Recent advances in the construction of Hadamard matrices

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

Recent advances in the construction of Hadamard matrices

Abstract

In the past few years exciting new discoveries have been made in constructing Hadamard matrices. These discoveries have been centred in two ideas:

(i) the construction of Baumert-Hall arrays by utilizing a construction of L. R. Welch, and

(ii) finding suitable matrices to put into these arrays.

We discuss these results, many of which are due to Richard J. Turyn or the author.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, Recent advances in the construction of Hadamard matrices, Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium, 8, (1973), 53-89.

RECENT ADVANCES IN THE CONSTRUCTION OF HADAMARD MATRICES

Jennifer Seberry Wallis*
University of Newcastle, N.S.W., 2308, Australia

ABSTRACT. In the past few years exciting new discoveries have been made in constructing Hadamard matrices. These discoveries have been centred in two ideas:

(i) the construction of Baumert-Hall arrays by utilizing a construction of L. R. Welch, and

(ii) finding suitable matrices to put into these arrays.

We discuss these results, many of which are due to Richard J. Turyn or the author.

---

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

PROC. 4TH S-E CONF. COMBINATORICS, GRAPH THEORY, AND COMPUTING, pp.53-89.

1. *Introduction.*

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

$$HH^T = H^TH = nI_n \quad , \tag{1.1}$$

where H^T denotes H transposed and I is the identity matrix.

Unless specifically stated the order of matrices should be determined from the context. We use $-$ for -1 and J for the matrix with every element $+1$.

The matrices

$$[1] \;,\; \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix} \;,\; \begin{bmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{bmatrix} \;,\; \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{bmatrix} \tag{1.2}$$

are Hadamard matrices of orders 1, 2, 4 and 4 respectively.

It can be shown, see [5], [12], that the order of an Hadamard matrix is necessarily 1, 2 or $4m$ for some $m = 1, 2, 3, \ldots$. It has been conjectured that Hadamard matrices of all these orders exist. For many years the first few unresolved cases have been 188, 236, 268 and 292 but Richard J. Turyn has announced, [8], that he has found Hadamard matrices for the orders 188 and 236 leaving 268 the first unresolved case.

The book [12] of Wallis, Street and Wallis gives all the constructions for Hadamard known to this author early in 1972 but many exciting results have been discovered more recently.

2. *Definitions and Preliminary Results*

DEFINITION 2.1. A *circulant matrix* $A = (a_{ij})$ of order n is one in which $a_{ij} = a_{1,j-i+1}$ where $j-i+1$ is reduced modulo n. For example:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad .$$

DEFINITION 2.2. A matrix $A = (a_{ij})$ of order n will be called *back circulant* if $a_{ij} = a_{1,i+j-1}$ where $i+j-1$ is reduced modulo n. For example:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix} \quad .$$

DEFINITION 2.3. A(1,-) matrix is a matrix whose only elements are $+1$ and -1.

LEMMA 2.4. *A back circulant matrix is symmetric.*

LEMMA 2.5. *The product of a back circulant matrix with a circulant matrix of the same order is symmetric. In particular, if* A *is back circulant and* B *is circulant*

$$AB^T = BA^T \quad .$$

Proof. Let $A = (a_{ij})$ where $a_{ij} = a_{1,j-i+1}$ and $B = (b_{ij})$ where $b_{ij} = b_{1,i+j-1}$. Then

$$BA^T = (\sum_k b_{ik}a'_{kj}) = (\sum_k b_{ik}a_{jk}) = (\sum_k a_{jk}b_{ik})$$

$$= (\sum_k a_{1,k-j+1}b_{1,i+k-1})$$

$$= (\sum_k a_{i,k-j+i} b_{j,i+k-j}) = (\sum_{\ell=i+k-j} a_{i\ell} b'_{\ell j})$$

$$= (\sum_\ell a_{i\ell} b'_{\ell j})$$

$$= AB^T \quad .$$

LEMMA 2.6. *Any two circulant matrices of the same order commute.*

Proof. With $A = (a_{ij})$ and $B = (b_{ij})$ both circulant

$$AB = (\sum_k a_{ik} b_{kj}) = (\sum_k b_{i,j-k+i} a_{j-k+i,j}) = (\sum_{\ell=j-k+i} b_{i\ell} a_{\ell j})$$

$$= BA \quad .$$

We now generalize the concepts of circulant and back-circulant matrices by considering two special incidence matrices of subsets of an additive abelian group.

DEFINITION 2.7. Let G be an additive abelian group with elements z_i . Let X be a subset of G . We define two types of incidence matrices $M = (m_{ij})$ and $N = (n_{ij})$. First we fix an ordering for the elements of G , then M of order $|G|$, defined by

$$m_{ij} = \psi(z_j - z_i) \ , \quad \psi(z_j - z_i) = \begin{cases} 1 & z_j - z_i \in X, \\ 0 & \text{otherwise,} \end{cases}$$

will be called the *type 1 incidence matrix of* X *in* G ; and N of order $|G|$, defined by

$$n_{ij} = \phi(z_j + z_i) \ , \quad \phi(z_j + z_i) = \begin{cases} 1 & z_j + z_i \in X, \\ 0 & \text{otherwise,} \end{cases}$$

will be called the *type 2 incidence matrix of* X *in* G .

LEMMA 2.8. *Suppose* M *and* N *are type 1 and type 2 incidence matrices of a subset* $C = \{c_i\}$ *of an additive abelian group*

$G = \{z_i\}$. *Then*

$$MM^T = NN^T \quad .$$

Proof. The inner products of distinct rows i and k in M and N respectively are given by

$$\sum_{z_j \varepsilon G} \psi(z_j - z_i)\psi(z_j - z_k) \qquad \text{and} \qquad \sum_{z_j \varepsilon G} \phi(z_j + z_i)\phi(z_j + z_k)$$

$$= \sum_{g \varepsilon G} \psi(g)\psi(g + z_i - z_k) \qquad\qquad = \sum_{h \varepsilon G} \phi(h + z_i - z_k)\phi(h)$$

since as z_j runs through G so does $z_j - z_i = g$ | since as z_j runs through G so does $z_j + z_k = h$

$$= \sum_{c \varepsilon C} (c + z_i - z_k) \qquad\qquad = \sum_{c \varepsilon C} \phi(c + z_i - z_k)$$

= number of times $c + z_i - z_k \;\varepsilon\; C$ | = number of times $c + z_i - z_k \varepsilon\; C$.

