

INTEGRAL EQUIVALENCE OF HADAMARD MATRICES

BY
W. D. WALLIS

ABSTRACT

Suppose A is a non-singular matrix with entries 0 and 1, the zero and identity elements of a Euclidean domain. We obtain a "best-possible" lower bound for the number of equivalence invariants of A (over the domain) which equal 1. From this it is proven that the sequence of invariants under integral equivalence of an Hadamard matrix must obey certain conditions. Finally, lower bounds are found for the number of inequivalent Hadamard matrices of order a power of 2, and consequently for the number of Hadamard-inequivalent Hadamard matrices of those orders.

1. Introduction and notations. This paper is a sequel to our joint paper with Jennifer Wallis [8] on the integral equivalence of Hadamard matrices.

An Hadamard matrix of order n is an $n \times n$ integer matrix with all entries $+1$ and -1 whose rows (and consequently columns) are mutually orthogonal. The determinant of such a matrix is $\pm n^{n/2}$. The matrix can only exist when n is divisible by 4, except for the trivial cases $n = 1$ and $n = 2$. Hadamard matrices are discussed in standard works such as [4] and [6].

We write I for an identity matrix, O for a zero matrix or vector, J for a square matrix with every entry $+1$, and ε for a column vector with every entry $+1$; dimension, if not clear from the context, is shown by a subscript. The determinant of A is denoted $|A|$; direct sum and direct (Kronecker) product are written \oplus and \times respectively. By $\Delta_i(A)$ we will mean the greatest common divisor of non-zero $i \times i$ subdeterminants of A .

2. Equivalence. Suppose E is a Euclidean domain. Matrices A and B over E are called E -equivalent if there exist unimodular E -matrices (matrices whose determinants are units of E) P and Q satisfying

Received December 1, 1970 and in revised form April 21, 1971

$$A = PBQ;$$

we write $A \sim B$. In other words, $A \sim B$ whenever B can be obtained by performing on A some finite sequence of the row operations "add an E -multiple of some row to another", "multiply some row by a unit of E ", "permute the rows", and the column operations derived by replacing "row" by "column" throughout. "Equivalence" is an equivalence relation.

If A is a square E -matrix of order n , then there exist n elements $\alpha_1, \alpha_2, \dots, \alpha_n$ of E , the (E -equivalence) invariants of A , which are uniquely defined up to multiplication by a unit and satisfy

$$\begin{aligned} A &\sim \text{diag}(\alpha_1, \alpha_2, \dots, \alpha_n) \\ \alpha_i &\neq 0 \text{ for } 1 \leq i \leq r, \text{ some } r; \alpha_i = 0 \text{ for } i > r \\ \alpha_i &\mid \alpha_{i+1} \text{ for } 1 \leq i \leq r-1 \\ \Delta_i(A) &= \alpha_1 \alpha_2 \cdots \alpha_i. \end{aligned}$$

If $1 \leq i \leq r-1$, and if

$$A \sim \text{diag}(\alpha_1, \alpha_2, \dots, \alpha_i) \oplus F,$$

then α_{i+1} is the greatest common divisor of the entries of F . Clearly $A \sim B$ if and only if A and B have the same invariants. (For proof, see standard texts.)

We are particularly interested in the case of integral equivalence, where E is the ring of integers. Then the only units are 1 and -1 ; we define the set of invariants uniquely by choosing each α_i to be non-negative.

Another equivalence relation used on Hadamard matrices is *Hadamard equivalence*, where the permissible operations are negation (of rows or of columns) and permutation (of rows or of columns). Obviously Hadamard equivalence implies integral equivalence. An Hadamard matrix is called normalized if every entry in its first row and column is $+1$; clearly every Hadamard matrix is Hadamard equivalent to a normalized matrix (in fact only negation need be used). Hadamard equivalence is defined, for example, in [4].

In [8] we proved the following results:

LEMMA 1. If A is an Hadamard matrix of order $4m$, then

$$(1) \quad \Delta_2(A) = 2, \quad \Delta_{4m-1}(A) = (4m)^{2m-1};$$

in other words

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

THEOREM 1. *An Hadamard matrix of order $4m$, where m is odd and square-free, has invariants*

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

COROLLARY 1. *Two Hadamard matrices of order $4m$, where m is odd and square-free, are integrally equivalent.*

The following results have been proven by Morris Newman in [5]*.

THEOREM 2. *If A is an Hadamard matrix of order $4m$, then*

$$a_i = 4m/a_{4m-i+1}$$

for $1 \leq i \leq 4m$.

COROLLARY 2. *$a_{4m-1} = 2m$, and the restriction that m is odd can be removed from Theorem 1 and Corollary 1.*

In the following section we obtain a general result which places restrictions on the invariants of an Hadamard matrix. Section 4 is concerned with the existence of inequivalent Hadamard matrices of various orders.

