Cyclotomy, Hadamard arrays and supplementary difference sets

David C. Hunt

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

Abstract

A 4n x 4n Hadamard array, H, is a square matrix of order 4n with elements ± A, ± B, ± C, ± D each repeated n times in each row and column. Assuming the indeterminates A, B, C, D commute, the row vectors of H must be orthogonal. These arrays have been found for n = 1 (Williamson, 1944), n = 3 (Baumert-Hall, 1965), n = 5 (Welch, 1971), and some other odd n < 43 (Cooper, Hunt, Wallis).

The results for n = 25, 31, 37, 41 are presented here, as is a result for n = 9 not based on supplementary difference sets. This gives the following new orders for Hadamard matrices < 4000: 1804, 3404, 3596, 3772. These results were obtained by using an adaption of cyclotomy which allows the product of incidence matrices to be easily derived. This adaption is developed and the constructions shown for some families of supplementary difference sets.

CYCLOTOMY, HADAMARD ARRAYS AND SUPPLEMENTARY DIFFERENCE SETS

David C. Hunt and Jennifer Wallis*

University of New South Wales, Kensington, N.S.W., 2033, Australia

and

University of Newcastle, N.S.W., 2308, Australia

ABSTRACT

A $4n \times 4n$ Hadamard array, H, is a square matrix of order 4n with elements $\pm A$, $\pm B$, $\pm C$, $\pm D$ each repeated n times in each row and column. Assuming the indeterminates A, B, C, D commute, the row vectors of H must be orthogonal. These arrays have been found for $n = 1$ (Williamson, 1944), $n = 3$ (Baumert-Hall, 1965), $n = 5$ (Welch, 1971), and some other odd $n < 43$ (Cooper, Hunt, Wallis).

The results for $n = 25, 31, 37, 41$ are presented here, as is a result for $n = 9$ not based on supplementary difference sets. This gives the following new orders for Hadamard matrices < 4000: 1804, 3404, 3596, 3772. These results were obtained by using an adaption of cyclotomy which allows the product of incidence matrices to be easily derived. This adaption is developed and the constructions shown for some families of supplementary difference sets.

---

* This paper was prepared while this author was a Post-doctoral Fellow in Statistics at the University of Waterloo, Canada.

PROC. SECOND MANITOBA CONFERENCE ON
NUMERICAL MATH., 1972, pp. 351 - 381.

1. INTRODUCTION AND DEFINITIONS

We use I for the identity matrix and J for the matrix with every element + 1, and the order, unless specifically stated, should be determined from the context. We sometimes use brackets, [ ], to denote matrices and H^T denotes H transposed.

Let $S_1, S_2, \ldots, S_n$ be subsets of V, a finite abelian group of order v written in additive notation, 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 of V a fixed number of times, λ say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ <u>supplementary difference sets</u>.

The parameters of $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets satisfy

$$\lambda(v-1) = \sum_{i=1}^{n} k_i(k_i-1). \tag{1}$$

If $k_1 = k_2 = \ldots = k_n = k$ we will write $n - \{v; k; \lambda\}$ to denote the n supplementary difference sets and (1) becomes

$$\lambda(v-1) = nk(k-1). \tag{2}$$

We shall be concerned with collections, (denoted by square brackets $[\![\ ]\!]$) defined on a fixed group V or order v, in which repeated elements are counted multiply, rather than with sets (denoted by braces { }). If T_1 and T_2 are two collections then T_1 and T_2 will denote the result of adjoining the elements of T_1 to T_2 with total multiplicities retained. For example: $x_1, x_2, x_3, \in V$ and $T_1 = [\![x_1, x_2, x_3,]\!]$, $T_2 = [\![x_1, x_2, x_4]\!]$ then

$$T_1 \,\&\, T_2 = [\![x_1, x_1, x_2, x_2, x_3, x_3]\!]. \tag{3}$$

The <u>class product</u> or <u>join</u> (see Storer [12] p. 3) of two collections T_1 and T_2 will be denoted by $T_1 \wedge T_2$, which is defined as

$$T_1 \wedge T_2 = [\![x_1 + x_2 : x_1 \in T_1, x_2 \in T_2]\!], \qquad T_1, T_2 \subset V. \tag{4}$$

Suppose $x_1, x_2, \ldots, x_v$ are the elements of V ordered in some fixed way. Let X be a subset of V. Further let ϕ and ψ be two maps from V into a commutative ring with unity (1). Then $M = [m_{ij}]$ is defined by

$$m_{ij} = \psi(x_j - x_i) \tag{5}$$

will be called type 1 and $N = [n_{ij}]$ defined by

$$n_{ij} = \phi(x_j + x_i) \tag{6}$$

will be called type 2.

If ϕ and ψ are defined by

$$\phi(x) = \psi(x) = \begin{cases} 1 & x \in X, \\ 0 & x \notin X, \end{cases} \tag{7}$$

then M and N will be called the type 1 incidence matrix of X (in V) and the type 2 incidence matrix of X (in V), respectively. While if ϕ and ψ are defined by

$$\phi(x) = \psi(x) = \begin{cases} 1 & x \in X, \\ -1 & x \notin X, \end{cases} \tag{8}$$

M and N will be called the type 1 (1, -1) matrix of X and the type 2 (1, -1) matrix of X respectively. M and N are of order $|V|$. These are discussed further in [20] and [21].

We note that there exists an $R = [r_{ij}]$ defined by

$$r_{ij} = \begin{cases} 1 & \text{if } x_i + x_j = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{9}$$

such that if M is the type 1 matrix of X, MR is a type 2 matrix.

Write $\#(x)$ for the number of times x occurs in the collection X. Define the type 1 incidence matrix, $[X] = [z_{ij}]$ of X by

$$z_{ij} = \#(x_j - x_i). \tag{10}$$

It is proved in [4] that is X and Y are collections of elements from the same abelian group V then, where the left hand side is the matrix multiplication of the two matrices:

(11) $$[X]\,[Y] = [X \wedge Y]\ .$$

An Hadamard matrix H of order h has every element + 1 or − 1 and satisfies $H\,H^T = h\,I_h$. It is shown in [20] that

(12) $$4 - \{v;\ k_1,\ k_2,\ k_3,\ k_4;\ \sum_{i=1}^{4} k_i - v\}\ \text{supplementary}$$

difference sets yield an Hadamard matrix of order 4v; and in [21] that

(13) $$4 - \{v;\ k_1,\ k_2,\ k_3,\ k_4;\ \sum_{i=1}^{4} k_i - v - 1\}\ \text{supplementary}$$

differences sets necessarily have each $k_i = m$ or $m + 1$ for $v = 2m + 1$ and $k_1 = m \pm 1$, $k_2 = k_3 = k_4 = m$ for $v = 2m$ and yield an Hadamard matrix of order $4(v+1)$.

