COMBINATORIAL MATHEMATICS, Vol. 403, Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1974, pp. 132-142.

WILLIAMSON MATRICES OF EVEN ORDER

Jennifer Seberry Wallis

Australian National University, Canberra

ABSTRACT

Recent advances in the construction of Hadamard matrices have depended on the existence of Baumert-Hall arrays and Williamson-type matrices. These latter are four (1,-1) matrices A,B,C,D, of order m, which pairwise satisfy

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

$$\text{and (ii)}\quad AA^T+BB^T+CC^T+DD^T = 4mI_m, \quad \text{where I is the identity matrix.}$$

Currently Williamson matrices are known to exist for all orders less than 100 except: 35,39,47,53,59,65,67,70,71,73,76,77,83,89,94.

This paper gives two constructions for Williamson matrices of even order, 2n. This is most significant when no Williamson matrices of order n are known. In particular we give matrices for the new orders 2.39,2.203,2.303,2.333,2.689,2.915, 2.1603.

1. INTRODUCTION AND BASIC DEFINITIONS

A matrix with every entry +1 or -1 is called a <u>(1,-1)-matrix</u>. An <u>Hadamard matrix</u> $H = (h_{ij})$ is a square (1,-1) matrix of order n which satisfies the equation

$$HH^T = H^TH = nI_n.$$

We use J for the matrix of all 1's and I for the identity matrix. The Kronecker product is written ×.

A <u>Baumert-Hall array</u> of order t is a 4t×4t array with entries A,-A,B,-B,C, -C,D,-D and the properties that:

(i) in any row there are exactly t entries ±A, t entries ±B, t entries ±C, and t entries ±D; and similarly for columns;

(ii) the rows are formally orthogonal, in the sense that if ±A,±B,±C,±D are realised as elements of any commutative ring then the distinct rows of the array are pairwise orthogonal; and similarly for columns.

The Baumert-Hall arrays are a generalisation of the following array of Williamson:

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix},$$

which gives, when A,B,C,D are replaced by matrices of <u>Williamson-type</u> - that is, (1,-1) matrices of order m which pairwise satisfy

(i) $MN^T = NM^T$,

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

- an Hadamard matrix of order 4m.

The status of knowledge about Williamson matrices and Baumert-Hall arrays is summarised below; these, together with the following theorem, give many infinite families of Hadamard matrices.

THEOREM 1. (Baumert and Hall) <u>If there exists a Baumert-Hall array of order t and a Williamson matrix of order m then there exists an Hadamard matrix of order 4mt.</u>

STATEMENT 1. There exist Baumert-Hall arrays of order

(i) $\{3,5,7,\ldots,59\} = B$,

(ii) $\{1+2^a.10^b.26^c:$ a,b,c natural numbers$\} = A$,

(iii) $5b$, $b \in A \cup B$.

STATEMENT 2. There exist Williamson-type matrices of order

(i) $\{1,3,5,7,\ldots,29,37,43\}$,

(ii) $\frac{1}{2}(p+1)$, $p \equiv 1 \pmod 4$ a prime power,

(iii) 9^d, d a natural number,

(iv) $\frac{1}{2}p(p+1)$, $p \equiv 1 \pmod 4$ a prime power,

(v) $s(4s+3), s(4s-1)$, $s \in \{1,3,5,\ldots,25\}$,

(vi) 93.

This leaves the following orders less than 100 for which Williamson-type matrices are not yet known: 35,39,47,53,59,65,67,70,71,73,76,77,83,89,94.

Four (1,-1) matrices A,B,C,D of order m with the properties

$$\begin{aligned}
&\text{(i)} \quad MN^T = NM^T \quad \text{for } M,N \in \{A,B,C,D\}, \\
&\text{(ii)} \quad (A-I)^T = -(A-I), \quad B^T = B, \quad C^T = C, \quad D^T = D, \qquad (1) \\
&\text{(iii)} \quad AA^T+BB^T+CC^T+DD^T = 4mI_m,
\end{aligned}$$

will be called good matrices. These are used in [2],[7],[12] to form skew-Hadamard matrices and exist for odd $m \leq 25$.

