There are no circulant symmetric Williamson matrices of order 39

Christos Koukouvinos
Department of Mathematics
University of Thessaloniki
Greece, 54006

and

Stratis Kounias
Department of Mathematics
University of Athens
Greece, 15784

Abstract. It is shown, through an exhaustive search, that there are no circulant symmetric Williamson matrices of order 39. The construction of symmetric but not circulant Williamson-type matrices of order 39, first given by Miyamoto, Seberry and Yamada, is given explicitly.

1. Introduction

An Hadamard matrix is a square matrix of ones and minus ones whose row (and hence column) vectors are orthogonal. The order n of an Hadamard matrix is necessarily $1, 2$ or $4m$, with m a positive integer. For more details of their construction see [8],[9],[10],[17], [20]. Since we can easily construct an Hadamard matrix of order $2n$, from one of order n, the interest lies in the case $n = 4m$ where m is odd.

In particular if an $OD(4t; t, t, t, t)$ (otherwise called Baumert-Hall array of order t) and Williamson-type matrices of order m are known, then there exists an Hadamard matrix of order $4mt$. Note that $OD(4t; t, t, t, t)$ are known for many values of t, see [1],[5],[6],[7]; [8, p. 145];[12],[13],[17],[18] and [20, p. 360]. Hence the potential number of solutions of order $4mt$ is increased by increasing the number of solutions of order n and/or t.

We give now two basic definitions:

(I) Williamson matrices of order m are four $(+1, -1)$ circulant symmetric matrices, A, B, C, D which satisfy

$$A^2 + B^2 + C^2 + D^2 = 4mI_m \tag{1}$$

(II) Williamson-type matrices of order m are four $(+1, -1)$ matrices A, B, C, D which satisfy

(i) $MN^T = NM^T$, $M, N \in \{A, B, C, D\}$

(ii) $AA^T + BB^T + CC^T + DD^T = 4mI_m$.

Williamson and Williamson-type matrices have been constructed for many values of m, see [1],[2],[3],[4],[11],[13], [14],[15],[16],[18],[19],[20, pp. 388–389], [21],[22],[23]. Originally Williamson [22] considered circulant and symmetric A, B, C, D and constructed them for $m \leq 21, m = 25, 37, 43$. Baumert, Golomb and Hall [3] constructed Williamson matrices for $m = 23$, Baumert and Hall [4] gave all solutions for $3 \leq m \leq 23$ and some solutions for $m = 25, 27, 37, 43$ and Baumert [2] gave one solution for $m = 29$. Sawade [14] did an exhaustive search for $m = 25, 27$. Yamada [23] considered a restricted class of Williamson matrices and gave a new one for $m = 37$.

The exhaustive search for Williamson matrices for $m \geq 29$, however, turns out to be much more difficult because of the formidable computational time.

Koukouvinos and Kounias [11] developed a method, and described an algorithm, for constructing Williamson matrices of order m, suitable for the case where m is not a prime. With this algorithm the computational time is reduced considerably. When m is odd, $m = p \cdot q$ with $p, q > 1$ this algorithm is implemented by first finding all solutions $\pmod{p}$, then $\pmod{q}$ and then merging them. This gives a considerable reduction in computer time. Koukouvinos and Kounias [11], applying their algorithm, found all solutions for $m = 33$.

In this paper we show, through an exhaustive search, that there are no circulant symmetric Williamson matrices (definition I) of order 39. We also give (explicitly) the construction of symmetric but not circulant Williamson-type matrices (definition II) of order 39 which has been proved previously by Seberry and Yamada [18].

The non-existence of circulant symmetric Williamson matrices of order 39

For $m = 39 = p \cdot q = 3 \cdot 13$ with $p, q > 1$ we apply the algorithm which is described by Koukouvinos and Kounias [11]. First we find all solutions $\pmod{13}$ and then merge them.