The Hadamard product, *, of two matrices $A = [a_{ij}]$, and $B = [b_{ij}]$ of the same size is given by

(14) $$A * B = [a_{ij}\ b_{ij}]\ .$$

We define an Hadamard array, H, of order 4n, to be a square matrix of order 4n with elements ± A, ± B, ± C, ± D each repeated n times in each row and column, with the property that, assuming the indeterminates A, B, C, D commute, the row vectors of H must be orthogonal.

The Hadamard array of order 4 is

(15) $$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

and is due to Williamson [27]. In 1965, Baumert and Hall published the 12 × 12 Hadamard array and in 1971 L. R. Welch found a 20 × 20 array. These may be found in [3] and [21]. Subsequently Hadamard arrays have been found for orders 4m, $m \in \{7, 9, 11, 13, 15, 17, 19\}$ by Cooper and Wallis (see [5], [19], [21]). In the next section we give some arrays obtained by partitioning the Galois Fields for some prime powers.

The constructions for Hadamard arrays that we quote in the next section rely on the following result, see [21] :

LEMMA A: Let P and Q be type 1 incidence matrices and R be a type 2 incidence matrix. Then

(i) $PQ = QP$, $P^TQ = QP^T$, $PQ^T = Q^TP$, $P^TQ^T = Q^TP^T$

(ii) $RQ = Q^TR^T$, $R^TQ = Q^TR$, $RQ^T = QR^T$, $R^TQ^T = QR$.

NOTATION: We will use the notation $C_a \sim C_b$, where $C_a \cap C_b = \phi$ and C_a and C_b are collections of elements from the same abelian group V, to mean the "collection" of elements

$$[c_{a_1}, c_{a_2}, \ldots, -c_{b_1}, -c_{b_2}, \ldots] \quad c_{a_i} \varepsilon C_a, \; c_{b_j} \varepsilon C_b,$$

where $-c_{b_j}$ does not mean the inverse $(c_{b_j}^{-1})$ of c_{b_j} in V, but means c_{b_j} with a negative sign attached.

The incidence matrix of $C_a \sim C_b$ and C_a & C_b are defined by

(16) $$[C_a \sim C_b] = [C_a] - [C_b], \text{ and } [C_a \,\&\, C_b] = [C_a] + [C_b]$$

respectively.

2. SOME RESULTS

In [5] and [21] the following theorem is given:

THEOREM 1. Suppose there exist four type 1 (0, 1, -1) matrices X_1, X_2, X_3, X_4 of order n, defined on the same abelian group V with n elements, such that

(i) $X_i * X_j = 0$, $i \neq j$, (* the Hadamard product).

(ii) $\sum_{i=1}^{4} X_i$ is a (1, -1) matrix

(iii) $\sum_{i=1}^{4} X_iX_i^T = nI_n$.

Further suppose A, B, C, D are indeterminates that pairwise commute. Define

(17)
$$\begin{aligned}
X &= X_1 \times A + X_2 \times B + X_3 \times C + X_4 \times D,\\
Y &= X_1 \times -B + X_2 \times A + X_3 \times D + X_4 \times -C,\\
Z &= X_1 \times -C + X_2 \times -D + X_3 \times A + X_4 \times B,\\
W &= X_1 \times -D + X_2 \times C + X_3 \times -B + X_4 \times A,
\end{aligned}$$

where $X_1 \times A$ denotes X with each 1 and -1 replaced by A and $-A$ respectively: (if a matrix is substituted for A, $X_1 \times A$ will become the usual Kronecker product.) If S denotes the R of (9) defined on V, then

$$H = \begin{bmatrix} X & YS & ZS & WS \\ -YS & X & -W^TS & Z^TS \\ -ZS & W^TS & X & -Y^TS \\ -WS & -Z^TS & Y^TS & X \end{bmatrix} \tag{18}$$

is an Hadamard array of order $4n$. ***

We note that the condition that X_1, X_2, X_3, X_4 are type 1 is only imposed so that we can ensure a suitable S exists. That other matrices are possible is demonstrated in the next lemma.

LEMMA 2. Let T and R be the matrices

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} ;$$

further let

$$X_1 = \begin{bmatrix} I & I & I \\ I & T & T^2 \\ I & T^2 & T \end{bmatrix}, \quad X_2 = \begin{bmatrix} T & T & T \\ -T & -T^2 & -I \\ 0 & 0 & 0 \end{bmatrix}, \quad X_3 = \begin{bmatrix} T^2 & T^2 & T^2 \\ 0 & 0 & 0 \\ -T^2 & -T & -I \end{bmatrix}, \quad X_4 = \begin{bmatrix} 0 & 0 & 0 \\ T^2 & I & T \\ -T & -I & -T^2 \end{bmatrix},$$

where 0 is the zero matrix of order 3. Then with $S = R \times R$, X, Y, Z, W and H of the previous theorem give an Hadamard array of order 36.

PROOF. Since $I + T + T^2 = J$ we have conditions (i), (ii) and (iii) of the theorem satisfied. The properties of H may be easily checked. ***

We note the row and column sum of the matrices X_i, $i = 1,2,3,4$ are not constant and so the matrices need not (and do not) satisfy the conditions of the following lemma (see [5] and [21]).

LEMMA 3. Suppose there exist four $(0, 1, -1)$ matrices X_1, X_2, X_3, X_4 of order n which satisfy

n		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 1

(i) <u>$X_i * X_j = 0, \quad i \neq j, \quad i, j = 1,2,3,4$</u>

(ii) $\sum_{i=1}^{4} X_i X_i^T = nI_n$.

<u>Let x_i be the number of positive elements in each row and column of X_i and y_i be the number of negative elements in each row and column of X_i. Then</u>

(a) <u>$\sum_{i=1}^{4} (x_i+y_i) = n$,</u> (b) <u>$\sum_{i=1}^{4} (x_i-y_i)^2 = n$.</u>

In Cooper and Wallis it is noted that some suitable matrices X_1, X_2, X_3, X_4 satisfying the conditions of theorem 1 may be formed by partitioning the Galois Field for a prime (or prime power) $p = ef + 1$ and using the incidence matrices of the subgroup and cosets of order f. The results for n = 13 and n = 19 given below are in [5], for n = 25 in [21] and n = 31, 37, 41 are presented here for the first time. Thus, we have from Table 1:

THEOREM 4. <u>There exist Hadamard arrays of order</u> 52, 76, 100, 124, 148, 164.

