Semi Williamson Type Matrices and the $W(2n, n)$ Conjecture

Jennifer Seberry
and
Xian-Mo Zhang

Department of Computer Science
University College
University of New South Wales
Australian Defence Force Academy
Canberra, ACT 2600, AUSTRALIA

Abstract

Four (1, -1, 0)-matrices of order m, $X = (x_{ij})$, $Y = (y_{ij})$, $Z = (z_{ij})$, $U = (u_{ij})$ satisfying

(i) $XX^T + YY^T + ZZ^T + UU^T = 2mI_m$,

(ii) $x_{ij}^2 + y_{ij}^2 + z_{ij}^2 + u_{ij}^2 = 2$, $i, j = 1, \ldots, m$,

(iii) X, Y, Z, U mutually amicable,

will be called semi Williamson type matrices of order m. In this paper we prove that if there exist Williamson type matrices of order $n_1, \ldots, n_k$ then there exist semi Williamson type matrices of order $N = \prod_{j=1}^{k} n_j^{r_j}$, where r_j are non-negative integers. As an application, we obtain a $W(4N, 2N)$. Although the paper presents no new $W(4n, 2n)$ for n, odd, $n < 3000$, it is a step towards proving the conjecture that there exists a $W(4n, 2n)$ for any positive integer n. This conjecture is a sub-conjecture of the Seberry conjecture [3, page 92] that $W(4n, k)$ exist for all $k = 0, 1, \ldots, 4n$. In addition we find infinitely many new $W(2n, n)$, n odd and the sum of two squares.

1 Introduction and Basic Definitions

Definition 1 Let A, B, C, D be four (1, -1)-matrices of order n. If $AA^T + BB^T + CC^T + DD^T = 4nI_n$ and $UV^T = VU^T$ (U and V are amicable), where $U, V \in \{A, B, C, D\}$. We call A, B, C, D *Williamson type matrices* of order n.

Definition 2 Let W be a (1, -1, 0)-matrix of order of order n satisfying $WW^T = cI_n$. We call W a *weighing matrix* of order n with weight c, denoted by $W(n, c)$.

Definition 3 Four (1, -1, 0)-matrices of order m, $X = (x_{ij})$, $Y = (y_{ij})$, $Z = (z_{ij})$, $U = (u_{ij})$ satisfying

(i) $XX^T + YY^T + ZZ^T + UU^T = 2mI_m$,

(ii) $x_{ij}^2 + y_{ij}^2 + z_{ij}^2 + u_{ij}^2 = 2$, $i, j = 1, \ldots, m$,

(iii) X, Y, Z, U mutually amicable,

will be called *semi Williamson type matrices* of order m. In particular, if X, Y, Z, U are circulant and symmetric we call X, Y, Z, U *semi Williamson matrices* of order m.

Let $M = (M_{ij})$ and $N = (N_{gh})$ be orthogonal matrices with t^2 block M-structure (see [4]) of order tm and tn respectively, where M_{ij} is of order m $(i, j = 1, \ldots, t)$ and N_{gh} is of order n $(g, h = 1, 2, \ldots, t)$. We now define the operation $\bigcirc$ as the following:

$$M \bigcirc N = \begin{bmatrix} L_{11} & L_{12} & \cdots & L_{1t} \\ L_{21} & L_{22} & \cdots & L_{2t} \\ & & \cdots & \\ L_{t1} & L_{t2} & \cdots & L_{tt} \end{bmatrix}$$

where M_{ij}, N_{ij} and L_{ij} are of order of m, n and mn, respectively and

$$L_{ij} = M_{i1} \times N_{1j} + M_{i2} \times N_{2j} + \cdots + M_{it} \times N_{tj},$$

where $\times$ is Kronecker product, $i, j = 1, 2, \ldots, t$. We call this the *strong Kronecker* multiplication of two matrices (see [**?**]).

Lemma 1 *Let $A = [A_1, A_2, A_3, A_4]$ be a (1, -1, 0)-matrix of order $m \times 4m$, where A_j is of order m, satisfying $\sum_{j=1}^{4} A_j A_j^T = pI_m$ and $B^T = [B_1^T, B_2^T, B_3^T, B_4^T]$, where B_i is of order $n \times 4n$, be a $W(4n, q)$. Set $C = \sum_{j=1}^{4} A_j \times B_j$. Then $CC^T = pqI_{mn}$.*

Proof. $CC^T = (\sum_{j=1}^{4} A_j \times B_j)(\sum_{j=1}^{4} A_j^T \times B_j^T) = \sum_{j=1}^{4} A_j A_j^T \times B_j B_j^T = (\sum_{j=1}^{4} A_j A_j^T) \times qI_n = pI_m \times qI_n = pqI_{mn}$.