We observe that if we have a quadruple of Williamson matrices of order m, $A = (a_0, a_1, \cdots, a_{m-1})$, $B = (b_0, b_1, \cdots, b_{m-1})$, $C = (c_0, c_1, \cdots, c_{m-1})$, $D = (d_0, d_1, \cdots, d_{m-1})$, then applying the transformation $j \to j \cdot s \pmod{m}$, $(s, m) = 1$, we obtain another quadruple of Williamson matrices. These quadruples are called equivalent and we need to know only one quadruple from each equivalence class.

In each equivalence class there are at most $\phi(m)/2$ such quadruples where $\phi(m)$ is the number of integers $s : (s, m) = 1, 0 < s < m$. This is because some quadruples may be transformed into themselves and the transformations $j \to j \cdot s$ $\pmod{m}$ and $j \to j(m - s) \pmod{m}$ are identical due to the symmetry of A, B, C, D.

There are four different representations of $156 = 4 \cdot 39$ as the sum of four odd squares, i. e.,

(i) $156 = 11^2 + 5^2 + 3^2 + 1^2$,
(ii) $156 = 9^2 + 7^2 + 5^2 + 1^2$,
(iii) $156 = 9^2 + 5^2 + 5^2 + 5^2$,
(iv) $156 = 7^2 + 7^2 + 7^2 + 3^2$.

With the application of our algorithm we found that there are no circulant symmetric Williamson matrices of order 39. It is known that if the Williamson equation is satisfied on the commutative (cyclic) group, then it is satisfied on a subgroup. this is essentially described in Theorem 1 (see [11] for the proof), but in a context suitable for our purposes. In Theorem 2 (see [11] for the proof), we describe a result similar to Williamson's which is useful for our algorithm.

Let $G_q^T = (I_p, I_p, \cdots, I_p)$ be a $p \times p \cdot q$ matrix, i. e. the unit matrix I_p of order p is repeated q times.

Theorem 1 (see[11]). *If (i) $m = p \cdot q \quad p, q > 1$, (ii) $V = (v_0, v_1, \cdots, v_{m-1})$ is a circulant matrix of order m, then*

(i) *$G_q^T \cdot V = U \cdot G_q^T$, where $U = (u_0, u_1, \cdots, u_{p-1})$ is circulant matrix of order p with*

$$u_j = \sum_{\substack{i \equiv j \pmod p \\ i < m}} v_i, \quad j = 0, 1, \cdots, p-1$$

(ii) *U is symmetric if V is symmetric.*

Now multiplying on the left A, B, C, D by G_q^T we obtain:

$$G_q^T A = X_p G_q^T, \quad G_q^T B = Y_p G_q^T, \quad G_q^T C = Z_p G_q^T, \quad G_q^T D = W_p G_q^T,$$

where

$$\begin{aligned} X_p &= (x_0, x_1, \cdots, x_{p-1}), \quad \text{with } x_j = \sum_i a_i \\ Y_p &= (y_0, y_1, \cdots, y_{p-1}), \quad \text{with } y_j = \sum_i b_i \\ Z_p &= (z_0, z_1, \cdots, z_{p-1}), \quad \text{with } z_j = \sum_i c_i \\ W_p &= (w_0, w_1, \cdots, w_{p-1}), \quad \text{with } w_j = \sum_i d_i \end{aligned} \tag{2}$$

and the summations are over all $i \equiv j \pmod p$, $i < m$. If we multiply both members of (1), on the left by G_q^T and on the right by G_q we obtain in the symmetric case:

$$X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4mI_p. \tag{3}$$

Of course we do not know A, B, C, D so we do not know X_p, Y_p, Z_p, W_p. However it is easier to find X_p, Y_p, Z_p, W_p satisfying (3) than A, B, C, D because p is much smaller than m. Now to construct X_p, Y_p, Z_p, W_p note that:

Theorem 2 (see [11]). *If (i) A, B, C, D are circulant and symmetric $(+1, -1)$-matrices satisfying (1) with row (and hence column) sums a, b, c, d, (ii) X_p, Y_p, Z_p, W_p are as defined in (2), then*

