J. Austral. Math. Soc. (*Series A*) **29** (1980), 235–242

SOME INFINITE CLASSES OF HADAMARD MATRICES

JENNIFER SEBERRY

(Received 28 March 1979)

Communicated by W. D. Wallis

Abstract

A recursive method of A. C. Mukhopadhay is used to obtain several new infinite classes of Hadamard matrices. Unfortunately none of these constructions give previously unknown Hadamard matrices of order $<40{,}000$.

1980 Mathematics subject classification (*Amer. Math. Soc.*) : 05 B 20.

1. Preliminaries

We refer the reader to Wallis, Street and Wallis (1972) or Geramita and Seberry (1979) for all the definitions and notation used in this paper.

2. First construction

THEOREM 1. *Suppose there exists a skew-Hadamard matrix U of order $p+1$. Further, suppose there exist two $(1,-1)$ matrices A_r, B_r of order q satisfying:*

(i) $A_r B_r^{\mathrm{T}} = B_r A_r^{\mathrm{T}}$,

(ii) $A_r A_r^{\mathrm{T}} + pB_r B_r^{\mathrm{T}} = q(1+p) I_q$.

Then there are two $(1,-1)$ matrices of order $p^j q, j \geqslant 0$ satisfying

(i)′ $A_{r+j} B_{r+j}^{\mathrm{T}} = B_{r+j} A_{r+j}^{\mathrm{T}}$,

(ii)′ $A_{r+j} A_{r+j}^{\mathrm{T}} + pB_{r+j} B_{r+j}^{\mathrm{T}} = qp^j(p+1)I$.

Also, there exists an Hadamard matrix of order $qp^j(p+1)$ *for every* $j \geqslant 0$.

PROOF. Define $A_{r+1} = J_p \times B_r$ and $B_{r+1} = I \times A_r + S \times B_r$, where the rows and columns of U are arranged until it is in the form

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & I+S & \\ -1 & & & \end{bmatrix} = I + V$$

with $VV^{\mathrm{T}} = pI_{p+1}$, $S^{\mathrm{T}} = -S$, $JS = 0$, $SS^{\mathrm{T}} = pI - J$. Now we have

(i)′ $A_{r+1} B_{r+1}^{\mathrm{T}} = B_{r+1} A_{r+1}^{\mathrm{T}}$,

(ii)′ $A_{r+1} A_{r+1}^{\mathrm{T}} + pB_{r+1} B_{r+1}^{\mathrm{T}} = pJ \times B_r B_r^{\mathrm{T}} + pI \times A_r A_r^{\mathrm{T}} + p(pI - J) \times B_r B_r^{\mathrm{T}}$

$$= qp(1+p) I_{qp}.$$

We proceed by induction to obtain the matrices of order $p^j q$, $j \geqslant 0$.

The required Hadamard matrix is now obtained by considering $I \times A_{j+r} + V \times B_{j+r}$. //

It now remains to find initial matrices A_r and B_r. If there is a skew-Hadamard matrix or order p + 1 written in the form

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & I+S & \\ -1 & & & \end{bmatrix},$$

then $A_r = J_p$, $B_r = I_p + S_p$ are suitable matrices. If there exists a symmetric Hadamard matrix of order $p+5$ written in the form

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & M & \\ 1 & & & \end{bmatrix},$$

then $A_r = J_{p+4} - 2I_{p+4}$, $B_r = M$ are suitable matrices. Further, if Q is the back-circulant $(1, -1)$ incidence matrix of a cyclic (v, k, λ) difference set and there exists a cyclic $(v, (v-1)/2, (v-3)/4)$ difference set with $(1, -1)$ incidence matrix L where

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

$p = v-4k+4\lambda$, then $A_r = Q$ and $B_r = L$ are suitable matrices. We summarize these results for convenience :

COROLLARY 2. *Suppose there exists a skew-Hadamard matrix of order* $p+1$. *Then*
(*a*) *there exist Hadamard matrices of order* $p^{j+1}(p+1, j \geqslant 0$;
(*b*) *when there exists a symmetric Hadamard matrix of order* $p+5$ *there exist Hadamard matrices of order* $p^j(p+1)(p+4), j \geqslant 0$;
(*c*) *when there exists a cyclic* (v,k,λ) *configuration and a* $(v,(v-1)/2,(v-3)/4)$ *configuration with* $p = v-4(k-\lambda)$, *there exist Hadamard matrices of order* $vp^j(p+1), j \geqslant 0$.

