1969

Equivalence of Hadamard matrices

W. D. Wallis

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

Abstract
Suppose In is a square-free odd integer, and A and B are any two Hadamard matrices of order 4m. We will show that A and B are equivalent over the integers (that is, B can be obtained from A using elementary row and column operations which involve only integers).

Publication Details
W.D.Wallis and Jennifer Seberry Wallis, Equivalence of Hadamard matrices, Israel Journal of Mathematics, 7, (1969), 122-128.

EQUIVALENCE OF HADAMARD MATRICES

BY
W. D. WALLIS AND JENNIFER WALLIS

ABSTRACT

Suppose m is a square-free odd integer, and A and B are any two Hadamard matrices of order $4m$. We will show that A and B are equivalent over the integers (that is, B can be obtained from A using elementary row and column operations which involve only integers).

Integral equivalence. If A and B are matrices over the ring $\mathbf{Z}$ of integers, A and B are called *equivalent* ($A \sim B$) if there are $\mathbf{Z}$-matrices P and Q, of determinant ± 1, such that

$$B = PAQ.$$

This is the same as saying that B can be obtained from A by performing some sequence of the following operations:

(a) add an integer multiple of one row to another,

(b) negate some row,

(c) reorder the rows,

and the corresponding column operations. The main result about equivalence is

LEMMA. *If A is any $n \times n$ $\mathbf{Z}$-matrix, then there is a unique $\mathbf{Z}$-matrix*

$$D = \mathrm{diag}(a_1, a_2, \cdots, a_n)$$

such that $A \sim D$ and

$$a_1 | a_2 | \cdots | a_r, \ a_{r+1} = \cdots = a_n = 0,$$

Received January 29, 1969.

where the a_i are non-negative. The greatest common divisor of $i \times i$ subdeterminants of A is

$$a_1 a_2 a_3 \cdots a_i.$$

If $A \sim E$ where

$$E = \left[\begin{array}{cccc|c} a_1 & & & & \\ & a_2 & & & 0 \\ & & \cdots & & \\ & & & a_i & \\ \hline & & 0 & & F \end{array}\right]$$

then a_{i+1} is the greatest common divisor of non-zero elements of F.

The a_i are called *invariants* of A.

Hadamard matrices. An Hadamard matrix A of order n is an $n \times n$ matrix whose elements are ± 1 and which satisfies

$$AA^T = nI_n.$$

(See, for example, Chapter 14 of [1]). If A is any Hadamard matrix we can find an Hadamard matrix H satisfying

$$H \sim A,$$

$$H = \left[\begin{array}{c|cccc} 1 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & \\ 1 & & & B & \\ \vdots & & & & \\ 1 & & & & \end{array}\right]$$

simply by negating rows and columns, H is then *normalized.*

The determinant of an Hadamard matrix is

$$\pm\, n^{1/2n}$$

Certain invariants. Suppose A is an Hadamard matrix of order $n = 4m$. We will find some of the invariants of A. There is no loss of generality in assuming that A is normalized.

Since every element is ± 1, a_1 must be 1. Now subtract the first row from every other row, and then the first column from every other column. The resulting matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & K \end{bmatrix}$$

is equivalent to A, and every element of K is 0 or -2. So

$$a_2 = 2.$$

By definition

$$a_{4m} = \pm \frac{|A|}{a_1 a_2 \cdots a_{4m-1}};$$

the numerator is $(4m)^{2m}$, and the denominator is the greatest common divisor of the $(4m-1)$-subdeterminants of A. We shall now evaluate this greatest common divisor.

Suppose C is any $(4m-1)$-subdeterminant of A. Then

$$A \sim \left[\begin{array}{c|c} \pm 1 & \pm 1 \cdots \pm 1 \\ \hline \pm 1 & \\ \cdots & C \\ \pm 1 & \end{array}\right]$$

$$\sim \left[\begin{array}{c|c} 1 & 1 \cdots 1 \\ \hline 1 & \\ \cdots & B \\ 1 & \end{array}\right] = F;$$

B is obtained from C by negating rows and columns, hence

$$|B| = \pm |C|.$$

F is Hadamard, so

$$FF^T = 4mI_{4m};$$

but

$$FF^T = \left[\begin{array}{c|c} 4m & \\ \hline & BB^T + J_{4m-1} \end{array}\right]$$

where J_v is the $v \times v$ matrix whose every element is $+1$. Therefore

$$BB^T = 4mI_{4m-1} - J_{4m-1}.$$

$$|(r-\lambda)I_v + \lambda J_v| = \{r + (v-1)\lambda\}(r-\lambda)^{v-1}$$

[2, p. 99], whence, putting $v = r = 4m - 1$, $\lambda = -1$,

$$|B|^2 = (4m)^{4m-2},$$

$$|C| = \pm (4m)^{2m-1}.$$

This works for any $(4m-1)$-subdeterminant, so the greatest common divisor is $(4m)^{2m-1}$, and

