BULL. AUSTRAL. MATH. SOC. 05B05, 05B20
VOL. 7 (1972), 269-277.

A construction for Hadamard arrays

Joan Cooper and Jennifer Wallis

We give a construction for Hadamard arrays and exhibit the arrays of orders $4t$, $t \in \{1, 3, 5, 7, \ldots, 19\}$. This gives seventeen new Hadamard matrices of order less than 4000.

An *Hadamard matrix* H of order h has every element $+1$ or -1 and satisfies $HH^T = hI_h$, where I is the identity matrix of order h. h is necessarily $1, 2$ or congruent to zero modulo 4.

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

$$A * B = (a_{ij}b_{ij}) .$$

We define an *Hadamard array of order* $4n$, based on the indeterminates A, B, C and D, to be a $4n \times 4n$ array with entries chosen from A, $-A$, B, $-B$, C, $-C$, D and $-D$ in such a way that:

(i) in any row there are n entries equal to A or $-A$, n entries $\pm B$, n entries $\pm C$ and n entries $\pm D$; and similarly for columns;

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

The Hadamard array of order 4 is

Received 17 May 1972.

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

and is due to Williamson [*10*].

Suppose V is a finite abelian group with v elements, written in additive notation. A *difference set* D with parameters (v, k, λ) is a subset of V with k elements and such that in the totality of all the possible differences of elements from D each non-zero element of V occurs λ times.

If V is the set of integers modulo v then D is called a *cyclic difference set*: these are extensively discussed in Baumert [*1*].

A *circulant matrix* $B = (b_{ij})$ of order v satisfies $b_{ij} = b_{1,j-i+1}$ ($j-i+1$ reduced modulo v), while B is *back-circulant* if its elements satisfy $b_{ij} = b_{1,i+j-1}$ ($i+j-1$ reduced modulo v).

Throughout the remainder of this paper I will always mean the identity matrix and J the matrix with every element $+1$, where the order, unless specifically stated, is determined by the context. The Kronecker product of two matrices will be denoted by $\times$.

Let $S_1, S_2, \ldots, S_n$ be subsets of a finite abelian group V , $|V| = v$, 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 of V a fixed number of times, λ say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ *supplementary difference sets.*

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

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

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

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

See [7] and [8] for more details.

The incidence matrix $A = \left(a_{ij}\right)$ of a subset X of an abelian group G of order v, with elements $g_1, g_2, g_3, \ldots, g_v$, is found by choosing

$$a_{ij} = \begin{cases} 1 & \text{if } g_j - g_i \in X , \\ 0 & \text{otherwise.} \end{cases}$$

If $A_1, A_2, \ldots, A_n$ are the incidence matrices of $n - \{v;\ k_1, k_2, \ldots, k_n;\ \lambda\}$ supplementary difference sets then

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

and the $(1, -1)$ matrices $B_i = 2A_i - J$ satisfy

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

We define the matrix $R = \left(r_{ij}\right)$ of order v on G by

$$r_{ij} = \begin{cases} 1 & \text{if } g_i + g_j = 0 , \\ 0 & \text{otherwise.} \end{cases}$$

For example, if G is the integers modulo n with the usual ordering,

$$r_{i,n-i} = 1 , \quad r_{ij} = 0 \text{ otherwise.}$$

The construction

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

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

https://doi.org/10.1017/S0004972700045019 Published online by Cambridge University Press

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

Suppose x_i *is the number of positive elements in each row and column of* X_i *and* y_i *is the number of negative elements in each row and column of* X_i . *Then*

$$(a) \quad \sum_{i=1}^{4} \left(x_i+y_i\right) = n \ ,$$

$$(b) \quad \sum_{i=1}^{4} \left(x_i-y_i\right)^2 = n \ .$$

Proof. *(a)* follows immediately from *(ii)*. To prove *(b)* we consider the four $(1, -1)$ matrices