EXAMPLE. (a) gives Hadamard matrices of orders $2^3 \cdot 7^{j+1}$, $2^2 \cdot 3 \cdot 11^{j+1}$, $2^2 \cdot 5 \cdot 19^{j+1}$, $j \geqslant 0$.

(b) gives Hadamard matrices $2^3 \cdot 11 \cdot 7^j$, $2^2 \cdot 45 \cdot 11^j$, $2^3 \cdot 19 \cdot 3^j \cdot 5^j$, j $\geqslant 0$.

(c) gives Hadamard matrices of order $2^2 \cdot 3 \cdot 31 \cdot 11^j$, $j \geqslant 0$.

COMMENT. The matrices just constructed of orders 7^{j+1} and $11 \cdot 7^j$, $j \geqslant 0$, have been called 8-*Williamson matrices* as there are eight of them and they can be used in a Plotkin array.

Hence, since there is an orthogonal design of type (3, 3, 3, 3, 3, 3, 3, 3) in order 24 (see Geramita and Seberry (1979)) there are Hadamard matrices of order $8 \cdot 3 \cdot 7^{j+1}$ and $8 \cdot 3 \cdot 11 \cdot 7^j$, $j \geqslant 0$.

Now suppose there is a conference matrix of order $p+3$ which can be written as

$$\begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & X & \\ 1 & & & \end{bmatrix},$$

where $X^{\mathrm{T}} = X$, $XJ = 0$, $XX^{\mathrm{T}} = (p+2)I - J_{p+2}$. Then

$$A_r = \begin{pmatrix} J & J-2I \\ -J+2I & J \end{pmatrix} \quad \text{and} \quad B_r = \begin{pmatrix} X+I & X-I \\ X-I & -X+I \end{pmatrix}$$

satisfy

$$\begin{aligned} A_r A_r^{\mathrm{T}} + pB_r B_r^{\mathrm{T}} &= I_2 \times [(p+2)J + (p-2)J + 4I] + 2pI_2 \times (XX^{\mathrm{T}} + I) \\ &= I_2 \times [2pJ + 4I - 2pJ + 2p(p+3)I] \\ &= 2(p+2)(p+1)I. \end{aligned}$$

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

This gives Mukhopadhyay's Theorem 3.1 as a corollary to the theorem :

COROLLARY 3. *Suppose there exists a skew-Hadamard matrix of order* $p+1$ *and a symmetric conference matrix of order* $p+3$ *then there is an Hadamard matrix of order* $2p^j(p+1)(p+2)$ *for* $j \geqslant 0$.

EXAMPLE. This means there are Hadamard matrices of orders $2^3 \cdot 3^j \cdot 5$, $2^4 \cdot 7^j \cdot 9$, $2^3 \cdot 11^j \cdot 3 \cdot 13$, $2^5 \cdot 15^j \cdot 17$, $2^4 \cdot 23^j \cdot 3 \cdot 25$, $2^3 \cdot 27^j \cdot 7 \cdot 29$, $j \geqslant 0$ an integer.

Using the result of Mathon (1978) that there are symmetric conference matrices of order $(q+2)q^2+1$ when q is a prime power and $q+3$ is the order of a conference matrix we have :

EXAMPLE. There exist Hadamard matrices of order $8 \cdot 11 \cdot 45 \cdot 43^r$, $16 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 439^r$ for every $r \geqslant 0$.

