J. Austral. Math. Soc. **24** (Series A) (1977), 252–526

AN INFINITE FAMILY OF WILLIAMSON MATRICES

EDWARD SPENCE

(Received 3 March 1976; revised 20 November 1976)
Communicated by W. D. Wallis

Abstract

In this paper the following result is proved. Suppose there exists a C-matrix of order $n+1$. Then if $n\equiv 1 \pmod 4$ there exists a Hadamard matrix of order $2n^r(n+1)$, while if $n\equiv 3 \pmod 4$ there exists a Hadamard matrix of order $n^r(n+1)$ for all $r\geqslant 0$. If $n\equiv 1 \pmod 4$ is a prime power, the method is adapted to prove the existence of a Hadamard matrix of the Williamson type, of order $2n^r(n+1)$, for all $r\geqslant 0$.

1. C-matrices

A C-matrix of order $n+1$ is a square matrix C with zero diagonal and other elements ± 1 satisfying $CC^{\mathrm{T}} = nI$. Turyn (1971) has found a method of deriving new C-matrices from old, while Delsarte et al. (1971, Corollary 2.2) prove that if $n\equiv 1 \pmod 4$ C is equivalent (under multiplication of rows and columns by -1) to a symmetric matrix, but if $n\equiv 3 \pmod 4$ C is equivalent to a skew-symmetric matrix.

Case 1. $n\equiv 1 \pmod 4$. Here we may assume that

$$C = \begin{bmatrix} 0 & e \\ e^{\mathrm{T}} & Q \end{bmatrix},$$

where e is the all-one vector of order n, Q is a square symmetric matrix of order n with zero diagonal, and satisfying $Q^2 = nI_n - J_n$, $J_n Q = QJ_n = 0$, where J_n is the $n\times n$ matrix with every entry 1. We use this decomposition of C to define inductively a sequence of matrices $\{A_r, B_r\}$ $(r\geqslant 0)$ by $A_0 = C+I$, $B_0 = C-I$,

$$A_{r+1} = \tfrac{1}{2}(A_r - B_r)\times J_n + \tfrac{1}{2}(A_r + B_r)\times(Q + I_n),$$
$$B_{r+1} = \tfrac{1}{2}(A_r - B_r)\times J_n + \tfrac{1}{2}(A_r + B_r)\times(Q - I_n)$$

for $r\geqslant 0$ (where $\times$ denotes Kronecker product). We have

THEOREM 1. *For each $r\geqslant 0$, A_r, B_r are symmetric commuting ± 1 matrices of order $n^r(n+1)$ such that*

$$(A_r - B_r)^2 = 4n^r I, \quad (A_r + B_r)^2 = 4n^{r+1} I.$$

PROOF. The first part of the theorem is obvious. For the second, observe that

$$(A_{r+1}-B_{r+1})^2 = (A_r+B_r)^2 \times I,$$

while

$$(A_{r+1}+B_{r+1})^2 = (A_r-B_r)^2 \times nJ_n + (A_r+B_r)^2 \times (nI_n - J_n).$$

The proof is completed by induction.

COROLLARY 2. *If there exists a C-matrix of order* $n+1$ *where* $n \equiv 1 \pmod 4$ *then there exists a symmetric Hadamard matrix* H_r *of order* $2n^r(n+1)$ *for all* $r \geqslant 0$.

PROOF. Take

$$H_r = \begin{bmatrix} A_r & B_r \\ B_r & -A_r \end{bmatrix}.$$

In particular, since a C matrix exists when $n \equiv 1 \pmod 4$ is a prime power (Paley, 1933), we have

COROLLARY 3. *If* $q \equiv 1 \pmod 4$ *is a prime power there exists a symmetric Hadamard matrix of order* $2q^r(q+1)$ *for all* $r \geqslant 0$.

However, in this case a little more can be said, for a similar construction yields Hadamard matrices of the Williamson type of order $2q^r(q+1)$. (This generalizes a result of Whiteman, 1976, and Wallis, 1973.)

Williamson (1944) considered Hadamard matrices of the form

$$H = \begin{bmatrix} D & E & F & G \\ -E & D & -G & F \\ -F & G & D & -E \\ -G & -F & E & D \end{bmatrix}, \tag{1.1}$$

where D, E, F, G are ± 1 matrices of order v which pairwise satisfy

$$MN^{\mathrm{T}} = NM^{\mathrm{T}} \tag{1.2}$$

and for which

$$DD^{\mathrm{T}} + EE^{\mathrm{T}} + FF^{\mathrm{T}} + GG^{\mathrm{T}} = 4vI. \tag{1.3}$$

To satisfy condition (1.2) Williamson used symmetric circulant matrices D, E, F, G. We shall call a Hadamard matrix of the form (1.1) a Williamson matrix if it satisfies conditions (1.2) and (1.3).