Matrices A, B, C and D which may be used to replace the indeterminates of Theorem 1 are known to exist when n is a member of the set

$$M = \{3, 5, 7, \ldots, 29, 37, 43\},$$

[9] and when 2m-1 is a prime power congruent to 1 modulo 4, see [14] and [25]. So we have

COROLLARY 5. <u>There exist Hadamard matrices of orders</u> 52m, 76m, 100m, 124m, 148m, 164m, <u>for</u> $m \in M$.

COROLLARY 6. <u>There exist Hadamard matrices of orders</u> 26(q+1), 38(q+1), 50(q+1), 62(q+1), 74(q+1), 82(q+1) <u>whenever</u> q <u>is a prime power congruent to</u> 1 <u>modulo</u> 4.

RESULTS: The last three new classes give the following new Hadamard matrices of order < 4000; 1804, 3404, 3596, 3772.

We now make a minor adaption of the cyclotomic arrays in order to facilitate the examination of structure in matrices based on cyclotomic classes. The adaption is most useful for e even, f odd. In all cases we indicate a source for the proofs we need but do not attempt to give the original reference.

NOTATION. Henceforth we use square brackets, [ ], for matrices and write $[\{0\}] = I$. Let X and Y be two collections, then [X] will mean the (type 1) incidence matrix of X, X^T will mean that collection such that $[X^T] = [X]^T$ and aX will be the collection with each element of X repeated a times, so $[aX] = a[X]$. We recall from [Cooper] that

$$(19) \qquad [X \wedge Y] = [X][Y],$$

and we use the definition

$$(20) \qquad [X \sim Y] = [X] - [Y],$$

$$(21) \qquad [X \cup Y] = [X] + [Y], \; X \cap Y = \phi$$

(or $[X \,\&\, Y] = [X] + [Y]$, $X \cap Y \neq \phi$).

In the matrix cases we consider, expressions of the type

$$[X \cup Y][X \cup Y]^T \text{ or } [X \sim Y][X \sim Y]^T = [X][X^T] \pm [X][Y^T] \pm [Y][X^T] + [Y][Y^T] \qquad (X \cap Y = \phi)$$

$$= [X \wedge X^T] \pm [(X \wedge Y^T) \,\&\, (Y \wedge X^T)] + [Y \wedge Y^T], \; (X \cap Y = \phi)$$

will arise so it is valuable to have

$$(22) \qquad [X \wedge X^T] \text{ and } [(X \wedge Y^T) \,\&\, (Y \wedge X^T)] \qquad (X \cap Y = \phi)$$

readily available.

We now turn to Storer [12; p. 24-25] for the elementary theory of cyclotomy:

Let x by a primitive root of $F = GF(q)$ where $q = p^\alpha = e\,f + 1$ is a prime power. Write $G = \langle x \rangle \setminus \{0\}$. The <u>cyclotomic classes</u> C_i in F are:

$$C_i = \{x^{es+i} : s = 0, 1, \ldots, f-1\} \; i = 0,1,\ldots,e-1.$$

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

For fixed i and j, the cyclotomic number (i, j) is defined to be the number of solutions of the equation

$$z_i + 1 = z_j \quad (z_i \in C_i, \; z_j \in C_j),$$

where $1 = x^0$ is the multiplicative unit of F. That is (i,j) is the number of ordered pairs s, t such that

$$x^{es+i} + 1 = x^{et+j} \quad (0 \le s,t \le f-1).$$

Now with . the multiplicative operation in F

$$\begin{aligned} C_i \wedge C_j &= [a+b: a \in C_i, \; b \in C_j] \\ &= [x^{es+i} + x^{et+j}: 0 \le s, \; t \le f-1] \\ &= [x^{es+i}.(1+x^{e(t-s)+j-i}) : 0 \le s,t \le f-1] \\ &= [C_i.(1+x^{er+j-i}) : 0 \le r \le f-1] \\ &= (j-i,0)C_i \;\&\; (j-i,1)C_{i+1} \;\&\ldots\&(j-i, \; e-1)C_{i+e-1} \\ &\qquad \& \; f\,\theta_{j-i}\{0\} \end{aligned} \tag{23}$$

where θ_k is given by

$$\theta_k = \begin{cases} 1 & \text{f is even and } k = 0 \\ 1 & \text{if f is odd and } k = e/2 \\ 0 & \text{otherwise.} \end{cases} \tag{24}$$

We note

$$C_i \wedge C_j = z_i.(C_0 \wedge C_{j-i}) = z_i.((j-i,0)C_0 \;\&\ldots\& \; (j-i,e-1)C_{e-1} \;\&\; f\theta_{j-i}\{0\}) \text{ where } z_i \in C_i. \tag{25}$$

Now $(j-i,k)$ is just the $j-i,k$ entry in the appropriate cyclotomic array, so the expression for $C_i \wedge C_j$ can be easily determined. We note

LEMMA 7.
$$C_i^T = \begin{cases} C_i & \underline{\text{f is even}} \\ C_{i+e/2} & \underline{\text{f is odd}} \end{cases}$$

PROOF. From Storer [12; lemma 2, page 25],

$$-1 \in \begin{cases} C_0 & \text{if f is even,} \\ C_{e/2} & \text{if f is odd.} \end{cases}$$

Now if $z \in C_i$ then $-z \in C_i^T$, where $-z$ is the inverse of z in the additive group G, and so the result follows. ***

Thus for f even

$$C_i \wedge C_i^T = C_i \wedge C_i$$

and then the cyclotomic arrays can be used immediately. We thus restrict our attention to f odd and note

