

## Some $(1, -1)$ Matrices

JENNIFER WALLIS

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

*Communicated by Marshall Hall, Jr.*

Received January 16, 1969

### ABSTRACT

We define an  $n$ -type  $(1, -1)$  matrix  $N = I + R$  of order  $n \equiv 2 \pmod{4}$  to have  $R$  symmetric and  $R^2 = (n-1)I_n$ . These matrices are analogous to skew-type matrices  $M = I + W$  which have  $W$  skew-symmetric.

If  $n$  is the order of an  $n$ -type matrix,  $h_1$  and  $h_2$  the orders of Hadamard matrices,  $h$  the order of a skew-Hadamard matrix, and  $p^r \equiv 1 \pmod{4}$  is a prime power then we show there are:

$n$ -type matrices of orders  $p^r + 1$ ,  $(h-1)^2 + 1$ ,  $(n-1)^2 + 1$ ,  $(n-1)^3 + 1$ ;  
symmetric Hadamard matrices of orders  $2n$ ,  $2n(n-1)$ ,  $2p^r(p^r + 1)$ ;  
Hadamard matrices of orders  $h_1n$ ,  $h_1h_2n(n-1)$ ,  $h_1h_2n(n-3)$

(this latter with  $n+4$  also the order of an  $n$ -type matrix);

Hadamard matrices of orders 452, 612, 2452 and 3044, all "new."

We also give existence conditions for many other classes of Hadamard matrices and another formulation for Goldberg's skew-Hadamard matrix of order  $(h-1)^3 + 1$ .

### INTRODUCTION

An *Hadamard matrix*  $H$  is a matrix of order  $n$ , all of whose elements are  $+1$  or  $-1$  and which satisfies  $HH^T = nI_n$ . It is conjectured that an Hadamard matrix exists for  $n = 2$  and 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 [2], [3], and [4]. Hadamard matrices are known for all orders less than 188.

An Hadamard matrix  $H = S + I$  is called *skew-Hadamard* if  $S^T = -S$ . It is conjectured that, whenever there exists an Hadamard matrix of order  $n$ , there exists a skew-Hadamard matrix of the same order. As the existence of skew-Hadamard matrices is needed for some of my results I list the classes of orders for which skew-Hadamard matrices are known to exist:

- |       |                     |   |
|-------|---------------------|---|
| I.    | $2^t \prod k_i$     | $t, r_i$ all positive integers, $k_i = p_i^{r_i} + 1 \equiv 0 \pmod{4}$ $p_i$ a prime; from [5].                            |
| II.   | $(p-1)^3 + 1$       | $p$ the order of a skew Hadamard matrix; from [1].  |
| III.  | $2^t(q+1)$          | $t \geq 1$ an integer, $q$ (prime power) $\equiv 5 \pmod{8}$ ; from [7].  |
| IV.   | 52                  | From [6].   |
| V.    | 36                  | From [8].   |
| VI.   | $p^r(p^r + 1)(m-1)$ | $(m-1)(p^r + 1)/m$ the order of a skew-Hadamard matrix, $m$ of class I and $p^r \equiv 3 \pmod{4}$ a prime power; from [4]. |
| VII.  | $p^r(p^r - 3)(m-1)$ | $(m-1)(p^r + 3)/m$ the order of a skew-Hadamard matrix, $m$ and $p^r$ as in class VI; from [4].                             |
| VIII. | $h(p^r + 1)$        | $h$ the order of a skew-Hadamard matrix, $p^r \equiv 3 \pmod{4}$ a prime power; from [4].                                   |
| IX.   | $2h$                | $h$ the order of a skew-Hadamard matrix.  |

The only orders up to 200 for which skew-Hadamard matrices have not yet been discovered are 92, 100, 116, 148, 156, 172, 184, 188, and 196.