Notation 1 Write $OD(A, B, C, D) = \begin{bmatrix} A & B & C & D \\ D & C & -B & -A \\ B & -A & D & -C \\ C & -D & -A & B \end{bmatrix}$.

□

2 Preliminaries

Lemma 2 *Let $a, b, c, d \in \{1, -1, 0\}$, $a^2 + b^2 + c^2 + d^2 = 2$ and $k, m, l, q \in \{1, -1\}$. Set $[x, y, z, u] = \frac{1}{2}[a, b, c, d]OD(k, m, l, q)$. Then $x, y, z, u \in \{1, -1, 0\}$, $x^2 + y^2 + z^2 + u^2 = 2$.*

Proof. By Lemma 1, $x^2 + y^2 + z^2 + z^2 = \frac{1}{4} \cdot 2 \cdot 4 = 2$. Each of x, y, z, u is half the sum of four numbers, two of which are zero, and the other two of which are units. It follows that x, y, z, $u \in \{1, -1, 0\}$.
We note that the operation of Lemma 2 is norm preserving.

Lemma 3 *If there exist Williamson type matrices of order m then there exist semi Williamson type matrices of order m.*

Proof. Let A, B, C, D be the Williamson type matrices of order m then $\frac{1}{2}(A+B)$, $\frac{1}{2}(A-B)$, $\frac{1}{2}(C+D)$, $\frac{1}{2}(C-D)$ are semi Williamson type matrices. □

Lemma 4 *If there exist semi Williamson type matrices of order m and Williamson type matrices of order n then there exist semi Williamson type matrices of order mn.*

Proof. Let $X=(x_{ij})$, $Y=(y_{ij})$, $Z=(z_{ij})$, $U=(u_{ij})$ be the semi Williamson type matrices of order m and $K=(k_{st})$, $L=(l_{st})$, $M=(m_{st})$, $Q=(q_{st})$ be the Williamson type matrices of order n. We now construct four matrices, say $R=(r_{\mu\nu})$, $S=(s_{\mu\nu})$, $V=(v_{\mu\nu})$, $W=(w_{\mu\nu})$, $i,j=1,\ldots,mn$, of order mn, where

$$[r_{\mu\nu}, s_{\mu\nu}, v_{\mu\nu}, w_{\mu\nu}] = \frac{1}{2}[x_{ij}, y_{ij}, z_{ij}, u_{ij}]OD(k_{st}, m_{st}, q_{st}, l_{st}).$$

By Lemma 2, $r_{\mu\nu}, s_{\mu\nu}, v_{\mu\nu}, w_{\mu\nu} \in \{1,-1,0\}$ and $r_{\mu\nu}^2 + s_{\mu\nu}^2 + v_{\mu\nu}^2 + w_{\mu\nu}^2 = 2$, $\mu,\nu = 1,\ldots,mn$. By Lemma 1, $RR^T + SS^T + VV^T + WW^T = \frac{1}{4}8mnI_{mn} = 2mnI_{mn}$. Since X,Y,Z,U are mutually amicable and K,L,M,Q are mutually amicable, R,S,V,W are also mutually amicable. □

3 Main Results

Throughout this section we write $N = \prod_{j=1}^{k} n_j^{r_j}$, where r_j are non-regative integers.

Theorem 1 *If there exist Williamson type matrices of order $n_1,\ldots,n_k$ then there exist semi Williamson type matrices of order N.*

Proof. By Lemma 3, there exist semi Williamson type matrices of order n_1. By Lemma 4, there exist semi Williamson type matrices of order $n_1 n_2$. Using Lemma 4 repeatedly, we prove the Theorem. □

Corollary 1 *If there exist Williamson type matrices of order $n_1,\ldots,n_k$ then there exists a $W(4N,2N)$.*

Proof. By Theorem 1, there exist semi Williamson type matrices of order N, say E,F,G,H. Then $A = OD(E,F,G,F)$ is a $W(4N,2N)$. □

Corollary 2 *If there exist Williamson type matrices of order $n_1,\ldots,n_k$ and an Hadamard matrix of order $4h$ then there exists a $W(4Nh,2Nh)$.*