(i)

$$\sum_{j=0}^{p-1} x_j = a, \quad \sum_{j=0}^{p-1} y_j = b, \quad \sum_{j=0}^{p-1} z_j = c, \quad \sum_{j=0}^{p-1} w_j = d, \tag{4}$$

$$a^2 + b^2 + c^2 + d^2 = 4m, \quad -q \le x_j, y_j, z_j, w_j \le q, \quad x_j, y_j, z_j, w_j, \textit{ odd},$$

$$x_j = x_{p-j}, \; y_j = y_{p-j}, \; z_j = z_{p-j}, \; w_j = w_{p-j}, \; j = 1, 2, \cdots, (p-1)/2,$$

(ii) *If moreover* $a_0 + b_0 + c_0 + d_0 = 0, \pm 4$, *then*

$$\begin{aligned}(x_0 + y_0 + z_0 + w_0) - (a_0 + b_0 + c_0 + d_0) &\equiv 0 \pmod 8), \textit{if } q \equiv 1 \pmod 4), \\ &\equiv 4 \pmod 8), \textit{if } q \equiv 3 \pmod 4),\end{aligned} \tag{5}$$

$$x_j + y_j + z_j + w_j \equiv 2 \pmod 4), \quad j = 1, 2, \cdots, (p-1)/2.$$

Corollary 1 (see [11]). *If in Theorem 2 we have (ii)' $a_0 + b_0 + c_0 + d_0 = \pm 2$ instead of (ii), then*

$$(x_o + y_0 + z_0 + w_0) - (a_0 + b_0 + c_0 + d_0) \equiv 0 \pmod 8),$$

$$x_j + y_j + z_j + w_j \equiv 0 \pmod 4), \quad j = 1, 2, \cdots, (p-1)/2.$$

Now for a given decomposition $a^2 + b^2 + c^2 + d^2 = 4m$, we can take a, b, c, d to be positive and so a_0, b_0, c_0, d_0 are uniquely determined.

In our algorithm we first find all sequences $X_p = (x_0, x_1, \cdots, x_{p-1})$ such that

$$-q \le x_j \le q, \quad j = 0, 1, 2, \cdots, p-1$$

$$x_j = x_{p-j}, \quad x_j \textit{ is odd}, \quad j = 1, 2, \cdots, (p-1)/2$$

$$\sum_{j=0}^{p-1} x_j = a.$$

Similarly we construct all sequences, $Y_p = (y_0, y_1, \cdots, y_{p-1})$, $Z_p = (z_0, z_1, \cdots, z_{p-1})$, $W_p = (w_0, w_1, \cdots, w_{p-1})$.

Now we examine which quadruples X_p, Y_p, Z_p, W_p satisfy also (3). However it is computationally faster to examine first if for a given quadruple X_p, Y_p, Z_p, W_p the relations in Theorem 2 (ii) hold when

$$a_0 + b_0 + c_0 + d_0 = 0, \pm 4$$

(or of Corollary 1 when $a_0 + b_0 + c_0 + d_0 = \pm 2$). These quadruples are then examined to ascertain whether they satisfy (3). We repeat this procedure interchanging p and q. Another serious reduction of the computational time is achieved if we consider only non-equivalent quadruples, i. e. if we apply the transformation $j \rightarrow j \cdot s \pmod{m}$, where $(s,m) = 1$, then $a_j \rightarrow a_j \cdot s$, $b_j \rightarrow b_j \cdot s$, $c_j \rightarrow c_j \cdot s$, $d_j \rightarrow d_j \cdot s$, $j = 0,1,2,\cdots,m-1$ and the transformed A, B, C, D remain circulant and symmetric.

Note that j and $m-j$ give identical quadruples because of the symmetry of A, B, C, D.

We need only to know one quadruple in every equivalence class. For $m = 39$ there are at most 12 equivalent quadruples in each equivalence class ($s = 1,2,4,5,7,8,10,11,14,16,17,19$).

