Yamada, 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., 431-560, 1992.
24. J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and *Phil. Mag.*, (4) 34, (1867) 461–475.
25. G. Szekeres, A note on skew type orthogonal $\pm 1$ matrices, *Coll. Math. Soc. Janos Bolyai*, eds. A.Hajnal, L. Lovasz, and V. T. Sos, 52, (1987), 489–498. Presented at the Combinatorics Conference, Eger (Hungary).
26. Jennifer Seberry Wallis, Hadamard matrices, in W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-Free Sets and Hadamard Matrices,* Lecture Notes in Mathematics, Springer Verlag, Berlin, 1972.
27. Jennifer (Seberry) Wallis, *Combinatorial Matrices,* PhD Thesis, La Trobe University, Melbourne, 1971.
28. Jennifer (Seberry) Wallis, Some remarks on supplementary sets. Infinite and Finite Sets, *Colloquia Mathematica Societatis Janos Bolyai*, 10 (1973), 1503-1506.
29. Jennifer (Seberry) Wallis, Williamson matrices of even order, Combinatorial Mathematics: Proceedings of the Second Australian Conference, (D.A. Holton, (Ed.)), Lecture Notes in Mathematics, 403, SpringerVerlag, BerlinHeidelbergNew York, (1974), 132-142.
30. Jennifer (Seberry) Wallis, A skew-Hadamard matrix of order 92, *Bull. Austral. Math. Soc.,* 5, (1971), 203-204.
31. Jennifer Wallis, Construction of Williamson type matrices, *J. Linear and Multilinear Algebra*, 3, (1975), 197-207.
32. Jennifer Wallis and A. L. Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.*, 7, (1972), 233–249.
33. J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, 11, (1944), 65–81.