For the same row

$$\sum_{z_j \varepsilon G} [\psi(z_j - z_i)]^2 \qquad \text{and} \qquad \sum_{z_j \varepsilon G} [\phi(z_j + z_i)]^2$$

$$= \sum_{g \varepsilon G} [\psi(g)]^2 \qquad\qquad = \sum_{h \varepsilon G} [\phi(h)]^2$$

$$= \sum_{c \varepsilon C} [\psi(c)]^2 \qquad\qquad = \sum_{c \varepsilon C} [\phi(c)]^2$$

= number of elements in C | = number of elements in C .

So $MM^T = NN^T$.

Now type 1 and type 2 incidence matrices of X in G are $(0,1)$-matrices, but we shall on occasion use the corresponding matrices which have elements from a commutative ring. So we extend the definition to

DEFINITION 2.9. Let G be an additive abelian group with elements z_i, which are ordered in some convenient way and the ordering fixed. Let $X = \{x_i\}$ be a subset of G, $X \cap \{0\} = \emptyset$. Then two matrices $M = (m_{ij})$ and $N = (n_{ij})$ defined by

$$m_{ij} = \psi(z_j - z_i) \quad \text{and} \quad n_{ij} = \phi(z_j + z_i) \quad ,$$

where ψ and ϕ map G into a commutative ring, will be called *type 1* and *type 2* respectively.

Further if ψ and ϕ are defined by

$$\psi(x) = \begin{cases} a & x \in X \\ b & x = 0 \\ c & x \notin X \cup \{0\} \end{cases} \quad , \qquad \phi(x) = \begin{cases} d & x \in X \\ e & x = 0 \\ f & x \notin X \cup \{0\} \end{cases}$$

then M and N will be called *type 1 matrix of* ψ *on* X and *type 2 matrix of* ϕ *on* X respectively. But if ψ and ϕ are defined by

$$\psi(x) = \begin{cases} 1 & x \in X \\ -1 & x \notin X \end{cases} \quad , \quad \phi(x) = \begin{cases} 1 & x \in X \\ -1 & x \notin X \end{cases} \quad ,$$

then M and N will be called *type 1* (1,-1) *incidence matrix* and *type 2* (1,-1) *incidence matrix* respectively.

EXAMPLE. Consider the additive group $GF(3^2)$, which has elements

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2 \quad .$$

Define the set $X = \{y : \ y = z^2 \text{ for some } z \in GF(3^2)\}$

$\qquad = \{x+1, 2, 2x+2, 1\}$

using the irreducible equation $x^2 = x+1$. Now a type 1 matrix of ψ on X , $A = (a_{ij})$, is determined by the function of the type

$$a_{ij} = \psi(g_j - g_i) \quad \text{where} \quad \psi(x) = \begin{cases} 0 & x = 0 \\ 1 & x \in X \\ -1 & \text{otherwise} \end{cases} .$$

So let us order the elements as we have above and put

$$g_1 = 0,\ g_2 = 1,\ g_3 = 2,\ g_4 = x,\ g_5 = x+1,\ g_6 = x+2,$$
$$g_7 = 2x,\ g_8 = 2x+1,\ g_9 = 2x+2 .$$

Then the type 1 matrix of ψ on X is

$$A = \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 0 & 1 & -1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 0 & 1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{bmatrix}$$

Let the function $\phi(x) = \begin{cases} 0 & x = 0 \\ 1 & x \in X \\ -1 & \text{otherwise} \end{cases}$ and $a_{ij} = \phi(g_i + g_j)$

define a type 2 matrix B . Then keeping the same ordering as above the type 2 matrix of ϕ on X is

$$B = \left[\begin{array}{rrr|rrr|rrr} 0 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 0 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ \hline -1 & 1 & -1 & -1 & -1 & 1 & 0 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 0 & 1 \\ \hline -1 & -1 & 1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 & -1 & -1 & 1 \end{array}\right]$$

LEMMA 2.10. *Suppose* G *is an additive abelian group of order* ν *with elements* $z_1, z_2, \ldots, z_\nu$. *Say* ϕ *and* ψ *are maps from* G *to a commutative ring* R. *Define*

$$A = (a_{ij}), \qquad a_{ij} = \phi(z_j - z_i),$$
$$B = (b_{ij}), \qquad b_{ij} = \psi(z_j - z_i),$$
$$C = (c_{ij}), \qquad c_{ij} = \mu(z_j + z_i).$$

Then (independently of the ordering of $z_1, z_2, \ldots, z_\nu$ *save only that it is fixed)*

(i) $C^T = C$,

(ii) $AB = BA$,

(iii) $AC^T = CA^T$.

Proof. (i) $c_{ij} = \mu(z_j+z_i) = \mu(z_i+z_j) = c_{ji}$.

(ii) $(AB)_{ij} = \sum_{g\in G} \phi(g-z_i)\psi(z_j-g)$

putting $h = z_i+z_j-g$, it is clear that as g ranges through G so does h, and the above equation becomes

$$\sum_{h\varepsilon G} \phi(z_j-h)\psi(h-z_i)$$

$$= \sum_{h\varepsilon G} \psi(h-z_i)\phi(z_j-h)$$

(since R is commutative); this is $(BA)_{ij}$.

(iii) $$(AC^T)_{ij} = \sum_{g\varepsilon G} \phi(g-z_i)\mu(z_j+g)$$

$$= \sum_{h\varepsilon G} \phi(h-z_j)\mu(z_i+h) \qquad (h = z_j+g-z_i)$$

$$= (CA^T)_{ij} .$$

COROLLARY 2.11. *If* X *and* Y *are type 1 matrices and* Z *is a type 2 matrix then*

$$XY = YX$$

$$XZ^T = ZX^T \quad .$$

LEMMA 2.12. *If* X *is a type* i, i = 1,2, *matrix then so is* X^T .

Proof. (i) If $X = (x_{ij}) = \phi(z_j+z_i)$ is type 2 then so is $X^T = (y_{ij}) = \phi(z_i+z_j)$.

(ii) If $X = (x_{ij}) = \psi(z_j-z_i)$ is type 1 then so is $X^T = (y_{ij}) = \mu(z_j-z_i)$ where μ is the map $\mu(z) = \psi(-z)$.

COROLLARY 2.13. *(i) If* X *and* Y *are type 1 matrices then*

$$XY = YX ,$$

$$X^TY = YX^T ,$$

$$XY^T = Y^TX ,$$
$$X^TY^T = Y^TX^T .$$

(ii) If P *is a type 1 matrix and* Q *is a type 2 matrix then*

$$PQ^T = QP^T ,$$
$$PQ = Q^TP^T ,$$
$$P^TQ^T = QP ,$$
$$P^TQ = Q^TP .$$

We note that if the additive abelian group in definition 2.7 is the integers modulo p with the usual ordering then

(i) the type 1 incidence matrix is circulant since $m_{ij} = \psi(j-i) = \psi(j-i+1-1) = m_{1,i-j+1}$

(ii) the type 2 incidence matrix is backcirculant since $n_{ij} = \psi(i+j) = \psi(i+j-1+1) = n_{1,i+j-1}$.