$$a_{4m} = 4m.$$

When m is odd and square-free. We continue the notation of the last section, and further suppose that m is odd and square-free. Since 2 must divide every invariant but a_1, write

$$b_i = \tfrac{1}{2}a_i, \quad i > 1.$$

$$|A| = \pm (4m)^{2m} = \pm 2^{4m}m^{2m};$$

but on the other hand

$$|A| = \pm \prod a_i$$

$$= \pm 2^{4m} m \prod_{i=2}^{4m-1} b_i;$$

therefore

$$\prod_{i=2}^{4m-1} b_i = m^{2m-1}.$$

If p is any prime factor of m, then p^{2m-1} is a factor of this product. p^2 does not divide a_{4m}, so p^2 cannot divide any of the b_i. Hence exactly $2m - 1$ of them must have a factor p. By the property

$$a_1 \,|\, a_2 \,|\, a_3 \cdots,$$

these must be $b_{2m+1}, \cdots, b_{4m-1}$. Hence m divides each of these b_i; the rest must all be 1. We have

THEOREM 1. *If A is Hadamard of order $4m$, where m is odd and square-free then the invariants of A are*

$$\begin{aligned} &1 \text{ (once)} \\ &2 \ (2m-1 \text{ times}) \\ &2m \ (2m-1 \text{ times}) \\ &4m \text{ (once).} \end{aligned}$$

COROLLARY. *Any two Hadamard matrices of order* $4m$, *where* m *is and odd square-free, are* $\mathbf{Z}$*-equivalent.*

When m is even. We can partially extend Theorem 1 to the case where m is even and square-free. If H is an Hadamard matrix of order $2m$, then

$$A = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is Hadamard of order $4m$. Now

$$\begin{aligned} A &\sim \begin{bmatrix} H & 0 \\ 0 & -2H \end{bmatrix} \\ &\sim \begin{bmatrix} D & 0 \\ 0 & 2D \end{bmatrix}, \end{aligned}$$

where D is the diagonal matrix of Theorem 1 corresponding to H. (The theorem can be applied, as $\frac{1}{2}m$ is odd). Thus A is equivalent to a diagonal matrix with elements

$$\begin{aligned} &1 \text{ (once)} \\ &2 \ (m \text{ times}) \\ &m \ (m-1 \text{ times}) \\ &2m \ (m \text{ times}) \\ &4 \ (m-1 \text{ times}) \\ &4m \text{ (once).} \end{aligned}$$

There is a $(2m)$-subdeterminant

$$1 \cdot 2^m \cdot m^{m-1} = 2^{2m-1}k,$$

where k is odd, and another

$$1 \cdot 2^m \cdot 4^{m-1} = 2^{3m-2}.$$

The greatest common divisor of these is 2^{2m-1}, so

$$a_1 a_2 \cdots a_{2m} \leqq 2^{2m-1}.$$

On the other hand each a_i (after a_1) is divisible by 2, hence

$$a_1 a_2 \cdots a_{2m} \geqq 2^{2m-1};$$

equality holds, and

$$a_1 = 1,\ a_2 = a_3 = \cdots = a_{2m} = 2.$$

Now we find a_{4m-1}. From an earlier result

$$a_1 a_2 \cdots a_{4m-1} = (4m)^{2m-1}.$$

One $(4m-2)$-subdeterminant is

$$\delta = 2(4m)^{2m-2}$$

obtained by deleting the diagonal elements $4m$ and $2m$. Every other $(4m$–$2)$-subdeterminant results from replacing one or two of the diagonal elements of δ by $2m$ or $4m$ (or both); every diagonal element of δ divides $2m$, so δ divides every other $(4m-2)$-subdeterminant. Therefore

$$a_1 a_2 \cdots a_{4m-2} = 2(4m)^{2m-2},$$
$$a_{4m-1} = 2m.$$

Since m is square-free,

$$a_{2m+1} = a_{2m+2} = \cdots = a_{4m-2} = 2m.$$

Thus we have proven

THEOREM 2. *If m is even and square-free, and if there is an Hadamard matrix of order $2m$, then there is an Hadamard matrix of order $4m$ of the type in Theorem* 1.

However it is possible that there are also matrices of these orders with other invariants.

Trivial cases. In the trivial cases ($n = 1$ or 2) the invariants are of the type in Theorem 1.

A matrix of order 16. Finally we show that there is an Hadamard matrix whose invariants are not in the form of Theorem 1. Let H be an Hadamard matrix of order 4. The invariants of H are thus $\{1, 2, 2, 4\}$. If A is the direct product $H \times H$ then

$$A \sim \operatorname{diag}(1,2,2,4) \times \operatorname{diag}(1,2,2,4).$$

This is a diagonal matrix with elements

1 (once)
2 (four times)
4 (six times)
8 (four times)
16 (once),

and these are clearly the invariants of A.

REFERENCES

1. M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.
2. H. J. Ryser, *Combinatorial Mathematics*, (Carus Monograph No. 14), Wiley, New York, 1963.

La Trobe University,
Bundoora,
Victoria, 3083,
Australia