

Complex Hadamard Matrices

JENNIFER WALLIS

Queen's University, Kingston, Ontario, Canada

(Received March 22, 1973)

R. J. Turyn introduced complex Hadamard matrices and showed that if there is a complex Hadamard matrix of order c and a real Hadamard matrix of order $h > 1$, then there is a real Hadamard matrix of order hc .

Previously, complex Hadamard matrices were only known for a few small orders and the orders for which symmetric conference matrices were known. These latter are known only to exist for orders which can be written as $1 + a^2 + b^2$ where a, b are integers.

We give many constructions for new infinite classes of complex Hadamard matrices and show that they exist for orders 306, 650, 870, 1406, 2450 and 3782: for the orders 650, 870, 2450 and 3782, a symmetric conference matrix cannot exist.

1. INTRODUCTION

An Hadamard matrix H of order n , all of whose elements are $+1$ or -1 , satisfies $HH^T = nI_n$, where (as throughout this paper) I is the identity matrix, J the matrix with all entries $+1$, and A^T denotes the transpose of A . It is conjectured that an Hadamard matrix exists for $n = 4t$, where t is any positive integer. Many classes of Hadamard matrices are known; most of these can be found by reference to [3]. Hadamard matrices are known for all orders less than 188.

An Hadamard matrix $H = U + I$ is called *skew-Hadamard* if $U^T = -U$. It is conjectured that whenever there exists an Hadamard matrix of order n , there exists a skew-Hadamard matrix of the same order. The orders for which skew-Hadamard matrices exist may be found from Appendices *B* and *H* of [3].

The orders less than 1004 for which skew-Hadamard matrices are not yet known are:

116, 148, 156, 172, 188, 196, 232, 236, 260, 268, 276, 292, 324, 356, 372, 376, 388, 392, 404, 412, 428, 436, 472, 476, 484, 508, 516, 520, 532, 536,

580, 584, 596, 604, 612, 628, 652, 668, 676, 708, 712, 716, 724, 732, 756, 764, 772, 776, 784, 804, 808, 820, 836, 852, 856, 868, 872, 892, 900, 904, 916, 932, 940, 944, 952, 956, 964, 980, 988, 996.

A skew-type matrix $A = U + I$ has $U^* = -U$, where U^* is the hermitian conjugate of U .

A symmetric conference matrix $I + N$ of order n is a $(1, -1)$ matrix for which

$$N^T = N \text{ and } NN^T = (n - 1)I_n.$$

These matrices have been discovered for the following orders:

- NI $p^r + 1$ r a positive, p^r (prime power) $\equiv 1 \pmod{4}$;
- NII $(h - 1)^2 + 1$ h the order of a skew-Hadamard matrix;
- NIII $(n - 1)^u + 1$ n the order of a symmetric conference matrix, u an integer.

A proof of these results may be found in [3] as may the proof of the following theorem:

THEOREM A *A necessary condition for the existence of a symmetric conference matrix of order $n \equiv 2 \pmod{4}$ is that*

- (i) $n - 1 = a^2 + b^2$, where a and b are integers or equivalently
- (ii) the square free part of $n - 1$ must not contain a prime factor $\equiv 3 \pmod{4}$.

A complex Hadamard matrix C of order c is a matrix all of whose elements are $+1, -1, +i$ or $-i$ and which satisfies $CC^* = cI_c$, where $i = \sqrt{-1}$. It is conjectured that a complex Hadamard matrix exists for every even c .

A complex skew-Hadamard matrix $C = I + U$ has $U^* = -U$. The matrices $I + iN$, where $N + I$ is a symmetric conference matrix are of this type. In particular, this means there are complex skew-Hadamard matrices of order $p^r + 1$, where $p^r \equiv 1 \pmod{4}$ is a prime power.

We will show it is sometimes possible to find complex Hadamard matrices for orders for which symmetric conference matrices do not exist.

LEMMA 1 *Every complex Hadamard matrix has order 1 or divisible by 2.*

Proof There are real Hadamard matrices of order 1 and 2.

Suppose the matrix is of order $m > 2$. Then the first two rows may be chosen as

$$\begin{array}{cccccccc} 1 & 1 & \dots & \dots & \dots & \dots & \dots & 1 \\ i & i & \dots & i & -i & \dots & -i & \dots & -i \end{array} \quad \begin{array}{cccccccc} 1 & 1 & \dots & \dots & \dots & \dots & \dots & 1 \\ 1 & 1 & \dots & 1 & -1 & \dots & -1 & \dots & -1 \end{array}$$

$\underbrace{\hspace{1.5cm}}_x \quad \underbrace{\hspace{1.5cm}}_y \quad \underbrace{\hspace{1.5cm}}_z \quad \underbrace{\hspace{1.5cm}}_w$

by suitably multiplying through the columns by i , $-i$ and -1 and then rearranging the columns $-x, y, z, w$ are the numbers of columns of each type. So we have

$$x = y, \quad z = w \quad \text{and} \quad x + y + z + w = n,$$

and hence $2 \mid n$.