Proof. By Theorem 1, there exist semi Williamson type matrices of order N, say P,Q,R,S. Write $H=(H_{ij})$, $i,j=1,2,3,4$ for the Hadamard matrix of order $4h$, where H_{ij} is of order h. Set

$$B = \frac{1}{2}OD(P,Q,R,S) \bigcirc (H_{ij}).$$

From (ii) of Definition 3, B is a $(1,-1,0)$-matrix of order $4Nh$. By Theorem 1, [?],

$$BB^T = 2NhI_{4Nh}.$$

Hence B is the required $W(4Nh, 2Nh)$. □

4 Numerical Results

To construct $W(4n, 2n)$ we can use the known result that if there exist Hadamard matrices of order $4h_1$ and $4h_2$ then there exist two amicable and disjoint $W(4h_1h_2, 2h_1h_2)$ (see [?], [?]). Thus we obtain many $W(4n, 2n)$ whenever $n = h_1h_2$, where $4h_1$ and $4h_2$ are the order of Hadamard matrices. In particular, let $h_2 = 1$, we give the simple result that $W(4h, 2h)$ exists whenever an Hadamard matrix of order $4h$ exists (see [?], [?]). However Corollary 1 is new result. To show the advantages of Corollary 1 and Corollary 2, we now give new $W(4n, 2n)$. Let $a = 71 \cdot 79 \cdot 97$, $b = 71 \cdot 79$, $c = 71 \cdot 97$, $d = 79 \cdot 97$. Note Hadamard matrices of order $4b$, $4c$, $4d$ and $4a$ are not yet known and hence the method in [?] and [?] cannot be used. Since there exist Williamson type matrices of order 79, 97 and an Hadamard matrix of order 71, by Corollary 2, there exists a $W(4a, 2a)$. Similarly, we obtain new $W(4n, 2n)$, which cannot be obtained by using the method given in [?] or [?], for $n = 73 \cdot 83 \cdot 89$ and $83 \cdot 89 \cdot 103$. Also Corollary 1 and Corollary 2 give infinitely new $W(4h, 2h)$ directly for example $h = 5^j$ or $3^i5^j7^k$, where i, j, k are non-negative integers. Corollary 1 has many uses. First, this is a step towards proving the conjecture that there exists a $W(4n, 2n)$ for any positive integer n. This conjecture is a sub-conjecture of the Seberry conjecture [3, page 92] that $W(4n, k)$ exist for all $k = 0, 1, \dots, 4n$. In addition we find infinitely many new $W(2n, n)$, n odd and the sum of two squares. It is interesting that unlike the product of Hadamard matrices (see [1], [?]), where the number of 2-factors will increase when the number of Hadamard matrices used to form the product increases, the factor 4 in the order $4N = 4\prod_{j=1}^{k} n_j^{r_j}$ of $W(4N, 2N)$ will be invariant no matter how large k and r_j become.

Furthermore, let W_1 be the $W(4N, 2N)$ for $N = \prod_{j=1}^{k} n_j^{r_j}$, where r_j are non-negative integers, mentioned in Corollary 1. Suppose we have another $W(4N, 2N)$, say W_2, disjoint with W_1. Using Craigen's [2] orthogonal pairs, we would obtain a powerful result: there exists an Hadamard matrix of order hN whenever there exists an Hadamard matrix of order h. In particular there exists an Hadamard matrix of order $8N$, $N = \prod_{j=1}^{k} n_j^{r_j}$, where r_j are non-negative integers. $H = W_1 \times \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + W_2 \times \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$ is the required Hadamard matrix.

The state of the $W(4n, 2n)$ conjecture, for small n, can be summarized by noting that a $W(2^tq, 2^{t-1}q)$ exists for q, odd, $q < 3000$ for precisely those q and t for which an Hadamard matrix exists in the Appendix of Seberry and Yamada [?].

The conjecture that a $W(2n, n)$ for every odd n where n is the sum of two squares has previously been resolved in the affirmative for $n = 5, 9, 13$ and 17 (see [3]).

Lemma 5 *Let A_1, A_2, A_3, A_4 be type 1 (1 , -1)-matrices of order n satisfying*

$$\sum_{i=1}^{4} A_iA_i^T = 4nI_n \tag{1}$$

and

$$A_1A_2^T + A_2A_1^T + A_3A_4^T + A_4A_3^T = 0. \tag{2}$$

Then there exists a $W(2n,n)$.

