On the Existence of Hadamard Matrices

JENNIFER SEBERRY WALLIS[1]
Department of Mathematics, IAS, ANU, Canberra, Australia
Communicated by Marshall Hall, Jr.
Received June 20, 1975

Published: Journal of Combinatorial Theory, Vol 21, No. 2, September 1976, pp 188-195
Academic Press, New York and London

Given any natural number $q > 3$ we show there exists an integer $t \leq [2 \log_2 (q - 3)]$ such that an Hadamard matrix exists for every order $2^s q$ where $s > t$. The Hadamard conjecture is that $s = 2$.

This means that for each q there is a finite number of orders $2^v q$ for which an Hadamard matrix is not known. This is the first time such a statement could be made for arbitrary q.

In particular it is already known that an Hadamard matrix exists for each $2^s q$ where if $q = 2^m - 1$ then $s \geq m$, if $q = 2^m + 3$ (a prime power) then $s \geq m$, if $q = 2^m + 1$ (a prime power) then $s \geq m + 1$.

It is also shown that all orthogonal designs of types (a, b, m – a – b) and (a, b), $0 \leq a + b \leq m$, exist in orders $m = 2^t$ and $2^{t+2} \cdot 3$, $t \geq 1$ a positive integer.

1. INTRODUCTION

An orthogonal design of order n and type $(u_1, u_2, ..., u_s)$ $(u_i > 0)$ on the commuting variables $x_1, x_2, ..., x_s$ is an $n \times n$ matrix A with entries from $\{0, \pm x_1, ..., \pm x_s\}$ such that

$$AA^T = \sum_{i=1}^{s} (u_i x_i^2) I_n .$$

Alternatively, the rows of A are formally orthogonal and each row has precisely u_i entries of the type $\pm x_i$.

In [1], where this was first defined and many examples and properties of such designs were investigated, we mentioned that

$$A^T A = \sum_{i=1}^{s} (u_i x_i^2) I_n ;$$

[1] This paper was written while the author was visiting the Department of Computer Science, University of Manitoba.

and so our alternative description of A applies equally well to the columns of A. We also showed in [1] that $s \leq p(n)$, where p(n) (Radon's function) is defined by

$$p(n) = 8c + 2^d$$

when

$$n = 2^a \cdot b, \qquad b \text{ odd}, \qquad a = 4c + d, \qquad 0 \leq d < 4.$$

The most recent existence results may be found in [6, 10].

An Hadamard matrix, H, of order n is a square matrix with entries +1 or –1 satisfying $HH^T = nI_n$. It is a famous conjecture that Hadamard matrices exist for orders 1, 2, and 4t, where t is a natural number. Hadamard matrices, which are so named because they satisfy the equality of Hadamard's inequality, have many applications (see [7] for some) and have been studied since at least 1867.

Throughout this paper we use J for the matrix with every entry +1.

We refer the reader to [7, pp. 284, 291–292] for the salient features of how to construct the matrices B, X, .Y of order v mentioned in the proofs of Lemmas 8 and 9. We note

$B^T = B$, $BJ = J$, $B(J - 21) = (J - 2I)B$, $BB^T = (v + 1)I - J$,

$X^T = X$, $Y^T = Y$, $XY^T = YX^T$, $XX^T + YY^T = 2(v + 1)I - 2J$,

$XJ = YJ = J$, $X(J - 2I) = (J - 2I)X$, $Y(J - 2I) = (J - 2I)Y$.

2. A RESULT ON ORTHOGONAL DESIGNS

First we state two results from [1, 6] that we shall use.

LEMMA 1. If X is an orthogonal design of order n and type $(u_1, u_2, ..., u_s)$ on the variables $x_1, ..., xs$, then there is an orthogonal design of order n and type $(u_1, ..., u_i + u_j, ..., u_s)$ on the $s - 1$ variables $x_1, ..., \overline{x}_j, ..., x_s$.

LEMMA 2. If there exists an orthogonal design of order n and type $(u_1, u_2, ..., u_s)$, then there exist orthogonal designs of type

(i) $(e_1u_1, e_2u_2, ..., e_su_s)$, where $e_i = 1$ or 2,

(ii) $(u_1, u_1, fu_2, ..., fu_s)$, where $f = 1$ or 2,

in order 2n.

Hence we may show

LEMMA 3. Suppose all orthogonal designs of type (a, b, n – a – b), $0 \leq a, b \leq n$, *exist in order n. Then all orthogonal designs of type (x, y,* 2n – x – y), $0 \leq x, y \leq$ 2n, exist in order 2n.

