QUATERNIONS AND HADAMARD MATRICES

W. A. RUTLEDGE[1]

1. **Introduction.** J. Hadamard has proved [4][2] that a real or complex matrix of order n with elements bounded in absolute value by 1 has a determinant bounded in absolute value by $n^{n/2}$. A real matrix satisfying the above will be called an Hadamard matrix. Let H be a matrix of order n with elements chosen from the sixteen quaternions $(1/2)(\pm 1 \pm i \pm j \pm k)$, and H^* be the quaternionic conjugate transpose of H. If $HH^* = nI_n$, the real regular representation of $2H$ is then an Hadamard matrix of order $4n$.

The purpose of this paper is to study the structure of such matrices and the main theorem obtains a canonical form (under equivalence) for the case where n is a product of distinct primes.

The first sections are devoted to a discussion of specific properties of integral quaternions most of which are derived as special cases of the general theory of principal ideal domains and simple algebras.

2. **Definitions.** The real quaternions form a linear associative algebra over the real numbers having as a basis four independent elements 1, i, j, k where 1 is the unit of multiplication and $i^2 = j^2 = k^2 = ijk = -1$. Standard notation will be employed for the conjugate, $\bar{q}$, and norm, $N(q)$, of a quaternion q.

Following Hurwitz [5] an *integral quaternion* is defined as a real quaternion in which the components are either all rational integers or all halves of odd rational integers. This set of quaternions, to be denoted by J, forms a principal ideal domain in which there exist greatest common left and right divisors. An integral quaternion is called *primitive* if it cannot be expressed as a product of an integral quaternion and a rational integer not a unit. By an *odd quaternion* is meant an integral quaternion whose norm is an odd rational integer.

Two right (left) ideals aJ and bJ (Ja and Jb) are called *right* (*left*) *similar* if the J-right (left)-moduli $J - aJ$ and $J - bJ$ ($J - Ja$ and $J - Jb$) are J-isomorphic. Two elements a and b are called right (left) similar if the ideals aJ and bJ (Ja and Jb) are similar. Since right similarity and left similarity are equivalent [3], we may say simply "a is

Received by the editors December 18, 1951.

[1] This paper is a part of the author's thesis prepared under the direction of Professor J. W. Givens and submitted to the Graduate School of the University of Tennessee in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

[2] Numbers in brackets refer to the bibliography at the end of the paper.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

similar to b"; in symbols, $a \approx b$.

Following Jacobson, an element a of a principal ideal domain is called *bounded* if there exists a nonzero two-sided ideal contained in aJ. The maximal two-sided ideal contained in aJ is called the *bound* of a. Since J is a maximal integral domain of a simple algebra, every nonzero element of J is bounded. Further, since every integral quaternion a can be written in the form $a = r(1+i)^e c$ where r is a rational integer, $e=0$ or 1, and c is an odd primitive quaternion [1], the generator of the bound of a is of the form $r(1+i)^e \cdot N(c)$.

3. **Characterization of similarity.** It is easily seen that if $N(a)=2$, $a \approx b$ if and only if $N(b)=2$. If $N(a)>2$, the number of residue classes in $J-aJ$ equals $N^2(a)$, from which it follows that if $a \approx b$, then $N(a)=N(b)$.

It is known that in a principal ideal domain D a necessary and sufficient condition for D-isomorphism of any two finitely-generated D-modules is that the totality of bounds of the indecomposable components[3] that occur in a decomposition of one of the modules coincides with the totality of bounds occuring in a decomposition of the other (cf. [6, p. 79]). An integral quaternion is indecomposable if and only if either it is primitive and its norm is a power of an odd rational prime or else its norm is a power of 2. Then, since two indecomposable integral quaternions are similar if and only if they have the same bound, we get as a consequence a specific characterization of similar quaternions in the following theorem.

THEOREM 1. *Two integral quaternions are similar if and only if they have the same norm and bound.*

4. **Determinant of a matrix over** J. The concept of determinant is usually associated with matrices over a field. The extension to a division ring given by Dieudonné [2] in which the determinant is defined in terms of the cosets modulo the commutator subgroup of the nonzero elements will be used here. In this the mapping $A \rightarrow \det(A)$ is a homomorphism onto an abelian group, which, for the case of matrices over real quaternions, is essentially a homomorphism onto the set of non-negative real numbers. Many of the usual properties of determinants are carried over, in particular $\det(A) \cdot \det(B) = \det(AB)$, and $\det(A)$ is an invariant under the usual elementary row and column operations.

