NOTE ON HADAMARD'S DETERMINANT THEOREM

JOHN WILLIAMSON

Introduction. We shall call a square matrix A of order n an Hadamard matrix or for brevity an H-matrix, if each element of A has the value ± 1 and if the determinant of A has the maximum possible value $n^{n/2}$. It is known that such a matrix A is an H-matrix [1][1] if, and only if, $AA' = nE_n$ where A' is the transpose of A and E_n is the unit matrix of order n. It is also known that, if an H-matrix of order $n>1$ exists, n must have the value 2 or be divisible by 4. The existence of an H-matrix of order n has been proved [**2**, **3**] only for the following values of $n>1$: (a) $n=2$, (b) $n=p^h+1\equiv 0 \bmod 4$, p a prime, (c) $n=m(p^h+1)$ where $m\geqq 2$ is the order of an H-matrix and p is a prime, (d) $n=q(q-1)$ where q is a product of factors of types (a) and (b), (e) $n=172$ and for n a product of any number of factors of types (a), (b), (c), (d) and (e).

In this note we shall show that an H-matrix of order n also exists when (f) $n=q(q+3)$ where q and $q+4$ are both products of factors of types (a) and (b), (g) $n=n_1n_2(p^h+1)p^h$, where $n_1>1$ and $n_2>1$ are orders of H-matrices and p is an odd prime, and (h) $n=n_1n_2m(m+3)$ where $n_1>1$ and $n_2>1$ are orders of H-matrices and m and $m+4$ are both of the form p^h+1, p an odd prime.

It is interesting to note the presence of the factors n_1 and n_2 in the types (g) and (h) and their absence in the types (d) and (f). Thus, if p is a prime and $p^h+1\equiv 0 \bmod 4$, an H-matrix of order $p^h(p^h+1)$ exists but, if $p^h+1\equiv 2 \bmod 4$, we can only be sure of the existence of an H-matrix of order $n_1n_2p^h(p^h+1)$ where $n_1>1$ and $n_2>1$ are orders of H-matrices. This is analogous to the simpler result that, if $p^h+1\equiv 0 \bmod 4$ an H-matrix of order p^h+1 exists but, if $p^h+1\equiv 2 \bmod 4$, we can only be sure of the existence of an H-matrix of order $n(p^h+1)$ where $n>1$ is the order of an H-matrix.

We shall denote the direct product of two matrices A and B by $A\cdot B$ and the unit matrix of order n by E_n.

Theorems on the existence of H-matrices. If a symmetric H-matrix of order $m>1$ exists, there exists an H-matrix H of order m with the form

$$H = \begin{pmatrix} 1 & e \\ e' & D \end{pmatrix},$$

Received by the editors December 6, 1946.

[1] Numbers in brackets refer to the references cited at the end of the paper.

where e is the row vector $(1, 1, \cdots, 1)$ of dimension $m-1$ and e' the column vector which is the transpose of e. Since H is a symmetric H-matrix

$$H^2 = HH' = mE_m$$

and accordingly

$$\begin{pmatrix} m & e + eD \\ e' + De' & e'e + D^2 \end{pmatrix} = \begin{pmatrix} m & 0 \\ 0 & mE_{m-1} \end{pmatrix}.$$

Therefore

$$eD = -e, \qquad De' = -e' \tag{1}$$

and

$$D^2 = mE_{m-1} - R, \tag{2}$$

where

$$R = e'e \tag{3}$$

and R is the square matrix of order $m-1$ each element of which has the value 1. It follows easily that

$$R^2 = (m-1)R \tag{4}$$

and by (1) and (3) that

$$RD = -R = DR. \tag{5}$$

If $F = 2E_{m-1} - R$, F is a symmetric matrix each element of which has the value ± 1. Further

$$FD = DF \tag{6}$$

by (5) and

$$F^2 = 4E_{m-1} + (m-5)R \tag{7}$$

by (4). If n is a product of factors of types (a) and (b) there exists [3, p. 67] an H-matrix of order n with the form $E_n + S$ where S is skew-symmetric so that

$$S^2 = -(n-1)E_n. \tag{8}$$

If

$$W = F \cdot E_n + D \cdot S,$$

each element of W has the value ± 1 and

$$\begin{aligned} WW' &= (F\cdot E_n + D\cdot S)(F\cdot E_n - D\cdot S) \\ &= F^2\cdot E_n - D^2\cdot S^2 && \text{(by (6))} \\ &= [4E_{m-1} + (m-5)R]\cdot E_n + (mE_{m-1} - R)\cdot(n-1)E_n \\ & && \text{(by (7), (2) and (8))} \\ &= [(4 + mn - m)E_{m-1}]\cdot E_n + (m - n - 4)R\cdot E_n. \end{aligned}$$

Therefore, if $n = m - 4$,

$$WW' = (m-1)(m-4)E_{m-1}\cdot E_{m-4} = n(n+3)E_n\cdot E_{n+3}$$

and W is an H-matrix.