LEMMA 8. $(C_i \wedge C_j^T) \,\&\, (C_j \wedge C_i^T) = (C_i \wedge C_{j+e/2}) \,\&\, (C_j \wedge C_{i+e/2}),$

$$= (C_i \wedge C_{j+e/2}) \,\&\, (C_{i+e/2} \wedge C_j).$$

Hence, for f odd, if

$$C_i \wedge C_j = \mathop{\&}_{s=0}^{e-1} (j-i,s)\ C_{s+i} \,\&\, f\theta_{j-i}\ \{0\}$$

then, with δ_{ij} the Kronecker delta,

$$(C_i \wedge C_j^T) \,\&\, (C_j \wedge C_i^T) = \mathop{\&}_{s=0}^{e-1} (j+e/2-i,s) C_{s+i} \,\&$$

$$\mathop{\&}_{t=0}^{e-1} (j-i-e/2,t)\ \ C_{t+i+e/2} \,\&\, f(\theta_{j+e/2-i}+\theta_{j-e/2-i})\{0\}$$

$$= \mathop{\&}_{s=0}^{e-1} (j-i+e/2,s)(C_{s+i} \cup C_{s+i+e/2}) \,\&\, 2f\ \delta_{ij}\{0\}$$

$$= \mathop{\&}_{r=0}^{e/2-1} ((j-i+e/2,r) + (j-i+e/2,r+e/2))(C_{r+i} \cup C_{r+i+e/2})$$

$$\&\, 2f\ \delta_{ij}\ \{0\}.$$

Thus we have proved the following rule. Note that in the case of $[X \wedge X^T]$ (see equation (22)), we do not want

$$(X \wedge X^T) \ \& \ (X \wedge \dot{X}^T)$$

so the first row of these tables gives $X \wedge X^T$ only.

RULE TO OBTAIN ARRAYS FROM THOSE OF LITERATURE FOR e EVEN, f ODD:

(1) rearrange the rows by putting $(e/2+i)$th row of original array into ith row, $i = 1,2,\ldots,e$.

(2) add element in ith column to element in $(i+e/2)$th column and put in ith column, $i = 1,2,\ldots,e/2$, except for the first row which should not be altered.

For example for $e = 4$, f odd:

$$\begin{array}{c|cccc|} & 0 & 1 & 2 & 3 \\ \hline 0 & A & B & C & D \\ 1 & E & E & D & B \\ 2 & A & E & A & E \\ 3 & E & D & B & E \\ \hline \end{array} \rightarrow \begin{array}{|cccc|} \hline A & E & A & E \\ E & D & B & E \\ A & B & C & D \\ E & E & D & B \\ \hline \end{array} \rightarrow \begin{array}{c|cc|} & 0,2 & 1,3 \\ \hline 0 & A & E \\ 1 & E+B & D+E \\ 2 & A+C & B+D \\ 3 & E+D & E+B \\ \hline \end{array}$$

RULE TO USE ADAPTED ARRAY $A = [a_{ij}]$ FOR e EVEN, f ODD:

Write $A_i = [C_i \cup C_{i+e/2}]$, reduce all subscripts modulo $e/2$.

$$\left\{\begin{array}{l}
[C_0 \wedge C_0^T] = a_{11}A_0 + a_{12}A_1 + \ldots + a_{1,e/2}\, A_{e/2-1} + fI \\
[C_s \wedge C_s^T] = a_{1,1+s}A_0 + a_{1,2+s}\, A_1 + \ldots + a_{1,e/2+s}A_{e/2-1} + fI \\
[C_0 \wedge C_i^T] + [C_i \wedge C_0^T] = a_{i+1,1}\, A_0 + a_{i+1,2}\, A_1 + \ldots + \\
\qquad\qquad a_{i+1,e/2}\, A_{e/2-1}, \\
[C_s \wedge C_{i+s}^T] + [C_{i+s} \wedge C_s^T] = a_{i+1,1+s}\, A_0 + a_{i+1,2+s}\, A_1 + \ldots + \\
\qquad\qquad a_{i+1,e/2+s}\, A_{e/2-1}.
\end{array}\right\}$$

ADAPTED CYCLOTOMIC ARRAYS: e even, f odd

e = 2

	0,1	
0	A	A = (f-1)/2
1	A+B	A+B = f

e = 4

	0,2	1,3	
0	A	E	A+E = (f-1)/2
1	E+B	D+E	B+D+2E = f
2	A+C	B+D	A+B+C+D = f
3	D+E	E+B	

e = 6

	0,3	1,4	2,5	
0	A	G	H	A+G+H = (f-1)/2
1	B+G	F+H	I+J	B+F+G+H+I+J =f
2	C+H	2I	E+G	C+E+G+H+2I = f
3	A+D	B+E	C+F	A+B+C+D+E+F = f
4	E+G	C+H	2I	
5	F+H	I+J	B+G	

ADAPTED CYCLOTOMIC ARRAYS: e even, f odd

e = 8

	0,4	1,5	2,6	3,7	
0	A	I	N	J	A+I+N+J = (f-1)/2
1	B+I	H+J	M+O	K+O	B+H+I+J+K+M+2O = f
2	C+N	K+M	G+N	L+O	C+G+K+L+M+2N+O = f
3	D+J	L+K	L+M	F+I	D+F+I+J+K+2L+M = f
4	A+E	B+F	C+G	D+H	A+B+C+D+E+F+G+H = f
5	F+I	D+J	K+L	L+M	
6	G+N	L+O	C+N	K+M	
7	J+H	M+O	K+O	B+I	

e = 10

	0,5	1,6	2,7	3,8	4,9	
0	A	K	R	T	L	A+K+L+R+T=(f-1)/2
1	B+K	J+L	Q+S	U+V	M+S	B+J+K+L+M+Q+2S+U+V=f
2	C+R	M+Q	I+T	P+V	N+V	C+I+M+N+P+Q+R+T+2V=f
3	D+T	N+U	P+U	H+R	O+S	D+H+N+O+P+R+S+T+2U=f
4	E+L	M+O	N+P	O+Q	G+K	E+G+K+L+M+N+2O+P+Q=f
5	A+F	B+G	C+H	D+I	E+J	A+B+C+D+E+F+G+H+I+J=f
6	G+K	E+L	M+O	N+P	O+Q	
7	H+R	O+S	D+T	N+U	P+U	
8	I+T	P+V	N+V	C+R	M+Q	
9	J+L	Q+S	U+V	M+S	B+K	

To illustrate the use of these arrays we now prove a lemma:

LEMMA 9: If $p = 4f + 1$ (f odd) is a prime power, $i = \sqrt{-1}$ then

$$A = i[C_0] - [C_1] - i[C_2] + [C_3]$$

satisfies

$$AA^* = pI - J$$

where A^* denotes A transpose complex conjugate

PROOF. $AA^* = ([C_3 \sim C_1] + i[C_0 \sim C_2])([C_3 \sim C_1]^T - i[C_0 \sim C_2]^T)$

$$= [C_3 \sim C_1][C_3 \sim C_1]^T + [C_0 \sim C_2][C_0 \sim C_2]^T$$

$$+ i([C_0 \sim C_2][C_3 \sim C_1]^T - [C_3 \sim C_1][C_0 \sim C_2]^T).$$

From the array for $e = 4$, f odd we get (writing ii for $C_i \wedge C_i^T$ and ij for $(C_i \wedge C_j^T)$ & $(C_j \wedge C_i^T)$):

	0,2	1,3	{0}
33	E	A	f
11	E	A	f
-13	-B-D	-A-C	
00	A	E	f
22	A	E	f
-02	-A-C	-B-D	
Total	-1	-1	4f

So $AA^* = (4f+1)\, I - J + i(XY^T - YX^T)$

where $X = [C_0 \sim C_2]$, $Y = [C_3 \sim C_1]$, and hence $X^T = -X$, $Y^T = -Y$.

