1973

Some matrices of Williamson type

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Some matrices of Williamson type

Abstract

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

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

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

We show that if p = 1 (mod 4) is a prime power then such matrices exist for m = $^1/_2$p(p+1). The matrices constructed are not circulant and need not be symmetric. This means there are Hadamard matrices of order 2p(P+1)t and 10p(p+1)t for t E {1,3,5,...,59} u {1 + 2^a $10^b 26^c$,a,b,c non-negative integers} , which is a new infinite family.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, Some matrices of Williamson type, Utilitas Mathematica, 4, (1973), 147-154.

SOME MATRICES OF WILLIAMSON TYPE

Jennifer Seberry Wallis

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

$$\text{(i)} \qquad MN^T = NM^T, \text{ and}$$

$$\text{(ii)} \quad AA^T + BB^T + CC^T + DD^T = 4mI_m .$$

We show that if $p \equiv 1 \pmod 4$ is a prime power then such matrices exist for $m = \frac{1}{2}p(p+1)$. The matrices constructed are not circulant and need not be symmetric.

This means there are Hadamard matrices of order $2p(p+1)t$ and $10p(p+1)t$ for $t \in \{1,3,5,\ldots,59\} \cup \{1 + 2^a 10^b 26^c, a,b,c$ non-negative integers$\}$, which is a new infinite family.

1. *Introduction.*

We wish to form four $(1,-1)$ matrices A, B, C, D of order m which pairwise satisfy

$$(1) \qquad \begin{array}{ll} \text{(i)} & MN^T = NM^T \\ \text{and (ii)} & AA^T + BB^T + CC^T + DD^T = 4mI_m . \end{array}$$

Williamson first used such matrices and we call them *Williamson type*. The matrices Williamson originally used were both circulant and symmetric but we will show that neither the circulant nor symmetric properties are necessary in order to satisfy (1).

This paper was prepared while the author was visiting the Department of Computer Science, University of Manitoba, Canada.

UTILITAS MATHEMATICA, Vol. 4 (1973), pp. 147 - 154.

Goethals and Seidel [1] found two $(1,-1)$ matrices $I+R$, S of order $\frac{1}{2}(p+1)$, $p \equiv 1 \pmod 4$ a prime power, which are circulant and symmetric and which satisfy

$$RR^T + SS^T = pI_{\frac{1}{2}(p+1)} ,$$

where I is the identity matrix.

Turyn [2] noted that $A = I+R$, $B = I-R$, $C = D = S$ satisfy the conditions (1) for $m = \frac{1}{2}(p+1)$ and hence are Williamson matrices. Whiteman [5] provided an alternate construction for A, B, C, D of these orders.

We are going to generalize the matrices of the following example: Let J, X, Y be of order 5, J the matrix of all 1's and suppose

$$XJ = -YJ = -J, \quad XY^T = YX^T, \quad XX^T + YY^T = 12I - 2J .$$

Consider

$$A = \begin{bmatrix} J & X & X \\ X & J & X \\ X & X & J \end{bmatrix}, \quad B = \begin{bmatrix} X & -X & -X \\ -X & X & -X \\ -X & -X & X \end{bmatrix}, \quad C = \begin{bmatrix} J & Y & Y \\ Y & J & Y \\ Y & Y & J \end{bmatrix}, \quad D = \begin{bmatrix} Y & -Y & -Y \\ -Y & Y & -Y \\ -Y & -Y & Y \end{bmatrix},$$

and note that A, B, C, D satisfy (1).

We use the following theorem (see Section 2 for definitions):

THEOREM 1. (Baumert and Hall, see [4]). *If there are Williamson type matrices of order* m *and a Baumert-Hall array of order* t *then there exists a Hadamard matrix of order* $4mt$.

Turyn has announced [3] that he has found Baumert-Hall arrays for the orders t and $5t$

(2) $\quad t \in \{1,3,5,\ldots,59\} \cup \{1 + 2^a 10^b 26^c,\ a,b,c \text{ non-negative integers}\}$.

Some Baumert-Hall arrays found by Cooper and Wallis may be found in [4] .

2. *Basic Definitions.*

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

$$HH^T = H^T H = nI_n \quad .$$

We use J for the matrix of all 1's.

A *Baumert-Hall array* of order t is a $4t \times 4t$ array with entries $A, -A, B, -B, C, -C, D, -D$ and the properties that:

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

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

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

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

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*. 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 [4] that if M is a type 1 $(1, -1)$ incidence matrix and N is a type 2 $(1, -1)$ incidence matrix of $2 - \{2q-1; q-1, q; q-1\}$ supplementary difference sets then

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

and

(3) $$MM^T + NN^T = 4qI - 2J .$$

If N were type 1 (3) would still be satisfied.

3. The Construction.

THEOREM 2. *Suppose there exist* $(1,-1)$ *matrices* $I+R, S$ *of order* q *which satisfy*

$$I + RR^T + SS^T = 2qI, \quad R^T = R, \quad S^T = S, \quad RS = SR$$

and $2 - \{2q-1; q-1, q; q-1\}$ *supplementary difference sets with incidence matrices* X, Y *which satisfy* $XY^T = YX^T$. *Then*

$$\begin{aligned} A &= I\times J + R\times X \\ B &= S\times X \\ C &= I\times J + R\times Y \\ D &= S\times Y \end{aligned}$$

are four Williamson type matrices of order $q(2q-1)$.