Proof. It is merely necessary to note that the existence of the design of type (a, b, n – a –b) in order n implies the existence of the design of type (a, a, 2b, 2n – 2a – 2b), and consequently the designs of types (2a, 2b, 2n – 2a – 2b) and (a, 2b + a, 2n – 2a – 2b) in order 2n.

COROLLARY 4. Since all the orthogonal designs of type (a, b, 4 – a – b) exist in order 4 for $0 \leq$ a, b $\leq$ 4, we have all orthogonal designs of type (x, y, n – x – y) for $0 \leq$ x, y $\leq$ n whenever n is a power of 2.

A. V. Geramita pointed out the following nice corollary.

COROLLARY 5. Since all orthogonal designs of type (x, y, n – x – y), $0 \leq$ x, y $\leq$ n, exist in all orders for which n is a power of 2, all designs of type (z, w), $0 \leq$ z + w $\leq$ n, exist in all orders n which are powers of 2.

3. THE MAIN THEOREM

The following theorem of Sylvester, which he studied because of a problem posed by Frobenius, is well known.

THEOREM 6. Given any two relatively prime integers x and y, then every integer N > (x - 1)(y – 1) can be written in the form ax + by for some nonnegative integers a and b.

COROLLARY 7. Given x = (v + 1) and y = (v – 3), where v is odd and v $\geq$ 9, there exist nonnegative integers a and b such that $a(v + 1) + b(v – 3) = n = 2^t$ for some t.

Proof. Let g be the greatest common divisor of v + 1 and v – 3. Then g = 1, 2, or 4. Let m be the smallest power of 2 greater than N = ((v + 1)/(g – 1)) ((v – 3)/(g – 1)). Then by the theorem there exist integers a and b such that (a(v + 1)/g) + (b(v – 3)/g) = m and hence we have the corollary.

LEMMA 8. Let v ≡ 3 (mod 4) be a prime $\geq$ 9. Then there exists a t such that an Hadamard matrix exists of every order $2^s \cdot v$ for s $\geq$ t.

Proof. Let x = v + 1 and y = v – 3 then by the previous corollary there exists an a and b such that ax + by = n = 2^t for some t. Now we

know the orthogonal design, D, of type (a, b, n – a – b) exists with order 2^t on the variables x_1, x_2, x_3 .

Then replace each variable x_1 by the matrix J, each variable x_2 by J – 21 and each variable x_3 by the back-circulant (1, –1) matrix, B, generated by the (v, (v – 1)/2, (v – 3)/4) difference set to form a matrix E.

Now

$$DD^T = (ax_1^2 + bx_2^2 + (n - a - b)\, x_3^2)\, I_n \text{ and}$$

$$EE^T = (aJ^2 + b(J - 2I)^2 + (n - a - b)\, BB^T) \times I_n$$

$$= [avJ + 4bI + b(v - 4)J + (n - a - b)(v + 1)I - (n - a - b)\, J] \times I_n$$

$$= ([n(v + 1) - a(v + 1) - b(v - 3)]I + [a(v + 1) + b(v - 3) - n]J) \times I_n$$

$$= nvI_{nv} .$$

LEMMA 9. Let $v \equiv 1 \pmod 4$ be a prime ≥ 9. Then there exists a t such that an Hadamard matrix exists in every order $2^s \cdot v$ for $s \geq t + 1$.

Proof. Choose x, y, n, t, a, b, and D as in the previous lemma. Now note there exists an orthogonal design F, of type (2a, 2b, n – a – b, n – a – b) in order $2n = 2^{t+1}$ on the variables x_1 , x_2 , x_3 , x_4.

Form the matrix E by replacing each variable x_1 of F by J, each variable x_2 of F by J – 2I and the variables x_3 and x_4 by the two circulant (1, –1) incidence matrices X, Y of the 2 – {v; (v – 1)/2; (v – 3)/2} supplementary difference sets.

Now

$$FF^T = (2ax_1^2 + 2bx_2^2 + (n - a - b)x_3^2 + (n - a - b)x_4^2)\, I_{2n}$$

and

$$EE^T = (2aJ^2 + 2b(J - 2I)^2 + (n - a - b)(XX^T + YY^T)) \times I_{2n}$$

$$= [2avJ + 8bI + 2b(v - 4)J + (n - a - b)(2(v + 1)I - 2J)] \times I_{2n}$$

$$= [2n(v + 1) - 2a(v + 1) - 2b(v - 3)]\, I_{2nv} + [2a(v + 1) + 2b(v - 3) - 2n]\, J_v \times I_{2n}$$

$$= 2nvI_{2n}.$$

LEMMA 10. There exist Hadamard matrices of orders 2, 4, $2^t \cdot 2$, $2^t \cdot 3$, $2^t \cdot 5$ and $2^t \cdot 7$ for all positive integers $t \geq 2$.