We propose to use the following theorems to construct Hadamard matrices:

THEOREM 1 (Turyn) *If C is a complex Hadamard matrix of order c and H is a real Hadamard matrix of order h , then there exists a real Hadamard matrix of order hc .*

THEOREM 2 (Turyn) *If C and D are complex Hadamard matrices of orders r and q , then $C \times D$ (where \times is the Kronecker product) is a complex Hadamard matrix of order rq .*

We also note that the following theorems ensure the existence of complex Hadamard matrices for all even orders less than 64. The unsettled cases less than 200 are:

66, 70, 78, 94, 106, 118, 130, 134, 142, 146, 154, 162, 166, 178, 186, 188, 190.

THEOREM 3 (Turyn) *If $I + N$ is a symmetric conference matrix, then $iI + N$ is a (symmetric) complex Hadamard matrix and $I + iN$ is a complex skew-Hadamard matrix.*

THEOREM 4 (Turyn) *Let A, B, C, D be $(1, -1)$ matrices of order m such that*

$$AA^T + BB^T + CC^T + D^TT = 4mI_m,$$

and $MN^T = NM^T$ for $N, M \in \{A, B, C, D\}$ (i.e. A, B, C, D may be used to form a Williamson type Hadamard matrix) then write

$$X = \frac{1}{2}(A + B), \quad Y = \frac{1}{2}(A - B), \quad V = \frac{1}{2}(C + D), \quad W = \frac{1}{2}(C - D)$$

and

$$\begin{bmatrix} X + iY & V + iW \\ V^* - iW^* & -X^* + iY^* \end{bmatrix}$$

is a complex Hadamard matrix of order $2m$.

In particular, by these results of Turyn, since matrices A, B, C, D satisfying the conditions of Theorem 4 are known for all odd m less than 31, there are complex Hadamard matrices of orders 22 and 34 for which orders, by Theorem A, there can be no symmetric conference matrix.

We now note a small but useful fact.

LEMMA 5 *Suppose $AB^* = BA^*$. Then if $C = iA$, $CB^* = -BC^*$. Specifically, if A and B are real and $AB^T = BA^T$, then if $C = iA$, $CB^* = -BC^*$.*

Proof $CB^* = iAB^* = iBA^* = B(iA^*) = -BC^*$.

We will show that complex Hadamard matrices exist for the following list of orders. Our constructions are actually more general than the list suggests; as will be seen, many of our theorems are of the form: "if a certain matrix exists, then . . .", so that further results about the existence of skew-Hadamard matrices, symmetric conference matrices and amicable Hadamard matrices may immediately give new classes of complex Hadamard matrices. We use the notation:

- n n is the order of a symmetric conference matrix,
 h h is the order of a skew-Hadamard matrix,
- CI n Turyn; Theorem 3.
 CII $(h - 1)^t + 1$ from [3]; $t = 2^r$, r a positive odd integer, $i \geq 1$ an integer.
 $(n - 1)^s + 1$ from [3]; s an integer.
 CIII 22, 34 Turyn [2]; Theorem 4.
 CIV $n(n - 1)$ Corollary 11 or Corollary 17.
 CV $2(n - 1)(n - 4)$ $n - 4$ the order of a symmetric conference matrix; from Corollary 19.
 CVI $2n(n - 3)$ $n - 3$ the order of symmetric matrix W with elements $1, -1, i, -i$ satisfying $WW^* = (n - 2)I - J$ can be obtained; from Corollary 24.
 CVII $c_1 c_2$ Turyn; c_1 and c_2 both the orders of complex Hadamard matrices, Theorem 2.

Naturally, there is a complex Hadamard matrix for every order for which there is a real Hadamard matrix (see [3]), so the conjecture that complex Hadamard matrices exist for every even order includes the conjecture that Hadamard matrices exist for every order divisible by 4.

A square matrix $A = (a_{ij})$ of order n will be called *circulant* if $a_{ij} = a_{1, (j-i+1) \pmod n}$ and *back-circulant* if $a_{ij} = a_{1, (i+j-1) \pmod n}$. We recall, see [3], that a back-circulant matrix is symmetric and if A is circulant and B is back-circulant, then $AB^T = BA^T$. If A is circulant, then AR is back-circulant when $R = (r_{ij})$ of order n , that is $r_{ij} = \delta_{i+j, n+1}$ where δ is the Kronecker delta.

If g_1, g_2, \dots, g_n are the elements of an additive abelian group G of order n , then the square matrices $A = (a_{ij})$ and $B = (b_{ij})$ defined on some subsets X and Y of G by

$$a_{ij} = \begin{cases} 1 & g_j - g_i \in X \\ 0 & \text{otherwise} \end{cases} \quad b_{ij} = \begin{cases} 1 & g_j + g_i \in X \\ 0 & \text{otherwise} \end{cases}$$

all called type 1 and type 2 incidence matrices respectively. Then, see [3],

$$AB^T = BA^T.$$

Any matrix W of order h with zero diagonal and nondiagonal elements $1, -1, i, -i$ satisfying

$$WW^* = hI - J, \quad WJ = 0, \quad W^* = eW, \quad e = (-1)^{\alpha(h)}$$

$\alpha(h)$ a function of h , will be called a *core*. Any symmetric conference matrix or skew-Hadamard matrix may be put in the form

$$\left[\begin{array}{c|c} 1 & e \\ \hline \pm e^T & W + I \end{array} \right]$$

where e is the $1 \times h$ matrix of all 1s and W is a core.