Thus $$XY^T - YX^T = -XY + YX = 0,$$

since X and Y are both type 1 incidence matrices and hence commute. So we have the result. ***

The following lemmas are quoted from Storer [12; lemmas 19 and 30]:

LEMMA 10: When $e = 4$, f odd, the cyclotomic numbers are determined from the adapted array for $e = 4$, together with the relations:

$$16A = q - 7 + 2s$$

$$16B = q + 1 + 2s - 8t$$

$$16C = q + 1 - 6s$$

$$16D = q + 1 + 2s + 8t$$

$$16E = q - 3 - 2s$$

where $q = s^2 + 4t^2$, with $s \equiv 1 \pmod 4$, is the proper representation of q if $p \equiv 1 \pmod 4$, where the sign of t is ambiguously determined.

LEMMA 11. When $e = 8$, f odd the cyclotomic numbers are determined from the adapted array for $e = 8$, together with the relations:

I. If 2 is a 4th power in G	II. If 2 is not a 4th power in G
$64A = q - 15 - 2x$	$64A = q - 15 - 10x - 8a$
$64B = q + 1 + 2x - 4a + 16y$	$64B = q + 1 + 2x - 4a - 16b$
$64C = q + 1 + 6x + 8a - 16y$	$64C = q + 1 - 2x + 16y$
$64D = q + 1 + 2x - 4a - 16y$	$64D = q + 1 + 2x - 4a - 16b$
$64E = q + 1 - 18x$	$64E = q + 1 + 6x + 24a$
$64F = q + 1 + 2x - 4a + 16y$	$64F = q + 1 + 2x - 4a + 16b$
$64G = q + 1 + 6x + 8a + 16y$	$64G = q + 1 - 2x - 16y$
$64H = q + 1 + 2x - 4a - 16y$	$64H = q + 1 + 2x - 4a + 16b$
$64I = q - 7 + 2x + 4a$	$64I = q - 7 + 2x + 4a + 16y$
$64J = q - 7 + 2x + 4a$	$64J = q - 7 + 2x + 4a - 16y$
$64K = q + 1 - 6x + 4a + 16b$	$64K = q + 1 + 2x - 4a$
$64L = q + 1 + 2x - 4a$	$64L = q + 1 - 6x + 4a$
$64M = q + 1 - 6x + 4a - 16b$	$64M = q + 1 + 2x - 4a$
$64N = q - 7 - 2x - 8a$	$64N = q - 7 + 6x$
$64O = q + 1 + 2x - 4a$	$64O = q + 1 - 6x + 4a$

where x,y,a and b are specified by:

I. $q = x^2 + 4y^2$, $x \equiv 1 \pmod 4$ is the unique proper representation of $q = p^{\alpha}$ if $p \equiv \pmod 4$; otherwise,

$$q = (\pm p^{\alpha/2})^2 + 4.0^2; \text{ i.e., } x = \pm p^{\alpha/2},\ y = 0.$$

II. $q = a^2 + 2b^2$, $a \equiv 1 \pmod 4$ is the unique proper representation of $q = p^{\alpha}$ if $p \equiv 1$ or $3 \pmod 8$; otherwise,

$$q = (\pm p^{\alpha/2})^2 + 2.0^2; \text{ i.e., } a = \pm p^{\alpha/2},\ b = 0.$$

The signs of y and b are ambiguously determined.

4. CONSTRUCTIONS FOR SUPPLEMENTARY DIFFERENCE SETS

We recall from [20; lemma 9] and [21]:

LEMMA 12. Let A_1, A_2, ..., A_n be the type 1 incidence matrices of $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets then

$$\sum_{i=1}^{n} A_i A_i^T = (\sum_{i=1}^{n} k_i - \lambda)I + \lambda J.$$

If B_1, B_2, ..., B_n are the type 1 (1, -1) incidence matrices of the supplementary difference sets then

$$\sum_{i=1}^{n} B_i B_i^T = 4(\sum_{i=1}^{n} k_i - \lambda)I + (nv - 4\sum_{i=1}^{n} k_i + 4\lambda)J. \qquad ***$$

In particular we use

COROLLARY 13. Let B_1, B_2, B_3, B_4 be the type 1 (1, -1) incidence matrices of $4 - \{v; k_1, k_2, k_3, k_4; \lambda\}$ supplementary difference sets then $$\sum_{i=1}^{n} B_i B_i^T = 4(\sum_{i=1}^{4} k_i-\lambda)I + 4(v - \sum_{i=1}^{4} k_i+\lambda)J. \qquad ***$$

In this section we will assume that X_1, X_2, X_3, X_4 are 4 (0, 1, -1) matrices of order v which have the following properties:

$$(30)\quad \begin{cases} \text{(i)} & \sum_{i=1}^{n} X_i \quad \text{is a (1, -1) matrix,} \\ \text{(ii)} & X_i * X_j = 0, \quad i \neq j, \\ \text{(iii)} & \sum_{i=1}^{4} X_i X_i^T = aI + (v-a)J, \\ \text{(iv)} & X_i \text{ has } x_i \text{ positive and } y_i \text{ negative elements per row} \\ & \text{and column.} \end{cases}$$

We now show how such matrices may be used to construct supplementary difference sets. Let

$$\begin{aligned} Y_1 &= -X_1 + X_2 + X_3 + X_4, & Z_1 &= X_1 + X_2 + X_3 + X_4, \\ Y_2 &= X_1 - X_2 + X_3 + X_4, & Z_2 &= X_1 - X_2 + X_3 - X_4. \\ Y_3 &= X_1 + X_2 - X_3 + X_4, & Z_3 &= X_1 - X_2 - X_3 + X_4, \\ Y_4 &= X_1 + X_2 + X_3 - X_4, & Z_4 &= X_1 + X_2 - X_3 - X_4. \end{aligned}$$