In any case:

a type 1 matrix is analogous to a circulant matrix;
a type 2 matrix is analogous to a backcirculant matrix.

All the theorems stated above remain true if for

"type 1" we substitute "circulant"

and for

"type 2" we substitute "backcirculant" .

LEMMA 2.14. *Let* $R = (r_{ij})$ *be the permutation matrix of order* n *, defined on an additive abelian group* $G = \{g_i\}$ *of order* n *by*

$$r_{\ell,j} = \begin{cases} 1 & \text{if } g_\ell + g_j = 0 , \\ 0 & \text{otherwise} . \end{cases}$$

Let M *by a type 1 matrix of a subset* $X = \{x_i\}$ *of* G *. Then* MR *is a type 2 matrix. In particular, if* G *is the set of integers modulo* n *then* MR *is a backcirculant matrix.*

Proof. Let $M = (m_{ij})$ be defined by $m_{ij} = \psi(g_j - g_i)$ where ψ maps G into a commutative ring. Let $\mu(-x) = \psi(x)$. Then MR is

$$(MR)_{ij} = \sum_k m_{ik} r_{kj} = m_{i\ell} \quad \text{where} \quad g_\ell + g_j = 0$$

$$\psi(g_\ell - g_i) = \psi(-g_j - g_i) = \mu(g_j + g_i)$$

which is a type 2 matrix.

NOTATION. By [A] we will mean the type 1 incidence matrix of the set A .

DEFINITION 2.15. If $M = (m_{ij})$ is a $m \times p$ matrix and $N = (n_{ij})$ is an $n \times q$ matrix, then the *Kronecker product* $M \times N$ is the $mn \times pq$ matrix given by

$$M \times N = \begin{bmatrix} m_{11}N & m_{12}N & \cdots & m_{1p}N \\ m_{21}N & m_{22}N & \cdots & m_{2p}N \\ \vdots & & & \\ m_{m1}N & m_{m2}N & \cdots & m_{mp}N \end{bmatrix}$$

LEMMA 2.16. *The following properties of Kronecker product follow immediately from the definition:*

(a) $p(M \times N) = (pM) \times N = M \times (pN) \qquad p$ *a scalar* ,

(b) $(M_1 + M_2) \times N = (M_1 \times N) + (M_2 \times N)$

(c) $M \times (N_1 + N_2) = M \times N_1 + M \times N_2$

(d) $(M_1 \times N_1)(M_2 \times N_2) = M_1M_2 \times N_1N_2$

(e) $(M \times N)^T = M^T \times N^T$

(f) $(M \times N) \times P = M \times (N \times P)$.

EXAMPLE. Let $M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $N = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$. Then

$$M \times N = \begin{bmatrix} N & N \\ N & -N \end{bmatrix} = \begin{bmatrix} -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \end{bmatrix}$$

3. *Baumert-Hall arrays.*

In 1944 Williamson [12] introduced a special type of Hadamard matrix

$$(3.1) \qquad H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

based on a matrix representation of the quaternions.

THEOREM 3.1. H *is an Hadamard matrix of order* $4m$ *whenever there exist four* ± 1 *matrices* A,B,C,D *of order* m *satisfying*

$$(3.2) \qquad XY^T = YX^T \quad , \qquad X,Y \in \{A,B,C,D\}$$

$$(3.3) \qquad AA^T + BB^T + CC^T + DD^T = 4mI_m \quad .$$

Baumert and Hall, see [1], in 1965 published the 12×12 array given in (3.4) .

$$(3.4) \qquad \left[\begin{array}{rrrrrrrrrrrr}
A & A & A & B & -B & C & -C & -D & B & C & -D & -D \\
A & -A & B & -A & -B & -D & D & -C & -B & -D & -C & -C \\
A & -B & -A & A & -D & D & -B & B & -C & -D & C & -C \\
B & A & -A & -A & D & D & D & C & C & -B & -B & -C \\
B & -D & D & D & A & A & A & C & -C & B & -C & B \\
B & C & -D & D & A & -A & C & -A & -D & C & B & -B \\
D & -C & B & -B & A & -C & -A & A & B & C & D & -D \\
-C & -D & -C & -D & C & A & -A & -A & -D & B & -B & -B \\
D & -C & -B & -B & -B & C & C & -D & A & A & A & D \\
-D & -B & C & C & C & B & B & -D & A & -A & D & -A \\
C & -B & -C & C & D & -B & -D & -B & A & -D & -A & A \\
-C & -D & -D & C & -C & -B & B & B & D & A & -A & -A
\end{array}\right]$$

This array contains precisely $3 \pm A$'s, $3 \pm B$'s, $3 \pm C$'s, $3 \pm D$'s in each row and column. Furthermore, its rows (hence also its columns) are formally orthogonal, in the sense that if the A,B,C,D are realized as any elements from a commutative ring then the distinct rows of the array are pairwise orthogonal. If the A,B,C,D are matrices which pairwise satisfy $XY^T = YX^T$ then

$$HH^T = I_{12} \times 3(AA^T + BB^T + CC^T + DD^T) .$$

More generally we consider

DEFINITION 3.2. A $4t \times 4t$ array of the indeterminates $\pm A$, $\pm B$, $\pm C$, $\pm D$ in which

(i) each indeterminate, $\pm X$, occurs precisely t times in each row and column, and

(ii) the distinct rows are formally orthogonal, in the sense that if the A, B, C, D are realized as any elements from a commutative ring then the distinct rows of the array are orthogonal, will be called a *Baumert-Hall array of order* t or BH[4t].

Then we have

THEOREM 3. *If there exist a Baumert-Hall array of order* t *and four* ± 1 *matrices* A,B,C,D *of order* m *satisfying*

$$XY^T = YX^T \quad , \qquad X,Y \in \{A,B,C,D\}$$
$$AA^T + BB^T + CC^T + DD^T = 4mI_m$$

then there exists an Hadamard matrix of order $4mt$.