Two matrices $M = I + U$ and N will be called (complex) *amicable Hadamard matrices* if M is a (complex) skew-Hadamard matrix and N an hermitian matrix satisfying

$$MN^* = NM^*.$$

There exist amicable Hadamard matrices for the orders

- AI 2 [3]
- AII $p^r + 1$ p^r (prime power) $\equiv 3 \pmod{4}$; [3]
- AIII $2(q + 1)$ q (prime power) $\equiv 1 \pmod{4}$ and $2q + 1$ a prime power; [3]
- AIV $2(q + 1)$ q (prime power) $\equiv 5 \pmod{8} = p^2 + 4$; [4]
- AV $4(q + 1)$ q (prime power) $\equiv 5 \pmod{8} = p^2 + 36$; [4]
- AVI s where s is the product of any of the above orders [3].

It would be interesting to find more of these matrices, both real and complex: currently, only real amicable Hadamard matrices are known.

Two Hadamard matrices M and N will be called *special Hadamard matrices* if $MN^T = -NM^T$. M and N will be called *complex special Hadamard matrices* if $MN^* = -NM^*$.

LEMMA 6 *Special (complex) Hadamard matrices exist for every order for which there exists a (complex) Hadamard matrix.*

Proof Let C be any (complex) Hadamard matrix of order c (c even). Let Q be $R_{\frac{1}{2}c} \times \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Then $Q^T = -Q$, $QQ^T = I$. Then if $M = C$ and $N = CQ$,

$$MN^* = CQ^*C^* = CQ^TC^* = -CQC^* = -NM^*.$$

So M and N are (complex) special Hadamard matrices.

2. CIRCULANT COMPLEX MATRICES

In earlier papers, this author used circulant matrices extensively to construct Hadamard matrices. We shall now give some complex analogues of these circulant matrices.

Let N of order n be the core of a symmetric conference matrix. Then

$$NN^T = nI - J, \quad NJ = 0, \quad N^T = N.$$

Choose

$$\begin{aligned} X &= \frac{1}{2}(J - I + N) \\ Y &= \frac{1}{2}(J - I - N). \end{aligned} \tag{1}$$

Now let W of order h be the core of a skew-Hadamard matrix. Then

$$WW^T = hI - J, \quad WJ = 0, \quad W^T = -W.$$

Choose

$$Z = \frac{1}{2}(J - I + W); \tag{2}$$

then

$$Z^T Z = ZZ^T = [(h + 1)I + (h - 3)J]/4, \quad Z + Z^T + I = J. \tag{3}$$

In the table, we give some matrices with elements $i, -i, 1, -1$ with interesting properties and how they may be formed.

Ref. no.	Equation	Construction	Order
1	$SS^* = [(h + 1)I + (h - 1)J]/2$	$S = I + Z + iZ^T$	$\equiv 3(\text{mod } 4)$
2	$SS^* = (n + 1)I - J$	$S = iI + N$	$\equiv 1(\text{mod } 4)$
3	$SS^* = 2I + (n - 2)J$	$S = J - I + iI$	any integer
4	$SS^* + RR^* = (n + 3)I + (n - 3)J$	$R = I + X + iY, S = -I + X + iY$	$\equiv 1(\text{mod } 4)$
5	$SS^* + RR^* = (n + 5)I + (n - 5)J$	$R = -I + X + iY, S = I + iX - Y$	$\equiv 1(\text{mod } 4)$
6	$SS^* + RR^* = 2(h + 1)I - 2J$	$R = iI + W, S = iI - W$	$\equiv 3(\text{mod } 4)$
		$RS^* = SR^*$	
7	$SS^* + RR^* = (h + 1)I + (h - 1)J$	$R = -I + Z + iZ^T, S = -I + iZ + Z^T$	$\equiv 3(\text{mod } 4)$
8	$SS^* + RR^* = (h + 5)I + (h - 5)J$	$R = I + Z + iZ^T, S = I + iZ + Z^T$	$\equiv 3(\text{mod } 4)$
9	$SS^* + RR^* = (h + 5)I + (h - 5)J$	$R = -I + Z - iZ^T, S = -I + Z + iZ^T$	$\equiv 3(\text{mod } 4)$

The existence of other matrices S and R with complex elements satisfying $SS^* + RR^* = aI + bJ, SR^* = RS^*$ would be valuable. The following lemma is proved in [3] and may also be easily proved using cyclotomy.

