A NEW CLASS OF HADAMARD MATRICES

by E. SPENCE

(Received 20 June, 1966)

1. Introduction. A Hadamard matrix H is an orthogonal square matrix of order m all the entries of which are either $+1$ or -1; i.e.

$$HH' = mI_m,$$

where H' denotes the transpose of H and I_m is the identity matrix of order m. For such a matrix to exist it is necessary [**1**] that

$$m = 1 \text{ or } 2, \quad \text{or} \quad m \equiv 0 \pmod 4.$$

It has been conjectured, but not yet proved, that this condition is also sufficient. However, many values of m have been found for which a Hadamard matrix of order m can be constructed. The following is a list of such m (p denotes an odd prime).

(i) $m = 2^k$,

(ii) $m \equiv p^k + 1 \equiv 0 \pmod 4$,

(iii) $m = h(p^k + 1)$, where $h \geqq 2$ is the order of a Hadamard matrix,

(iv) $m = n'(n' - 1)$, where n' is a product of numbers of the forms (i) and (ii),

(v) $m = 92$, 116, 156 and 172,

(vi) $m = n_1 n_2 p^k(p^k + 1)$, where $n_1 \geqq 2$ and $n_2 \geqq 2$ are both orders of Hadamard matrices,

(vii) $m = n_1 n_2 h(h+3)$, where $n_1 \geqq 2$ and $n_2 \geqq 2$ are both orders of Hadamard matrices and h and $h+4$ are both of the form $p^k + 1$,

(viii) $m = n'(n' + 3)$, where n' and $n' + 4$ are both products of numbers of the forms (i) and (ii),

(ix) $m = (n-1)^2$, where $n+1$ is a product of numbers of the forms (i) and (ii) and $n - 2 = p^k$,

(x) $m = (h-1)^3 + 1$, where h is a product of numbers of the forms (i) and (ii),

(xi) m is a product of numbers of the forms (i)–(x).

These results are given in [**1**], [**2**], [**3**], [**4**], [**5**], [**6**], [**7**] and [**8**].

The only values of $m \leqq 400$ that are not covered by this list are 188, 236, 260, 268, 292, 356, 372 and 376.

The following theorem, which we shall prove, adds another set of values.

THEOREM 1. *If the primes* $p, p_1, p_2, \ldots, p_r$ *and the positive integers* $\alpha, \alpha_1, \ldots, \alpha_r$ *are such that*

$$p^\alpha \equiv 1 \pmod 4, \quad p_i^{\alpha_i} \equiv -1 \pmod 4 \quad (1 \leqq i \leqq r),$$

$m = 1+p^\alpha+p^{2\alpha}+\ldots+p^{h\alpha}$ $(h \geqq 2)$ *is a prime congruent to* 3 (mod 4) *or a product of twin primes, and*

$$q = m+1-4p^{(h-1)\alpha} = 2^s \prod_{i=1}^{r} (p_i^{\alpha_i}+1) \quad (s \geqq 0),$$

then there exists a Hadamard matrix of order qm.

That there are integers satisfying the conditions of the theorem is seen by taking $p = 5$, $\alpha = 1$ and $h = 2$. Then $m = 31$ and $q = 12 = 11+1$. It follows that there exists a Hadamard matrix of order 372, a number which is not of the forms (i)–(xi).

2. It was shown in [2] that if $q = 2^s \prod_{i=1}^{r} (p_i^{\alpha_i}+1)$ $(s \geqq 0)$, then there exists a Hadamard matrix H_1 of order q such that

$$H_1 = I_q + S,$$

where I_q is the identity matrix of order q and S is skew-symmetric. Since $H_1 H_1' = qI_q$, it is immediate that

$$SS' = (q-1)I_q. \tag{1}$$

Now let X and Y be square matrices of order m and denote the direct product of two matrices A and B by $A \cdot B$. If the $qm \times qm$ matrix K is defined by

$$K = I_q \cdot X + S \cdot Y, \tag{2}$$

then

$$KK' = (I_q \cdot X + S \cdot Y)(I_q \cdot X' + S' \cdot Y') = I_q \cdot \{XX' + (q-1)YY'\} + S \cdot (YX' - XY'),$$

by (1). It follows that if X and Y can be chosen so that

$$XX' + (q-1)YY' = qmI_m, \tag{3}$$

$$XY' = YX', \tag{4}$$

and the entries of X and Y are $+1$ or -1, then K is a Hadamard matrix of order qm.

3. Perfect difference sets. By a perfect difference set (or simply a difference set) is meant a set $D = \{d_1, d_2, \ldots, d_k\}$ of distinct integers modulo v such that every $d \not\equiv 0 \pmod v$ can be expressed in exactly λ ways in the form

$$d_i - d_j \equiv d \pmod v,$$

with $d_i, d_j \in D$. The parameters v, k, λ clearly satisfy

$$k(k-1) = \lambda(v-1).$$

https://doi.org/10.1017/S0017089500000094 Published online by Cambridge University Press

Associated with such a difference set we define the $v \times v$ circulant matrix $A = [a_{ij}]$ by

$$a_{ij} = \begin{cases} +1 & \text{if} \quad j-i \in D, \\ -1 & \text{if} \quad j-i \notin D. \end{cases}$$

Then it is straightforward to verify that

$$AA' = 4nI_v + (v-4n)J_v,$$

where $n = k - \lambda$, and J_v is the square matrix of order v all the entries of which are $+1$.