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

From [7] we know that $4 - \left\{n;\ k_1,\ k_2,\ k_3,\ k_4;\ \sum_{i=1}^{4} k_i-n\right\}$ supplementary difference sets may be used to form an Hadamard matrix of order $4n$. Now

$$\sum_{i=1}^{4} Y_i Y_i^T = 4nI_n \ ,$$

so $Z_i = \frac{1}{2}\left(Y_i+J\right)$, $i = 1, 2, 3, 4$ are the incidence matrices (or permutations of them) of

$$4 - \left\{n;\ y_1+x_2+x_3+x_4,\ x_1+y_2+x_3+x_4,\ x_1+x_2+y_3+x_4,\ x_1+x_2+x_3+y_4;\ 2\sum_{i=1}^{4} x_i\right\}$$

supplementary difference sets. Using (1) we have

$$2\sum_{i=1}^{4} x_i(n-1) = \sum_{i=1}^{4} \left(x_1+x_2+x_3+x_4+y_i-x_i\right)\left(x_1+x_2+x_3+x_4+y_i-x_i-1\right) ,$$

or writing $x_1 + x_2 + x_3 + x_4 = w$, $t = y_1 + y_2 + y_3 + y_4$, $n = w + t$,

$$2w(n-1) = \sum_{i=1}^{4} \left(x+y_i-x_i\right)\left(w+y_i-x_i-1\right)$$

$$= 4w^2 + 2w \sum_{i=1}^{4} \left(y_i-x_i\right) + \sum_{i=1}^{4} \left(y_i-x_i\right)^2 - \sum_{i=1}^{4} \left(y_i-x_i\right) - 4w$$

$$= 4w^2 + 2w(t-w) + \sum_{i=1}^{4} \left(y_i-x_i\right)^2 - (t-w) - 4w .$$

So

$$\sum_{i=1}^{4} \left(y_i-x_i\right)^2 = n ,$$

as required.

THEOREM 2. *Suppose there exist four* $(0, 1, -1)$ *circulant matrices* X_1, X_2, X_3, X_4 *of order* n *satisfying the conditions of the above theorem. Then there exists an Hadamard array of order* $4n$.

Proof. Consider the following matrices, where A, B, C, D are indeterminates which commute in pairs

$$Y_1 = X_1 \times A + X_2 \times B + X_3 \times C + X_4 \times D ,$$
$$Y_2 = X_1 \times -B + X_2 \times A + X_3 \times D + X_4 \times -C ,$$
$$Y_3 = X_1 \times -C + X_2 \times -D + X_3 \times A + X_4 \times B ,$$
$$Y_4 = X_1 \times -D + X_2 \times C + X_3 \times -B + X_4 \times -A ,$$

and

$$H = \begin{bmatrix} Y_1 & Y_2R & Y_3R & Y_4R \\ -Y_2R & Y_1 & -Y_4^TR & Y_3^TR \\ -Y_3R & Y_4^TR & Y_1 & -Y_2^TR \\ -Y_4R & -Y_3R & Y_2^TR & Y_1 \end{bmatrix} ,$$

where R is the Goethals-Seidel matrix (see [3, 6]).

Now clearly H is of order $4n$. Since each indeterminate is

https://doi.org/10.1017/S0004972700045019 Published online by Cambridge University Press

associated with X_1, X_2, X_3 and X_4 in each row and column, and *(a)* of Theorem 1 holds, each indeterminate occurs exactly n times in each row and column. It may be verified that

$$HH^T = I_4 \times \sum_{i=1}^{4} Y_i Y_i^T .$$

It remains to show that

$$\sum_{i=1}^{4} Y_i Y_i^T = nI_n \times \left(AA^T+BB^T+CC^T+DD^T\right) ;$$

but this is clearly true since $\sum_{i=1}^{4} X_i X_i^T = nI_n$.

There is an equivalent enunciation for both Theorems 2 and 3 when X_1, X_2, X_3, X_4 are matrices defined on subsets of abelian groups.

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

(i) $X_i * X_j = 0$, $i \neq j$, $i, j = 1, 2, 3, 4$,

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

Further suppose there exist four $(1, -1)$ *matrices* A, B, C, D *of order* m *which pairwise satisfy* $MN^T = NM^T$ *and for which*

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

Then there exists an Hadamard matrix of order $4mn$.

Proof. This follows by replacing the indeterminates A, B, C, D of the previous theorem by the matrices A, B, C, D .

COROLLARY 4. *There exists an Hadamard array of order* $4t$ *for* $t \in \{x : x$ *is an odd integer,* $1 \le t \le 19\}$.

