J. Austral. Math. Soc. 21 (Series A) (1976), 481–486.

HADAMARD MATRICES OF WILLIAMSON TYPE

Dedicated to George Szekeres

ALBERT LEON WHITEMAN*

(Received 17 February 1975)

Communicated by Jennifer Seberry Wallis

Abstract

Let p be a prime $\equiv 1 \pmod 4$ and put $v = p(p+1)/2$. It is proved in this paper that there exist four symmetric circulant matrices A, B, C, D of order v such that

$$A^2 + B^2 + C^2 + D^2 = 4vI_v,$$

where I_v is the identity matrix of order v. This result is used to construct Hadamard matrices of order $4v$ that are of the type originally prescribed by Williamson.

1. Introduction

An Hadamard matrix $H = [h_{ij}]$ is a square matrix of order v with $h_{ij} = \pm 1$ which satisfies the matrix equation $HH^T = H^TH = vI_v$. Here H^T denotes the transpose of H and I_v is the identity matrix of order v. It is known that the order v of an Hadamard matrix is necessarily 1,2 or a multiple of 4, and it is conjectured that Hadamard matrices for all these orders exists. For a definitive account of the extensive literature on this conjecture see Wallis, Street and Wallis (1972).

In 1944 Williamson (1944) introduced a special type of Hadamard matrix

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \tag{1}$$

* Partially supported by a National Science Foundation Grant.

whose structure is based on a matrix representation of quaternions. Williamson noted that if A, B, C, D are circulant and symmetric $(1, -1)$ matrices of order v for which the matrix equation

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

is satisfied, then H is an Hadamard matrix of order $4v$.

Hadamard matrices of the type prescribed by Williamson are known to exist

(i) for all odd $v \leqq 29$ and $v = 37$ and 43.

(ii) for $v = (q+1)/2$, where q is a prime power and $q \equiv 1 \pmod 4$. The matrices in class (i) are listed in Appendix II of Hall's book (1967, pp. 299–300), and are also tabulated in the book by Wallis, Street and Wallis (1972, pp. 388–389). These matrices were constructed mainly by Williamson but some are due to Baumert, Golomb and Hall. Class (ii) is a remarkable infinite family of Hadamard matrices discovered by Richard Turyn (1972). For an alternate derivation of Turyn's result see Whiteman (1973).

Recent advances in the construction of Hadamard matrices have employed four $(1, -1)$ matrices A, B, C, D of order v satisfying

$$MN^T = NM^T (M, N \in \{A, B, C, D\}), \tag{3}$$

and

$$AA^T + BB^T + CC^T + DD^T = 4vI_v. \tag{4}$$

When such matrices exist the matrix H in (1) is an Hadamard matrix of order $4v$. If A, B, C, D are symmetric and circulant the condition (3) is automatically satisfied and (4) reduces to (2).

The following result is due to Wallis (1973): If q is a prime power and $q \equiv 1 \pmod 4$, then there exist four $(1, -1)$ matrices A, B, C, D of order $v = q(q+1)/2$ satisfying the conditions (3) and (4). The matrices A, B, C, D of this construction are not circulant and need not be symmetric. In the present paper we give an alternative construction in which A, B, C, D are not only circulant but are symmetric as well. The construction is applicable whenever q is a prime (but not a prime power). Specifically, we prove that if $v = p(p+1)/2$, where p is a prime $\equiv 1 \pmod 4$, then there exist four circulant and symmetric $(1, -1)$ matrices A, B, C, D of order v which satisfy condition (2). The corresponding matrix H in (1) is an Hadamard matrix of order $4v$.

This result yields new orders of Hadamard matrices of Williamson's original type. The first five orders not produced by classes (i) or (ii) correspond to $v = 153, 435, 703, 1891, 2415$.

2. Two Lemmas

Let p be an odd prime. The p-th roots of unity are the numbers $\exp(2\pi ih/p)$, $h = 0, 1, \cdots, p-1$. Let ε be any root of the equation $\varepsilon^p = 1$ other than $\varepsilon = 1$. We shall require the following elementary lemma (see for example the book by Landau (1927), vol. 1, p. 156).