Five years passed from the publication of the Baumert-Hall array of order 3 until Lloyd Welch (1971, unpublished) found his deceptively simple Baumert-Hall array of order 5, given in (3.5).

$$
\left(\begin{array}{rrrrr|rrrrr|rrrrr|rrrrr}
-D & B & -C & -C & -B & C & A & -D & -D & -A & -B & -A & C & -C & -A & A & -B & -D & D & -B \\
-B & -D & B & -C & -C & -A & C & A & -D & -D & -A & -B & -A & C & -C & -B & A & -B & -D & D \\
-C & -B & -D & B & -C & -D & -A & C & A & -D & -C & -A & -B & -A & C & D & -B & A & -B & -D \\
-C & -C & -B & -D & B & -D & -D & -A & C & A & C & -C & -A & -B & -A & -D & D & -B & A & -B \\
B & -C & -C & -B & -D & A & -D & -D & -A & C & -A & C & -C & -A & -B & -B & -D & D & -B & A \\
\hline
-C & A & D & D & -A & -D & -B & -C & -C & B & -A & B & -D & D & B & -B & -A & -C & C & -A \\
-A & -C & A & D & D & B & -D & -B & -C & -C & B & -A & B & -D & D & -A & -B & -A & -C & C \\
D & -A & -C & A & D & -C & B & -D & -B & -C & D & B & -A & B & -D & C & -A & -B & -A & -C \\
D & D & -A & -C & A & -C & -C & B & -D & -B & -D & D & B & -A & B & -C & C & -A & -B & -A \\
A & D & D & -A & -C & -B & -C & -C & B & -D & B & -D & D & B & -A & -A & -C & C & -A & -B \\
\hline
B & -A & -C & C & -A & A & B & -D & D & B & -D & -B & C & C & B & -C & A & -D & -D & -A \\
-A & B & -A & -C & C & B & A & B & -D & D & B & -D & -B & C & C & -A & -C & A & -D & -D \\
C & -A & B & -A & -C & D & B & A & B & -D & C & B & -D & -B & C & -D & -A & -C & A & -D \\
-C & C & -A & B & -A & -D & D & B & A & B & C & C & B & -D & -B & -D & -D & -A & -C & A \\
-A & -C & C & -A & B & B & -D & D & B & A & -B & C & C & B & -D & A & -D & -D & -A & -C \\
\hline
-A & -B & -D & D & -B & B & -A & C & -C & -A & C & A & D & D & -A & -D & B & C & C & -B \\
-B & -A & -B & -D & D & -A & B & -A & C & -C & -A & C & A & D & D & -B & -D & B & C & C \\
D & -B & -A & -B & -D & -C & -A & B & -A & C & D & -A & C & A & D & C & -B & -D & B & C \\
-D & D & -B & -A & -B & C & -C & -A & B & -A & D & D & -A & C & A & C & C & -B & -D & B \\
-B & -D & D & -B & -A & -A & C & -C & -A & B & A & D & D & -A & C & B & C & C & -B & -D
\end{array}\right) \tag{3.5}
$$

The author believes that Turyn has used this Welch array to allow certain Baumert-Hall arrays of order t to be multiplied by 5 to obtain a Baumert-Hall array of order 5t . We note that Welch's array is based on five 5×5 matrices:

$$I, \quad W_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & - \\ - & 0 & 1 & 0 & 0 \\ 0 & - & 0 & 1 & 0 \\ 0 & 0 & - & 0 & 1 \\ 1 & 0 & 0 & - & 0 \end{bmatrix}, \quad W_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$W_3 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \quad W_4 = \begin{bmatrix} 0 & 0 & 1 & - & 0 \\ 0 & 0 & 0 & 1 & - \\ - & 0 & 0 & 0 & 1 \\ 1 & - & 0 & 0 & 0 \\ 0 & 1 & - & 0 & 0 \end{bmatrix}$$

which satisfy for $n = 5$

$$(3.6) \qquad \begin{cases} W_1^T = -W_1,\ W_2^T = W_2,\ W_3^T = W_3,\ W_4^T = -W_4, \\ W_1W_1^T + W_2W_2^T = W_3W_3^T + W_4W_4^T = (n-1)I_n \ . \end{cases}$$

If circulant $(0,1,-1)$ matrices satisfying (3.6) can be found for other n than 5 then it will be possible to use Turyn's construction to multiply the orders of some Baumert-Hall arrays by these other n .

Shortly after Welch's matrix was discovered Jennifer Wallis [10] and Richard J. Turyn [9] independently announced that a construction of Goethals and Seidel [3] was important in finding Baumert-Hall arrays. Their theorem is

THEOREM 3.4. (Goethals and Seidel) *If* X, Y, Z, W *are square circulant* $(1,-)$ *matrices of order* t , *if* $U = X - I$ *is skew symmetric, and if*

$$XX^T + YY^T + ZZ^T + WW^T = 4tI_t$$

then

$$(3.7) \qquad GS = \begin{bmatrix} X & YR & ZR & WR \\ -YR & X & -W^TR & Z^TR \\ -ZR & W^TR & X & -Y^TR \\ -WR & -Z^TR & Y^TR & X \end{bmatrix}$$

is a skew-Hadamard matrix of order 4t *when* $R = (r_{ij})$ *of order* n *given by*

$$r_{ij} = \begin{cases} 1 & j = t + 1 - i \\ 0 & \text{otherwise} . \end{cases}$$

Wallis and Whiteman [11] showed how a similar matrix may be defined using an additive abelian group G .

THEOREM 3.5 (Wallis and Whiteman). *Let* X, Y, W *be type 1* (1,-) *incidence matrices and* Z *be a type 2* (1,-) *incidence matrix defined on the same additive abelian group of order* t. *If*

$$XX^T + YY^T + ZZ^T + WW^T = 4tI_t$$

then

$$(3.8) \qquad H = \begin{bmatrix} X & Y & Z & W \\ -Y^T & X^T & -W & Z \\ -Z & W^T & X & -Y^T \\ -W^T & -Z & Y & X^T \end{bmatrix}$$

is an Hadamard matrix of order 4t . *Further if* X - I *is skew,* H *is a skew-Hadamard matrix.*

We illustrate the use of the Goethals-Seidel array in constructing Baumert-Hall arrays: Suppose X, Y, Z, W are of order t and have elements which are (1,-) matrices A, B, C, D of order m which satisfy

$$
(3.9) \qquad \begin{cases} MN^T = NM^T \ , \quad M,N \quad A,\ B,\ C,\ D \\ AA^T + BB^T + CC^T + DD^T = 4mI_m \end{cases}
$$

and that

$$
(3.10) \qquad XX^T + YY^T + ZZ^T + WW^T = tI_t \times (AA^T + BB^T + CC^T + DD^T) \ .
$$

Then X, Y, Z, W may be used in GS to form a Baumert-Hall array of order t and an Hadamard matrix of order $4mt$.