A  $(v, k, \lambda)$ -configuration is an arrangement of  $v$  elements  $x_1, x_2, \dots, x_v$  into  $v$  sets  $S_1, S_2, \dots, S_v$  such that every set contains exactly  $k$  elements, every pair of sets has exactly  $\lambda$  elements in common. A  $(v, k, \lambda)$ -configuration can be characterized by its *incidence matrix*  $A = (a_{ij})$  defined by  $a_{ij} = 1$  if  $x_j \in S_i$  and  $a_{ij} = -1$  if  $x_j \notin S_i$ . This matrix  $A$ , of order  $v$ , consists entirely of 1's and  $-1$ 's, and it can be seen that  $A$  satisfies the *incidence equation*

$$AA^T = 4(k - \lambda)I + v - 4(k - \lambda)J$$

where  $I$  is the identity matrix of order  $v$  and  $J$  is the matrix of order  $v$  with every element  $+1$ .

A set of elements  $D = \{x_1, x_2, \dots, x_k\}$  will be said to generate a *circulant*  $(1, -1)$  matrix  $A = (a_{ij})$  if  $a_{ij} = a_{1, j-i+1} = 1$  when  $j - i + 1 \in D$  (all numbers modulo  $v$ ) and  $-1$  otherwise. A *back-circulant* matrix  $A = (a_{ij})$  of order  $v$  has  $a_{1i} = a_{1+j, i-j}$  where  $1 + j$  and  $i - j$  are reduced to modulo  $v$ .

DEFINITION. A (1, -1) matrix  $N = I + R$  of order  $n \equiv 2 \pmod{4}$  will be called  $n$ -type if  $N$  can be written as

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & D & \\ 1 & & & \end{bmatrix} + I_n, \quad (1)$$

where  $D^T = D$  and  $D^2 = (n-1)I_{n-1} - J_{n-1}$  or equivalently if  $R^T = R$  and  $R^2 = (n-1)I_n$ .

We now investigate the existence of  $n$ -type matrices and we will show three classes of these matrices exist:

- I.  $p^r + 1$   $p^r \equiv 1 \pmod{4}$  is a prime power.
- II.  $(n-1)^2 + 1$  Where  $n$  is either the order of a skew-Hadamard matrix or the order of an  $n$ -type matrix.
- III.  $(n-1)^3 + 1$  Where  $n$  is the order of an  $n$ -type matrix.

PROOF OF CLASS I. The observation that matrices of order  $p^r + 1 \equiv 2 \pmod{4}$ , where  $q = p^r$  is a prime power, can be found satisfying the requirements for  $n$ -type matrices is due to Williamson [5, p. 66]. As in [5] we define  $D = (d_{ij})$  of order  $q$  by

$$\begin{aligned} d_{ii} &= 0, \\ d_{ij} &= \chi(a_i - a_j), \quad i \neq j, \end{aligned}$$

where  $a_1, a_2, \dots, a_q$  are the elements of a Galois field in some fixed order and  $\chi(a) = 1$  or  $-1$  according as  $a$  is or is not the square of an element of the  $GF(p^r)$ . Since  $q \equiv 1 \pmod{4}$ ,  $\chi(x) = \chi(-x)$ , so  $D$  is symmetric and  $D^2 = p^r I - J$ .

Then

$$N = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & D & \\ 1 & & & \end{bmatrix} + I_{p^r+1},$$

is an  $n$ -type matrix of order  $p^r + 1$ .

PROOF OF CLASS II. If  $N$  is an  $n$ -type matrix of order  $n$  then  $N$  may be written as

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & D & \\ 1 & & & \end{bmatrix} + I_{n-1} \quad (3)$$

where  $D^T = D$ ,  $DD^T = (n-1)I_{n-1} - J_{n-1}$  and  $DJ_{n-1} = 0$ .

If  $V$  is a skew-Hadamard matrix of order  $n$  then  $V$  may be written as

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & W & \\ -1 & & & \end{bmatrix} + I_{n-1}, \quad (4)$$

where  $W^T = -W$ ,  $WW^T = (n-1)I_{n-1} - J_{n-1}$  and  $WJ_{n-1} = 0$ .