Then we have

LEMMA 14. _If there exist_ 4 (0, 1, -1) _matrices_ X_1, X_2, X_3, X_4 _of order v satisfying the conditions_ (i), (ii), (iii), (iv) _above then there exist_

(a) $4 - \{v;\ y_1+x_2+x_3+x_4,\ x_1+y_2+x_3+x_4,\ x_1+x_2+y_3+x_4,\ x_1+x_2+x_3+y_4;\ 2\sum_{i=1}^{4} x_i+v-a\}$,

and (b) $4 - \{v;\ x_1+x_2+x_3+x_4,\ x_1+y_2+x_3+y_4,\ x_1+y_2+y_3+x_4,\ x_1+x_2+y_3+y_4;\ 2x_1-2y_1+2v-a\}$

supplementary difference sets, where

(c) $\sum_{i=1}^{4} (x_i+y_i) = v$ and

(d) $\sum_{i=1}^{4} (x_i-y_i)^2 = v^2-a(v-1)$.

PROOF. $\sum_{i=1}^{4} Y_i Y_i^T = \sum_{i=1}^{4} Z_i Z_i^T = 4 \sum_{i=1}^{4} X_i X_i^T = 4aI + 4(v-a)J.$

Now using Corollary 13 we have that Y_1, Y_2, Y_3, Y_4 and Z_1, Z_2, Z_3, Z_4 are the incidence matrices (or permutations of them) of $4-\{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i-a\}$ for some non-negative integers k_1, k_2, k_3, k_4. The actual values of k_i in each case may be determined by counting the number of positive elements in each row and column of Y_i and Z_i $(i = 1, 2, 3, 4)$.

The condition

$$\sum_{i=1}^{4} (x_i+y_i) = v$$

follows immediately from property (i) of the X_1, X_2, X_3, X_4.

So for case (a)

$$\sum_{i=1}^{4} k_i-a = 3 \sum_{i=1}^{4} x_i + \sum_{i=1}^{4} y_i-a = 2\sum_{i=1}^{4} x_i+v-a;$$

for case (b)

$$\sum_{i=1}^{4} k_i-a = 2x_1-2y_1 + 2\sum_{i=1}^{4} (x_i+y_i)-a = 2x_1-2y_1+2v-a.$$

The condition

$$\sum_{i=1}^{4} (x_i-y_i)^2 = v^2-a(v-1)$$

for case (a) is proved (as in [5]) by considering the constraints placed by equation (1). Write

$$\sum_{i=1}^{4} (x_i-y_i)^2 = s, \quad \sum_{i=1}^{4} x_i = w, \quad \sum_{i=1}^{4} y_i = v-w$$

Then from (1), in case (a),

$$\begin{aligned}(2w+v-a)(v-1) &= \sum_{i=1}^{4} (w+y_i-x_i)(w+y_i-x_i-1) \\ &= 4w^2+2w(v-2w)+s-4w-v+2w\end{aligned}$$

that is

$$s = v^2-a(v-1).$$

From equation (1), in case (b),

$$(2x_1-2y_1+2v-a)(v-1)$$

$$= w(w-1) + (w-x_2-x_4+y_2+y_4)^2 + (w-x_2-x_3+y_2+y_3)^2 + (w-x_3-x_4+y_3+y_4)^2$$
$$- (3w+2x_1-2y_1+2\sum_{i=1}^{4}(-x_i+y_i))$$

$$= w^2 - 2(x_1-y_1+v) + 3w^2 + 2w(2x_1-2y_1+2\sum_{i=1}^{4}(-x_i+y_i))$$
$$+ (x_2+x_3+x_4-y_2-y_3-y_4)^2 + \sum_{i=1}^{4}(x_i-y_i)^2$$

$$= 2(x_1-y_1)(2w-1)-2v+4w(v-w) + (\sum_{i=1}^{4}(x_i-y_i))^2 - 2(2w-v)(x_1-y_1)$$
$$+ \sum_{i=1}^{4}(x_i-y_i)^2$$

$$= -2v + 4w(v-w) + 2(x_1-y_1)(v-1) + (v-2w)^2 + \sum_{i=1}^{4}(x_i-y_i)^2.$$

So $\sum_{i=1}^{4}(x_i-y_i)^2 = v^2-a(v-1)$. ***

The difference sets given by lemma 14 may not be essentially different but we were not able to decide this problem.

We now apply the adapted arrays of section 3 to the constructions we have given in table 1 to see if more general results can be obtained.

LEMMA 15. Let $q = 4f+1 = 9+4t^2$ (f odd) be a prime power. Then

$$X_1 = [C_0],\quad X_2 = [C_1\sim\{0\}],\quad X_3 = [C_2\sim C_3],\quad X_4 = 0,$$

satisfy

(i) $\sum_{i=1}^{4} X_i$ is a $(1, -1)$ matrix,

(ii) $\quad X_i * X_j = 0 \qquad i \neq j,$

(iii) $\quad \sum_{i=1}^{4} X_i X_i^T = \tfrac{1}{2}(7f+5)I + \tfrac{1}{2}(f-3)J.$

PROOF. (i) and (ii) are clear. To show (iii) we consider the appropriate array, lemma 10, and use the following table of contributions from the terms in the incidence matrices

	0,2	1,3	{0}
00	A	E	f
11	E	A	f
- {0} 1		-1	
22	A	E	f
33	E	A	f
-23	-A-C	-B-D	
{0}			1
Total	f-1-A-C	f-2-B-D	4f+1

From lemma 10 $\quad f - 1 - A - C = f - 1 - (2q-6-4s)/16$

$$f - 2 - B - D = f - 2 - (2q+2+4s)/16$$

so if $s = -3$

$$f - 1 - A - C = (f-3)/2 = f - 2 - B - D$$

and we have the result. ***

We note that if $p = 13$, that is $f = 3$, then condition (iii) of the lemma gives

$$\sum_{i=1}^{4} X_i X_i^T = 13I$$

and so the matrices given satisfy the conditions for theorem 1.