Proof. Set $W = \frac{1}{2}\left[\begin{array}{cc} A_1+A_2 & A_3+A_4 \\ A_3^T+A_4^T & -A_1^T-A_2^T \end{array}\right]$ is a $W(2n,n)$. Then W is a $W(2n,n)$. □

We note that if n is odd in Lemma 5 then by Corollary 2.11 [3] n is the sum of two squares. We call four (1, -1) type 1 matrices that satisfy (1) and (2) *tight Williamson-like matrices.*

Corollary 3 *Let* $M = \prod_{j=1}^{k} p_j^{4r_j}$, *where* $p_j \equiv 3(mod 4)$, *a prime and* r_j *is a non-negative integer,* $j = 1,\ldots,k$. *Then there exists a* $W(2n,n)$, *where* $n = 5\cdot 9^t M,\ 13\cdot 9^t M,\ 25\cdot 9^t M$.

Proof. By Theorem 2, [6], there exist four type 1 (1 , -1)-matrices of order $5\cdot 9^t$, $13\cdot 9^t$, $25\cdot 9^t$, satisfying (1) and (2). From [?], There exist four symmetric, mutually commutative type 1 (1 , -1)-matrices of order M, say B_1, B_2, B_3, B_4, satisfying $\sum_{i=1}^4 B_iB_i^T = 4nI_n$, $B_1B_2^T + B_3B_4^T = 0$, $B_1B_3^T + B_2B_4^T = 0$, $B_1B_4^T + B_2B_3^T = 0$. By Theorem 1, [6], there exist four type 1 matrices of order $5\cdot 9^t M$, $13\cdot 9^t M$, $25\cdot 9^t M$, satisfying (1) and (2). By Lemma 5, we have a $W(2n,n)$, where $n = 5\cdot 9^t M,\ 13\cdot 9^t M,\ 25\cdot 9^t M$. □

We now give tight Williamson-like matrices of order 5, 13 and 25. By the method given by Xia [5], we construct cyclic (1, -1) tight Williamson-like matrices of order 5 and 13 with first rows

$+-++-,\ \ ++-++,\ \ --++-,\ \ ++++-$ and

$++---+--++-++,\ \ --+++-++++++-+,$
$+--+-+++----+-,\ \ +-++++++++--++-$ respectively.

From [5] we also construct type 1 tight Williamson-like matrices of order 25. Any element in the abelian group $Z_5 \oplus Z_5$ can be expressed as (a,b), where a, $b \in Z_5$, and the additive addition in $Z_5 \oplus Z_5$ can be defined as $(a,b)+(c,d) = (a+b, c+d)$. Set

$$\begin{aligned}
S_1 &= \{(0,0),(0,1),(1,2),(3,3),(0,3),(4,4),(3,4),(2,0),(2,2),(1,0),(1,4),(0,2),(3,0)\},\\
S_2 &= \{(0,1),(4,0),(3,1),(4,4),(0,4),(4,2),(1,0),(1,1),(3,2)\},\\
S_3 &= \{(1,2),(3,3),(1,3),(4,1),(3,4),(2,0),(2,3),(4,3),(1,4),(0,2),(2,4),(2,1)\},\\
S_4 &= \{(3,3),(4,1),(0,3),(2,0),(4,3),(2,2),(0,2),(2,1),(3,0)\}.
\end{aligned}$$

Hence the type 1 (1, -1) incidence matrices of S_1, S_2, S_3, S_4 form the tight Williamson-like matrices of order 25.

Finally we note that if $N+I$ is a symmetric conference matrix of order $n \equiv 2(mod\,4)$ then $N+I$, $N-I$, $N+I$, $-N+I$ are tight Williamson-like matrices of order n.

References

[1] Agayan, S. S. *Hadamard Matrices and Their Applications*, vol. 1168 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1985.

[2] Craigen, R. Constructing Hadamard matrices with orthogonal pairs. *Ars Combinatoria 33* (1992), 57–64.

[3] Geramita, A. V., and Seberry, J. *Orthogonal Designs: Quadratic Forms and Hadamard Matrices.* Marcel Dekker, New York-Basel, 1979.

[4] Seberry, J., and Yamada, M. On the products of Hadamard matrices, Williamson matrices and other orthogonal matrices using M-structures. *JCMCC 7* (1990), 97–137.

[5] Xia, M. Y. Some supplementary difference sets and hadamard matrices. *Acta. Math. Sci. 4 (1)* (1984), 81–92.

[6] Xia, M. Y. Hadamard matrices. *Combinatorial designs and applications, Lecture Notes in Pure and Appl. Math., Dekker, New York 126* (1990), 179–181.