LEMMA 7 Let $p = 4m + 1$ be a prime power and let x be a primitive root of $GF(p)$ and generate the cyclic group G of order $p - 1 = 4m$. Define

$$C_j = \{x^{4k+j} : 0 \leq k \leq m - 1\} \quad j = 0, 1, 2, 3$$

and let D_j be the type 1 incidence matrix of C_j . Then

$$A = D_0 + iD_1 - D_2 - iD_3, \quad i = \sqrt{-1}$$

has zero diagonal and other elements $i, -i, 1, -1$ and satisfies

$$AA^* = pI - J.$$

3. CONSTRUCTIONS USING AMICABLE HADAMARD MATRICES

THEOREM 8 Let $W = I + S$ be a complex skew-Hadamard matrix of order s . Let $M = I + U$, $U^* = -U$ and N , where $N^* = N$ be complex amicable Hadamard matrices of order m . Suppose A , B , and C are matrices of order p with elements $1, -1, i, -i$ satisfying

$$\begin{aligned} AB^* &= BA^*, & AC^* &= CA^*, & BC^* &= CB^* \\ AA^* &= aI + (p - a)J, \\ BB^* &= bI + (p - b)J, & b &= mp - a(m - 1) - m(s - 1), \\ CC^* &= (p + 1)I - J. \end{aligned}$$

Then $K = I \times I \times B + I \times U \times A + S \times N \times C$ is a complex Hadamard matrix of order mps .

Proof
$$\begin{aligned} KK^* &= I \times I \times BB^* + I \times UU^* \times AA^* + SS^* \times NN^* \times CC^* \\ &\quad + I \times (U + U^*) \times AB^* + (S + S^*) \times N \times BC^* \\ &\quad + (S + S^*) \times UN^* \times AC^* \\ &= I \times I \times [bI + (p - b)J] + I \times (m - 1)I \times [aI + (p - a)J] \\ &\quad + (s - 1)I \times mI \times [(p + 1)I - J] \\ &= [b + a(m - 1) + m(s - 1)(p + 1)]I_{mps} \\ &\quad + [p - b + (m - 1)(p - a) - m(s - 1)]I_{ms} \times J_p \\ &= mpsI_{mps}. \end{aligned}$$

So K is a complete Hadamard matrix of order mps . ■

This theorem gives new infinite families of complex Hadamard matrices, but we have not found any new Hadamard matrices by using it.

COROLLARY 9 If, in Theorem 8, $B = I + R$ has $R^* = -R$ and A and C are hermitian, then K is a complex skew-Hadamard matrix.

COROLLARY 10 Suppose $S + I$ is a complex skew-Hadamard matrix of order s and A and C are matrices of order p with elements $1, -1, i, -i$ satisfying

$$\begin{aligned} AC^* &= CA^*, & AA^* &= (p - s + 1)I + (s - 1)J, \\ CC^* &= (p + 1)I - J. \end{aligned}$$

Then $K = I \times A + S \times C$ is a complex Hadamard matrix of order ps .

Proof Put $m = 1$, $B = A$ in the theorem. ■

COROLLARY 11 Suppose $S + I$ is a complex skew-Hadamard matrix of order s and there exists a core of order $p = s - 1$. Then there is a complex Hadamard matrix of order $s(s - 1)$.

Proof Choose $A = J$ and $C = I + \text{core}$ (if $s \equiv 3 \pmod{4}$) and $C = I + i \text{ core}$ (if $s \equiv 1 \pmod{4}$) in Corollary 9. ■

We may use Corollary 11 and Theorem 3 with $s = 18$ to obtain a complex Hadamard matrix of order 306, and with $s = 26$, to obtain a complex Hadamard matrix of order $650 = 59 \times 11 + 1$ for which order (by Theorem A) a symmetric conference matrix is impossible. We believe R. J. Turyn was aware of the result of Corollary 11.

Using Corollary 11, we get the following orders for complex Hadamard matrices. * signifies that a symmetric conference matrix for this order is not possible by Theorem A.

s	complex Hadamard order	comment
18	306	
26	$650 = 59 \times 11 + 1$	*
30	$870 = 79 \times 11 + 1$	*
38	$1406 = 281 \times 5 + 1$	
50	$2450 = 79 \times 31 + 1$	*
62	$3782 = 199 \times 19 + 1$	*

COROLLARY 12 Let $p \equiv 3 \pmod{4}$ be a prime power or equal to $q(q + 2)$ where both q and $q + 2$ are prime powers. Suppose there exists a symmetric conference matrix of order

- i) $p - 1$
- ii) $p - 2r^{n-1} + 1$ where $p = (r^{n+1} - 1)/(r - 1)$ and r is a prime power.

Then there exist complex Hadamard matrices of order

- i) $2p(p - 1)$
- ii) $2(r^{n+1} - 1)((r^{n+1} - 1)/(r - 1) - 2r^{n-1} + 1)/(r - 1)$

respectively.

Proof Choose for M and N the real amicable Hadamard matrices of order 2. Let $C - I$ be the core of the Hadamard matrix of order $p + 1$.