We require the following

LEMMA. *If B is a $v \times v$ circulant matrix and $P = [p_{ij}]$ is the permutation matrix of order v defined by*

$$p_{ij} = \begin{cases} 1 & \textit{if} \quad i+j \equiv 2 \pmod v, \\ 0 & \textit{otherwise}, \end{cases}$$

then PB is symmetric.

For if the first row of B is $(b_1, b_2, \ldots, b_v)$, then the jth column of B is $\{b_j, b_{j-1}, \ldots, b_{j-v+1}\}$, the subscripts being reduced modulo v. Consequently, $[PB]_{ij} = b_{i+j-1} = [PB]_{ji}$, which completes the proof.

Suppose now that there exist two difference sets (mod v) with parameters (v, k_1, λ_1), (v, k_2, λ_2) and corresponding matrices A_1 and A_2, as described above. Since A_1 and A_2 are both circulant matrices, so also is A_1A_2' and we deduce from the lemma that

$$P(A_1A_2') \quad \text{and} \quad PA_1$$

are symmetric. Consequently

$$A_2(PA_1) = (PA_1)A_2'. \tag{5}$$

Also, from the fact that

$$A_1A_1' = 4n_1I_v + (v-4n_1)J_v \quad (n_1 = k_1 - \lambda_1),$$

it is clear that $(PA_1)(PA_1)' = A_1A_1'$. Writing

$$X = PA_1, \quad Y = A_2, \tag{6}$$

we see that the entries of X and Y are $+1$ or -1, that

$$XX' + (q-1)YY' = \{4n_1 + (q-1)4n_2\}I_v + \{v - 4n_1 + (v-4n_2)(q-1)\}J_v,$$

and from (5) that

$$XY' = YX'.$$

The matrices X and Y therefore satisfy conditions (3) and (4), with $m = v$, if and only if

$$4n_1 + (q-1)4n_2 = qv. \tag{7}$$

If now v is chosen so that

$$v = 1 + p^{\alpha} + p^{2\alpha} + \ldots + p^{h\alpha},$$

https://doi.org/10.1017/S0017089500000094 Published online by Cambridge University Press

where $h \geqq 2$ and p is a prime, it is well known [9] that there exists a difference set with parameters (v, k_1, λ_1), where $k_1 = 1+p^\alpha+\ldots+p^{(h-1)\alpha}$ and $\lambda_1 = 1+p^\alpha+\ldots+p^{(h-2)\alpha}$.

Moreover, if p, α and h are chosen so that

$$v \equiv 3 \pmod 4,$$

and v is a prime, or a product of twin primes p_1 and $p_2 = p_1+2$, there exists [10], [11], a difference set with parameters

$$(v, k_2, \lambda_2) \equiv (v, \tfrac{1}{2}(v-1),\ \tfrac{1}{4}(v-3)).$$

Since $n_1 = p^{(h-1)\alpha}$, $n_2 = \frac{1}{4}(v+1)$, (7) is satisfied if and only if

$$q = v+1-4p^{(h-1)\alpha}.$$

Taking $m = v$ shows that, if the conditions of the theorem are satisfied, then the matrix K defined by (2), where X and Y are given by (6), is a Hadamard matrix of order qm. This completes the proof of Theorem 1.

Finally, since the direct product of two Hadamard matrices is again a Hadamard matrix, we obtain

THEOREM 2. *If N is a product of numbers of the forms* (i)–(xi), *there exists a Hadamard matrix of order qmN, where m and q are as in Theorem* 1.

REFERENCES

1. R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.

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

3. J. Williamson, Note on Hadamard's determinant theorem, *Bull. Amer. Math. Soc.* **53** (1947), 608–613.

4. L. Baumert, S. W. Golomb and Marshall Hall, Jr, Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* **68** (1962), 237–238.

5. L. D. Baumert and Marshall Hall, Jr, Hadamard matrices of the Williamson type, *Math. Comp.* **10** (1965), 442–447.

6. K. Goldberg, Hadamard matrices of order cube plus one, *Proc. Amer. Math. Soc.* **17** (1966), 744–746.

7. L. D. Baumert, Hadamard matrices of orders 116 and 232, *Bull. Amer. Math. Soc.* **72** (1966), 237.

8. H. Ehlich, Neue Hadamard-Matrizen, *Arch. Math.* **16** (1965), 34–36.

9. J. Singer, A Theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

10. H. J. Ryser, *Combinatorial mathematics*, Carus Mathematical Monographs No. 14, 1963.

11. A. Brauer, On a new class of Hadamard determinants, *Math. Z.* **58** (1953), 219–225.

UNIVERSITY OF GLASGOW
GLASGOW, W.2