Proof. The matrices X_1, X_2, X_3, X_4 for $t = 7, 9, 11$ may be found in [6]. These matrices were found by Welch for $t = 5$, (unpublished result) but we give it here for completeness.

In each case we give a set which may be used to determine the first row of X_1, X_2, X_3, X_4. This is possible because the X_i are circulant. If $\pm i$ is in the set for X_j then the i-th element of the first row of X_j is ± 1, all the other elements are zero. Use the sets from the following table:

n		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}
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}

The matrices X_1, X_2, X_3, X_4 for $n = 13 = 3^2 + 2^2 + 0^2 + 0^2$ were found by listing the multiplicative cyclic group of order 12 generated by 2 to form the subgroup $C_0 = \{2^{4j} : j = 0, 1, 2\}$ of order 3 and its

https://doi.org/10.1017/S0004972700045019 Published online by Cambridge University Press

cosets $C_i = \{2^{4j+i} : j = 0, 1, 2\}$, $i = 1, 2, 3$. Then the first rows of X_1, X_2, X_3, X_4 may be obtained by using the sets

$$C_0 \cup (-C_1) \ , \ C_3 \cup \{-13\} \ , \ C_2 \ , \ \emptyset$$

or

$$C_2 \cup (-C_3) \ , \ C_1 \cup \{-13\} \ , \ C_0 \ , \ \emptyset$$

where $-C_i = \{-i : i \in C_i\}$, and the X_j are formed as described in the proof of Corollary 4.

For $n = 19 = 3^2 + 3^2 + 1^2 + 0^2$ the multiplicative cyclic group of order 18 generated by 2 was used to form the subgroup $C_0 = \{2^{6j} : j = 0, 1, 2\}$ of order 3 and its cosets $C_i = \{2^{6j+i} : j = 0, 1, 2\}$, $i = 1, \ldots, 5$. Then X_1, X_2, X_3, X_4 were found, as above, by using the sets

$$C_1, C_3, C_2 \cup \{-C_1\} \ , \ \{0\} \cup C_4 \cup \{-C_5\} \ .$$

Matrices A, B, C and D satisfying the conditions of Theorem 3 have previously been used to construct Hadamard matrices of orders $4m$ [10], $12m$ [2], $20m$ (unpublished result of Welch, communicated to the authors by Baumert), $28m$, $36m$, $44m$ [6]. They are known to exist when m is a member of the set

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

[4], and when $2m - 1$ is a prime power congruent to 1 modulo 4 [5, 9].

COROLLARY 5. *There exist Hadamard matrices of orders* $52m$, $60m$, $68m$, $76m$ *whenever* $m \in M$.

COROLLARY 6. *There exist Hadamard matrices of orders* $26(q+1)$, $30(q+1)$, $34(q+1)$, $38(q+1)$ *whenever* q *is a prime power congruent to* 1 *modulo* 4 .

This gives the following new Hadamard matrices of order < 4000:

988, 1196, 1444, 1508, 1564, 1612, 1900, 1972, 2108,
2356, 2516, 2788, 2924, 3116, 3128, 3172, 3876.

https://doi.org/10.1017/S0004972700045019 Published online by Cambridge University Press

References

[1] Leonard D. Baumert, *Cyclic difference sets* (Lecture Notes in Mathematics, 182. Springer-Verlag, Berlin, Heidelberg, New York, 1971).

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

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

[4] Marshall Hall, Jr, *Combinatorial theory* (Blaisdell Publishing Co. [Ginn & Co.], Waltham, Massachusetts; Toronto; London; 1967).

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

[6] Jennifer Wallis, "Hadamard matrices of order $28m$, $36m$ and $44m$", *J. Combinatorial Theory* (to appear).

[7] Jennifer Wallis, "On supplementary difference sets", *Aequationes Math.* (to appear).

[8] Jennifer Wallis, "A note on BIBDs", *J. Austral. Math. Soc.* (to appear).

[9] Albert Leon Whiteman, "An infinite family of skew Hadamard matrices", (to appear).

[10] John Williamson, "Hadamard's determinant theorem and the sum of few squares", *Duke J. Math.* 11 (1944), 65-81.

Department of Mathematics,
University of Newcastle,
New South Wales.

https://doi.org/10.1017/S0004972700045019 Published online by Cambridge University Press