The following two classes of Williamson matrices of order $4v$ have been found:

(i) when $v = (q+1)/2$, $q \equiv 1 \pmod 4$, q a prime power (Turyn, 1972; Whiteman, 1973),

(ii) when $v = q(q+1)/2$, $q \equiv 1 \pmod 4$, q a prime power, (Wallis, 1973; Whiteman, 1976).

https://doi.org/10.1017/S1446788700020255 Published online by Cambridge University Press

We shall extend these results by showing that we can take $v = q^r(q+1)/2$ for all $r \geqslant 0$.

Goethals and Seidel (1967) have shown that when $q \equiv 1 \pmod 4$ is a prime power there exists a C-matrix of order $q+1$, with zero diagonal and other elements ± 1 of the form $\begin{bmatrix} R & S \\ S & -R \end{bmatrix}$, where R, S are symmetric circulants of order $(q+1)/2$. Turyn (1972) observed that if we take $D = E = S$, $F = I+R$, $G = -I+R$, then H as constructed in (1.1) is a Williamson matrix of order $2(q+1)$. In what follows Q will denote the Paley matrix of order q (see Paley, 1933), so that Q is a symmetric matrix with zero diagonal and other elements ± 1 satisfying $Q^2 = qI - J_q$, $J_q Q = Q J_q = 0$.

Write $D_0 = E_0 = S$, $F_0 = I+R$, $G_0 = -I+R$ and define a sequence of matrices $\{D_r, E_r, F_r, G_r\}$ $(r \geqslant 0)$ inductively by

$$\begin{aligned} D_{r+1} &= \tfrac{1}{2}(D_r - E_r) \times J + \tfrac{1}{2}(D_r + E_r) \times (Q+I), \\ E_{r+1} &= \tfrac{1}{2}(D_r - E_r) \times J + \tfrac{1}{2}(D_r + E_r) \times (Q-I), \\ F_{r+1} &= \tfrac{1}{2}(F_r - G_r) \times J + \tfrac{1}{2}(F_r + G_r) \times (Q+I), \\ G_{r+1} &= \tfrac{1}{2}(F_r - G_r) \times J + \tfrac{1}{2}(F_r + G_r) \times (Q-I), \end{aligned}$$

where J is of order q and, as before, $\times$ denotes Kronecker product. We then have

THEOREM 4. *For each $r \geqslant 0$ the matrices D_r, E_r, F_r, G_r have elements ± 1, are symmetric, commute in pairs and satisfy the conditions*

$$\begin{aligned} (D_r - E_r)^2 + (F_r - G_r)^2 &= 4q^r I, \\ (D_r + E_r)^2 + (F_r + G_r)^2 &= 4q^{r+1} I, \\ D_r^2 + E_r^2 + F_r^2 + G_r^2 &= 2q^r(q+1) I. \end{aligned}$$

PROOF. Again the proof is by induction.

As an immediate corollary we have

COROLLARY 5. *For each $r \geqslant 0$ the matrix*

$$\begin{bmatrix} D_r & E_r & F_r & G_r \\ -E_r & D_r & -G_r & F_r \\ -F_r & G_r & D_r & -E_r \\ -G_r & -F_r & E_r & D_r \end{bmatrix}$$

of order $2q^r(q+1)$ is a Williamson type Hadamard matrix. Thus if t is the order of a Baumert–Hall array and $q \equiv 1 \pmod 4$ a prime power, then there exists a Hadamard matrix of order $2q^r(q+1)t$ for all $r \geqslant 0$.

The known values of t are $t \in \{2k+1 : 0 \leqslant k \leqslant 30\} \cup \{1 + 2^a 10^b 13^c,\ a, b, c$ non-negative integers$\}$.

https://doi.org/10.1017/S1446788700020255 Published online by Cambridge University Press

Case 2. $n \equiv 3 \pmod 4$. Here we may assume the C-matrix to have the form

$$C = \begin{bmatrix} 0 & e \\ -e^{\mathrm{T}} & Q \end{bmatrix},$$

where Q is *skew*-symmetric and satisfies $QQ^{\mathrm{T}} = nI - J_n$, $J_n Q = QJ_n = 0$.

Define a sequence of matrices $\{U_r, V_r\}$ $(r \geqslant 1)$ by

$$U_1 = I_{n+1} \times J_n + C \times Q, \quad V_1 = C \times I_n$$

and

$$U_{r+1} = U_r \times J_n + V_r \times Q, \quad V_{r+1} = V_r \times I_n \quad \text{if } r \text{ is even},$$

while

$$U_{r+1} = U_r \times I_n, \quad V_{r+1} = V_r \times J_n + U_r \times Q \quad \text{if } r \text{ is odd}.$$

We then have the following theorem

THEOREM 6. *For each* $r \geqslant 1$

(i) U_r *and* V_r *have order* $n^r(n+1)$ *and have entries* $0, \pm 1$, *while* $U_r + V_r$ *is a* ± 1 *matrix,*

(ii) U_r *and* V_r *commute,*

(iii) U_r *is symmetric and* V_r *is skew-symmetric,*

(iv) $U_r U_r^{\mathrm{T}} = n^{r+1} I$ *and* $V_r V_r^{\mathrm{T}} = n^r I$ *if* r *is odd, while* $U_r U_r^{\mathrm{T}} = n^r I$ *and* $V_r V_r^{\mathrm{T}} = n^{r+1} I$ *if* r *is even,*

(v) $H_r = U_r + V_r$ *is a Hadamard matrix of order* $n^r(n+1)$.