Example: $t = 3$, use

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

$$
Z = \begin{bmatrix} C & D & -A \\ -A & C & D \\ D & -A & C \end{bmatrix} , \qquad W = \begin{bmatrix} D & A & -B \\ -B & D & A \\ A & -B & D \end{bmatrix}
$$

then provided (3.9) is satisfied (3.10) is satisfied and we have the following Baumert-Hall array of order 3

$$
\begin{array}{ccc|ccc|ccc|ccc}
A & B & C & B & -C & D & C & D & -A & D & A & -B \\
C & A & B & -C & D & B & D & -A & C & A & -B & D \\
B & C & A & D & B & -C & -A & C & D & -B & D & A \\
\hline
-B & C & -D & A & B & C & -D & B & -A & C & -A & D \\
C & -D & -B & C & A & B & B & -A & -D & -A & D & C \\
-D & -B & C & B & C & A & -A & -D & B & D & C & -A \\
\hline
-C & -D & A & D & -B & A & A & B & C & -B & -D & C \\
-D & A & -C & -B & A & D & C & A & B & -D & C & -B \\
A & -C & -D & A & D & -B & B & C & A & C & -B & -D \\
\hline
-D & -A & B & -C & A & -D & B & D & -C & A & B & C \\
-A & B & -D & A & -D & -C & D & -C & B & C & A & B \\
B & -D & -A & -D & -C & A & -C & B & D & B & C & A
\end{array}
$$

Example: t = 5, use

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

$$
Z = \begin{bmatrix} -C & D & D & A & -A \\ -A & -C & D & D & A \\ A & -A & -C & D & D \\ D & A & -A & -C & D \\ D & D & A & -A & -C \end{bmatrix}, \quad
W = \begin{bmatrix} -D & -C & -C & B & -B \\ -B & -D & -C & -C & B \\ B & -B & -D & -C & -C \\ -C & B & -B & -D & -C \\ -C & -C & B & -B & -D \end{bmatrix}
$$

then provided (3.9) is satisfied (3.10) is also satisfied and we can use the array GS to get a Baumert-Hall array of order 5 .

We note that the example for $t = 3$ uses the matrices

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

$$T^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

and

$$X = I \times A + T \times B + T^2 \times C$$

$$Y = I \times B + T \times -C + T^2 \times D$$

$$Z = I \times C + T \times D + T^2 \times -A$$

$$W = I \times D + T \times A + T^2 \times -B ,$$

while the example for $t = 5$ uses the matrices

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$R = \begin{bmatrix} 0 & 0 & 0 & 1 & - \\ - & 0 & 0 & 0 & 1 \\ 1 & - & 0 & 0 & 0 \\ 0 & 1 & - & 0 & 0 \\ 0 & 0 & 1 & - & 0 \end{bmatrix}$$

and

$$X = I \times A + S \times B + R \times C$$
$$Y = I \times -B + S \times A + R \times -D$$
$$Z = I \times -C + S \times D + R \times A$$
$$W = I \times -D + S \times -C + R \times B \quad .$$

Three examples illustrate the following result.

THEOREM 3.6 (Joan Cooper and Jennifer Wallis). *Suppose there exist four type 1* $(0,1,-)$ *matrices* X_1, X_2, X_3, X_4 *of order* t *, defined on the same abelian group* G *of order* t *, such that each of the* t^2 *positions is nonzero in precisely one of the* X_i *and that*

$$X_1X_1^T + X_2X_2^T + X_3X_3^T + X_4X_4^T = tI_t \ .$$

Further suppose that A, B, C, D *satisfy* $MN^T = NM^T$ *and let*

$$X = X_1 \times A \ + \ X_2 \times B \ + \ X_3 \times C \ + \ X_4 \times D$$
$$Y = X_1 \times -B \ + \ X_2 \times A \ + \ X_3 \times D \ + \ X_4 \times -C$$
$$Z = (X_1 \times -C \ + \ X_2 \times -D \ + \ X_3 \times A \ + \ X_4 \times B)R$$
$$W = X_1 \times -D \ + \ X_2 \times C \ + \ X_3 \times -B \ + \ X_4 \times A$$

with $R = (r_{ij})$ *defined on the elements of* G, $g_1,g_2,\ldots,g_t$ *by*

$$r_{\ell,j} = \begin{cases} 1 & \text{if } g_\ell + g_j = 0 \\ 0 & \text{otherwise} \end{cases} \quad . \tag{3.11}$$

Then (3.8) *gives a Baumert-Hall array of order* $4t$.

We note from the preceding examples that for $t = 3$:

$$IJ + TJ + T^2J = J + J + J = aJ + bJ + cJ$$
$$\text{and} \quad a^2 + b^2 + c^2 = t = 3 \ ;$$

$t = 5$:

$$IJ + SJ + RJ = J + 2J + 0J = aJ + bJ + cJ$$

$$\text{and} \quad a^2 + b^2 + c^2 = t = 5 .$$

THEOREM 3.7 (Joan Cooper and Jennifer Wallis). *Suppose there exist four* $(0,1,-)$ *matrices* X_1, X_2, X_3, X_4 *of order* t *and such that each of the* t^2 *positions is nonzero in precisely one of the* X_i *and for which*

$$X_1X_1^T + X_2X_2^T + X_3X_3^T + X_4X_4^T = tI_t \quad .$$

Further let x_i *be the number of positive elements and* y_i *be the number of negative elements in each row and column of* X_i . *Then*

(a) $x_1 + x_2 + x_3 + x_4 + y_1 + y_2 + y_3 + y_4 = n$,

(b) $(x_1-y_1)^2 + (x_2-y_2)^2 + (x_3-y_3)^2 + (x_4-y_4)^2 = n$.

Proof. (a) is immediate from the suppositions. Now

$$X_i^TJ = (x_i-y_i)J = JX_i$$

so consider

$$\sum_{i=1}^{4} JX_iX_i^TJ = t^2J$$

$$= \sum_{i=1}^{4} (x_i-y_i)^2tJ \; .$$

Equating coefficients we have (b) .

LEMMA 3.8 (Joan Cooper and Jennifer Wallis). *There exist Baumert-Hall arrays of order* $t \in \{x: x$ is an odd integer, $1 \le x \le 19\}$.