Now the transformation $j \rightarrow j \cdot s \pmod{m}, (s,m) = 1$ because of (2) transforms equivalence classes of A, B, C, D into equivalence classes of X_p, Y_p, Z_p, W_p and X_q, Y_q, Z_q, W_q with corresponding transformations

$$\begin{aligned} &j \rightarrow j \cdot s \pmod{p}, \quad (s,m) = 1, \quad s < p \quad \text{and} \\ &j \rightarrow j \cdot s \pmod{q}, \quad (s,m) = 1, \quad s < q. \end{aligned}$$

(From $j \rightarrow j \cdot s \pmod{p}$ and $j \rightarrow j(p-s) \pmod{p}$ apply only one, because they give identical transformations due to the symmetry of X_p, Y_p, Z_p, W_p, similarly for $j \rightarrow j \cdot s \pmod{q}$ and $j \rightarrow j(q-s) \pmod{q}$.)

Knowing (X_p, Y_p, Z_p, W_p) and (X_q, Y_q, Z_q, W_q) we can find their equivalence classes.

Care is needed here because for a given representative of a class A, B, C, D we do not know which is the pair of representatives from the corresponding classes of X_p, Y_p, Z_p, W_p and X_q, Y_q, Z_q, W_q.

However, if we consider one representative from each class of X_q, Y_q, Z_q, W_q $(q > p)$ and combine it with all solutions (equivalent or not) of X_p, Y_p, Z_p, W_p, then all non-equivalent A, B, C, D will be found.

The Algorithm

For a given decomposition $4m = a^2 + b^2 + c^2 + d^2$, with $m = p \cdot q, p < q$, our algorithm consists of four stages:

I)

(1) Form all sequences $X_p = (x_0, x_1, \cdots, x_{p-1})$ satisfying

(i) $\sum_{i=0}^{p-1} x_i = a$,

(ii) $-q \leq x_i \leq q$,

(iii) x_i odd,

(iv) $x_i = x_{p-i}, \quad i = 1,2,\cdots,(p-1)/2.$

(2) Repeat the consruction for Y_p, Z_p, W_p replacing a with b, c, d, respectively.

(3) Examine which quadruples X_p, Y_p, Z_p, W_p satisfy

$$X_p^2 + Y_p^2 + Z_p^2 + W_p^2 = 4\,mI_p.$$

II)

(1) Repeat stage I interchanging p and q.

(2) Find all non-equivalent solutions by applying the transformation $j \to j \cdot s \pmod{q}$ to each solution X_q, Y_q, Z_q, W_q, where $(s, m) = 1$ for every $s < q$. (From $j \to j \cdot s \pmod{q}$ and $j \to j(q-s) \pmod{q}$ apply only one).

III)

(1) If there are h_1 solutions X_p, Y_p, Z_p, W_p and h_2 non-equivalent solutions $\widehat{X}_q, \widehat{Y}_q, \widehat{Z}_q, \widehat{W}_q$, form the $h_1 \cdot h_2$ combined solutions $X_p, Y_p, Z_p, W_p, \widehat{X}_q, \widehat{Y}_q, \widehat{Z}_q, \widehat{W}_q$.

(2) Find $A = (a_0, a_1, \cdots, a_{m-1})$ from:

$$a_i = a_{m-i}, \quad i = 1, 2, \cdots (m-1)/2,$$

$$\sum_{\substack{i \equiv j \pmod{p} \\ i<m}} a_i = x_j, \quad j = 0, 1, 2, \cdots, (p-1)/2,$$

$$\sum_{\substack{i \equiv j \pmod{q} \\ i<m}} a_i = \widehat{x}_j, \quad j = 0, 1, 2, \cdots, (q-1)/2$$

where $X_p = (x_0, x_1, \cdots, x_{p-1}), \widehat{X}_q = (\widehat{x}_0, \widehat{x}_1, \cdots, \widehat{x}_{q-1})$.

(3) Find B, C, D similarly.

IV) Examine which quadruples A, B, C, D satisfy $A^2 + B^2 + C^2 + D^2 = 4\,mI_m$. Now repeat stages I, II, III, IV for every decomposition of $4\,m$ as the sum of four odd squares.