LEMMA 1. *The familiar Gauss sum*

$$G = \sum_{s=0}^{p-1} \chi(s)\varepsilon^s, \tag{5}$$

where $\chi(s)$ denotes the Legendre symbol $(s \mid p)$, satisfies the relation

$$G^2 = \chi(-1)p. \tag{6}$$

Let $GF(p)$ denote the residue class field of p incongruent numbers modulo p. If w is a quadratic non-residue of p, then the polynomial $P(x) = x^2 - w$ is irreducible over $GF(p)$ and the polynomials $ax + b (a, b \in GF(p))$ modulo $P(x)$ form a finite field $GF(p^2)$ of order p^2. This concrete representation of $GF(p^2)$ is used in the next lemma (compare Theorem 1 in Whiteman (1973)).

LEMMA 2. *Let p be a prime $\equiv 1 \pmod 4$ and put $n = (p+1)/2$. Let γ be a primitive element of $GF(p^2)$. Put $\gamma^r = ax + b (a, b \in GF(p))$ and define $a_r = \chi(a)$, $b_r = \chi(b)$. Then the sums*

$$f(\zeta) = \sum_{r=0}^{n-1} a_{4r}\zeta^r, \quad g(\zeta) = \sum_{r=0}^{n-1} b_{4r}\zeta^r \tag{7}$$

satisfy the identity

$$f^2(\zeta) + g^2(\zeta) = p. \tag{8}$$

for each n-th root of unity ζ including $\zeta = 1$.

With the exception of $a_0 = 0$, the coefficients a_{4r}, b_{4r} of the polynomials $f(\zeta)$, $g(\zeta)$ are $+1$ or -1. Furthermore, it is proved in [Whiteman (1973), p. 338] that

$$a_{4(n-r)} = a_{4r}, \quad b_{4(n-r)} = b_{4r} (r = 0, 1, \cdots, n-1). \tag{9}$$

Note that for $\zeta = 1$ the identity (8) reduces to the classical result that every prime $p \equiv 1 \pmod 4$ is the sum of two squares of integers.

3. The Main Theorem

The main feature of Williamson's method may be summarized as follows. Williamson associated with the circulant matrices A, B, C, D of order v in (1) the polynomials

https://doi.org/10.1017/S1446788700019327 Published online by Cambridge University Press

$$\psi_1(\alpha) = a_0 + a_1\alpha + \cdots + a_{v-1}\alpha^{v-1},$$

$$\psi_2(\alpha) = b_0 + b_1\alpha + \cdots + b_{v-1}\alpha^{v-1},$$

$$\psi_3(\alpha) = c_0 + c_1\alpha + \cdots + c_{v-1}\alpha^{v-1},$$

$$\psi_4(\alpha) = d_0 + d_1\alpha + \cdots + d_{v-1}\alpha^{v-1},$$

where α is a v-th root of unity. The coefficients $a_i, b_i, c_i, d_i (i = 0, 1, \cdots, v-1)$ comprise the first rows of A, B, C, D respectively. The condition that the matrices A, B, C, D be symmetric requires that

$$a_{v-i} = a_i,\ b_{v-i} = b_i,\ c_{v-i} = c_i,\ d_{v-i} = d_i (i = 1, 2, \cdots, v-1). \tag{10}$$

Consequently the numbers $\psi_1(\alpha), \psi_2(\alpha), \psi_3(\alpha), \psi_4(\alpha)$ are actually real numbers. From the finite Parseval relation it follows that the identity

$$\sum_{i=0}^{v-1} (a_i a_{i+k} + b_i b_{i+k} + c_i c_{i+k} + d_i d_{i+k})$$

$$= \frac{1}{v} \sum_{j=0}^{v-1} (\psi_1^2(\alpha^j) + \psi_2^2(\alpha^j) + \psi_3^2(\alpha^j) + \psi_4^2(\alpha^j))\alpha^{jk}$$

holds for each integer k. Hence the matrix H in (1) is an Hadamard matrix of order $4v$ if the elements of A, B, C, D are $+1$ or -1 and if the identity

$$\psi_1^2(\alpha) + \psi_2^2(\alpha) + \psi_3^2(\alpha) + \psi_4^2(\alpha) = 4v \tag{11}$$

prevails for each v-th root of unity α including $\alpha = 1$.

We now state the main theorem of this paper.