3. The number of invariants equal to 1. We know from (2) that an Hadamard matrix has exactly one invariant equal to 1, and that the next invariant is 2. In this section a lower limit for the number of invariants equal to 2 is found as a consequence of a general result of independent interest. We write $[x]$ for the largest integer not exceeding x .

THEOREM 3. *Suppose B is an $n \times n$ matrix of non-zero determinant whose entries are all 0 and 1, the zero and identity elements of a Euclidean domain E . Then the number of invariants of B under E -equivalence which equal 1 is at least*

$$[\log_2 n] + 1.$$

PROOF. Write t for $[\log_2 n]$; that is, t is the unique integer such that $2^t \leq n < 2^{t+1}$. We shall use a sequence of E -equivalence operations to transform B to

* These results have also been found by E. Spence (private communication). The author is indebted to the referee for informing him of Newman's result, thus obviating a long and tedious proof of Corollary 2.

$$I_t \oplus D,$$

where 1 is a greatest common divisor of the entries in D .

The first part of the process is to reorder the rows and columns of B so that, in the reordered matrix, columns 1 and 2 have different entries in the first row, columns 3 and 4 are identical in the first row but have different entries in the second row, and in general columns $2i - 1$ and $2i$ are identical in the first $i - 1$ rows but differ in row i for $i = 1, 2, \dots, t$. This is done using the following algorithm.

Step 1. Select two columns of B which have different entries in the first row. (If the first row of B has every entry 1, it will first be necessary to subtract some other row from row 1.) Reorder columns so that the two chosen columns become columns 1 and 2 (in either order).

Step 2. Select two columns of the matrix just formed, neither of them being columns 1 or 2, which have identical entries in the first row. Reorder the rows of the matrix other than row 1 so that the two columns chosen have different entries in the new second row. Reorder columns after column 2 so that the new pair become columns 3 and 4.

Step k . In the matrix resulting from step $k - 1$, select two columns to the right of column $2k - 2$ which are identical in rows 1 to $k - 1$. Reorder the rows after row $k - 1$ and the columns after column $2k - 2$ so that the chosen columns become columns $2k - 1$ and $2k$ and differ in their k th row.

It is always possible in step k to find a row in which the two chosen columns differ, since the matrix cannot have two identical columns. Therefore, step k only requires that we can choose two columns from the $n - 2k + 2$ available ones which are identical in their first $k - 1$ places. Since there are only 2^{k-1} different $(0, 1)$ -vectors of length $k - 1$, this will be possible provided

$$2^{k-1} < n - 2k + 2,$$

and this is always true for $1 \leq k \leq t$ except when $k = t$ and $n = 4$ or $n = 8$. In the case $n = 4$, it is easy to check by hand that every $(0, 1)$ matrix of non-zero determinant is E -equivalent to a matrix on which t steps can be carried out. If $n = 8$, step 3 will be impossible if the first two rows of the last four columns contain all $(0, 1)$ -vectors of length 2; typically the first two rows are

$$\begin{array}{cccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ * & * & 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

and in this case we can proceed with step 3 if we first apply the column permutation (37) (48). Consequently t steps can always be carried out.

In the second stage, select if possible two columns (columns a and b say) which are identical in rows 1 to t ; reorder the later rows so that columns a and b differ in row $t + 1$. If the selection was impossible then $n = 2^t$ and the first t rows of the matrix constitute the 2^t different column vectors, so one column (column a say) will start with t zeros; reorder the rows from $t + 1$ on so that there is a 1 in the $(t + 1, a)$ position. In either case, if column a was in a pair chosen in stage 1, reorder the pair if necessary so that a is even; and similarly for b if two were chosen.

The third stage isolates certain entries ± 1 by carrying out t steps:

Step 1. Subtract column 2 from column 1, so that the $(1, 1)$ entry becomes ± 1 . Then add a suitable multiple of the first column to every other column to ensure that row 1 has every entry 0 except the first, and similarly eliminate all entries except the first from column 1 by adding suitable multiples of row 1 to the other rows.

After step 1 the matrix has first row and column $(\pm 1, 0, 0, \dots, 0)$; whatever multiple of column 1 was added to column $2k - 1$ ($2 \leq k \leq t$), the same multiple was added to column $2k$, so that the $(k, 2k - 1)$ and $(k, 2k)$ entries still differ by 1. It will be seen from the description of the general step that, after $k - 1$ steps, the matrix will have its first $k - 1$ rows zero except for entries ± 1 in the $(i, 2i - 1)$ positions, $1 \leq i \leq k - 1$; the first $k - 1$ odd-numbered columns will be zero except at those positions; and for $k \leq i \leq t$ the $(i, 2i - 1)$ and $(i, 2i)$ entries differ by 1 and the $(j, 2i - 1)$ and $(j, 2i)$ entries are equal when $j < i$. After step k this description can be extended by replacing $k - 1$ by k .

