1973

Hadamard matrices of order 28m, 36m, and 44m

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

Hadamard matrices of order 28m, 36m, and 44m

Abstract

We show that if four suitable matrices of order m exist then there are Hadamard matrices of order 28 m, 36 m, and 44 m. In particular we show that Hadamard matrices of orders 14(q + 1), 18(q + 1), and 22(q + 1) exist when q is a prime power and q = l(mod 4).

Also we show that if n is the order of a conference matrix there is an Hadamard matrix of order 4mn. As a consequence there are Hadamard matrices of the following orders less than 4000:

476, 532, 836, 1036, 1012, 1100, 1148, 1276, 1364, 1372, 1476, 1672, 1836,2024, 2052, 2156, 2212, 2380, 2484, 2508, 2548, 2716, 3036, 3476, 3892.

All these orders seem to be new.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, Hadamard matrices of order 28m, 36m, and 44m, Journal of Combinatorial Theory, Ser. A., 15, (1973), 323-328.

Reprinted from JOURNAL OF COMBINATORIAL THEORY Vol. 15, No. 3, November 1973

Note

Hadamard Matrices of Order 28m, 36m and 44m

JENNIFER WALLIS

I.A.S., A.N.U., Canberra, Australia

Communicated by Marshall Hall, Jr.

Received March 16, 1972

We show that if four suitable matrices of order m exist then there are Hadamard matrices of order 28 m, 36 m, and 44 m. In particular we show that Hadamard matrices of orders $14(q+1)$, $18(q+1)$, and $22(q+1)$ exist when q is a prime power and $q \equiv 1 (\text{mod } 4)$.

Also we show that if n is the order of a conference matrix there is an Hadamard matrix of order $4mn$.

As a consequence there are Hadamard matrices of the following orders less than 4000:

476, 532, 836, 1036, 1012, 1100, 1148, 1276, 1364, 1372, 1476, 1672, 1836, 2024, 2052, 2156, 2212, 2380, 2484, 2508, 2548, 2716, 3036, 3476, 3892.

All these orders seem to be new.

Suppose a square matrix $A = (a_{ij})$ of side n has the property that the entry in position (i, j) always equals the entry in position $(i + 1, j + 1)$, where these coordinates are reduced modulo n if necessary. Then the matrix is completely determined by its first row; in fact if $T = T_n = (t_{ij})$ is the $n \times n$ matrix defined by

$$\begin{aligned} t_{i,i+1} &= 1, \qquad i = 1, 2, \ldots, n-1, \\ t_{n,1} &= 1, \\ t_{i,j} &= 0, \qquad \text{otherwise,} \end{aligned}$$

then A can be written

$$A = \sum_{j=1}^{n} a_{1j} T^{j-1}.$$

We say A is a *circulant* matrix, formed by *circulating* the row

$$(a_{11}, a_{12}, \ldots, a_{1n}).$$

Similarly, if P is an $n \times n$ array of $m \times m$ submatrices P_{ij} where $P_{i+1,j+1} = P_{ij}$ (subscripts reduced modulo n), that is

$$P = \sum_{j=1}^{n} T^{j-1} \times P_{1j}$$

(where $\times$ denotes Kronecker product), we shall say P is formed by circulating

$$(P_{11}, P_{12}, \ldots, P_{1n}).$$

We denote by R a square back-diagonal matrix whose order shall be determined by context : if $R = (r_{ij})$ is of order n then

$$r_{ij} = 1, \qquad \text{when } i + j = n + 1,$$
$$r_{ij} = 0, \qquad \text{otherwise.}$$

We consider a set of four $n \times n$ arrays X, Y, Z, and W which are formed by circulating their first rows; the entries shall be $m \times m$ matrices chosen from a set of four matrices $\{A, B, C, D\}$.

LEMMA 1. *If A, B, C, and D commute in pairs then X, Y, Z, and W commute in pairs.*

In particular, Lemma 1 is satisfied if A, B, C, and D are circulant.