3. Second construction

Suppose there exist amicable orthogonal designs of types $((1,p);(1,p))$ in order $p+1$ which can be written in the form

$$(*)\ X = \begin{bmatrix} x & y & \dots & y \\ -y & & & \\ \vdots & & xI+yS & \\ -y & & & \end{bmatrix} \quad \text{and} \quad Y = \begin{bmatrix} -u & \dots & v \\ v & & \\ \vdots & & uU+vV \\ v & & \end{bmatrix},$$

where

$$S^{\mathrm{T}} = -S, \quad U^{\mathrm{T}} = U, \quad V^{\mathrm{T}} = V, \quad SJ = 0, \quad VJ = 0, \quad UJ = 0,$$

$$SS^{\mathrm{T}} = VV^{\mathrm{T}} = pI - J, \quad UU^{\mathrm{T}} = I, \quad SU^{\mathrm{T}} = US^{\mathrm{T}} \quad \text{and} \quad SV^{\mathrm{T}} = VS^{\mathrm{T}}.$$

In Geramita and Seberry (1979), Theorem 5.52, it is proved these amicable orthogonal designs exist whenever $p \equiv 3 \pmod 4$ is a prime power.

THEOREM 4. *Suppose there exist amicable orthogonal designs of types* $((1,p);(1,p))$ *in order* $p+1$ *which can be written in the form* (*). *Further suppose there exist four* $(1,-1)$ *matrices* A_r, B_r, C_r, D_r *of order* q *satisfying*

(i) $X_r Y_r^{\mathrm{T}} = Y_r X_r^{\mathrm{T}}$ *when* $X_r, Y_r \in \{A_r, B_r, C_r, D_r\}$,

(ii) $A_r A_r^{\mathrm{T}} + B_r B_r^{\mathrm{T}} + pC_r C_r^{\mathrm{T}} + pD_r D_r^{\mathrm{T}} = 2(p+1)qI_q$.

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

Then there are four $(1,-1)$ *matrices or order* $p^j q$ *satisfying*

(i)′ $X_{r+j} Y_{r+j}^{\mathrm{T}} = Y_{r+j} X_{r+j}^{\mathrm{T}}$ *when* $X_{r+j}, Y_{r+j} \in \{A_{r+j}, B_{r+j}, C_{r+j}, D_{r+j}\}$,

(ii)′ $A_{r+j} A_{r+j}^{\mathrm{T}} + B_{r+j} B_{r+j}^{\mathrm{T}} + pC_{r+j} C_{r+j}^{\mathrm{T}} + pD_{r+j} D_{r+j}^{\mathrm{T}} = 2p^j(p+1)qI.$

Also, there exists an Hadamard matrix of order $2p^j(p+1)q$ *for every* $j \geqslant 0$.

PROOF. Define $A_{r+1} = J_p \times C_r$, $B_{r+1} = J_p \times D_r$, $C_{r+1} = I_p \times A_r + S \times C_r$, $D_{r+1} = U \times B_r + V \times D_r$.

Now $A_{r+1}, B_{r+1}, C_{r+1}, D_{r+1}$ are four $(1,-1)$ matrices of order pq for which

(i)′ $X_{r+1} Y_{r+1}^{\mathrm{T}} = Y_{r+1} X_{r+1}^{\mathrm{T}}$ when $X_{r+1}, Y_{r+1} \in \{A_{r+1}, B_{r+1}, C_{r+1}, D_{r+1}\}$,

(ii)′ $A_{r+1} A_{r+1}^{\mathrm{T}} + B_{r+1} B_{r+1}^{\mathrm{T}} + pC_{r+1} C_{r+1}^{\mathrm{T}} + pD_{r+1} D_{r+1}^{\mathrm{T}} = 2p(p+1)qI_{pq}$.

We proceed by introduction to obtain the matrices of order $p^j q$, $j \geqslant 0$.

We now note that if an orthognal design of type $(1,1,p,p)$ exists in order $2(p+1)$ then the A_r, B_r, C_r, D_r are called 'suitable' matrices, that is they can be substituted for the variables of the orthogonal design to form an Hadamard matrix. We further observe that an orthogonal design of type $(1,1,p,p)$ exists in order $2(p+1)$ whenever there is a skew-Hadamard matrix of order $p+1$. This shows the required Hadamard matrices exist. //