Step k. Subtract column $2k$ from column $2k - 1$, so that the $(k, 2k - 1)$ entry becomes ± 1 . Add a suitable multiple of column $2k - 1$ to every subsequent column, and then add suitable multiples of row k to the later rows, so that row k and column $2k - 1$ become zero except at their intersection.

Observe that if $k < i \leq t$ the $(k, 2i - 1)$ and $(k, 2i)$ entries were equal before step k , so the same multiple of column $2k - 1$ was added to both columns $2i - 1$ and $2i$ and the difference between these columns is unchanged. If two columns, a and b , were chosen at stage two, then the difference between those columns is unaltered in the t steps; if only one column was chosen then that column is unaltered in the t steps since it has never had a non-zero entry in its k th row to be eliminated.

Finally, reorder the columns so that the former columns $1, 3, \dots, 2t - 1$ become the first t columns. We obtain

$$\begin{bmatrix} I_t & 0 \\ 0 & D \end{bmatrix};$$

D contains either two entries which differ by 1 (corresponding to the former $(a, t + 1)$ and $(b, t + 1)$ entries) or has an entry 1 (the former $(a, t + 1)$ entry) depending on the course followed at stage 2, and in either case the greatest common divisor of entries of D is 1.

Therefore, B has at least $t + 1$ invariants equal to 1.

COROLLARY 3. *An Hadamard matrix of order $4m$ has at least*

$$[\log_2(4m - 1)] + 1$$

invariants equal to 2, and by Theorem 2 it has at least this number of invariants equal to $2m$.

PROOF. Let A be an Hadamard matrix of order $4m$; assume A to be normalized. Subtract row 1 from every other row and then column 1 from every other column: we obtain

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -2B \end{pmatrix}$$

where B is an $(0, 1)$ -matrix of size $4m - 1$ with non-zero determinant. The first invariant of A is 1; the others are double the invariants of B . The result follows from Theorem 3.

THEOREM 4. *Suppose E is a Euclidean domain with characteristic not equal to 2, and suppose f and g are monotonic nondecreasing functions which satisfy:*

- (i) *any Hadamard matrix of order N has at least $f(N)$ invariants equal to 2;*
- (ii) *any $(0, 1)$ -matrix over E which has non-zero determinant and is of size $r \times r$ has at least $g(r)$ invariants equal to 1.*

Then

$$(3) \quad f(N) \leq [\log_2(N - 1)] + 1$$

and, if 2 is a non-unit of E ,

$$g(r) \leq [\log_2 r] + 1.$$

PROOF. The function on the right hand side of (3) is a step-function which

increases in value just after N takes as its value a power of 2. So, if (3) is false, we must have

$$f(2^t) > [\log_2(2^t - 1)] + 1 = t$$

for some t . However, for every t , there is an Hadamard matrix A of order 2^t which has precisely t invariants 2. Let

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

which has invariants $\{1, 2\}$, and define A as the direct product of t copies of H . Then $A \sim D$, where D is the direct product of t copies of $\text{diag}(1, 2)$; D is a diagonal matrix whose entries are powers of 2, and 2^a occurs $\binom{t}{a}$ times. These must be the invariants of A . A has precisely t invariants equal to 2.

If we consider A as a matrix over E , rather than an integer matrix, and pass to B as in the proof of Corollary 4, then B is a $(0, 1)$ -matrix over E of size $r = 2^t - 1$, and has non-zero determinant (as the characteristic of E is not 2). The invariants of B are 2^a , $\binom{t}{a+1}$ times each, for $a = 0, 1, \dots, t-1$. 2^a and 2^b are the same invariant if and only if 2^{b-a} is a unit of E , and this cannot occur when $a \neq b$ provided 2 is a non-unit. So the matrix B can be used to prove the part of the Theorem involving g .

Theorem 4 shows that the results of Theorem 3 and Corollary 3 are best-possible in a certain sense unless E has characteristic 2 or 2 is a unit of E . If 2 were a unit then the matrix B has every invariant 2 (or 1, which is the same thing), and if E had characteristic 2 then we could not divide by 2 to get B .

4. The number of inequivalent matrices. The results of the preceding sections place restrictions on the possible invariants of Hadamard matrices, even when the order is divisible by 16 or by an odd square. For example, the invariants of an Hadamard matrix of order 16 must be of the form

1 (once)

2 (α times)

4 (β times)

8 (α times)

16 (once);

since the number of invariants is 16 and their product is 16^8 , we must have

these four matrices are integrally inequivalent; A, B, C and D have four, five, six and seven invariants respectively equal to 2.