LEMMA 2. *If S and P are chosen from $\{X, Y, Z, W\}$ and if A, B, C, and D are circulant matrices then*

$$SRP^T = PRS^T. \tag{1}$$

Proof. It is known (see [6]) that equation (1) would hold if S and P were circulant. In particular

$$E_i RF_j^T = F_j RE_i^T$$

when E_i and F_j belong to $\{A, B, C, D\}$, and

$$T^i RT^{n-j} = T^j RT^{n-i}.$$

If we write

$$S = \sum_{i=0}^{n-1} T^i \times E_i, \qquad P = \sum_{j=0}^{n-1} T^j \times F_j,$$

then

$$
\begin{aligned}
SRP^T &= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} (T^i \times E_i)\, R(T^{n-j} \times F_j{}^T) \\
&= \sum\sum (T^i \times E_i)(R \times R)(T^{n-j} \times F_j{}^T) \\
&= \sum\sum (T^i R T^{n-j} \times E_i R F_j{}^T) \\
&= \sum\sum (T^j R T^{n-i} \times F_j R E_i{}^T) \\
&= PRS^T.
\end{aligned}
$$

Suppose

$$XX^T + YY^T + ZZ^T + WW^T = I_n \times n(AA^T + BB^T + CC^T + DD^T). \tag{2}$$

Then it is easy to verify that the matrix

$$H = \begin{bmatrix} X & YR & ZR & WR \\ -YR & X & -W^TR & Z^TR \\ -ZR & W^TR & X & -Y^TR \\ -WR & -Z^TR & Y^TR & X \end{bmatrix}$$

(which is a form of block-matrix introduced by Goethals and Seidel in [2]) satisfies

$$HH^T = nI_{4n} \times (AA^T + BB^T + CC^T + DD^T) \tag{3}$$

provided that X, Y, Z, and W pairwise commute and pairwise satisfy (1).

LEMMA 3. *If A, B, C, and D are such that AB^T, AC^T, AD^T, BC^T, BD^T, and CD^T are symmetric, then the first rows*

$$
\begin{array}{rl}
(C, A, -A, -B, -B, A, D) & \textit{for}\ \ X, \\
(-D, -B, B, -A, -A, -B, C) & \textit{for}\ \ Y, \\
(-A, C, -C, D, D, C, B) & \textit{for}\ \ Z, \\
(B, -D, D, C, C, -D, A) & \textit{for}\ \ W
\end{array}
$$

give matrices which satisfy (2) *for the case $n = 7$, the first rows*

$$
\begin{array}{rl}
(C, B, -A, -A, A, C, A, B, -D) & \textit{for}\ \ X, \\
(A, -C, -D, A, B, B, -B, -D, -B) & \textit{for}\ \ Y, \\
(A, -C, D, B, A, D, C, C, -C) & \textit{for}\ \ Z, \\
(-B, D, C, A, -B, C, -D, -D, D) & \textit{for}\ \ W
\end{array}
$$

give matrices which satisfy (2) *for the case* $n = 9$, *and the first rows*

$$\begin{array}{rl} (C, B, A, A, -A, B, -A, B, B, -B, A) & \textit{for} \quad X, \\ (D, A, -B, -B, B, A, B, A, A, -A, -B) & \textit{for} \quad Y, \\ (-A, D, C, C, -C, D, -C, D, D, -D, C) & \textit{for} \quad Z, \\ (-B, C, -D, -D, D, C, D, C, C, -C, -D) & \textit{for} \quad W \end{array}$$

give matrices which satisfy (2) *for the case* $n = 11$.

The verification is straightforward.

If $AA^T + BB^T + CC^T + DD^T = 4mI_m$ and if H has all its entries 1 or -1, then equation (3) means that H is Hadamard. So, gathering together the foregoing results, we have the following theorem:

THEOREM 4. *If there exist square circulant* $(1, -1)$ *matrices* A, B, C, *and* D *of order* m *which satisfy*

$$AA^T + BB^T + CC^T + DD^T = 4mI$$

and are such that AB^T, AC^T, AD^T, BC^T, BD^T, *and* CD^T *are symmetric, then there are Hadamard matrices of orders* $28m$, $36m$, *and* $44m$.