Proof. This is folklore but almost certainly known to Sylvester and Scarpis.

THEOREM 11. Given any integer q there exists t dependent on q such that an Hadamard matrix exists of every order $2^s q$ for $s \geq t$.

Proof. Decompose q into its prime factors, and apply the previous lemmas to each factor. The result follows because the Kronecker product of any two Hadamard matrices is an Hadamard matrix.

4. SOME COROLLARIES

COROLLARY 12. If $q = 2^t - 1$, there exists an Hadamard matrix of order $2^s q$ for every $s \geq t$.

Proof. There is a skew-Hadamard matrix of order $k = 2^t$, and we use Williamson's theorem that there is an Hadamard matrix of order $k(k - 1)$ [7, p. 370, 449].

COROLLARY 13. If $q = 2^t + 3$ is a prime power, there exists an Hadamard matrix order $2^s q$ for every $s \geq t$.

Proof. Since $u = 2^t$ and $u + 4 = q + 1$ are both of the form $2^a \prod (p_i^{r_i} + 1)$, we use Williamson's theorem that there is an Hadamard matrix of order $u(u + 3)$. [7, p. 371, 449].

COROLLARY 14. If $q = 2^t + 1$ is a prime power, there exists an Hadamard matrix of order $2^s q$ for every $s \geq t + 1$.

Proof Since $k = q - 1$ is the order of a skew-Hadamard matrix, we use a theorem of J. Wallis to show that there is an Hadamard matrix of order $2k(k + 1) = 2(q - 1)q$ [7, p. 380, 450].

Of course, many other corollaries can be found.

5. FULL ORTHOGONAL DESIGNS IN ORDERS $2^t \cdot 3$

Using the results of [1, 6] we have this lemma:

LEMMA 15. All orthogonal designs of type (a, b, 24 – a – b), $0 \leq a + b \leq 24$, *exist in order* 24. Hence all orthogonal designs of type (x, y, m – x – y), $0 \leq x + y \leq m$, *exist in orders* $2^t \cdot 3 = m$, $t \geq 3$ *a positive integer.*

This result may be used in a similar fashion to that employed in Section 3 to construct Hadamard matrices of order $2^s \cdot 3q$, for sufficiently large s. It may happen that proceeding via Lemma 15, for appropriate natural numbers 3q, gives a smaller s than if Theorem 11 were used. We note

COROLLARY 16. All orthogonal designs of type (a, b), $0 \leq a + b \leq 2^t \cdot 3$, **exist in orders $2^t \cdot 3$, $t \geq 3$ a positive integer.**

CONJECTURE. All orthogonal designs of type (x, y, m – x – y), $0 \leq x + y \leq m$ exist in orders $m = 2^t q$ for any natural number q and sufficiently large t.

6. EVALUATING THE POWER OF TWO IN THE THEOREM

In Corollary 7 we choose t so that $2^j > ((v + 1)/(g – 1)(v – 3)/(g – 1))$. Hence if $v \equiv 1 \pmod 4$, $g = 2$ and we need $2^t > \frac{1}{4}(v – 1)(v – 5)$. Thus, if we choose $t = [2 \log_2 (v – 3)] – 1$, we can ensure the existence of an Hadamard matrix of order $2^{t+1} \cdot v$ in Lemma 9.

For $v \equiv 3 \pmod 4$, $g = 4$ and choosing $t = [\log_2 (v – 5)] – 3$ ensures the existence of an Hadamard matrix of order $2^j \cdot v$ in Lemma 8.

We observe that if $v = p \cdot q$ where p and q are primes $\equiv 1 \pmod 4$ we can ensure the existence of an Hadamard matrix of order $2^r \cdot pq$ where $r = [2 \log_{g2} (p – 3)] + [2 \log_2 (q – 3)] < [2 \log_2 (pq – 3)]$. Since a v comprising a product of primes $\equiv 1 \pmod 4$ would give the highest theoretical t for which an Hadamard matrix of order $2^j v$ exists we can say

THEOREM 17. Given any natural number $q > 3$ there exists an Hadamard matrix of order $2^s q$ for every $s \geq [2 \log_2 (q – 3)]$.