If the full facilities of the division ring of real quaternions are used,

[3] A module is indecomposable if it cannot be written as a direct sum of two nonintersecting modules.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

a matrix A is equivalent to a diagonal matrix $D = \{1, 1, \cdots, 1, d\}$ with $[N(d)]^m = \det(D) = \det(A)$, $m \neq 0$ being an arbitrary real number. If a matrix A is equivalent to a diagonal matrix $B = \{b_1, b_2, \cdots, b_n\}$, then $\det(A) = \prod [N(b_k)]^m$. Since any matrix over J may be reduced by elementary row and column operations in J to a diagonal matrix, its determinant will be a non-negative integer independent of the division ring used. If we set $m = 1$, then $\det(A)$ is equal to the product of the norms of the diagonal matrix equivalent to A. For this case the notation $\det(A) = \nabla A$ will be used, while if A is real, $\det(A)$ will represent the ordinary determinant of A.

With a matrix A having real quaternions as elements there is an associated matrix formed by replacing in A each quaternion by its regular representation, the *(real) regular representation* of A, and will be denoted by the symbol $\tilde{A}$. Then $\det(\tilde{A}) = (\nabla A)^2$.

5. **Hadamard matrices.** In 1893 Hadamard [4] proved that if the absolute values of the elements of a real or complex matrix of order n are bounded by one, then the absolute value of the determinant has as an upper bound $n^{n/2}$, and he raised the question of the values of n for which this bound is attained. For the complex case the answer is known, but for real matrices the complete answer is not known. It is easily seen that for a real matrix we may as well assume that all elements are ± 1, and it is necessary that n be one, two, or a multiple of four. Further, a necessary and sufficient condition is that $AA^T = nI_n$ where I_n is the unit matrix of order n. A matrix satisfying these conditions will be called an Hadamard matrix. Explicit formulas for the construction of several classes of such matrices have been given by Paley [8] and Williamson [10].

Consider a matrix A of order n with elements chosen from the sixteen quaternions $\{\pm 1 \pm i \pm j \pm k\}$. The regular representation $\tilde{A}$ of such a matrix will have elements ± 1. For A to be an Hadamard matrix

$$\tilde{A} \cdot \tilde{A}^T = 4n \cdot I_{4n}. \tag{1}$$

Now the regular representation of the quaternionic conjugate transpose A^* of A is the transpose of $\tilde{A}$. Thus for a matrix A satisfying (1), $\nabla(AA^*) = [\det(\tilde{A}\tilde{A}^T)]^{1/2} = (4n)^{2n}$. It is easily shown that $\nabla A = \nabla A^*$ and thus $\nabla A = (4n)^n$. This is equivalent to $\nabla(A/2) = n^n$ and $A/2$ is a matrix with elements in J. Conversely, if H is a matrix of order n each element of which is one of the set $\{\pm 1 \pm i \pm j \pm k\}$ and $HH^* = n \cdot I_n$, then $2H = A$ will satisfy (1) and $2\tilde{H}$ is an Hadamard matrix of order $4n$. Such a matrix H will be called a *quaternionic Hadamard matrix*. This name is appropriate since Wallace Givens has

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

proved (oral communication) an Hadamard type theorem for matrices over real quaternions; if B is of order n and $N(b_{ij}) \leqq 1$, then $\nabla B \leqq n^n$.

Teichmüller [16] has shown that any matrix over a principal ideal domain is equivalent to a diagonal matrix $\{d_1, d_2, \cdots, d_n\}$ in which each d_i is a total divisor[4] of d_j for $j > i$. For elements of J since 2 is the only ramifying rational prime, if we write a and b in the forms $a = 2^f \cdot r_1(1+i)^m \cdot c_1$, $b = 2^h \cdot r_2(1+i)^s \cdot C_2$, where the r_i are rational integers, c_i are odd primitive quaternions, we get the result that a is a total divisor of b if and only if $f \leqq h$, $f + m \leqq h + s$, and $r_1 \cdot N(c_1)$ divides r_2. A diagonal matrix of the form above will be called a Jacobson-Teichmüller normal form of any matrix equivalent to it.

Nakayama [7] has shown that if two matrices in Jacobson-Teichmüller normal form are equivalent, then the corresponding diagonal elements are similar. Further if the first diagonal elements are units, the converse also holds. Thus in the case of a quaternionic Hadamard matrix the diagonal elements of the Jacobson-Teichmüller normal form are unique to within similarity.