- i) Let $n = p - 1$, $A = J$ and $B = (J - 2I)$ in the theorem.
- ii) Let $n = p - 2r^{n-1} + 1$, $A = J$ and B , the type 1 $(1, -1)$ incidence matrix of the Singer difference set of appropriate order, in the theorem.

4. USING SPECIAL HADAMARD MATRICES

THEOREM 13 Let $W = I + S$ be a skew-Hadamard matrix (real or complex) of order s , and M and N be special (real or complex) Hadamard matrices of order m . Suppose A and B are matrices of order p with elements $1, -1, i, -i$ satisfying

$$\begin{aligned} AB^* &= BA^*, \\ AA^* &= aI + (p - a)J, \quad a = p - s + 1 \\ BB^* &= (p + 1)I - J. \end{aligned}$$

Then $K = I \times iM \times A + S \times N \times B$ is a complex Hadamard matrix of order mps .

$$\begin{aligned} \text{Proof } KK^* &= I \times MM^* \times AA^* + SS^* \times NN^* \times BB^* + \\ &\quad S^* \times iMN^* \times AB^* + S \times -iNM^* \times BA^* \\ &= I \times mI \times [aI + (p - a)J] + \\ &\quad (s - 1)I \times mI \times [(p + 1)I - J] \\ &= [ma + m(s - 1)(p + 1)]I_{mps} + \\ &\quad [m(p - a) - m(s - 1)]I_{ms} \times J_p \\ &= mpsI_{mps} \end{aligned}$$

and so is the required complex Hadamard matrix. ■

The results of Theorem 8 include the results of Theorem 11 which is given because the construction is different and the results may differ as new complex circulants are discovered.

COROLLARY 14 *Let m be the order of special Hadamard matrices and s be the order of a symmetric conference matrix. Then there exists a complex Hadamard matrix of order $ms(s - 1)$.*

Proof Choose $p = s - 1$, $A = J$ and $B = I + iN$ in the theorem.

This corollary shows that if $m = p + 1$ where $p \equiv 1 \pmod{4}$ is a prime power, there is a complex Hadamard matrix for all orders 306m, 650m, 870m, 1406m, 2450m, 3782m even though no symmetric conference matrix is known for the orders 306, 650, 870, 1406, 2450, 3782.

5. OTHER CONSTRUCTIONS

THEOREM 15 *If there exists a skew-Hadamard matrix $I + U$ of order $h = n - 1$ and a real symmetric conference matrix of order $n + 1$, then there exists a complex Hadamard matrix of order $2n(n - 1)$.*

Proof Let N be the core of the real symmetric conference matrix. Choose N, I, J of order n and

$$A = \begin{bmatrix} J - I + iI & J - I - iI \\ -J + I - iI & J - I - iI \end{bmatrix} \quad B = \begin{bmatrix} iI + N & -iI + N \\ iI + N & iI - N \end{bmatrix}.$$

Then $AB^* = BA^*$, $AA^* = I_2 \times (4I + 2(n - 2)J)$, $BB^* = I_2 \times (2(n + 1) - 2J)$. Hence

$$K = I \times A + U \times B$$

is the required complex Hadamard matrix. ■

This construction gives orders for which real Hadamard matrices are known but it may be able to be generalized.

We note that if $X^T = X$, $NX^T = XN^T$ and if $X - I + iI$ has elements 1, -1 , i , $-i$, then X could replace J in the above proof.

THEOREM 16 Suppose there exists symmetric conference matrices N and $M + I$ respectively of orders n and $m = n - a$. Further, suppose L is the core of N and there exists a complex matrix A of order $n - 1$ satisfying

$$LA^* = -AL^*, \quad AA^* = aI + (n - a - 1)J, \quad A = A^*$$

then there exists a complex Hadamard matrix of order $(n - 1)(n - a)$.

Proof $K = I \times A + M \times (L + iI)$ is the required matrix. ■

The next corollary may also be obtained from Theorem 8. So, although Theorem 16 potentially gives a new infinite family of complex Hadamard matrices, the lack of knowledge about possible matrices A restricts us.

COROLLARY 17 If there exists a symmetric conference matrix of order n , there exists a complex Hadamard matrix of order $n(n - 1)$.

Proof Choose $A = J_n$ in the Theorem 16. ■

THEOREM 18 Suppose there exists a symmetric conference matrix $C + I$ of order $n = m - a + 1$ and another of order $n + a$ with core N . Further suppose there exists a real matrix A of order $n + a - 1$ satisfying

$$A^T = A, \quad AN = NA \quad \text{and} \quad AA^* = aI + (n - 1)J.$$

Then there exists a complex Hadamard matrix of order $2n(n + a - 1)$.

Proof Let

$$X = \begin{bmatrix} iA & iA \\ -iA & iA \end{bmatrix} \quad Y = \begin{bmatrix} I + N & -I + N \\ -I + N & -I - N \end{bmatrix}$$

then

$$\begin{aligned} XX^* &= I_2 \times (2aI + 2(m - a)J), \\ YY^* &= I_2 \times (2(m + 1)I - 2J), \\ XY^* &= -YX^*. \end{aligned}$$

Now $K = I \times X + C \times Y$ is the required complex Hadamard matrix. ■

Again more knowledge of the matrices A is desirable. The corollaries indicate that we have new families of complex Hadamard matrices even though no new real Hadamard matrices of small order seem to arise.