This result—that integral equivalence and Hadamard-equivalence-plus-transposition come to the same thing—is trivially true for Hadamard matrices of order less than 16 (there is only one matrix of each order under Hadamard equivalence); however, it is false for order 20. Hall [3] finds three inequivalent Hadamard matrices under Hadamard equivalence, and these remain inequivalent if transposition is allowed; however, all Hadamard matrices of order 20 are integrally equivalent by Theorem 1.

To discuss higher powers of 2 we use a generating function for the numbers of invariants. Suppose H , of order 2^a , has invariants 2^i occurring α_i times. Put

$$f(H, t) = 1 + \alpha_1 t + \alpha_2 t^2 + \cdots + t^a.$$

Then if

$$f(K, t) = 1 + \beta_1 t + \beta_2 t^2 + \cdots + t^b,$$

the direct product $H \times K$ will be equivalent to the direct product of the two diagonal matrices, which has 2^k as an entry $\alpha_k + \alpha_{k+1}\beta_1 + \cdots + \beta_k$ times; so

$$f(H \times K, t) = f(H, t)f(K, t).$$

Suppose H and K are Hadamard matrices of order 2^a with

$$f(H, t) = \sum \alpha_i t^i, \quad f(K, t) = \sum \beta_i t^i.$$

Write H_2 for an Hadamard matrix of order 2;

$$f(H_2, t) = (1 + t),$$

so

$$f(H_2 \times H, t) = \sum_{i=0}^{a+1} (\alpha_i + \alpha_{i-1}) t^i$$

$$f(H_2 \times K, t) = \sum_{i=0}^{a+1} (\beta_i + \beta_{i-1}) t^i$$

(with the conventions $\alpha_{-1} = \alpha_{a+1} = \beta_{-1} = \beta_{a+1} = 0$). Clearly these functions cannot be identical unless $f(H, t) = f(K, t)$. Therefore

LEMMA 3. $H_2 \times H$ and $H_2 \times K$ are integrally equivalent if and only if H and K are integrally equivalent.

The generating functions of A and B , the given matrices of order 16, are

$$f(A, t) = 1 + 4t + 6t^2 + 4t^3 + t^4$$

$$f(B, t) = 1 + 5t + 4t^2 + 5t^3 + t^4.$$

Consider the direct product H_{ab} of a copies of A with b copies of B .

$$f(H_{ab}, t) = f(A, t)^a f(B, t)^b = 1 + (4a + 5b)t + t^2(\dots).$$

If we vary a from 0 to n and put $b = n - a$, we get $n + 1$ different coefficients of t , and consequently $n + 1$ inequivalent matrices of order 16^n . From Lemma 3 there will be at least $n + 1$ inequivalent matrices of double this order, so there are at least $[m/4] + 1$ inequivalent Hadamard matrices of order 2^m .

COROLLARY 4. *Given any positive integer N , there are infinitely many orders for which there are at least N integrally inequivalent (and therefore Hadamard inequivalent) Hadamard matrices of that order. The smallest such order is at most 16^{N-1} .*

The best previous result along those lines, apart from those of Hall mentioned above, is that of L. D. Baumert [1] who showed that there are 6 Hadamard-inequivalent matrices of order 2^n when $n \geq 5$. Some other work on Hadamard equivalence is contained in [7].

The numerical estimates in Corollary 4 and the preceding discussion can be improved using the other Hadamard matrices of order 16, but this seems pointless at this stage. We could only prove, for example, that 4 distinct matrices of order 32 exist. The results of the earlier sections leave 11 possible sets of invariants of that order, and we conjecture that all 11 can be realized.

REFERENCES

1. L. D. Baumert, *Six inequivalent Hadamard matrices of order 2^n , $n \geq 5$* , J.P.L. Research Summary No. 36-12, 1 (1962), 74-76.
2. M. Hall Jr., *Hadamard matrices of order 16*, J.P.L. Research Summary No. 36-10, 1 (1961), 21-26.
3. M. Hall Jr., *Hadamard matrices of order 20* (Technical Report No. 32-761), J.P.L., Pasadena, 1965.
4. M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham, 1967.
5. Morris Newman, *Invariant factors of combinatorial matrices*, Israel J. Math. 10 (1971), 126-130.
6. H. J. Ryser, *Combinatorial Mathematics* (M.A.A. Carus Monograph No. 14), Wiley, New York, 1963.
7. J. J. Stiffler and L. D. Baumert, *Inequivalent Hadamard matrices*, J.P.L. Research Summary No. 36-9, 1 (1961), 28-30.
8. W. D. Wallis and Jennifer Wallis, *Equivalence of Hadamard matrices*, Israel J. Math. 7 (1969), 122-128.