TABLE I

q	a, b	equation: a(q + 1)/g + b(q – 3)/g	t	$2^t q$
107	18, 1	18.27 + 1.26 = 512	9	$2^9 \cdot 107$
179	12, 11	12.45 + 11.44 = 1024	10	$2^{10} \cdot 179$
191	27, 16	27.48 + 16.47 = 2048	11	$2^{11} \cdot 191$
223	13, 24	13.56+ 24.55 = 2048	11	$2^{11} \cdot 223$
233	28, 113	28.117 + 113.116 = 16384	14	$2^{14} \cdot 233$
239	25, 44	25.60 + 44.59 = 4096	12	$2^{12} \cdot 239$

Clearly in general there will be Hadamard matrices, given by the construction, of order $2^t q$ where $t < [2 \log_2 (q - 3)]$. We analysed a few small primes and found the smallest t indicated by the construction of this paper. For $q = 239$, $t = [2 \log_2 (q - 3)] - 3$, in the other cases the Hadamard matrix can be constructed for a smaller t than indicated by the formula.

In Table I we tabulate the results for a few small q (the a, b, t in the table refer to Corollary 7). The first twenty-five orders, q, for which an Hadamard matrix of order 4q is not known are now listed by giving the smallest power of 2 for which $2^t q$ is known:

$2^5 \cdot 67$, $2^3 \cdot 103$, $2^9 \cdot 107$, $2^3 \cdot 127$, $2^3 \cdot 151$, $2^3 \cdot 163$, $2^4 \cdot 167$, $2^8 \cdot 179$,

$2^{11} \cdot 191$, $2^3 \cdot 213$, $2^3 \cdot 219$, $2^3 \cdot 223$, $2^4 \cdot 233$, $2^4 \cdot 239$,

$2^3 \cdot 249$, $2^6 \cdot 251$, $2^3 \cdot 267$, $2^8 \cdot 269$, $2^3 \cdot 283$, $2^{13} \cdot 311$,

$2^6 \cdot 335$, $2^{15} \cdot 347$, $2^4 \cdot 359$, $2^7 \cdot 373$, $2^4 \cdot 419$, $2^6 \cdot 443$.

As a rough guide, we found that for q(odd) < 1000, Hadamard matrices are known for orders $2^t q$ with t = 2, 80% of the time, t = 3, 10% of the time, t = 4, 5, or 6 in a further 5% of cases. For $1000 < q < 1500$, q odd, the relative proportions are approximately t = 2, 70%, t = 3, 12%, t = 4, 5, or 6, 9% and t > 6, 9%.

We claim that plotting t against q shows that

$$\frac{\text{the total number of orders for which an Hadamard matrix is known}}{\text{the total number of orders for which an Hadamard matrix might exist}} > \frac{1}{2}.$$

REFERENCES

1. A.V. GERAMITA, J. MURPHY GERAMITA, AND J. SEBERRY WALLIS, Orthogonal designs, Linear and Multilinear Algebra, to appear.
2. R. E. A. C. PALEY, On orthogonal matrices, J. Math. Phys. 12 (1933), 311–320.
3. V. SCARPIS, Sui determinanti di valore massimo, Rend. R. Inst. Lombardo Sci. e Lett. 31, No. 2 (1898), 1441–1446.
4. J. J. SYLVESTER, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tesselated pavements in two or more colours, with applications to Newton's Rule, ornamental tile-work, and the theory of numbers, Phil. Mag. 34, No. 4 (1867), 461–475.
5. J. WALLIS, A note on a class of Hadamard matrices, J. Combinatorial Theory 6 (1969), 222–223.
6. J. SEBERRY WALLIS, Orthogonal designs V: orders divisible by eight, Utilitas Math. to appear.
7. W. D. WALLIS, A. PENFOLD STREET, and J. SEBERRY WALLIS, Combinatorics: Room squares, sum-free sets, Hadamard matrices, in "Lecture Notes in Mathematics," 272 Springer–Verlag, Berlin/Heidelberg/New York, 1972.

8. J. WILLIAMSON, Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11 (1944), 65-81.

9. J. WILLIAMSON, Note on Hadamard's determinant theorem, Bull. Amer. Math. Soc. 53 (1947), 608-613.

10. W. W. WOLFE, Rational quadratic forms and orthogonal designs, Queen's Math. Preprints No. 1975-22.