COROLLARY 19 Suppose there exist symmetric conference matrices of orders

- i) $m + 1$ and
- ii) $m + 1$ and $m - 3$ respectively,

then there exist complex Hadamard matrices of orders

- i) $2m(m + 1)$ and
- ii) $2m(m - 3)$ respectively.

Proof Choose (i) $A = J_m$ and (ii) $A = J_m - 2I$ in the theorem. ■

This corollary gives a complex Hadamard matrix of order 3116 for which order an Hadamard matrix was only found between the writing and revising of this paper.

COROLLARY 20 *Suppose there exists a symmetric conference matrix of order n and another with type 1 core of order*

- i) $n + 4q^{t-1} - 1$, where $n = (q^{t+1} - 1)/(q - 1) + 1 - 4q^{t-1}$, q a prime power;
- ii) $n + 3x^2$, where $n = x^2 + 1$, $4x^2 + 1$ is prime, x odd;
- iii) $n + 3x^2 + 8$, where $n = x^2 + 1$, $4x^2 + 9$ is prime, x odd;
- iv) $n + 4(7b^2 + 1) - 1$, where $n = 36b^2 + 6$, $64b^2 + 9 = 8a^2 + 1$ is prime, a, b odd;
- v) $n + 4(7b^2 + 49) - 1$, where $n = 36b^2 + 246$, $64b^2 + 441 = 8a^2 + 49$ is prime, a odd, b even;

respectively; then there exist complex Hadamard matrices of orders

- i) $2n(n + 4q^{t-1} - 1)$;
- ii) $2(x^2 + 1)(4x^2 + 1)$;
- iii) $2(x^2 + 1)(4x^2 + 9)$;
- iv) $12(6b^2 + 1)(64b^2 + 9)$;
- v) $12(6b^2 + 41)(64b^2 + 441)$.

Proof In Theorem 19, choose for A the type 2 matrix given by the difference sets of the types

- i) Singer;
- ii) quartic residues;
- iii) quartic residues and zero;
- iv) octic residues;
- v) octic residues and zero;

respectively and for N the type 1 core of the appropriate symmetric conference matrix (see list of orders in Section 1).

THEOREM 21 *Suppose there exists a symmetric conference matrix $C + I$ of order $m = n + 1 - 2a$ and another of order $n + 2a$ with core N . Further suppose there exists a real matrix A of order $n + 2a - 1$ satisfying*

$$A^T = A, \quad AN = NA \quad \text{and} \quad AA^* = 4aI + (n - 2a - 1)J.$$

Then there exists a complex Hadamard matrix of order $2n(n + 2a - 1)$.

Proof Let

$$X = \begin{bmatrix} iJ & iA \\ -iA & iJ \end{bmatrix}, \quad Y = \begin{bmatrix} I + N & -I + N \\ -I + N & -I - N \end{bmatrix}$$

then

$$\begin{aligned} XX^* &= I_2 \times 4aI + (2m - 4a)J \\ YY^* &= I_2 \times 2(m + 1) - 2J \\ XY^* &= -YX^*. \end{aligned}$$

Now $K = I \times X + C \times Y$ is the required complex Hadamard matrix.

We again have a new infinite family of complex Hadamard matrices, but no new real Hadamard matrices of small order.

COROLLARY 22 *Suppose there exist symmetric conference matrices of order n and another with type 1 core of order*

- i) $(q^{t+1} - a)/(q - 1)$ where $n = (q^{t+1} - 1)/(q - 1) - 2a + 1$,
 $4a = 4q^{t-1} \equiv 0 \pmod{8}$, q a prime power,
- ii) $64b^2 + 9$ where $n = 64b^2 + 10 - 2a$, $4a = 4(7b^2 + 1) \equiv 0 \pmod{8}$,
 $64b^2 + 9 = 8d^2 + 1$ prime, d, b odd;
- iii) $64b^2 + 441$ where $n = 64b^2 + 442 - 2a$, $4a = 4(7b^2 + 49) \equiv 0 \pmod{8}$,
 $64b^2 + 441 = 8d^2 + 49$ prime, d odd, b even;

respectively, then there exist complex Hadamard matrices of orders

- i) $2[(q^{t+1} - 1)/(q - 1) - 2q^{t-1} - 1](q^{t+1} - 1)/(q - 1)$;
- ii) $4(25b^2 + 4)(64b^2 + 9)$;
- iii) $4(25b^2 + 172)(64b^2 + 441)$;

respectively.

Proof Use the type 2 matrices formed from the following difference sets for A

- i) Singer;
- ii) octic residues;
- iii) octic residues and zero;

respectively.