Let $S_1,S_2,\ldots,S_n$ be subsets of V, an additive abelian group of order v, containing $k_1,k_2,\ldots,k_n$ elements respectively. Write T_i for the totality of all differences between elements of S_i (with repetitions), and T for the totality of elements of all the T_i. If T contains each non-zero element a fixed number of times, λ say, then the sets $S_1,S_2,\ldots,S_n$ will be called n-$\{v; k_1,k_2,\ldots,k_n; \lambda\}$ supplementary difference sets. This will be abbreviated to sds. If n = 1 we have a (v,k,λ) difference set which is cyclic or abelian according as V is cyclic or abelian. Henceforth we assume V is always an additive abelian group of order v with elements $g_1,g_2,\ldots,g_v$.

The type 1 (1,-1) incidence matrix $M = (m_{ij})$ of order v of a subset X of V is defined by

$$m_{ij} = \begin{cases} +1 & g_j-g_i \in X, \\ -1 & \text{otherwise;} \end{cases}$$

while the type 2 (1,-1) incidence matrix $N = (n_{ij})$ of order v of a subset Y of V is defined by

$$n_{ij} = \begin{cases} +1 & g_j+g_i \in Y, \\ -1 & \text{otherwise.} \end{cases}$$

It is shown in [12] that if M is a type 1 (1,-1) incidence matrix and N is a type 2 (1,-1) incidence matrix of 2-$\{v;\ k_1,k_2;\ \lambda\}$ supplementary difference sets then

$$MN^T = NM^T.$$

Also in [12], it is shown that $R = (r_{ij})$ of order v, defined on V by

$$r_{i,j} = \begin{cases} 1 & \text{if } g_i+g_j = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

then if M is type 1, MR is type 2.

Hence if M and N are type 1 of order v, $MN = NM$ and $M(NR)^T = (NR)M^T$.

In general the (1,-1) incidence matrices $A_1,\ldots,A_n$ of n-$\{v;\ k_1,k_2,\ldots,k_n;\ \lambda\}$ supplementary difference sets satisfy

$$\sum_{i=1}^{n} A_iA_i^T = 4\left(\sum_{i=1}^{n} k_i-\lambda\right) I + \left[nv-4\left(\sum_{i=1}^{n} k_i-\lambda\right)\right] J.$$

Let $v = ef+1 = p^{\alpha}$ (p a prime). Let x be a primitive element of $GF(v) = F$ and write $G = \{z_1,\ldots,z_{v-1}\}$ for the cyclic group of order v-1 generated by x.

Define the <u>cyclotomic classes</u>, C_i, of G (see Storer [4] for more details) by

$$C_i = \{x^{ej+i}:\ 0 \leq j \leq f-1\}, \qquad 0 \leq i \leq e-1.$$

For any results implied, but unproved in this paper, on forming supplementary difference sets from cyclotomic classes, the reader is referred to [9] or [12].

2. USING GOOD MATRICES

THEOREM 2. <u>Let A,B,C,D be four good matrices of order s. Suppose there exist four (1,-1) matrices of order p,X,Y,P,Q which satisfy</u>

<u>(i) $SR^T = RS^T$, for $R,S \in \{X,Y,P,Q\}$,</u>

(ii) $PP^T+QQ^T = 2aI+(2p-2a)J$,

(iii) $XX^T+YY^T = 2(p+1)I-2J$.

Then there exist Williamson-type matrices of order 2sp, when $4s = p-a+1$.

PROOF. Let

$$M = \begin{bmatrix} P & Q \\ -Q & P \end{bmatrix}, \qquad N = \begin{bmatrix} X & Y \\ Y & -X \end{bmatrix}.$$

Then

$$MN^T = NM^T,$$
$$MM^T = I_2\times\big(2aI+(2p-2a)J\big),$$
$$NN^T = I_2\times\big(2(p+1)I-2J\big).$$

Now consider

$$A_1 = I\times M + (A-I)\times N$$
$$A_2 = B\times N$$
$$A_3 = C\times N$$
$$A_4 = D\times N.$$

Clearly

$$A_iA_j^T = A_jA_i^T, \qquad i,j = 1,2,3,4,$$

and

$$\sum_{i=1}^{4} A_iA_i^T = I\times MM^T + (4s-1)I\times NN^T$$
$$= I_s\times I_2\times[\big(2a+2(4s-1)(p+1)\big)I+(2p-2a-8s+2)J]$$
$$= 8spI_{2sp}, \qquad \text{when } s = (p-a+1)/4.$$

Hence we have the result.