Proof. In table 1 sets of elements g_i from the cyclic group of order t are given, and to some of the g_i a sign - is attached. This sign does *not* indicate inverse in the cyclic group. Rather, for each set one forms the circulant (type 1) incidence matrix of the subset of elements which are not preceded by - , and subtracts from it the circulant (type 1) incidence matrix of the subset of elements which are preceded by minus. The four matrices thus formed should be used in theorem 3.6 to obtain the result.

t		X_1, X_2, X_3, X_4
3	$1^2+1^2+1^2+0^2$	{1}, {2}, {3}
5	$2^2+1^2+0^2+0^2$	{1,2}, {5}, {3,-4}
7	$2^2+1^2+1^2+1^2$	{1,2}, {5}, {3,6,-7}, {4}
		or
		{1,-2,-3,-5}, {4}, {6}, {7}
9	$2^2+2^2+1^2+0^2$	{1,6}, {2,8}, {9}, {3,4,-5,-7}
	$3^2+0^2+0^2+0^2$	{1,2,7}, {3,-9}, {4,-8},{5,-6}
11	$3^2+1^2+1^2+0^2$	{1,5,7,8,-9}, {11}, {2,3,-4,-6,10}
13	$3^2+2^2+0^2+0^2$	{1,7,9}, {4,5,8,-10}, {-2,-3,6,11,-12,13}
		or
		{1,3,9}, {2,5,6,-13}, {4,-7,-8,10,-11,12}
	$2^2+2^2+2^2+1^2$	{1,5}, {3,4,-6,-9,10,12}, {7,13}, {-2,8,11}
		or
		{1,2,5,-9}, {3,4,-6,10,-11,12}, {7,13}, {8}
15	$3^2+2^2+1^2+1^2$	{1,2,6}, {8,9}, {10,-11,-13}, {-3,-4,5,7,12,14,-15}
17	$4^2+1^2+0^2+0^2$	{1,4,8,16}, {2,13,-15}, {9,-17},{3,5,-6,-7,-10,-11,12,14}
		or
		{1,5,10,12}, {3,4,-9}, {8,-15}, {2,-6,-7,11,-13,14,16,-17}
		or
		{1,2,-3,-4,-5,-6,-9,-14,15,-16}, {10,11,-17}, {7,-8}, {12,-13}
19	$3^2+3^2+1^2+0^2$	{1,2,13}, {7,11,17}, {4,-9,-12,-14,15,16,18}, {3,5,-6,8,-10,-19}

TABLE 1

LEMMA 3.9 (David Hunt and Jennifer Wallis). *There exist Baumert-Hall arrays of order* $t \in \{13, 19, 25, 31, 37, 41\}$.

Proof. Let x be a primitive root of $GF(q)$ where $q = p^\alpha = ef + 1$ is a prime power. Write $G = \langle x \rangle \backslash \{0\}$. The *cyclotomic classes* C_i in $GF(q)$ are:

$$C_i = \{x^{es+i} : s = 0,1,\dots,f-1\} \qquad i = 0,1,\dots,e-1$$

We note the C_i are pairwise disjoint and their union is G.

We write $[C_a]$ for the incidence matrix of C_a and define the incidence matrix of $C_a \sim C_b$ and $C_a \& C_b$ by

$$[C_a \sim C_b] = [C_a] - [C_b] , \quad \text{and}$$

$$[C_a \& C_b] = [C_a] + [C_b] .$$

The results of [6] may be used, or direct calculation, to show the matrices in table 2 give four matrices which can be used in theorem 3.6 to obtain the result.

t		X_1, X_2, X_3, X_4
$13=4.3+1$	$3^2+2^2+0^2+0^2$	$[C_0]$, $[C_1\sim\{0\}]$, $[C_2\sim C_3]$, $[\phi]$
$19=6.3+1$	$3^2+3^2+1^2+0^2$	$[C_0]$, $[C_2]$, $[\{0\} \& C_3\sim C_4]$, $[C_1\sim C_5]$
$25=8.3+1$	$5^2+0^2+0^2+0^2$	$[C_0 \& C_5\sim\{0\}]$, $[C_1\sim C_7]$, $[C_2\sim C_3]$, $[C_4\sim C_6]$
$31=10.3+1$	$3^2+3^2+3^2+2^2$	$[C_0 \& C_3\sim C_2]$, $[C_4 \& C_5\sim C_9]$, $[C_7 \& C_8\sim C_6]$, $[C_1\sim\{0\}]$
$37=12.3+1$	$6^2+1^2+0^2+0^2$	$[C_0 \& C_1\sim C_2\sim C_3 \& C_4 \& C_5]$, $[\{0\}]$, $[C_6\sim C_7 \& C_8\sim C_9 \& C_{10}\sim C_{11}]$, $[\phi]$
$41=8.5+1$	$5^2+4^2+0^2+0^2$	$[C_0\sim C_2\sim C_3]$, $[C_4 \& C_6\sim C_1\sim\{0\}]$, $[C_5\sim C_7]$, $[\phi]$

TABLE 2

The following results have also been reported:

LEMMA 3.11 (Richard J. Turyn). *There exist Baumert-Hall arrays of order* t *and* $5t$ *for* $t \in \{i : i = 1 + 2^a 10^b 26^c$, a, b, c *non-negative integers,* <u>*or*</u> $i \leq 59\}$.

4. *Williamson Type Matrices*

Repeatedly in section 3 we have desired to form four (1,-) matrices A, B, C, D of order in which pairwise satisfy

$$(4.1) \quad \begin{cases} \text{(i)} \quad MN^T = NM^T, \\ \text{and (ii)} \quad AA^T + BB^T + CC^T + DD^T = 4mI_m, \end{cases}$$

Williamson first used such matrices and this is why we call them *Williamson type.* The matrices Williamson used were both circulant and symmetric but we will show neither the circulant nor symmetric properties are necessary.

The following theorem is a summary of the results contained in the table of Marshall Hall Jr [5] or Wallis, Street and Wallis [12; pp 388-389]. The results are mainly due to Williamson but some are due to Baumert, Golomb and Hall.

THEOREM 4.1. *There exist four circulant, symmetric (1,-) matrices A, B, C, D of order m satisfying (4.1) for*

$$m \in \{1, 3, 5, 7, \ldots, 29, 37, 43\}.$$

We note that the condition that the four matrices are circulant and symmetric reduces the condition $MN^T = NM^T$ to

$$MN = NM$$

which is satisfied because A, B, C, D are all polynomials in the matrix F of order m given by (4.2)

(4.2)
$$F = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix} .$$

We now use a result of Goethals and Seidel which is most valuable.