We use the theory of cyclotomy to obtain possible starting 'suitable' matrices for our theorem. In Wallis (1973) it is shown that for a prime power $q = 25+4t^2 = 4f+1$ (f odd) there are two supplementary difference with parameters $2-\{4f+1;\ 2f, f;\ \frac{1}{4}(5f-3)\}$ which have circulant symmetric $(1,-1)$ incidence matrices A_r, B_r which satisfy

$$A_r A_r^{\mathrm{T}} + B_r B_r^{\mathrm{T}} = (7f+3)I + (f-1)J.$$

Let Q be the quadratic residue matrix (defined in Lemma 1.19 of Wallis *et al.* (1972)) then with $C_r = Q+1$, $D_r = Q-I$ and $p = \frac{1}{2}(f-1)$ we have

$$A_r A_r^{\mathrm{T}} + B_r B_r^{\mathrm{T}} + pC_r\ C_r^{\mathrm{T}} + pD_r D_r^{\mathrm{T}} = (f+1)(4f+1)I.$$

Hence, using the theorem we have

COROLLARY 5. *Let* $q = 25+4t^2 = 4f+1 [f \equiv 7 \pmod 8]$ *be a prime power. Suppose there exist amicable orthogonal designs of types* $((1, \frac{1}{2}(f-1)); (1, \frac{1}{2}(f-1)))$ *in order* $\frac{1}{2}(f+1)$ *which can be written in the form* (*). *Then there exists an Hadamard matrix of order* $2^{-j}(f-1)^j(f+1)(4f+1)$ *for every* $j \geqslant 0$.

EXAMPLE. The conditions are satisfied for $f = 7, 15, 447, \ldots$ and so there are Hadamard matrices of orders $8 \cdot 3^j \cdot 29$, $16 \cdot 7^j \cdot 61$, $2^6 \cdot 7 \cdot 223^j \cdot 1879$, ..., $j \geqslant 0$ an integer.

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

There will of course be many other sets of matrices satisfying the conditions of the theorem. For example, suppose there is a symmetric conference matrix of order $q+1 = p+3$. Write it in the form

$$C = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & N & \\ 1 & & & \end{bmatrix},$$

where $NJ = 0$, $NN^{\mathrm{T}} = (p+2)I - J$, $N^{\mathrm{T}} = N$.
Then, choosing

$$A_r = J_{p+2}, \quad B_r = J_{p+2} - 2I_{p+2}, \quad C_r = N+I, \quad D_r = N-I,$$

we observe (i) and (ii) of the theorem are satisfied. This gives the following corollary of the theorem which is very similar to Theorem 3.1 of Mukhopadhyay (1978):

COROLLARY 6. *Suppose there exists amicable orthogonal designs of types* $((1,p);(1,p))$ *in order* $p+1$ *which can be written in the form* (*). *Further, suppose there is a symmetric conference matrix of order* $p+3$. *Then there is an Hadamard matrix of order* $2p^{r-1}(p+1)(p+2)$ *for every non-negative integer* r.

4. Third construction

The proof of the next theorem is quite straightforward:

THEOREM 7. *Suppose there exists an orthogonal design of type* (a, a, ap, ap) *in order* $2a(p+1)$. *Now suppose there exist two* $(1, -1)$ *matrices* A_r *and* B_r *of order* q *such that*

(a) $A_r B_r^{\mathrm{T}} = B_r A_r^{\mathrm{T}}$,

(b) $A_r A_r^{\mathrm{T}} + pB_r B_r^{\mathrm{T}} = (1+p)qI$.

Further suppose $X^{\mathrm{T}} = X$, $XJ = 0$, $XX^{\mathrm{T}} = pI - J$ *and* $X+I$ *is a* $(1, -1)$ *matrix then*

$$A_{r+1} = J \times B_r, \quad B_{r+1} = J \times B_r,$$

$$C_{r+1} = I \times A_r + X \times B_r, \quad D_{r+1} = I \times A_r - X \times B_r$$

are four matrices of order pq *satisying the conditions*

(i) $X_{r+1} Y_{r+1}^{\mathrm{T}} = Y_{r+1} X_{r+1}^{\mathrm{T}}$ *when* $X_{r+1}, Y_{r+1} \in \{A_{r+1}, B_{r+1}, C_{r+1}, D_{r+1}\}$,

(ii) $A_{r+1} A_{r+1}^{\mathrm{T}} + B_{r+1} B_{r+1}^{\mathrm{T}} + pC_{r+1} C_{r+1}^{\mathrm{T}} + pD_{r+1} D_{r+1}^{\mathrm{T}} = 2p(1+p)qI$.