Now where  $X$  is either  $W$  or  $D$  define  $A$  by

$$A = J_{n-1} \times -I_{n-1} + I_{n-1} \times J_{n-1} + X \times X;$$

then

$$\begin{aligned} AA^T &= (n-1)J_{n-1} \times I_{n-1} + I_{n-1} \times (n-1)J_{n-1} \\ &\quad + [(n-1)I_{n-1} - J_{n-1}] \times [(n-1)I_{n-1} - J_{n-1}] \\ &\quad - 2J_{n-1} \times J_{n-1} \\ &= (n-1)^2 I_{(n-1)^2} - J_{(n-1)^2}. \end{aligned}$$

Now  $A^T = A$  if  $X \times X = X^T \times X^T$ , but this is true for both  $W$  and  $D$  and so

$$M = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix} + I_{(n-1)^2+1}$$

is an  $n$ -type matrix of order  $(n-1)^2 + 1$ .

**PROOF OF CLASS III.** With  $D$  as in (3) and  $D, J$ , and  $I$  all of order  $n-1$  we define

$$A = I \times D \times J + J \times I \times D + D \times J \times I + D \times D \times D.$$

This is similar to Goldberg's construction for Hadamard matrices as his matrix may be written as

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & B & \\ -1 & & & \end{bmatrix},$$

where  $B$  is given by

$$B = I \times I \times I + I \times W \times J + J \times I \times W + W \times J \times I + W \times W \times W$$

with  $W$  as defined in (4).

Now  $DJ = 0$  so

$$\begin{aligned} AA^T &= I \times D^2 \times J^2 + J^2 \times I \times D^2 + D^2 \times J^2 \times I + D^2 \times D^2 \times D^2 \\ &= I \times [(n-1)I - J] \times (n-1)J + (n-1)J \times I \times [(n-1)I - J] \\ &\quad + [(n-1)I - J] \times (n-1)J \times I + [(n-1)I - J] \times [(n-1)I - J] \\ &\quad \times [(n-1)I - J] \\ &= (n-1)^3 I_{(n-1)^3} - J_{(n-1)^3}, \end{aligned}$$

and clearly  $A^T = A$ .

So

$$M = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{bmatrix} + I_{(n-1)^3+1}$$

is an  $n$ -type matrix of order  $(n-1)^3 + 1$ .

LEMMA 1. *If there is an  $n$ -type matrix of order  $n$ , then there is a symmetric Hadamard matrix of order  $2n$ .*

PROOF: Let  $N = I + P$  be the  $n$ -type matrix of order  $n$ . Then  $P^2 = (n-1)I_n$  and  $P^T = P$ , Now choose

$$X = \begin{bmatrix} -P - I & P - I \\ P - I & P + I \end{bmatrix};$$

then  $X^T = X$  and  $XX^T = 2nI_{2n}$ . So  $X$  is the required symmetric Hadamard matrix.

Since there are skew-Hadamard matrices of orders 16, 36, and 40 using class II we see there are  $n$ -type matrices of order 226, 1226, and 1522. Then using the above lemma there are symmetric Hadamard matrices of orders 452, 2452, and 3044. These orders are new.

LEMMA 2. *If there is an  $n$ -type matrix of order  $n$  and an Hadamard matrix of order  $h$ , then there is an Hadamard matrix order  $hn$ .*



then

$$X^T = X, Y^T = Y, XX^T = 2(n-1)J_{n-1} \times I_2, YY^T = (2nI_{n-1} - 2J_{n-1}) \times I_2,$$

and  $XY^T + YX^T = 0$ .

Then, if

$$H = I_n \times X \dot{+} R \times Y,$$

$H$  is symmetric and, since

$$\begin{aligned} HH^T &= I_n \times XX^T + R \times (YX^T + XY^T) \dot{+} RR^T \times YY^T \\ &= I_n \times 2(n-1)J_n \times I_2 + (n-1)I_n \times (2nI_{n-1} - 2J_{n-1}) \times I_2 \\ &= 2n(n-1)I_{2n(n-1)}, \end{aligned}$$

$H$  is Hadamard.