For $m = 39, p = 3, q = 13$ we use $s = 2, 4, 5, 7, 10$ to find all non-equivalent solutions $\widehat{X}_q, \widehat{Y}_q, \widehat{Z}_q, \widehat{W}_q$. With the application of our algorithm for $m = 39$ we have:

(i) For $156 = 11^2 + 5^2 + 3^2 + 1^2$ we found 14 solutions for $p = 3$ and 676 non-equivalent solutions for $q = 13$. So we examined $14 \cdot 676 = 9464$ pairs of solutions which gave no solution for A, B, C, D.

(ii) For $156 = 9^2 + 7^2 + 5^2 + 1^2$ we found 14 solutions for $p = 3$ and 615 non-equivalent solutions for $q = 13$. So we examined $14 \cdot 615 = 8610$ pairs of solutions which gave no solution for A, B, C, D.

(iii) For $156 = 9^2 + 5^2 + 5^2 + 5^2$ we found 14 solutions for $p = 3$ and 149 non-equivalent solutions for $q = 13$. So we examined $14 \cdot 149 = 2086$ pairs of solutions which gave no solution for A, B, C, D.

(iv) For $156 = 7^2 + 7^2 + 7^2 + 3^2$ we found 14 solutions for $p = 3$ and 202 non-equivalent solutions for $q = 13$. So we examined $14 \cdot 202 = 2828$ pairs of solutions which gave no solution for A, B, C, D.

So we obtain the required result that there are no circulant symmetric Williamson matrices of order 39.

Remark: The detailed calculations can be obtained from the first author if required but have been omitted from the paper in order to be concise.

3. Construction of symmetric but not circulant Williamson-type matrices of order 39

We use a result of Miyamoto [13], reformulated by Seberry and Yamada [18, Lemma 25, Corollary 26]. Since $37 \equiv 1 \pmod 4$, we use B, the skew-symmetric core of order $\frac{(37+1)}{2} = 19$, formed via the quadratic residues:

$$B = (0 + - - + + + + - + - + - - - - + + -).$$

If R is the back-diagonal matrix, i. e.

$$R = \begin{bmatrix} 0 & 0 & . & . & . & 0 & 1 \\ 0 & 0 & . & . & . & 1 & 0 \\ . & . & . & . & . & . & . \\ 1 & 0 & . & . & . & 0 & 0 \end{bmatrix}$$

then the matrix BR is back-circulant and symmetric.

Let

$$M = (0 - - + + + + - + + + + - + + + + - -)$$
$$N = (- + - + + + - - + - - + - - + + + - +)$$

be the two circulant symmetric matrices of order $(37 + 1)/2 = 19$, satisfying

$$MM^T + NN^T = 37 I_{19}.$$

The four $(+1, -1)$ matrices

$$X_1 = \begin{bmatrix} 1 & -e_{38} \\ -e_{38}^T & S_1 \end{bmatrix}, \quad X_i = \begin{bmatrix} 1 & e_{38} \\ e_{38}^T & S_i \end{bmatrix}, \; i = 2, 3, 4$$

are of the Williamson-type of order 39, where

$$S_1 = \begin{bmatrix} I + M & I - M \\ I - M & I + M \end{bmatrix} \quad \text{with row sum 2,}$$

$$S_2 = \begin{bmatrix} N & -N \\ -N & N \end{bmatrix},$$

$$S_3 = S_4 = \begin{bmatrix} BR + R & BR - R \\ BR - R & BR + R \end{bmatrix} \quad \text{with row sum 0.}$$

It is easy to see (Seberry and Yamada [18]) that

$$\begin{aligned}\sum_{i=1}^{4} X_i X_i^T &= \begin{bmatrix} 39 & -3\,e_{38} \\ -3\,e_{38}^T & J + S_1 S_1^T \end{bmatrix} + \sum_{i=2}^{4} \begin{bmatrix} 39 & e_{38} \\ e_{38}^T & J + S_i S_i^T \end{bmatrix} \\ &= \begin{bmatrix} 4 \cdot 39 & 0 \\ 0 & 4\,J + 4 \cdot 39\,I - 4\,J \end{bmatrix} \\ &= 4 \cdot 39\,I_{39}.\end{aligned}$$

These Williamson-type matrices are symmetric but not circulant.