THEOREM 23 *Suppose there exists a symmetric conference matrix $I + S$ of order s and two matrices A, W with elements $1, -1, i, -i$ of order p satisfying*

$$\begin{aligned} AW^* &= WA^* \\ AA^* &= aI + (p - a)J, \quad a = 2(p - s + 1) \\ WW^* &= (p + 1)I - J. \end{aligned}$$

Then there exists a complex Hadamard matrix of order $2ps$.

Proof Let

$$X = \begin{bmatrix} iJ & iA \\ -iA & iJ \end{bmatrix}, \quad Y = \begin{bmatrix} W & W \\ W & -W \end{bmatrix}$$

then

$$\begin{aligned} XX^* &= I_2 \times (aI + (2p - a)J), \\ YY^* &= I_2 \times (2(p + 1)I - 2J), \\ XY^* &= -YX^*, \end{aligned}$$

when A is type 1 and W is type 2. Now $K = I \times X + S \times Y$ is the required complex Hadamard matrix. ■

As before, more knowledge of A might allow us to find new real Hadamard matrices. Again, we have a new infinite family of complex Hadamard matrices.

COROLLARY 24 *Suppose there exists a symmetric conference matrix of order s and a symmetric matrix W with elements $1, -1, i, -i$ of order $s - 3$ satisfying $WW^* = (s - 2)I - J$. Then there exists a complex Hadamard matrix of order $2s(s - 3)$.*

Proof Use $p = s - 3$ and $A = J - 2I$ in the theorem. ■

6. USING COMPLEX HADAMARD MATRICES AND QUATERNION MATRICES TO CONSTRUCT REAL HADAMARD MATRICES

In this section, we use the matrices

$$\begin{aligned} P &= \begin{bmatrix} 0 & - \\ 1 & 0 \end{bmatrix} \times I_{\frac{1}{2}m}, & K &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ - & 0 & 0 & 0 \\ 0 & 0 & 0 & - \\ 0 & 0 & 1 & 0 \end{bmatrix} \times I_{\frac{1}{4}m}, \\ L &= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ - & 0 & 0 & 0 \\ 0 & - & 0 & 0 \end{bmatrix} \times I_{\frac{1}{4}m}, & M &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & - & 0 \\ 0 & 1 & 0 & 0 \\ - & 0 & 0 & 0 \end{bmatrix} \times I_{\frac{1}{4}m} \end{aligned}$$

which are all of order m .

We note

$$\begin{aligned} PP^T &= KK^T = LL^T = MM^T = I, & K^T &= -K, & L^T &= -L, \\ M^T &= -M, & KL &= M = -LK, & LM &= K = -ML, \\ MK &= L = -KM. \end{aligned}$$

The orders of K, L, M and P should be derived from the context.

THEOREM 25 *Let $k > 2$ be the order of an Hadamard matrix and c be the order of a complex Hadamard matrix with core $A + iB$ satisfying*

$$\begin{aligned} AA^T + BB^T &= (c - 1)I - J, & AB^T &= BA^T, \\ A^T &= A, & B^T &= B, & BJ &= 0 = AJ. \end{aligned}$$

Let $C + I$ be a symmetric conference matrix of order n . Further suppose W is the type 2 $(1, -1)$ matrix of a $(c - 1, \frac{1}{4}(c - n) + u, u)$ -group difference set and that

$$WA^T = AW^T, \quad WB^T = BW^T.$$

Then

$$Z = C \times A \times MH + C \times B \times LH + C \times I \times KH + I \times W \times H$$

is an Hadamard matrix of order $kn(c - 1)$, with M, L, K given above.

Proof First we show Z is a $(1, -1)$ matrix. On the diagonal, there is $W \times H$, a $(1, -1)$ matrix, while off the diagonal we have

$$A \times MH + B \times LH + I \times KH.$$

Now MH, LH and H are $(1, -1)$ matrices and $A + B + I$ is a $(1, -1)$ matrix. So Z is a $(1, -1)$ matrix.

If U is a complex Hadamard matrix, it may be normalized to

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \cdot & & & \\ \cdot & A + iB + I & & \\ \cdot & & & \\ 1 & & & \end{bmatrix} \quad \text{where } (A + iB)(A + iB)^* + J = (c - 1)I.$$

Then $AA^T + BB^T = (n - 1)I - J$, $AJ = BJ = 0$ and $AB^T = BA^T$.

So

$$\begin{aligned} ZZ^T &= CC^T \times AA^T \times MH(MH)^T + CC^T \times BB^T \times LH(LH)^T \\ &\quad + CC^T \times I \times (KH)(KH)^T + I \times WW^T \times HH^T \\ &= I_n \times k\{(n - 1)(c - 1) + (n - 1) + (c - n)\} \times I_k + \\ &\quad I_n \times k\{-(n - 1) + (n - 1)\}J \times I_k \\ &= kn(c - 1)I_{kn(c-1)}. \end{aligned}$$

Hence Z is Hadamard. ■

The restriction $k > 2$ means we are unlikely to get new Hadamard matrices of small order from these constructions even though the families are new.