**COROLLARY 4.** *If  $p^r \equiv 1 \pmod{4}$  is a prime power, then there is a symmetric Hadamard matrix of order  $2p^r(p^r + 1)$ .*

**PROOF:** This follows by putting  $n$  equal to orders of class I.

This corollary is important as it means class VII of Marshall Hall [2, p. 207] may be partially rewritten. The construction gives an Hadamard matrix of order 612 which was previously not known.

**THEOREM 5.** *If  $N = I \dot{+} R$  is an  $n$ -type matrix of order  $m$ , then, if there are symmetric (1, -1) matrices  $D \dot{+} I$  and  $M$  satisfying  $D^2 = nI_n - J_n$ ,  $M^2 = (n + 1 - m)I_n \dot{+} (m - 1)J_n$ , and  $MD = DM$ , where  $D$  has zero diagonal, there is an Hadamard matrix of order  $4mn$ .*

**PROOF:** Choose

$$X = \begin{bmatrix} M & M & M & M \\ M & -M & -M & M \\ M & -M & M & -M \\ M & M & -M & -M \end{bmatrix}$$

and

$$Y = \begin{bmatrix} D + I & -D - I & D - I & -D + I \\ -D - I & -D - I & D - I & D - I \\ -D + I & -D + I & -D - I & -D - I \\ +D - I & -D + I & -D - I & D + I \end{bmatrix};$$

then  $XY^T + YX^T = 0$ ,  $XX^T = [4(n+1-m)I_n + 4(m-1)J_n] \times I_4$  and  $YY^T = [4(n+1)I_n - 4J_n] \times I_4$ , so, if

$$H = I_m \times X + R \times Y$$

then

$$\begin{aligned} HH^T &= I_m \times XX^T + R \times (XY^T + YX^T) + R^2 \times YY^T \\ &= I_m \times [4(n+1-m)I_n + 4(m-1)J_n] \times I_4 \\ &\quad + (m-1)I_m \times [4(n-1)I_n - 4J_n] \times I_4 \\ &= 4nmI_{4nm}. \end{aligned}$$

So  $H$  is an Hadamard matrix of order  $4nm$ .

**COROLLARY 6.** *If  $m$  is the order of an  $n$ -type matrix, then, if there is a back-circulant  $(1, -1)$  matrix  $M$  of order  $p \equiv 1 \pmod{4}$ , a prime, satisfying  $M^2 = (p+1-m)I + (m-1)J$ , then there is an Hadamard matrix of order  $4pm$ .*

**PROOF:** This follows with  $n$  of the theorem of class I and  $D$  defined as in (2). By Theorem 1 of [3], a circulant  $D$  and a back-circulant  $M$  satisfy  $MD^T = DM^T$  and since  $M$  and  $D$  are both symmetric the conditions of the theorem are satisfied.

**COROLLARY 7.** *If there is a  $n$ -type matrix of order:*

- (i)  $p^r - 3$ ;
- (ii)  $p - 4q^{n-1} + 1$ , where  $p = q^n + q^{n-1} + \dots + 1$ ,  $n$  integer;
- (iii)  $q^2 - 3q + 2$ , where  $p = q^2 + q + 1$ ;
- (iv)  $x^2 + 1$ , where  $p = 4x^2 + 1$ ;
- (v)  $x^2 + 1$ , where  $p = 4x^2 + 9$ ;
- (vi)  $36b^2 + 6$ , where  $p = 8a^2 + 1 = 64b^2 + 9$ ,  $b$  odd;
- (vii)  $36b^2 + 250$ , where  $p = 8a^2 + 49 = 64b^2 + 441$ ,  $b$  even;

with  $p$  (prime)  $\equiv 1 \pmod{4}$ ,  $q$  prime power, and  $x$  and  $a$  odd, then there are Hadamard matrices of orders:

- (i)  $4p^r(p^r - 3)$ ;
- (ii)  $4(q^n + q^{n-1} + \dots + 1)(q^n - 3q^{n-1} + q^{n-2} + \dots + q^2 + q + 2)$ ;
- (iii)  $4(q-1)(q-2)(q^2 + q + 1)$ ;
- (iv)  $4(x^2 + 1)(4x^2 + 1)$ ;
- (v)  $4(x^2 + 1)(4x^2 + 9)$ ;



- (vi)  $24(6b^2 + 1)(64b^2 + 9)$ ;  
 (vii)  $8(18b^2 + 125)(64b^2 + 441)$ ;  
 respectively.