Matrices A, B, C, and D satisfying the conditions of Theorem 4 were previously used to construct Hadamard matrices of orders $4m$ [11], $12m$ [1], and $20m$ (unpublished result of L. R. Welch, communicated to the author by L. D. Baumert). They are known to exist when m is a member of the set

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

[3], and when $2m - 1$ is a prime power congruent to 1 modulo 4 [4, 10].

COROLLARY 5. *There exist Hadamard matrices of orders* $28m$, $36m$, *and* $44m$ *whenever* $m \in M$.

COROLLARY 6. *There exist Hadamard matrices of orders* $14(q + 1)$, $18(q + 1)$, *and* $22(q + 1)$ *whenever* q *is a prime power congruent to* 1 *modulo* 4.

This gives Hadamard matrices of twenty-two orders less than 4000 for which no matrices were previously known, namely,

476, 532, 836, 1012, 1036, 1100, 1148, 1276, 1364, 1372, 1476, 1672, 1836, 2024, 2052, 2156, 2212, 2380, 2484, 2508, 2548, 2716, 3036, 3476, 3892.

A *conference matrix* N is a $(0, 1, -1)$ matrix with zero diagonal and every other element $+1$ or -1 which satisfies

$$NN^T = (n-1)\, I_n, \qquad NJ = 0, \qquad N^T = eN, \qquad e = \pm 1,$$

where J is the matrix with every element $+1$. These are discussed in [5, 7, 8, 9] where they are sometimes called n-type and skew-Hadamard matrices. Some of Turyn's constructions for complex Hadamard matrices are equivalent to conference matrices when $n \equiv 2 (\bmod 4)$.

Symmetric conference matrices are known to exist for orders $p + 1$ when $p \equiv 1 (\bmod 4)$ is a prime power and $(h-1)^2 + 1$ when h is the order of a skew-Hadamard matrix. The skew-Hadamard matrices (skew-symmetric conference matrices) are listed in [7, 8, 9] but in particular they exist for orders $p + 1$, $p \equiv 3 (\bmod 4)$, a prime power.

Then we have:

THEOREM 7. *Let*

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad A_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix},$$

and let N be the core of a conference matrix of order n; if A, B, C, D are four $(1, -1)$ *matrices which pairwise satisfy $XY^T = YX^T$ and if*

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

then

$$\begin{aligned} H = {} & A_1 \times N \times A + A_1 \times I \times B + A_2 \times N \times -B + A_2 \times I \times A \\ & + A_3 \times N \times C + A_3 \times I \times D + A_4 \times N \times -D + A_4 \times I \times C \end{aligned}$$

is an Hadamard matrix of order $4mn$.

COROLLARY 8. *Let p be any prime power and $m \in M$; then there exists an Hadamard matrix of order* $4m(p + 1)$.

REFERENCES

1. L. D. BAUMERT AND M. HALL, JR., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169–170.
2. J. M. GOETHALS AND J. J. SEIDEL, A skew-Hadamard matrix of order 36. *J. Austral. Math. Soc.* **11** (1970), 343–344.
3. M. HALL, JR., "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
4. R. TURYN, An infinite class of Williamson matrices, *J. Combinatorial Theory* **12** (1972), 319–321.
5. R. J. TURYN, On *C*-matrices of arbitrary powers, *Canad. J. Math.* **23** (1971), 531–535.
6. J. WALLIS, A class of Hadamard matrices, *J. Combinatorial Theory* **6** (1969), 40–44.
7. J. WALLIS, (v, k, λ)-configurations and Hadamard matrices, *J. Austral. Math. Soc.* **11** (1970), 297–309.
8. J. WALLIS, A skew-Hadamard matrix of order 92, *Bull. Austral. Math. Soc.* **5** (1971), 203–204.
9. A. L. WHITEMAN, Skew-Hadamard matrices of Goethals-Seidel type, *Discrete Math.* **2** (1972), 397–405.
10. A. L. WHITEMAN, An infinite family of Hadamard matrices of Williamson type, *J. Combinatorial Theory*, to appear.
11. J. WILLIAMSON, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.