COROLLARY 1. Suppose there exist 2-$\{p;\ k_1,k_2;\ k_1+k_2-\frac{1}{2}(p+1)+2s\}$ sds, X_1,X_2, and 2-$\{p;\ \frac{1}{2}(p-1);\ \frac{1}{2}(p-3)\}$ sds, X_3,X_4, with the property that

$$x \in X_i \Rightarrow -x \in X_i, \qquad i = 2,3,4,$$

where s is the order of a good matrix. Then there exist Williamson-type matrices of order 2sp.

PROOF. Let Q,X,Y be the type 1 (1,-1) incidence matrices of X_2,X_3,X_4. Then Q,X,Y are symmetric.

Let P be the type 2 (1,-1) incidence matrix of X_1. Then (i) of the theorem is satisfied. Further

$$PP^T+QQ^T = (2p+2-8s)I+(8s-2)J,$$
$$XX^T+YY^T = (2p+2)I-2J.$$

Hence there exist Williamson-type matrices of order 2sp.

COROLLARY 2. <u>If $p = 4f+1$, f odd, is a prime power of the form $9+4t^2$ or $25+4t^2$ and there exist good matrices of order $(f+1)/8$, then there exist Williamson-type matrices of order $(f+1)(4f+1)/4$.</u>

PROOF. We note that for $9+4t^2$ and $25+4t^2$, C_0, C_0+C_2 and C_1, C_0+C_2 respectively are 2-{4f+1; 2f,f; (5f-3)/4} sds. Then using C_0+C_2 and C_1+C_3 for the other sds in the previous corollary we have the result.

COROLLARY 3. <u>If $p = 4f+1$, f odd, is a prime power of the form $1+4t^2$ or $49+4t^2$ and there exist good matrices of order $(f-1)/8$, then there exist Williamson-type matrices of order $(f-1)(4f+1)/4$.</u>

PROOF. We note that for $1+4t^2$ and $49+4t^2$, $\{0\}+C_0, C_0+C_2$ and $\{0\}+C_1, C_0+C_2$ respectively are 2-{4f+1; 2f,f+1; (5f-1)/4} sds. Then using C_0+C_2 and C_1+C_3 for the other sds in corollary 1 we have the result.

For f = 25 and 57 we get Williamson matrices for the following orders 2n where no Williamson matrix of order n is known: 2.303,2.1603.

COROLLARY 4. <u>If $p = 4f+1$ is a prime power and $(p-1)/4$ is the order of a good matrix, then there exist Williamson type matrices of order $\frac{1}{2}p(p-1)$.</u>

PROOF. Use the (p,p,p) and (p,p-1,p-2) difference sets to form the 2-{p; p,p-1; 2p-2} sds for the corollary.

For p = 13 we find there is a good matrix of order 3 = (p-1)/4 and hence Williamson-type matrices of order 2.39 even though Williamson-type matrices of order 39 are not yet known. This corollary also gives us Williamson-type matrices for the following orders 2n where no Williamson matrix of order n is known: 2.203,2.333, 2.689, 2.915.

COROLLARY 5. Let $p \equiv 1 \pmod 4$ be a prime power. Further suppose there exists a (p,k,λ) difference set; then if there exist good matrices of order

$$\text{(i)}\quad s = [2(\lambda-k)+p+1]/4; \qquad \text{(ii)}\quad s = [2(\lambda-k)+p-1]/4$$

respectively, there exist Williamson-type matrices of order $2sp$.