This gives, using lemma 14,

COROLLARY 16. <u>Let</u> $q = 4f+1 = 9+4t^2$ (f <u>odd</u>) <u>be a prime power</u>. <u>Then there exist</u>

(a) $4 - \{4f+1;\ 2f,\ 2f+1,\ 3f,\ 3f;\ \tfrac{1}{2}(13f-3)\}$

<u>and</u> (b) $4 - \{4f+1;\ 3f,\ 2f+1,\ 2f+1,\ 3f;\ \tfrac{1}{2}(13f-1)\}$

<u>supplementary difference sets</u>.

Similarly we obtain

LEMMA 17. <u>Let</u> $q = 6f+1 = x^2+3y^2$ (f <u>odd</u>) <u>be a prime power such that</u> $4q = a^2+3b^2 = c^2+27d^2$, $c \equiv 1 \pmod 6$, $2x-a+3d = 6$, $c-3b+6y = 16$. <u>Then</u> $X_1 = [C_0]$, $X_2 = [C_2]$, $X_3 = [\{0\} \& C_3 \sim C_4]$, $X_4 = [C_1 \sim C_5]$ <u>satisfy conditions (i), (ii), (iv) of (30) and</u>

$$\text{(iii)} \quad \sum_{i=1}^{4} X_i X_i^T = \frac{(17f+6)}{3} I + \frac{(f-3)}{3} J.$$

PROOF. (i), (ii), (iv) are clear. To obtain (iii) we consider the appropriate array, lemma 27 of [12], and use the following table of contributions from the terms of the incidence matrices. As before we denote $(C_i \wedge C_j^T) \& (C_j \wedge C_i^T)$ by ij.

		0,3	1,4	2,5	{0}
	00	A	G	H	f
	22	G	H	A	f
	{0} 3	1			
–	{0} 4		-1		
	{0}				1
	33	A	G	H	f
–	34	-B-G	-F-H	-I-J	
	44	H	A	G	f
	11	H	A	G	f
	55	G	H	A	f
–	15	-2I	-E-G	-C-H	
	Total	f-B-G-2I	f-2-E-F-G-H	f-1-C-H-I-J	6f+1

From the lemma 27 of [12]

$$f-B-G-2I = f - (8q-4+12x-6a+2c+12y-6b+18d)/72$$

$$f-2-E-F-G-H = f - 2 - (8q-16 \; . \; . -4c-24y+12b+ \quad)/72$$

$$f-1-C-H-I-J = f - 1 - (8q-4-12x+6a+2c+12y-6b-18d)/72$$

these are all equal to

$$(f-3)/3$$

when

$$2x-a+3d = 6 \quad \text{and} \quad 3b-c-6y = -16.$$

For $x = 4$, $y = -1$, $c = 7$, $d = -1$, $a = -1$, $b = -5$ we have the conditions satisfied for $q = 19$ which also satisfies theorem 1 but the conditions are rather awkward to satisfy. Now using lemma 14 we have

COROLLARY 18. *Let* $q = 6f+1 = x^2+3y^2$ *(f odd) be a prime power such that* $4q = a^2+3b^2 = c^2+27d^2$, $c \equiv 1 \pmod 6$, $2x-a+3d = 6$, $c-3b+6y = 16$. *Then there exist*

(a) $4 - \{6f+1;\ 3f+1,\ 3f+1,\ 4f,\ 4f+1;\ (25f+3)/3\}$ *and*

(b) $4 - \{6f+1;\ 4f+1,\ 3f+1,\ 3f,\ 4f;\ 25f/3\}$

supplementary difference sets.

LEMMA 19. *Let* $q = 8f+1$ *(f odd) be a prime power.*

Then

$$X_1 = [C_0 \;\&\; C_5 \sim \{0\}], \quad X_2 = [C_1 \sim C_7], \quad X_3 = [C_2 \sim C_3],$$

$X_4 = [C_4 \sim C_6]$ *satisfy conditions (i), (ii), (iv) of (30) and*

$$\text{(iii)} \quad \sum_{i=1}^{4} X_i X_i^T = (q-j)I + jJ,$$

only for $q = 25$ *and* $j = 0$

PROOF. (i), (ii), (iv) are clear. To show (iii) we consider the appropriate array, lemma 11, and use the following table of contributions from the terms of the incidence matrices.

	0,4	1,5	2,6	3,7	{0}
{0}, $\overset{7}{\underset{i=0}{\&}}$ ii	f-1	f-1	f-1	f-1	8f+1
05	F+I	D+J	K+L	L+M	
-{0} 0	-1				
-{0} 5		-1			
- 17	-K-M	-G-N	-L-0	-C-N	
- 23	-M-0	-K-0	-B-I	-H-J	
- 46	-C-N	-K-M	-G-N	-L-0	
Total	f-2+F+I -C-K-2M -N-0	f-2+D+J -G-2K-M -N-0	f-1+K -B-G-I -N-0	f-1+M -C-H-J -N-0	8f+1

Now write

$$f-2-C+F+I-K-2M-N-0 = \alpha$$

$$f-2+D-G+J-2K-M-N-0 = \beta$$

$$f-1-B-G-I+K-N-0 = \gamma$$

$$f-1-C-H-J+M-N-0 = \delta.$$

For supplementary difference sets

When 2 is a fourth power in F (from Lemma 11)

$$64\alpha = 4q-134+16x-8a+32y+16b$$

$$64\beta = 4q-134+16x-8a-32y-16b$$

$$64\gamma = 4q-54-16x+8a-32y+16b$$

$$64\delta = 4q-54-16x+89+32y-16b.$$

Solving we have $y = b = 0$, $a = 2x-5$, $\alpha = \beta = \gamma = \delta = (4q-94)/64$ which with the conditions $q = x^2+4y^2 = a^2+2b^2$ (of lemma 11) leads to no possible solutions.

When 2 is not a fourth power in F (from lemma 11)

$$64\alpha = 4q-140+8a+16b$$

$$64\beta = 4q-140+8a-16b$$

$$64\gamma = 4q-60-8a+16b$$

$$64\delta = 4q-60-8a-16b$$

Solving we have $b = 0$, $a = 5$, $\alpha = \beta = \gamma = \delta = (4q-100)/64$. So the only possible solution is for $q = a^2+2b^2 = 5^2+2.0^2 = 25$. ***

LEMMA 20. <u>Let</u> $q = 8f+1$ (f <u>odd</u>) <u>be a prime power</u>.