References

1. S. S. Agayan and A. G. Sarukhanyan, *Recurrence formulas for the construction of Williamson-type matrices*, Math. Notes **30** (1982), 796–804.
2. L. D. Baumert, *Hadamard matrices of orders 116 and 232*, Bull. Amer. Math. Soc. **72** (1966), 237.
3. L. D. Baumert, S. W. Golomb and M. Hall Jr., *Discovery of an Hadamard matrix of order 92*, Bull. Amer. Math. Soc. **68** (1962), 237–238.
4. L. D. Baumert and M. Hall Jr., *Hadamard matrices of the Williamson type*, Math. Comp. **19** (1965), 442–447.
5. L. D. Baumert and M. Hall Jr., *A new construction for Hadamard matrices*, Bull. Amer. Math. Soc. **71** (1965), 169–170.
6. J. Cooper and J. Wallis, *A construction for Hadamard arrays*, Bull. Austral. Math. Soc. **7** (1972), 269–278.
7. G. Cohen, D. Rubie, J. Seberry, K. Koukouvinos, S. Kounias and M. Yamada, *A survey of base sequences, disjoint complementary sequences and* $OD(4t; t, t, t, t)$, J. Comb. Math. Comb. Comp. (to appear).
8. A. V. Geramita and J. Seberry, "Orthogonal designs: Quadratic forms and Hadamard matrices", Marcel Dekker, New York-Basel, 1979.
9. M. Hall Jr., "Combinatorial Theory, 2nd Edition", Wiley and Sons, New York, 1986.
10. A. Hedayat and W. D. Wallis, *Hadamard matrices and their applications*, Ann. Statist. **6(6)** (1978), 1184–1238.
11. C. Koukouvinos and S. Kounias, *Hadamard matrices of the Williamson type of order* $4\,m$, $m = pq$. *An exhaustive search for* $m = 33$., Discrete Math. **68** (1988), 45–57.
12. C. Koukouvinos, S. Kounias and J. Seberry, *Further results on base sequences, disjoint complementary sequences,* $OD(4t; t, t, t, t)$ *and the excess of Hadamard matrices*, Ars Combinatoria (to appear).
13. M. Miyamoto, *A construction for Hadamard matrices*, J. Comb. Theory Ser. A (to appear).

14. K. Sawade, *Hadamard matrices of order 100 and 108*, Bull. Nagoya Inst. Technol. **29** (1977), 147–153.

15. J. Seberry, *A new construction for Williamson-type matrices*, Graphs and Combinatorics **2** (1986), 81–87.

16. J. Seberry Wallis, *Construction of Williamson type matrices*, Linear and Multilinear Algebra **3** (1975), 197–207.

17. J. Seberry Wallis, *On Hadamard matrices*, J. Comb. Theory Ser. A **18** (1975), 149–164.

18. J. Seberry and M. Yamada, *On the products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures.* (to appear).

19. R. J. Turyn, *An infinite class of Williamson matrices*, J. Comb. Theory Ser. A **12** (1972), 319–321.

20. W. D. Wallis, A.P. Street and J. Seberry Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard matrices Lecture notes*, in "Math. Vol. 292", Springer-Verlag, Berlin-Heidelberg-New York, 1972.

21. A. L. Whiteman, *An infinite family of Hadamard matrices of Williamson type*, J. Comb. Theory Ser. A **14** (1973), 334–340.

22. J. Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J. **11** (1944), 65–81.

23. M. Yamada, *On the Williamson type j matrices of orders* $4 \cdot 29, 4 \cdot 41$, *and* $4 \cdot 37$, J. Comb. Theory Ser. A **27** (1979), 378–381.