COROLLARY 26 Let $k > 2$ be the order of an Hadamard matrix H , n be the order of a symmetric conference matrix $C + I$ and suppose there exist $(1, -1)$ matrices $X + I, W$ of order $p \equiv 1 \pmod{4}$ satisfying

$$\text{a) } XW^T = WX^T, \quad X^T = X, \quad W^T = W,$$

$$\text{b) } XX^T = pI - J, \\ WW^T = (p - n + 1)I + (n - 1)J$$

then

$$Z = C \times H \times X + I \times LH \times W + C \times MH \times I$$

is an Hadamard matrix of order kpn , where

$$L = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \times I_{\frac{1}{2}k} \quad \text{and} \quad M = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \times I_{\frac{1}{2}k}.$$

Proof Off the diagonal we have $H \times X + MH \times I$ a $(1, -1)$ matrix and on the diagonal we have $LH \times W$ a $(1, -1)$ matrix. X replaces A and zero replaces B in the theorem. Then

$$\begin{aligned} ZZ^T &= CC^T \times HH^T \times XX^T + I \times LH(LH)^T \times WW^T + \\ &\quad CC^T \times MH(MH)^T \times I \\ &= (n - 1)I \times kI \times \{pI - J\} + \\ &\quad I \times kI \times \{(p - n + 1)I + (n - 1)J\} + k(n - 1)I \\ &= [kpn - kp + kp - kn + k + kn - k]I_{nkp} \\ &= kpnI_{kpn}. \end{aligned}$$

Hence Z is Hadamard. ■

COROLLARY 27 Let $k > 2$ be the order of an Hadamard matrix H , n be the order of a symmetric conference matrix $C + I$, then if $p \equiv 1 \pmod{4}$ p prime power, and there exists a $(p, \frac{1}{4}(p - n + 1) + u, u)$ -group difference set defined on the abelian group of $GF(p) \setminus \{0\}$, then there exists an Hadamard matrix of order kpn .

Proof Form the matrix Q by forming the type 1 incidence matrix of the set of quadratic residues of p . Then

$$Q^T = Q, \quad QQ^T = pI - J.$$

Let W be the type 2 $(1, -1)$ matrix of the $(p, \frac{1}{4}(p - n + 1) + u, u)$ -group difference set. Then

$$W^T = W, \quad WW^T = (p - n + 1)I + (n - 1)J.$$

Put $X = Q$ in the above corollary and we have the result. ■

COROLLARY 28 Let $k > 2$ be the order of an Hadamard matrix and n the order of a symmetric conference matrix, then there exists an Hadamard matrix of order

- i) $kn(n - 1)$,
- ii) $kn(n + 3)$, $n = p - 3$, $n + 4$ the order of a symmetric conference matrix,
- iii) $k(q - 1)(q - 2)(q^2 + q + 1)$ when q is a prime power, $q^2 + q + 1$ is prime and $n = q^2 - 3q + 2$,

- iv) $k(x^2 + 1)(4x^2 + 1)$ when x is odd, $4x^2 + 1$ is prime and $n = x^2 + 1$,
- v) $k(x^2 + 1)(4x^2 + 9)$ when x is odd, $4x^2 + 9$ is prime and $n = x^2 + 1$.

Proof Use the following results in the above corollary:

- i) a (p, p, p) -difference set always exists;
- ii) a $(p, p - 1, p - 2)$ -difference set always exists;
- iii) an S -type difference set $(p = q^2 + q + q + 1, q + 1, 1)$ exists for q a prime power;
- iv) a B -type difference $(p = 4x^2 + 1, x^2, \frac{1}{2}(x^2 - 1))$ exists for p a prime, x odd;
- v) a BO -type difference set $(p = 4x^2 + 9, x^2 + 3, \frac{1}{2}(x^2 + 3))$ exists for p a prime, x odd. ■

Clearly other difference sets could be used in the corollary, but these are omitted because they involve high order Hadamard matrices. W -type of Whiteman is omitted because of the difficulty in satisfying the condition $WX^T = XW^T$ of the corollary.

We note that the restriction $k > 2$ is not good as a result of Goethals and Seidel allows $k > 1$ in part (i) of Corollary 28.

COROLLARY 29 *There exists a symmetric conference matrix of order $q^s + 1$ where $q^s \equiv 1 \pmod{4}$. If $k > 2$ is the order of an Hadamard matrix, then there is an Hadamard matrix of order*

- i) $kq^s(q^s + 1)$,
- ii) $k(q^s + 1)(q^s + 4)$, when there is a symmetric conference matrix of order $q^s + 5$.

References

- [1] Marshall Hall, Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass. (1967).
- [2] Richard J. Turyn, Complex Hadamard matrices, *Combinatorial Structures and their Applications*, Gordon and Breach, New York (1970), pp. 435–437.
- [3] W. D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Springer-Verlag, Berlin–Heidelberg–New York (1972).
- [4] Jennifer Wallis, A note on amicable Hadamard matrices, *Utilitas Mathematica* **3** (1973), 119–125.