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

Hence, using the orthogonal design of type (a, a, ap, ap) *in order* $2a(p+1)$, *we have Hadamard matrices of order* $2ap(p+1)q$.

Now if there is a symmetric Hadamard matrix of order $p+3$ which can be written :

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & G & \\ 1 & & & \end{bmatrix},$$

then

$$A_r = \begin{pmatrix} J & J-2I \\ -J+2I & J \end{pmatrix} \quad \text{and} \quad B_r = \begin{pmatrix} G & G \\ G & -G \end{pmatrix}$$

satisfy

$$A_r A_r^{\mathsf{T}} + pB_r B_r^{\mathsf{T}} = 2(p+2)(p+1)I.$$

Hence we have

COROLLARY 8. *Suppose* $p \equiv 1 \pmod 4$ *is a prime power and there is a symmetric Hadamard matrix of order* $p+2$. *Then there is an Hadamard matrix of order* $8p(p+1)(p+2)$.

PROOF. This follows because an orthogonal design of type $(2, 2, 2p, 2p)$ in order $4(p+1)$ exists. //

EXAMPLE. Since there are orthogonal designs of types $(1, 1, 5, 5)$, $(1, 1, 9, 9)$, $(1, 1, 13, 13)$ and $(2, 2, 34, 34)$ known in orders 12, 20, 28 and 72 respectively we have Hadamard matrices of order $8 \cdot 3 \cdot 5 \cdot 7$, $8 \cdot 5 \cdot 9 \cdot 11$, $8 \cdot 7 \cdot 13 \cdot 15$, $16 \cdot 9 \cdot 17 \cdot 19$, ...

Final remarks

Whiteman (1976) was able to show that matrices of the same order as those obtained by Seberry Wallis (1973) could be obtained which were circulant and symmetric. It is possible that his methods could be used on the results of this paper to obtain circulant, symmetric matrices. Such matrices are far easier to use in orthogonal designs to obtain further results.

https://doi.org/10.1017/S1446788700021212 Published online by Cambridge University Press

References

A. V. Geramita and Jennifer Seberry (1979), *Orthogonal designs: Quadratic forms and Hadamard matrices* (Marcel Dekker, New York).

R. Mathon (1978), 'Symmetric conference matrices of order pq^2+1', *Canad. J. Math.* **30**, 321–331.

A. C. Mukhopadhay (1978), 'Some infinite classes of Hadamard matrices', *J. Combinatorial Theory, Ser. A* **25**, 128–141.

Jennifer Seberry (1978), 'A computer listing of Hadamard matrices', *Combinatorial theory: Proceedings of the international conference*, Canberra, August 1977, in *Lecture notes in mathematics* (Springer-Verlag, Berlin–Heidelberg–New York), Vol. 686, pp. 275–281.

Jennifer Seberry Wallis (1973), 'Some matrices of Williamson type', *Utilitas Math.* **4**, 147–154.

Jennifer Seberry Wallis (1974), 'Williamson matrices of even order', *Combinatorial mathematics: Proceedings of the second Australian conference* (editor D. A. Holton), in *Lecture notes in mathematics* (Springer-Verlag, Berlin–Heidelberg–New York), Vol. 403, pp. 132–142.

Jennifer Seberry Wallis (1975), 'Construction of Williamson type matrices', *Linear and Multilinear Algebra*, **3**, 197–207.

E. Spence (1977), An infinite family of Williamson matrices', *J. Austral. Math. Soc. Ser. A* **24**, 252–256.

Jennifer Wallis (1973), 'Some remarks on supplementary difference sets', *Colloq. Math. Societatis János Bolyai* **10**, 1503–1526.

W. D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis (1972), *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, in *Lecture notes in mathematics* (Springer-Verlag, Berlin–Heidelberg–New York.), Vol. 292.

A. L. Whiteman (1976), 'Hadamard matrices of Williamson type', *J. Austral. Math. Soc. Ser. A* **21**, 481–486.

Department of Applied Mathematics
University of Sydney
Sydney NSW 2006
Australia