THEOREM 4.2 (Goethals and Seidel). *Let* $q \equiv 1 (\mathrm{mod}\ 4)$ *be a prime power, then there exists a square matrix* P *of order* $q + 1$ *with diagonal elements* 0 *and all other elements* ± 1 *such that*

(4.3)
$$PP^T = qI_{q+1} \quad \textit{and} \quad P = \begin{bmatrix} R & S \\ S & -R \end{bmatrix}$$

where R, S *are symmetric circulants.*

Proof. Any linear mapping $u\colon V \to V$ satisfies

$$\det (u(x), u(y)) = \det u . \det (x,y)$$

for all $x, y \in V$. We define linear mappings v and w, which will be used in the proof of the theorem. Let z be any primitive element of $GF(q^2)$, the quadratic extension of $GF(q)$. We choose any basis in V. With respect to this basis, v is defined by the matrix

$$(v) = \tfrac{1}{2}\begin{bmatrix} z^{q-1} + z^{1-q} & (z^{q-1} - z^{1-q})z^{\frac{1}{2}(q+1)} \\ (z^{q-1} - z^{1-q})z^{-\frac{1}{2}(q+1)} & z^{q-1} + z^{1-q} \end{bmatrix},$$

which has its elements in $GF(q)$. Then $\det(v) = 1$ and the eigenvalues of v are z^{q-1} and z^{1-q}, both elements of $GF(q^2)$ whose $\frac{1}{2}(q+1)$th power, and no smaller, belongs to $GF(q)$. Hence v acts on $PG(1,q)$ as a permutation with period $\frac{1}{2}(q+1)$, without fixed points, ~~which divides the points,~~ which divides the points of $PG(1,q)$ into two sets of transitivity each containing $\frac{1}{2}(q+1)$ points. In addition, w is defined by the matrix

$$(w) = \begin{bmatrix} 0 & z^{q+1} \\ 1 & 0 \end{bmatrix}.$$

Then $\chi \det(w) = -\chi(-1)$. The eigenvalues of w are $\pm z^{\frac{1}{2}(q+1)}$, elements of $GF(q^2)$ whose square is in $GF(q)$. Hence w acts on $PG(1,q)$ as a permutation with period 2, which maps any point of one set of transitivity, defined above by v, into the other set. Indeed, for $i = 1, \ldots, \frac{1}{2}(q+1)$, the mapping $v^i w$ has no eigenvalue in $GF(q)$. Finally note $vw = wv$.

Represent the $q+1$ points of $PG(1,q)$ by the following $q+1$ vectors in V:

$$x, v(x), v^2(x), \ldots, v^{\frac{1}{2}(q-1)}(x), w(x), vw(x), v^2w(x), \ldots, v^{\frac{1}{2}(q-1)}w(x).$$

Observing that, for $i,j = 0,1,\ldots,\frac{1}{2}(q-1)$,

$\det(v^i w(x), v^j w(x)) = \det(w) \cdot \det(v^i(x), v^j(x)$
$= \det(w) \cdot \det(x, v^{j-i}(x)),$

$$\det (v^i(x), v^j w(x)) = -\det (v^i w(x), v^j(x)) = \det (v^j(x), v^i w)x)),$$
$$\det (v^i(x), v^j(x)) = -\det (v^{\frac{1}{2}(q+1)+i}(x), v^j(x)),$$

we conclude that the matrix P belonging to these vectors given by (2.4) has the desired form.

(4.4) $$P = [\chi \det (x_i, x_j)].$$

with χ the usual quadratic character (see, for example, [12]).
EXAMPLE (with thanks to L.D. Baumert).

Let $q = 5$, $p = 3$ and let α be a root of $x^2 + x + 2 = 0$ [a primitive polynomial over $GF(5)$], and consider

$$\alpha, \alpha^5, \ldots, \alpha^{4p-3}, \alpha^{p+1}, \alpha^{p+5}, \ldots, \alpha^{5p-3} .$$

We can take $x_0, \ldots, x_5$ as

$$\alpha = \begin{pmatrix}1\\0\end{pmatrix}, \alpha^5 = 4\alpha + 4 = \begin{pmatrix}4\\4\end{pmatrix}, \alpha^9 = 3\alpha + 4 = \begin{pmatrix}3\\4\end{pmatrix}, \alpha^4 = 3\alpha + 2 = \begin{pmatrix}3\\2\end{pmatrix},$$
$$\alpha^8 = 3\alpha + 1 = \begin{pmatrix}3\\1\end{pmatrix}, \alpha^{12} = 4 = \begin{pmatrix}0\\4\end{pmatrix}.$$

Since $\chi(1) = \chi(4) = 1$ and $\chi(2) = \chi(3) = -1$,

$$\det (x_i, x_j) = \left[\begin{array}{ccc|ccc} 0 & 4 & 4 & 2 & 1 & 4 \\ 1 & 0 & 4 & 1 & 2 & 1 \\ 1 & 1 & 0 & 4 & 1 & 2 \\ \hline 3 & 4 & 1 & 0 & 2 & 2 \\ 4 & 3 & 4 & 3 & 0 & 2 \\ 1 & 4 & 3 & 3 & 3 & 0 \end{array}\right] \quad \text{and}$$

$$P = [\chi \det (x_i, x_j)] = \left[\begin{array}{ccc|ccc} 0 & 1 & 1 & - & 1 & 1 \\ 1 & 0 & 1 & 1 & - & 1 \\ 1 & 1 & 0 & 1 & 1 & - \\ \hline - & 1 & 1 & 0 & - & - \\ 1 & - & 1 & - & 0 & - \\ 1 & 1 & - & - & - & 0 \end{array}\right]$$

Then Turyn noted

THEOREM 4.3 (Richard J. Turyn) *Let* R *and* S *be the matrices of order* $\frac{1}{2}(p+1)$, $p \equiv 1 \pmod 4$ *a prime power, of theorem 4.3. Then*

$$I + R,\ I - R,\ S, S$$

are four circulant, symmetric, (1,-) matrices which pairwise satisfy

$$MN^T = NM^T$$

$$\textit{and} \quad (I+R)^2 + (I-R)^2 + S^2 + S^2 = 2(p+1)\, I_{\frac{1}{2}(p+1)} \ .$$

An alternate proof to the theorem of Goethals and Seidel and Turyn has been found by A.L. Whiteman [13].

Turyn has also noted the following result announced in [9]:

THEOREM 4.4 (Richard J. Turyn). *There exist four symmetric (1,-) matrices* A,B,C,D *of order* $m = 9^a$, $a = 0, 1, 2, \ldots$ *which pairwise satisfy*

$$MN^T = NM^T$$

and for which

$$AA^T + BB^T + CC^T + DD^T = 4mI_m.$$

Finally we observe that

THEOREM 4.5 (Jennifer Wallis) *Let $p \equiv 1 \pmod 4$ be a prime power then there exist four $(1,-)$ matrices A, B, C, D of order $\frac{1}{2}p(p+1)$ which pairwise satisfy*

$$MN^T = NM^T$$

and for which

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

Proof.