Proof. Choose X and Y to be both type 1(1,-1) incidence matrices if the condition $XY^T = YX^T$ can be satisfied;otherwise choose X to be a type 1 (1,-1) incidence matrix and Y to be a type 2 (1,-1) incidence matrix. Then $XY^T = YX^T$ (see [4; p.288]) .

By lemma 1.20 of [4;p.291]

$$XX^T + YY^T = 4qI-2J ,$$

and from the size of the two supplementary difference sets

$$XJ = -J = -YJ .$$

That A, B, C, D pairwise satisfy $MN^T = NM^T$ is easily verified and

$$\begin{aligned} AA^T + BB^T + CC^T + DD^T = {} & I\times(2q-1)J + R^T\times JX^T + R\times XJ + SS^T\times XX^T + RR^T\times XX^T \\ & + I\times(2q-1)J + R^T\times JY^T + R\times YJ + SS^T\times YY^T + RR^T\times YY^T \\ = {} & 2I\times(2q-1)J + (SS^T + RR^T) \times (4qI-2J) \\ = {} & 4q(2q-1)I , \end{aligned}$$

as required.

Now we note that there exist $2 - \{2q-1; q-1, q; q-1\}$ supplementary difference sets for

(i) $2q-1$ a prime power; [4;p.283],

(ii) $4q-1$ a prime power; Szekeres, [4;p.303],

(iii) $2q-1$ $2q$ the order of a symmetric conference matrix, see [4], and that R,S exist [4;p.391] for orders q for which $2q-1$ is a prime power $\equiv 1 \pmod 4$. Thus we have

COROLLARY 3. *Let* $2q-1 = p$ *be a prime power* $\equiv 1 \pmod 4$; *then there exist four Williamson type matrices* A, B, C, D *of order* $\frac{1}{2}p(p+1)$.

COROLLARY 4. *Let* $p \equiv 1 \pmod 4$ *be a prime power; then using theorem 1, there is a Hadamard matrix of order* $2p(p+1)t$ *and* $10p(p+1)t$ *where* t *is given by* (2).

We note that the matrices constructed in corollary 3 are all symmetric but not circulant. In the following construction, none of the matrices are circulant and some are not symmetric.

LEMMA 5. *Let* $p \equiv 5 \pmod 8$ *be a prime power then there exist Williamson type matrices* A, B, C, D *of order* $\frac{1}{2}p(p+1)$ *which pairwise satisfy*

$$MN^{\top} = NM^{\top} ,$$

for which

$$AA^{\top} + BB^{\top} + CC^{\top} + DD^{\top} = 2p(p+1)I_{\frac{1}{2}p(p+1)},$$

but which are neither circulant nor symmetric.

Proof. We use a construction of Szekeres [4;p.321]. Let x be a primitive root of $GF(p)$ and consider the cyclotomic classes of $p = 4f+1$ (f odd) defined by

$$C_i = \{x^{4j+i} : j = 0,1,\ldots, f-1\} \qquad i = 0,1,2,3 .$$

Then

$$C_0 \cup C_1 \quad \text{and} \quad \{0\} \cup C_1 \cup C_2 \;,$$

are $2 - \{4f+1;\ 2f,\ 2f+1;\ 2f\}$ supplementary difference sets for which (since $-1 \in C_2$)

$$a \in C_0 \cup C_1 \Rightarrow -a \notin C_0 \cup C_1 \quad \text{and}$$
$$b \in \{0\} \cup C_1 \cup C_2 \Rightarrow -b \notin \{0\} \cup C_1 \cup C_2,\ b \neq 0 \;.$$

We form the type 1 (1,-1) incidence matrix, X, of $C_0 \cup C_1$ and the type 2 (1,-1) incidence matrix, Y, of $\{0\} \cup C_1 \cup C_2$. Then

$$(X+I)^T = -(X+I),\quad Y^T = Y,\quad XJ = -J = -YJ\;,$$

$$XX^T + YY^T = 2(4f+2)I-2J,\quad \text{and} \quad XY^T = YX^T\;.$$

We now proceed as in theorem 2 noting that A and B are not symmetric.

REFERENCES

[1] J.M. Goethals and J.J. Seidel, *Orthogonal matrices with zero diagonal*, Canad. J. Math. *19* (1967), 1001-1010.

[2] Richard J. Turyn, *An infinite class of Williamson matrices*, J. Combinatorial Th. *12* (1972), 319-321.

[3] Richard J. Turyn, *Computation of certain Hadamard matrices*, Notices of Amer. Math. Soc. *20* (1973), A-1.

[4] 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.

[5] Albert Leon Whiteman, *An infinite family of Hadamard matrices of Williamson type*, J. Combinatorial Th. (to appear).

Institute of Advanced Studies
Australian National University
Canberra
Australia

Received February 15, 1973.