<u>Then</u>

$$X_1 = [C_0 \sim C_2 \sim C_3], \quad X_2 = [C_4 \,\&\, C_6 \sim C_1 \sim \{0\}],$$

$X_3 = [C_5 \sim C_7]$, $X_4 = 0$ <u>satisfying conditions (i), (ii), (iv) of (30) and</u>

$$\text{(iii)} \quad \sum_{i=1}^{4} X_i X_i^T = (q-j)I+jJ,$$

<u>only for</u> $q = 41$ <u>and</u> $j = 0$.

PROOF. (i), (ii), (iii) are clear. To show (iii) we consider the appropriate array, Lemma 11, and use the following table of contributions from the terms of the incidence matrices.

	0,4	1,5	2,6	3,7	{0}
{0}, 7 & 11 1-0	f-1	f-1	f-1	f-1	8f+1
-02	-C-N	-K-M	-G-N	-L-0	
-03	-D-J	-K-L	-L-M	-F-I	
23	M+0	K+0	I+B	H+J	
46	C+N	K+M	G+N	L+0	
-14	-F-I	-J-D	-K-L	-L-M	
-{0} 4	-1				
-{0} 6			-1		
-16	-L-M	-I-F	-D-J	-K-L	
{0} 1		1			
-57	-L-0	-N-C	-K-M	-G-M	
Total	f-2-D-F -I-J-2L	f-C-D-F-I -J-L-N+0	f-2+B-D +I-J-2K -2L-2M	f-1-F-G +H-I+J-K -2L-M-N	8f+1

Now write

$$f-2-D-F-I-J-2L = \alpha$$
$$f-C-D-F-I-J-L-N+0 = \beta$$
$$f-2+B-D+I-J-2K-2L-2M = \gamma$$
$$f-1-F-G+H-I+J-K-2L-M-N = \delta.$$

For supplementary difference sets

$$\alpha = \beta = \gamma = \delta$$

When 2 is a fourth power in F (from lemma 11)

$$64\alpha = 2q-126-12x+8a$$

$$64\beta = 2q+10-12x \quad +16y$$

$$64\gamma = 2q-142+20x-8a+32y$$

$$64\delta = 2q-70+4x-48y$$

and these are equal for $a = 19$, $x = 9$, $y = 1$. In this case $\alpha = \beta = \gamma = \delta = 0$ implies $q = 41$ but 2 is not a fourth power for $GF(41)$. In lemma 11 part I we get $q = 85$ which is not a prime power and in part II $q = 19^2+2b^2$; so we have no result.

When 2 is not a fourth power in F, we have

$$64\alpha = 2q-126+4x-8a$$

$$64\beta = 2q+10-12x-16y$$

$$64\gamma = 2q-142+4x+8a+32y$$

$$64\delta = 2q-70+4x-16y.$$

These have solution $x = 5$, $y = 2$, $a = 3$, $\alpha = \beta = \gamma = \delta = 2q - 82$. In Lemma 11 part I we have $q = 5^2+4.2^2 = 41$ and in part II $q = (-3)^2+2b^2$. So there is only one solution, $q = 41$. ***

FINAL REMARK

We note that Joan Cooper has proved that this partitioning of the Galois Fields $GF(q)$ to give Hadamard arrays is not possible for $q = ef+1$ when f is even.

REFERENCES

[1] LEONARD D. BAUMERT, Cyclic Difference Sets, Lecture Notes, in Mathematics, Volume 182, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[2] L.D. BAUMERT AND H. FREDRICKSEN, The cyclotomic numbers of order eighteen with applications to difference sets, Math. Computation, 21(1967), 204-219.

[3] L.D. BAUMERT AND MARSHALL HALL, JR., A new construction for Hadamard matrices, Bull. Amer. math Soc. 71(1965), 169-170.

[4] JOAN COOPER, A binary composition for collections and sets, Proceedings of First Australian Conference on Combinatorial Mathematics, edited by Jennifer Wallis and W.D. Wallis, TUNRA, Newcastle, N.S.W., (to appear).

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

[6] E. LEHMER, On residue difference sets, Canad. J. Math. 5(1953), 425-432.

[7] E. LEHMER, On the number of solutions of $u^k + D \equiv w^2$ (mod p), Pacific J. Math. 5(1955), 103-118.

[8] MARSHALL HALL, JR., Characters and cyclotomy, Proceedings of the Symposia in Pure Mathematics, 8, American Mathematical Society, Providence, Rhode Island, (1965), 31-43.

[9] MARSHALL HALL, JR., Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.

[10] J.B. MUSKAT, The cyclotomic numbers of order fourteen, Acta. Arith. 11(1966), 263-279.

[11] JOSEPH B. MUSKAT AND ALBERT L. WHITEMAN, The cyclotomic numbers of order twenty, Acta Arithmetica, 17(1970), p. 185-216.

[12] THOMAS STORER, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics, Markham, Chicago, 1967.

[13] G. SZEKERES, Cyclotomy and complementary difference sets, Acta Arithmetica 18(1971), 349-353.

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

[15] JENNIFER WALLIS, Amicable Hadamard Matrices, J. Combinatorial Theory, ser. A. 11(1971), 296-298.

[16] JENNIFER WALLIS, A note on Amicable Hadamard Matrices, Utilitas Math. (to appear).

[17] JENNIFER WALLIS, Supplementary difference sets, Aequationes Math. (to appear).

[18] JENNIFER WALLIS, A note on supplementary difference sets, Aequationes Math. (to appear).

[19] JENNIFER WALLIS, Hadamard matrices of order 28m, 36m and 44m, J. Combinatorial Theory, (to appear).

[20] JENNIFER WALLIS AND ALBERT LEON WHITEMAN, Some classes of Hadamard matrix with constant diagonal, Bull. Austral. Math. Soc. 7(1972), 233-249.

[21] W.D. WALLIS, ANNE PENFOLD STREET, JENNIFER SEBERRY WALLIS, Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices, Volume 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[22] ALBERT LEON WHITEMAN, A family of difference sets, Illinois J. Math. 6(1962), 107-121.

[23] ALBERT LEON WHITEMAN, The cyclotomic numbers of order sixteen, Trans. Amer. Math. Soc. 86(1957), 401-413.

[24] ALBERT LEON WHITEMAN, The cyclotomic numbers of order ten, Proceedings of the Symposia in Applied Mathematics 10, American Mathematical Society, Providence, Rhode Island, 1960, 95-111.

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

[26] A.L. WHITEMAN, The cyclotomic numbers of order twelve, Acta Arith. 6(1960), 53-76.

[27] JOHN WILLIAMSON, Hadamard's determinant theorem and the sum of four squares, Duke J. Math. 11(1944), 65-81.