Since a symmetric H-matrix of order 2 exists and a symmetric H-matrix of order $p^h+1 \equiv 0$ mod 4, where p is a prime, exists [3, p. 67], there exists a symmetric H-matrix of order n where n is a product of factors of types (a) and (b). We have therefore proved the theorem:

THEOREM 1. *If n and $n+4$ are both products of factors of types* (a) *and* (b) *there exists an H-matrix of order $n(n+3)$.*

As a particular case of this theorem we have the corollary:

COROLLARY 1. *If $n-1$ and $n+3$ are both powers of primes and are congruent to* 3 *modulo* 4, *there exists an H-matrix of order $n(n+3)$.*

If $m = p^h+1 \equiv 2$ mod 4, where p is a prime, there exists [3, p. 66] a symmetric matrix T of order m, each diagonal element of which has the value 0 and each other element the value ± 1 and such that

$$T = \begin{pmatrix} 0 & e \\ e' & U \end{pmatrix}$$

and

$$T^2 = (m-1)E_m. \tag{9}$$

It follows therefore that

$$UU' = U^2 = (m-1)E_{m-1} - R, \tag{10}$$

where R is defined by (3). Let A_1 and B_1 be two H-matrices of order n_1 such that [3, p. 66]

$$A_1B_1' = -B_1A_1' \tag{11}$$

and let $K = A_1\cdot E_{m-1} + B_1\cdot U$. Then each element of K has the value ± 1 and

$$\text{(12)} \qquad \begin{aligned} \mathrm{KK}' &= A_1A_1' \cdot E_{m-1} + B_1B_1' \cdot U^2 && \text{(by (11))} \\ &= n_1E_{n_1} \cdot (mE_{m-1} - R) && \text{(by (10)).} \end{aligned}$$

Since $eU = 0 = Ue'$,

$$\text{(13)} \qquad RU = UR = 0.$$

Hence, if $\Gamma = A_1 \cdot R$,

$$\text{(14)} \qquad \Gamma\Gamma' = n_1E_{n_1} \cdot (m - 1)R \qquad \text{(by (4))}$$

and

$$\text{(15)} \qquad \Gamma\mathrm{K}' = A_1A_1' \cdot R = \mathrm{K}\Gamma' \qquad \text{(by (13)).}$$

Finally, if A_2 and B_2 are two H-matrices of order n_2 satisfying

$$\text{(16)} \qquad A_2B_2' = -B_2A_2',$$

and

$$\begin{aligned} W &= A_2 \cdot \Gamma \cdot E_m + B_2 \cdot \mathrm{K} \cdot T, \\ WW' &= A_2A_2' \cdot \Gamma\Gamma' \cdot E_m + B_2B_2' \cdot \mathrm{KK}' \cdot T^2 && \text{(by (15) and (16))} \\ &= n_2E_{n_2} \cdot n_1E_{n_1} \cdot [(m-1)R + (mE_{m-1} - R)(m-1)] \cdot E_m \\ & && \text{(by (9), (12) and (14))} \\ &= rE_r && (r = n_1n_2m(m-1)). \end{aligned}$$

Therefore W is an H-matrix and we have proved the theorem:

THEOREM 2. *If H-matrices of orders n_1 and n_2 exist, $n_1 > 1$, $n_2 > 1$, and p is a prime such that $p^h + 1 \equiv 2 \bmod 4$, there exists an H-matrix of order $n_1n_2p^h(p^h+1)$.*

Since, if p is a prime such that $p^h + 1 \equiv 0 \bmod 4$, there exists an H-matrix of order $p^h(p^h+1)$, we have the corollary:

COROLLARY 1. *If H-matrices exist of orders $n_1 > 1$ and $n_2 > 1$, there exists an H-matrix of order $n_1n_2(p^h+1)p^h$ where p is an odd prime.*

Since an H-matrix of order 2 exists we have the corollary:

COROLLARY 2. *If p is an odd prime an H-matrix exists of order $4p^h(p^h+1)$.*

In the proof of the final theorem we require the following lemma:

LEMMA 1. *If there exists an H-matrix A of order $n > 1$, there exist two H-matrices B and C of order n such that $AB' = -BA'$, $AC' = CA'$, $BC' = CB'$.*

In fact the matrices $B=XA$ and $C=YA$, where X is the diagonal block matrix

$$\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right]$$

and Y is the diagonal block matrix

$$\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right],$$

satisfy the conditions of the lemma. For $BB'=CC'=nE_n$, $AB'=nX'=-nX=-BA'$, $CA'=nY'=nY=CA'$ and $BC'=nXY'=nYX'=CB'$.