PROOF: In each case but (i)  $M$  of the corollary is a back-circulant matrix generated by a difference set: the notation we use for these difference sets is that of Marshall Hall [2, p. 141]. The proof follows with  $M$  given by (i)  $J-2I$ ; (ii)  $S$ ; (iii)  $S$  with  $n = 3$ ; (iv)  $B$ ; (v)  $B_0$ ; (vi)  $O$ ; (vii)  $O_0$ ; respectively.

THEOREM 8. *If  $h > 1$  is the order of an Hadamard matrix,  $n$  is the order of an  $n$ -type matrix and  $v \equiv 1 \pmod{4}$  the order of three (1, -1) matrices  $A$ ,  $B$ , and  $D + I$  which satisfy  $DD^T = vI - J$ ,  $AA^T = aI + (v - a)J$ ,  $BB^T = [2(v - n + 1) - a]I + [-v + 2(n - 1) + a]J$ , and  $AB^T$ ,  $BD^T$ , and  $AD^T$  all symmetric, where  $D$  has zero diagonal, then there is an Hadamard matrix of order  $2nvh$ .*

PROOF: Let  $I_n + R$  be the  $n$ -type matrix,  $H$  the Hadamard matrix, and  $K = HS$  be as defined in the proof of Lemma 2. Now choose

$$X = \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \quad \text{and} \quad Y = \begin{bmatrix} D + I & D - I \\ -D + I & D + I \end{bmatrix};$$

then  $XY^T = YX^T$ . So

$$W = I_n \times H \times X + R \times K \times Y$$

is the required matrix.

In the constructions of Williamson shown in Marshall Hall [2, pp. 214–216],  $m$  and  $n$  are defined as being of the form  $p^r + 1$ , where  $p^r \equiv 1 \pmod{4}$  is a prime power; if we read instead that  $m$  and  $n$  are the orders of  $n$ -type matrices, then the same proofs give us the theorem

THEOREM 9. *If Hadamard matrices of orders  $h_1$  and  $h_2$  exist,  $h_1 > 1$ ,  $h_2 > 1$  and (i)  $n$ ; (ii)  $n$  and  $n + 4$ , are the orders of  $n$ -type matrices; there exist Hadamard matrices of orders*

- (i)  $h_1 h_2 n(n - 1)$ ;  
 (ii)  $h_1 h_2 n(n + 3)$ ;  
 respectively.

THEOREM 10. *If there is an  $n$ -type matrix of order  $n$  and  $k$  is the order of three (1, -1) matrices  $A$ ,  $C$ , and  $D + I$  satisfying*

$$AA^T = aI + (k - a)J, \quad CC^T = (2k - 2n + 2 - a)I + (-k + 2n - 2 + a)J,$$

$DD^T = kI - J$ , and  $AC^T$ ,  $CD^T$ , and  $AD^T$  all symmetric where  $D$  has zero diagonal, then there is an Hadamard matrix of order  $4kn$ .

PROOF: Define

$$M = \begin{bmatrix} A & A & C & C \\ A & -A & C & -C \\ C & C & -A & -A \\ C & -C & -A & A \end{bmatrix}$$

and

$$P = \begin{bmatrix} -D - I & D + I & D - I & -D + I \\ D + I & D + I & -D + I & -D + I \\ -D + I & D - I & -D - I & D + I \\ D - I & D - I & D + I & D + I \end{bmatrix};$$

then, since  $AC^T$ ,  $CD^T$ , and  $AD^T$  are all symmetric,  $MP^T + PM^T = 0$ . Also

$$MM^T = \{4(k - n + 1)I_k + 4(n - 1)J_k\} \times I_4,$$

$$PP^T = \{4(k + 1)I_k - 4J_k\} \times I_4.$$

So, if  $N = I + R$  is the  $n$ -type matrix,  $R^T = R$  and  $R^2 = (n - 1)I_n$ . Now consider

$$H = I_n \times M + R \times P,$$

then

$$\begin{aligned} HH^T &= I_n \times MM^T + R \times \{MP^T + PM^T\} + R^2 \times PP^T \\ &= 4knI_{4kn}. \end{aligned}$$

So  $H$  is the required Hadamard matrix.