6. **Normal form of quarternionic Hadamard matrices.** In order to derive a canonical form for certain quaternionic Hadamard matrices there will be needed a theorem on real Hadamard matrices.

THEOREM 2. *Let H be a rational integral Hadamard matrix of order $n = 4r$, where r is a product of distinct prime factors. Then the invariant factors, h_i, of H are: $h_1 = 1$, $h_i = 2$ for $1 < i \leqq 2r$, $h_i = 2r$ for $2r < i < 4r$ and $h_{4r} = 4r$.*

PROOF. Since H has only ± 1 as elements, clearly $h_1 = 1$ and $h_2 = 2$. Now consider the orthogonal matrix $T = n^{-1/2}H$. The determinant of any $(n-1)$-rowed minor of T is $\pm n^{-1/2}$. Then the determinant of any $(n-1)$-rowed minor of H is $n^{-1/2}(n^{1/2})^{n-1} = (4r)^{2r-1}$ and the g.c.d. of the $(n-1)$-rowed minors is $(4r)^{2r-1} = \prod_{i=1}^{n-1} h_i = \det(H)/h_{4r} = (4r)^{2r}/h_{4r}$ from which $h_{4r} = 4r$.

Now $\det(H) = (4r)^{2r} = h_1 h_2 \cdots h_{4r}$, and every h_i divides h_j, $j > i$, so that $h_3, \cdots, h_{4r-1}$ are even, and using the values of h_1, h_2, h_{4r} we get $r^{2r} = (h_3/2) \cdots (h_{4r-1}/2)(r)$. Every factor of any $h_j/2$, $j = 3, 4, \cdots, 4r-1$, is a factor of r and the prime factors of $h_j/2$ are distinct. Each prime factor of r therefore occurs in $h_{2r+1}/2, \cdots, h_{4r-1}/2$ and does not occur in $h_2/2, \cdots, h_{2r}/2$, which completes the proof.

THEOREM 3. *Let A be a quaternionic Hadamard matrix of order n, where $n = p_1 p_2 \cdots p_k$ is a product of distinct odd primes. Let D*

[4] We say a is a total divisor of b in a principal ideal domain D if $DaD \subseteq bD \cap Db$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$=\{d_1, d_2, \cdots, d_n\}$ *be a Jacobson-Teichmüller normal form of* A. *Then to within replacement by similar elements,* $d_i=1$ *for* $i<(n+1)/2$; $d_{(n+1)/2}=c$, *with* c *an odd primitive quaternion of norm* n, $d_i=n$ *for* $(n+1)/2<i\leqq n$.

PROOF. Write $d_i=r_i 2^{f_i}(1+i)^{e_i}c_i$ where r_i is an odd rational integer. Then since n is odd, $f_i=e_i=0$. Thus $d_i=r_ic_i=p_1^{m_{1i}}p_2^{m_{2i}}\cdots p_k^{m_{ki}}\cdot c_i$ where the p_i are distinct primes. Since d_i is a total divisor of d_j, for $j>i$, it follows that $p_1^{m_{1i}}\cdots p_k^{m_{ki}}N(c_i)$ divides $p_1^{m_{1j}}p_2^{m_{2j}}\cdots p_k^{m_{kj}}$ for $j>i$. This requires that

$$N(c_i) = p_1^{s_{1i}}p_2^{s_{2i}}\cdots p_k^{s_{ki}} \tag{2}$$

and also

$$m_{hi}+s_{hi}\leqq m_{h,i+1} \tag{3}$$

where $h=1, 2, \cdots, k$ and $i=1, 2, \cdots, n$. Moreover, since $\nabla A = \prod_{i=1}^n r_i^2\cdot N(c_i)$, we have

$$\sum_{j=1}^{n}(2m_{hi}+s_{hi}) = n, \qquad h=1,2,\cdots,k. \tag{4}$$

Since n is odd, (4) implies that for every h and some i, $s_{hi}\neq 0$. Then (3) and (4) allow us to conclude that, for every h, $m_{hi}=0$ for $i\leqq(n+1)/2$, and $s_{hi}=0$ for $i<(n+1)/2$, so that $d_1=d_2=\cdots=d_{(n-1)/2}=$ a unit, and $d_{(n+1)/2}=c_{(n+1)/2}$.