PROOF. Use $Q = J$, $Q = J-2I$ respectively in the theorem and form X and Y from the type 1 incidence matrices of C_0+C_2 and C_1+C_3 respectively. For P use the type 2 incidence matrix of the difference set.

3. USING SOME OTHER WILLIAMSON MATRICES

THEOREM 3. Let $I+R, I-R, S, S$ be four Williamson matrices of order s. Suppose there exist four $(1,-1)$ matrices of order p, X, Y, P, Q which satisfy

$$\text{(i)}\quad ZW^T = WZ^T, \quad \text{for } Z,W \in \{X,Y,P,Q\},$$

$$\text{(ii)}\quad PP^T+QQ^T = 2aI+(2p-2a)J,$$

$$\text{(iii)}\quad XX^T+YY^T = 2(p+1)I-2J.$$

Then there exist Williamson matrices of order $2ps$, where $s = \frac{1}{2}(p-a+1)$.

PROOF. Let

$$M = \begin{bmatrix} P & Q \\ -Q & P \end{bmatrix}, \qquad N = \begin{bmatrix} X & Y \\ Y & -X \end{bmatrix}.$$

Then, as before,

$$MN^T = NM^T,$$

$$MM^T = I_2\times\big(2aI+(2p-2a)J\big),$$

$$NN^T = I_2\times\big(2(p+1)I-2J\big).$$

Now consider

$$A_1 = I\times M + R\times N$$

$$A_2 = S\times N$$

$$A_3 = I\times -M + R\times N$$

$$A_4 = S\times N.$$

Clearly

$$A_iA_j^T = A_jA_i^T, \qquad i,j = 1,2,3,4,$$

and

$$\begin{aligned}\sum_{i=1}^{4} A_iA_i^T &= 2I\times MM^T + 2(RR^T+SS^T)\times NN^T \\ &= I\times I_2\times[4aI+2(2p-2a)J] + I\times I_2\times[4(2s-1)(p+1)I-4(2s-1)J] \\ &= 8spI_{2sp}, \qquad \text{when } s = \tfrac{1}{2}(p-a+1);\end{aligned}$$

which gives the result.

COROLLARY 1. Suppose there exist Williamson-type matrices, $I+R, I-R, S, S$, of order s. Suppose there exist 2-$\{p;\ k_1,k_2;\ k_1+k_2+s-\tfrac{1}{2}(p+1)\}$ sds with incidence matrices P and Q, and 2-$\{p;\ \tfrac{1}{2}(p-1);\ \tfrac{1}{2}(p-3)\}$ sds with incidence matrices X and Y which satisfy

$$ZW^T = WZ^T \quad \text{for } Z,W \in \{P,Q,X,Y\}.$$

Then there exist Williamson matrices of order $2ps$.

COROLLARY 2. Suppose there exist Williamson-type matrices $I+R, I-R, S, S$, of order $p = \tfrac{1}{2}(s-1)$. Suppose there exists a symmetric Hadamard matrix of order $s+1 \equiv 0 \pmod 4$. Then there exist Williamson matrices of order $s(s-1)$.

PROOF. Normalize the Hadamard matrix to the form

$$\begin{bmatrix} 1 & 1 \; \cdots \; 1 \\ 1 & \\ \vdots & E \\ 1 & \end{bmatrix}, \quad E^T = E,$$

and use $P = J$, $Q = J-2I$, $X = Y = E$ in the theorem.

COROLLARY 3. Let $p \equiv 1 \pmod 4$ be a prime power. Suppose there exists a symmetric Hadamard matrix of order $p+3$. Then there exist Williamson matrices of order $(p+2)(p+1)$.

PROOF. There exist Williamson matrices of order $\tfrac{1}{2}(p+1)$ of the required form.

This gives Williamson matrices of the following orders $2n$ where none are known for n: 2.105, 2.171, 2.903.

COROLLARY 4. Let $p \equiv 1 \pmod 4$ be a prime power. Suppose there exists a (v,k,λ) difference set, where v is a prime power and $\lambda = k+\frac{1}{2}(p-v)$. Then there exist Williamson matrices of order $v(p+1)$.