The matrices R, S of theorems 4.2 and 4.3 satisfy

$$R^T = R,\ S^T = S,\ I + R^2 + S^2 = (p+1)I_{\frac{1}{2}(p+1)}$$

For p a prime power, it is well known, see for example [12; p 291], that if the elements $a_0, a_1, \ldots, a_{p-1}$ are ordered in some way and χ is the quadratic character then

$$Q = [\chi(a_j - a_i)]$$

has zero diagonal and other elements ± 1 and satisfies

$$QQ^T = pI - J,\quad QJ = JQ = 0,\ Q^T = (-1)^{\frac{1}{2}(p-1)}Q.$$

Let $X = I + Q$ and $Y = -I + Q$, then X, Y are

(1,-) matrices satisfying $X^T = X$, $Y^T = Y$, $XJ = J = -YJ$, $XY^T = YX^T$ and

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

Consider

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

It is easy to verify that $MN^T = NM^T$ for $M, N \varepsilon \{A,B,C,D\}$ and the result follows by noting

$$\begin{aligned} AA^T + BB^T + CC^T + DD^T &= 2I\times pJ + S^T\times(JX^T + JY^T) + S\times(XJ + YJ) + (SS^T + RR^T)\times(XX^T + YY^T) \\ &= 2pI\times J + pI\times 2(p + 1)I + pI\times 2J \\ &= 2p(p + 1)I_{\frac{1}{2}p(p + 1)}. \end{aligned}$$

We note the matrices A,B,C,D we have just constructed were symmetric but not circulant. We will now indicate another construction for the X and Y of the proof which will not yield symmetric matrices:

LEMMA 4.6 (Jennifer Wallis). *Let $p \equiv 5 \pmod 8$ be a prime power then there exist four (1,-) matrices A,B,C,D of order $\frac{1}{2}p(p + 1)$ which pairwise satisfy*

$$MN^T = NM^T$$

for which

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

but which are neither circulant nor symmetric.

Proof. We use a construction of Szekeres [12; p. 321]. Let x be a primitive root of $GF(p)$ and consider the cyclotomic classes of $p = 4f + 1$ (f odd) defined by

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

Then we take (using notation given previously)

$$P = [C_0 \mathbin{\&} C_1 \sim C_2 \sim C_3], \quad Q = [C_0 \sim C_1 \sim C_2 \mathbin{\&} C_3].$$

$-1 \varepsilon C_2$ so $P^T = -P$, $Q^T = -Q$. Further

$$\begin{aligned} PP^T + QQ^T &= 2 \sum_{i=0}^{3} [C_i][C_i]^T - \sum_{i=0}^{3} [C_i][C_{i+2}]^T \\ &= 2(f-1)(J-I) + 8fI - 2f(J-I) \quad \text{using results of [6]} \\ &= (8f+2)I - 2J. \end{aligned}$$

Let $X = P + I$ and $Y = (Q - I)V$ where V is the R is given by (3.11).
Then $XY^T = YX^T$ as X is type 1 and Y is type 2 (see lemmas 2.13 and 2.14).

$$XJ = PJ + J = J, \qquad YJ = QVJ - QJ = -J \quad \text{and}$$

$$\begin{aligned} XX^T + YY^T &= (P + I)(P + I)^T + (Q - I)VV^T(Q - I)^T \\ &= PP^T + I + QQ^T + I \\ &= (8f + 4)I - 2J \\ &= 2(p + 1)I - 2J . \end{aligned}$$

Now A, B, C, D may be constructed as in theorem 4.5 since $p \equiv 1 \pmod 4$ and the R and S of theorems 4.2 and 4.3 exist, but $X^T \neq X$ so A and B are not symmetric.

5. *Conclusion.*

We summarize the results quoted in this paper.

THEOREM 5.1. *If there exists a Baumert-Hall array of order* t *and four* (1,-) *matrices* A, B, C, D *of order* m *which*

(5.1)
(i) *pairwise satisfy* $MN^T = NM^T$, *and*
(ii) *satisfy* $AA^T + BB^T + CC^T + DD^T = 4mI_m$

then there is an Hadamard matrix of order 4mt .

THEOREM 5.2. *There exist Baumert-Hall arrays of order* t *and* 5t *for*

(5.2)
(i) $t \in \{1, 3, 5, \ldots, 59\}$,
(ii) $t \in \{i : i = 1 + 2^a 10^b 26^c$, a, b, c, *non-negative integers*$\}$.

THEOREM 5.3. *There exist Williamson type matrices* A, B, C, D *or order* m , *which are* (1,-) *matrices satisfying* (5.1) *for*

(5.3)
(i) $m \in \{1, 3, 5, \ldots, 29, 37, 43\}$,
(ii) $m = \frac{1}{2}(p+1)$, $p \equiv 1 \pmod 4$, *a prime power* ,
(iii) $m = \{9^a$, $a = 0, 1, \ldots\}$,
(iv) $m = \frac{1}{2}p(p+1)$, $p \equiv 1 \pmod 4$, *a prime power* .

REFERENCES

[1] L. D. Baumert and Marshall Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* 71 (1965), 169-170.

[2] Joan Cooper and Jennifer Wallis, A construction for Hadamard arrays, *Bull. Austral. Math. Soc.* 7 (1972), 269-278.

[3] J. M. Goethals and J. J. Seidel, A skew-Hadamard matrix of order 36, *J. Austral. Math. Soc.* 11 (1970), 343-344.

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

[5] Marshall Hall, Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.

[6] David C. Hunt and Jennifer Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, (to appear).

[7] Richard J. Turyn, An infinite class of Williamson matrices, *J. Combinatorial Theory* (series A), 12 (1972), 319-321.

[8] Richard J. Turyn, The computation of certain Hadamard matrices, *Notices. Amer. Math. Soc.*, 20 (1973), A-2.

[9] Richard J. Turyn, Hadamard matrices, algebras, and composition theorems, *Notices Amer. Math. Soc.*, 19 (1972), A-388.

[10] Jennifer Wallis, Hadamard matrices of order 28m, 36m, and 44m, *J. Combinatorial Theory*, (series A), (to appear).

[11] Jennifer Wallis and Albert Leon Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.*, 7 (1972), 233-249.

[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* (series A), (to appear).

[14] John Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.*, 11 (1964), 65-81.