COROLLARY 11. *If there is an  $n$ -type matrix of order*

- (i)  $q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q + 2$ , where  $p = q^n + q^{n-1} + \dots + q + 1$ ,  $n$  integer;
- (ii)  $q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q$ ,  $p$  as in (i);
- (iii)  $(5x^2 - 1)/2$ , where  $p = 4x^2 + 1$ ;
- (iv)  $(5x^2 + 7)/2$ , where  $p = 4x^2 + 9$ ;
- (v)  $50b^2 + 8$ , where  $p = 8a^2 + 1 = 64b^2 + 9$ ,  $b$  odd;
- (vi)  $50b^2 + 346$ , where  $p = 8a^2 + 49 = 64b^2 + 441$ ,  $b$  even;

with  $p$  (prime)  $\equiv 1 \pmod{4}$ ,  $q$  prime power, and  $x$  and  $a$  odd, then there are Hadamard matrices of orders

- (i)  $4(q^n + q^{n-1} + \dots + 1)(q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q + 2)$ ;
- (ii)  $4(q^n + q^{n-1} + \dots + 1)(q^n - q^{n-1} + q^{n-2} + \dots + q^2 + q)$ ;
- (iii)  $2(5x^2 - 1)(4x^2 + 1)$ ;
- (iv)  $2(5x^2 + 7)(4x^2 + 9)$ ;
- (v)  $8(25b^2 + 4)(64b^2 + 9)$ ;
- (vi)  $8(25b^2 + 173)(64b^2 + 441)$ .

PROOF. In each case  $C$  of the theorem is a back-circulant matrix generated by a difference set; we again use the notation of Marshall Hall [2, p. 141]. The proof follows with

- (i)  $A = J, C = S, q$  powers of 2;
- (ii)  $A = J - 2I, C = S, q \equiv 3 \pmod{4}$ ;
- (iii)  $A = J - 2I, C = B$ ;
- (iv)  $A = J - 2I, C = B_0$ ;
- (v)  $A = J, C = O$ ;
- (vi)  $A = J, C = O_0$ .

*Note Added in Proof.* Dr. J. M. Goethals has pointed out to me that some of the results of this paper overlap those of [9].

#### REFERENCES

1. K. GOLDBERG, Hadamard Matrices of Order Cube Plus One, *Proc. Amer. Math. Soc.* **17** (1966), 744-746.
2. M. HALL, JR., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.
3. J. WALLIS, A Class of Hadamard Matrices, *J. Combinatorial Theory* **6** (1969), 40-44.
4. J. WALLIS,  $(v, k, \lambda)$  Configurations and Hadamard Matrices, to appear in *J. Australian Math. Soc.*
5. J. WILLIAMSON, Hadamard's Determinant Theorem and the Sum of Four Squares, *Duke Math. J.* **11** (1944), 65-81.
6. D. BLATT AND G. SZEKERES, A Skew Hadamard Matrix of Order 52, *Canad. J. Math.* **22** (1970), 1319-1322.
7. G. SZEKERES, Tournaments and Hadamard Matrices, *Enseignement Math.* **XV** (1969), 269-278.
8. J. M. GOETHALS AND J. J. SEIDEL, A Skew Hadamard Matrix of Order 36, to appear in *J. Australian Math. Soc.*
9. J. M. GOETHALS AND J. J. SEIDEL, Orthogonal Matrices with Zero Diagonal, *Canad. J. Math.* **19** (1967), 1001-1010.