PROOF. Let $P = J, Q$ be the type 2 $(1,-1)$ incidence matrix of the (v,k,λ) difference set; let $X = Y$ be the type 1 $(1,-1)$ incidence matrix of the $\{v,(v-1)/2,(v-3)/4\}$ difference set for $v \equiv 3 \pmod 4$ and X,Y be the type 1 $(1,-1)$ incidence matrices of 2-$\{v;\ (v-1)/2;\ (v-3)/2\}$ sds for $v \equiv 1 \pmod 4$.

COROLLARY 6. Let $p \equiv 1 \pmod 4$ be a prime power. Suppose there exists a (v,k,λ) difference set, where v is a prime power and $\lambda = k+(p-v)/4$. Then there exist Williamson matrices of order $v(p+1)$.

PROOF. For $P = Q$ use the type 2 incidence matrix of the difference set. Form X and Y as in the previous corollary.

Neither of the last two corollaries give interesting matrices for small orders.

COROLLARY 7. Let $p = 4f+1$ (f odd) be a prime power of the form $9+4t^2$ or $25+4t^2$. Suppose $(f-1)/2 \equiv 1 \pmod 4$ is a prime power. Then there exist Williamson matrices of order $\frac{1}{2}(f+1)(4f+1)$.

PROOF. For P and Q in the theorem use the type 2 and type 1 incidence matrices respectively of C_0 and C_0+C_2 or C_1 and C_0+C_2 which are 2-$\{4f+1;\ 2f,f;\ (5f-3)/4\}$ sds for the prime powers of the theorem. For X and Y use the type 1 incidence matrices of C_0+C_2 and C_1+C_3 which are 2-$\{4f+1;\ 2f;\ 2f-1\}$ sds.

COROLLARY 8. Let $p = 4f+1$ (f odd) be a prime power of the form $1+4t^2$ or $49+4t^2$. Suppose $(f-3)/2 \equiv 1 \pmod 4$ is a prime power. Then there exist Williamson matrices of order $\frac{1}{2}(f-1)(4f+1)$.

PROOF. Proceed as in the previous corollary but use $\{0\}+C_0$ or $\{0\}+C_1$ to form P.

REFERENCES

1. JOAN COOPER AND JENNIFER WALLIS, A construction for Hadamard arrays, Bull. Austral.Math.Soc. 7 (1972), 269-278.

2. DAVID C. HUNT, Skew-Hadamard matrices of order less than 100, Proceedings of the First Australian Conference on Combinatorial Mathematics, (Editors Jennifer Wallis and W.D. Wallis), TUNRA, Newcastle, Australia, 1972, 23-27.

3. DAVID C. HUNT AND JENNIFER WALLIS, Cyclotomy, Hadamard arrays, and supplementary difference sets, Proceedings of the Second Manitoba Conference on Numerical Mathematics, (1972), 351-381.

4. THOMAS STORER, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics, Markham, Chicago, 1967.

5. RICHARD J. TURYN, An infinite class of Williamson matrices, J. Combinatorial Theory 12 (1972), 319-321.

6. RICHARD J. TURYN, Computation of certain Hadamard matrices, Notices of Amer. Math.Soc. 20 (1973), A-1.

7. JENNIFER WALLIS, A skew-Hadamard matrix of order 92, Bull.Austral.Math.Soc. 5 (1971), 203-204.

8. JENNIFER SEBERRY WALLIS, Some matrices of Williamson type, Utilitas Math. (to appear).

9. JENNIFER SEBERRY WALLIS, Some remarks on supplementary difference sets, Proceedings of International Colloquium on Infinite and Finite Sets (to appear).

10. JENNIFER SEBERRY WALLIS, Construction of Williamson-type matrices, (to appear).

11. JENNIFER SEBERRY WALLIS, Goethals-Seidel type Hadamard matrices, (to appear).

12. W.D. WALLIS, ANNE PENFOLD STREET, JENNIFER SEBERRY WALLIS, Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

13. ALBERT LEON WHITEMAN, An infinite family of Hadamard matrices of Williamson type, J. Combinatorial Theory (to appear).