THEOREM. *Let $v = p(p+1)/2$, where p is a prime $\equiv 1 \pmod 4$. Then there exist four circulant and symmetric $(1, -1)$ matrices A, B, C, D of order v that satisfy equation* (2.) *The corresponding matrix H in* (1) *is an Hadamard matrix of order $4v$ of Williamson's original type.*

PROOF. For a prime $p \equiv 1 \pmod 4$ put $n = (p+1)/2$ and $v = np$. The four matrices A, B, C, D of the theorem are determined by means of the following four associated polynomials

$\psi_1(\alpha), \psi_2(\alpha), \psi_3(\alpha), \psi_4(\alpha)$:

$$\psi_1(\alpha) = \sum_{s=0}^{p-1} \alpha^{sn} + \sum_{r=1}^{n-1} a_{4r}\alpha^{rp} + \sum_{r=1}^{n-1} a_{4r} \sum_{s=1}^{p-1} \chi(s)\alpha^{rp+sn},$$

$$\psi_2(\alpha) = \sum_{r=0}^{n-1} b_{4r}\alpha^{rp} + \sum_{r=0}^{n-1} b_{4r} \sum_{s=1}^{p-1} \chi(s)\alpha^{rp+sn},$$

https://doi.org/10.1017/S1446788700019327 Published online by Cambridge University Press

$$\psi_3(\alpha) = \sum_{s=0}^{p-1} \alpha^{sn} - \sum_{r=1}^{n-1} a_{4r}\alpha^{rp} + \sum_{r=1}^{n-1} a_{4r} \sum_{s=1}^{p-1} \chi(s)\alpha^{rp+sn},$$

$$\psi_4(\alpha) = -\sum_{r=0}^{n-1} b_{4r}\alpha^{rp} + \sum_{r=0}^{n-1} b_{4r} \sum_{s=1}^{p-1} \chi(s)\alpha^{rp+sn}.$$

The coefficients a_{4r}, b_{4r} appearing in these polynomials are $+1$ or -1 and are the same as the coefficients of the polynomials $f(\zeta)$, $g(\zeta)$ in (7). Since the $v = np$ numbers

$$rp + sn (r = 0, 1, \cdots, n-1;\ s = 0, 1, \cdots, p-1)$$

constitute a complete residue system modulo v it is clear that each of the four polynomials is actually of degree $v - 1$. Moreover, the polynomials are unchanged when r is replaced by $n - r$ and s by $p - s$. Since $\chi(-1) = 1$ for $p \equiv 1 \pmod 4$ it follows from (9) that the symmetry property (10) holds.

It remains to prove that the four polynomials satisfy the identity (11) for each v-th root of unity α including $\alpha = 1$. Since $\alpha^v = (\alpha^n)^p = (\alpha^p)^n = 1$ the number α^n is a p-th root of unity, and the number α^p is an n-th root of unity whenever α is a v-th root of unity. In agreement with the notation of Lemma 1 put $\alpha^n = \varepsilon$; in agreement with the notation of Lemma 2 put $\alpha^p = \zeta$. We consider two cases according as $\alpha^n = 1$ or $\alpha^n \neq 1$. In view of Lemmas 1 and 2 the four polynomials reduce to

$$\psi_1(\alpha) = p + f(\zeta),\ \psi_3(\alpha) = p - f(\zeta) \qquad (\alpha^n = 1),$$
$$\psi_2(\alpha) = g(\zeta),\ \psi_4(\alpha) = -g(\zeta) \qquad (\alpha^n = 1),$$

$$\psi_1(\alpha) = (1 + G)f(\zeta),\ \psi_3(\alpha) = (-1 + G)f(\zeta) \qquad (\alpha^n \neq 1),$$
$$\psi_2(\alpha) = (1 + G)g(\zeta),\ \psi_4(\alpha) = (-1 + G)g(\zeta) \qquad (\alpha^n \neq 1).$$

The number G is the Gauss sum defined in (5). If $\alpha^n = 1$ the sum of four squares in (11) reduces to $2p(p + 1)$ because of the identity (8). If $\alpha^n \neq 1$ the sum again reduces to $2p(p + 1)$ because of the identity (6). In either event we have established that (11) holds for each v-th root of unity α including $\alpha = 1$. The proof of the theorem is thus complete.

References

M. Hall Jr., (1967) *Combinatorial Theory* (Blaisdell, Waltham, Mass., 1967).

E. Landau (1927), *Vorlesungen über Zahlentheorie* (S. Hirzel, Leipzig. Chelsea reprint, New York, 1950).

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

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

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

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

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

University of Southern California
Los Angeles
California
U.S.A.