Let $\tau=(n+1)/2$. We now want to show that $N(c_\tau)=n$; that is, in (2), $s_{hi}=1$ for $i=\tau$. Evidently $s_{h\tau}\leqq 1$ for every h, since otherwise (3) would imply an inequality in (4). If $s_{h\tau}=1$, then $m_{hj}\geqq 1$, for $j>\tau$. To prove the theorem it will be sufficient to show that $s_{h\tau}=1$ for every h. This result is obtained by making use of the regular representation of A.

Let $PAQ=D=\{d_1, d_2, \cdots, d_n\}$ and we can require the d_i to have rational integral components. $\tilde{D}$ has a Smith normal form, $\{1, 1, \cdots, 1, 1, 1, N(c_\tau), N(c_\tau), r_{\tau+1}r_{\tau+1}, r_{\tau+1}N(c_{\tau+1}), r_{\tau+1}N(c_{\tau+1}), \cdots, r_n, r_n, r_nN(c_n), r_nN(c_n)\}$, where there are $2(n-1)+2$ 1's. Now $8\tilde{D}=(2\tilde{P})(2\tilde{A})(2\tilde{Q})$ and $2\tilde{P}$, $2\tilde{A}$, and $2\tilde{Q}$ have rational integral elements, so that the greatest common divisor of the h-rowed minors of $2\tilde{A}$ is a divisor of every h-rowed minor of $8D$. Therefore the greatest common divisor of the h-rowed minors of $2\tilde{A}$ divides 8^h times the greatest common divisor of the h-rowed minors of $\tilde{D}$. However, since $A=RDS$ for matrices R and S over J, $4\tilde{A}=(2\tilde{R})(\tilde{D})(2\tilde{S})$ and a similar argument shows that the greatest common divisor of the h-rowed minors of $\tilde{D}$ divides 2^h times the greatest common divisor of

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

the h-rowed minors of $2\tilde{A}$. Hence the common divisors in question must differ at most by a power of two.

By Theorem 2, $2\tilde{A}$ is equivalent to $B=\{b_1, b_2, \cdots, b_{4n}\}$ where $b_1=1$, $b_i=2$ for $1<i\leqq 2n$, $b_i=2n$ for $2n<i<4n$, and $b_{4n}=4n$. Hence the g.c.d. of the h-rowed minors of B differs from those of $8\tilde{D}$ by at most a power of two.

We now set $h=2n+2$. The greatest common divisor of the h-rowed minors of $2\tilde{A}=\prod_{i=1}^{h} b_i=2^{2n-1}(2n)^2$. The greatest common divisor of the h-rowed minors of $8\tilde{D}$ is $8^{2n+2}N(c_\tau^2)$. Thus $2^{2n-1}(2n)^2$ divides $8^{2n+2}N(c_\tau^2)$, and since n is odd, this requires that n^2 divide $N(c_\tau^2)$, or n divides $N(c_\tau)$. Thus, in (2), $s_h\geqq 1$ for all h, which completes the proof.

As an immediate consequence of the argument presented in the proof of the theorem we have an extension of a well known theorem.

THEOREM 4. *If U is a unitary matrix over the real quaternions (that is, $UU^*=I$), then the determinant of any r-rowed minor of U is equal to the determinant of its complementary minor.*

BIBLIOGRAPHY

1. L. E. Dickson, *Algebras and their arithmetics*, Chicago, 1933.

2. Jean Dieudonné, *Les déterminants sur un corps noncommutatif*, Bull. Soc. Math. France vol. 71 (1943) pp. 27–45.

3. Hans Fitting, *Über den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie*, Math. Ann. vol. 112 (1936) pp. 572–582.

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

5. Adolph Hurwitz, *Mathematische Werke*, vol. II, Basel, 1933.

6. N. Jacobson, *The theory of rings*, Mathematical Surveys, no. 2, New York, American Mathematical Society, 1943.

7. Tadasi Nakayama, *A note on the elementary divisor theory in non-commutative domains*, Bull. Amer. Math. Soc. vol. 44 (1938) pp. 719–721.

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

9. O. Teichmüller, *Der Elementarteilersatz für nichtkommutative Ringe*, Preuss. Akad. Wiss. Sitzungsber. (1937) XIV S. pp. 169–177.

10. John Williamson, *Note on Hadamard's determinant theorem*, Bull. Amer. Math Soc. vol. 53 (1947) pp. 608–613.

UNIVERSITY OF TENNESSEE

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use