PROOF. (i)–(iv) are proved by a straightforward application of induction with (v) as an immediate consequence. This theorem is a simple generalization of the case $r = 1$ due to Williamson (1944).

Mukhopadhyay (1973) has already established the existence of Hadamard matrices of the above orders. However, his proof is different and does not suggest the fact, established above, that such a Hadamard matrix can be written as the sum of two orthogonal $0, \pm 1$ matrices, one of which is symmetric and the other skew-symmetric (a fact which is used later in Theorem 10).

Since C-matrices of order $q+1$ exist when $q \equiv 3 \pmod 4$ is a prime power (Paley, 1933), we deduce

COROLLARY 7. *There exists a Hadamard matrix of order* $q^r(q+1)$ *for every prime power* $q \equiv 3$ *(mod* 4*) and all* $r \geqslant 0$.

Also skew-Hadamard matrices of order $2(q+1)$ exist for q a prime power such that

(i) $q \equiv 5 \pmod 8$ (Szekeres, 1969; Spence, to appear), or

(ii) $q = p^{2t}$ where $p \equiv 5 \pmod 8$ is a prime and t is odd (Whiteman, 1971).

Thus we have

COROLLARY 8. *For either of the two choices of* q *above there exists a Hadamard matrix of order* $2(q+1)(2q+1)^r$ *for all* $r \geqslant 0$.

https://doi.org/10.1017/S1446788700020255 Published online by Cambridge University Press

2. Some supplementary results

In the literature there are several constructions for Hadamard matrices based on C-matrices. More precisely, for a given C-matrix C it may be possible to find ± 1 matrices X, Y of order v such that $I \times X + C \times Y$ is a Hadamard matrix. Many such constructions are given in Wallis et al. (1972). The following two results generalize this idea.

THEOREM 9. *Let C be a (symmetric) C-matrix of order $n+1 \equiv 2 \pmod 4$. If X and Y are ± 1 matrices of order v such that $I \times X + C \times Y$ is a Hadamard matrix of order $v(n+1)$, then $\frac{1}{2}(A_r - B_r) \times X + \frac{1}{2}(A_r + B_r) \times Y$ (A_r, B_r as in Theorem 1) is a Hadamard matrix of order $n^r v(n+1)$.*

THEOREM 10. *Let C be a (skew-symmetric) C matrix of order $n+1 \equiv 0 \pmod 4$. If X, Y are ± 1 matrices of order v such that $I \times X + C \times Y$ is a Hadamard matrix of order $v(n+1)$ then one of*

$$U_r \times X + V_r \times Y, \quad V_r \times X + U_r \times Y$$

(depending on whether r is even or odd) is a Hadamard matrix of order $n^r v(n+1)$.

REFERENCES

P. Delsarte, J. M. Goethals and J. J. Seidel (1971), "Orthogonal matrices with zero diagonal II", *Canad. J. Math.* **23**, 816–832.

J. M. Goethals and J. J. Seidel (1967), "Orthogonal matrices with zero diagonal", *Canad. J. Math.* **19**, 1001–1010.

A. C. Mukhopadhyay (1973), "Some series of Hadamard matrices", unpublished result.

R. E. A. C. Paley (1933), "On orthogonal matrices", *J. Math. Phys.* **12**, 311–320.

E. Spence (to appear), "Skew-Hadamard matrices of order $2(q+1)$", *Discrete Math.*

G. Szekeres (1969), "Tournaments and Hadamard matrices", *Enseignement Math.* **15**, 269–278.

R. J. Turyn (1971), "On C-matrices of arbitrary powers", *Canad. J. Math.* **23**, 531–535.

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

J. S. Wallis (1973), "Some matrices of Williamson type", *Utilitas Math.* **4**, 147–154.

W. D. Wallis, A. P. Street and J. S. Wallis (1972), *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices* (Lecture Notes in Mathematics 292, Springer-Verlag, Berlin).

A. L. Whiteman (1971), "An infinite family of skew-Hadamard matrices", *Pacific J. Math.* **38**, 817–822.

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

A. L. Whiteman (1976), "Hadamard matrices of Williamson type", *J. Austral. Math. Soc.*, **21** (Series A), 481–486.

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

University of Glasgow
Glasgow G12 8QW
Scotland