Let $\mathrm{M}=C_1\cdot(2E_{m-1}-R)$ and $\mathrm{N}=A_1\cdot E_{m-1}+B_1\cdot U$, where R is defined by (14), U by (10) and A_1, B_1 and C_1 are matrices of order n_1 with the properties of Lemma 1. Then each element of the matrices M and N has the value ± 1. Further

$$\begin{aligned} \mathrm{MM}' &= n_1E_{n_1}\cdot(4E_{m-1}-4R+R^2) \\ &= n_1E_{n_1}\cdot[4E_{m-1}+(m-5)R] \qquad \text{(by (4))}, \end{aligned} \tag{17}$$

$$\mathrm{NN}' = n_1E_{n_1}\cdot(E_{m-1}+U^2) = n_1E_{n_1}\cdot(mE_{m-1}-R) \qquad \text{(by (10))} \tag{18}$$

and

$$\begin{aligned} \mathrm{MN}' &= C_1A_1'\cdot(2E_{m-1}-R)+C_1B_1'\cdot(2E_{m-1}-R)U \\ &= C_1A_1'\cdot(2E_{m-1}-R)+C_1B_1'\cdot 2U \qquad \text{(by (13))}. \end{aligned}$$

Therefore by Lemma 1

$$\mathrm{MN}' = \mathrm{NM}'. \tag{19}$$

Let A_2 and B_2 be two H-matrices of order $n_2>1$ satisfying (16) and let $n=p^h+1\equiv 2 \bmod 4$ where p is a prime. Then there exists a matrix G of order n and of the same form as T in (9) and satisfying

$$G^2 = (n-1)E_n. \tag{20}$$

If finally $W=A_2\cdot\mathrm{M}\cdot E_n+B_2\cdot\mathrm{N}\cdot G$, each element of W has the value ± 1 and

$$\begin{aligned} WW' &= n_2E_{n_2}\cdot(\mathrm{MM}'\cdot E_n+\mathrm{NN}'\cdot G^2) \qquad \text{(by (16) and (19))} \\ &= n_1n_2E_{n_1n_2}\cdot[4E_{m-1}+(m-5)R]\cdot E_n \\ &\quad + (mE_{m-1}-R)\cdot(n-1)E_n \qquad \text{(by (17), (18) and (20))} \\ &= n_1n_2E_{n_1n_2}\cdot[(4+mn-m)E_{m-1}+(m-4-n)R]\cdot E_n. \end{aligned}$$

Hence, if $m = n+4$ and $r = n_1n_2n(n+3) = n_1n_2(m-1)(m-4)$,

$$WW' = rE_r$$

and W is an H-matrix. We have therefore proved the theorem:

THEOREM 3. *If n and $n+4$ are both of the form $p^h+1 \equiv 2 \mod 4$ where p is a prime and if H-matrices of orders $n_1 > 1$ and $n_2 > 1$ both exist, there exists an H-matrix of order $n_1n_2n(n+3)$.*

As a consequence of Theorem 1 we have the corollary:

COROLLARY 1. *If n and $n+4$ are both of the form p^h+1 where p is an odd prime and if H-matrices of orders $n_1 > 1$ and $n_2 > 1$ both exist, there exists an H-matrix of order $n_1n_2n(n+3)$.*

Since an H-matrix of order 2 exists we also have the corollary:

COROLLARY 2. *If n and $n+4$ are both of the form p^h+1, where p is an odd prime, there exists an H-matrix of order $4n(n+3)$.*

Particular examples. That the above theorems do actually increase the values of n as orders of H-matrices which are known to exist is shown by the following examples.

By Theorem 1 an H-matrix of order (56)(59) exists. For $56 = 2(3^3+1)$ and 59 is prime. Further no one of (56)(59), (28)(59), (14)(59), 4(59) or 2(59) is of the form p^h+1. Therefore (56)(59) is not a product of factors of types (a), (b) or (c). By Theorem 2 an H-matrix of order 4(73)(74) exists and by Theorem 3 an H-matrix of order 4(230)(233) exists. Neither of the numbers 4(73)(74) nor 4(230)(233) is a product of factors of types (a), (b), (c) and (d).

REFERENCES

1. Jacques Hadamard, *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. (2) vol. 17 (1893) pp. 240–246.

2. R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics, Massachusetts Institute of Technology, vol. 12 (1933) pp. 311–320.

3. John Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J. vol. 11 (1944) pp. 65–81.

QUEENS COLLEGE