

Pacific Journal of Mathematics

AN INFINITE FAMILY OF SKEW HADAMARD MATRICES

ALBERT LEON WHITEMAN

AN INFINITE FAMILY OF SKEW HADAMARD MATRICES

ALBERT LEON WHITEMAN

It is proved in this paper that a skew Hadamard matrix of order $2(q + 1)$ exists if $q = p^t$ is a prime power such that $p \equiv 5 \pmod{8}$ and $t \equiv 2 \pmod{4}$.

1. **Introduction.** An Hadamard (H -) matrix is a square matrix of ones and minus ones whose row (and therefore column) vectors are orthogonal. The order n of such a matrix is necessarily 1, 2 or is a multiple of 4. A skew H -matrix is an H -matrix of the form

$$H = I + S, S' = -S,$$

where I is the identity matrix and S' the transpose of S . In particular,

$$SS' = -S^2 = (n - 1)I.$$

It has been conjectured that H -matrices and even skew H -matrices always exist for n divisible by 4. Constructions of both types of matrices have been given for particular values of n and also for various infinite classes of values (see [1] for the pertinent references).

In [1] D. Blatt and G. Szekeres constructed for the first time a skew H -matrix of order 52. Their construction is summarized in Theorems 1 and 2 of this paper.

Given an additive abelian group G of order $2m + 1$, two subsets $A \subset G$, $B \subset G$, each of order m , are called *complementary difference sets* in G if

(i) $a \in A \implies -a \notin A$, and

(ii) for each $d \in G$, $d \neq 0$, the total number of solutions $(a_1, a_2) \in A \times A$, $(b_1, b_2) \in B \times B$ of the equations

$$a_1 - a_2 = d, b_1 - b_2 = d$$

is $m - 1$.

We may now state

THEOREM 1. *If for some abelian group G of order $2m + 1$ there exists a pair of complementary difference sets A, B , then there exists a skew H -matrix of order $4(m + 1)$.*

Let $G = GF(q)$ denote the Galois field of order q , where $q = p^t$ and p is an odd prime. For $p^t = ef + 1$ the cyclotomic classes C_i in G are defined by

$$C_i = \{\gamma^{es+i} : s = 0, 1, \dots, f - 1\},$$

where γ is a primitive root of G .

We next state

THEOREM 2. *Let $e = 8$ so that $p^t = 8f + 1$, and let f be odd. Define the sets*

$$A = C_0 \cup C_1 \cup C_2 \cup C_3, \quad B = C_0 \cup C_1 \cup C_6 \cup C_7.$$

Suppose that the total number of solution vectors $(a_1, a_2) \in A \times A$, $(b_1, b_2) \in B \times B$ of

$$a_1 - a_2 = 1, \quad b_1 - b_2 = 1$$

is $4f - 1$. Then A and B are complementary difference sets in G .

In the case $p^t = 25$ Blatt and Szekeres used a root of $x^2 + x + 2 = 0$ as a primitive root and obtained

$$A = \{1, 3, x, x+1, x+4, 2x+3, 3x, 3x+1, 3x+3, 3x+4, 4x+2, 4x+3\},$$

$$B = \{1, 2, x, x+1, x+2, x+3, 2x, 2x+2, 2x+3, 3x+1, 3x+4, 4x+1\}.$$

There are 11 solutions altogether of $a_1 - a_2 = 1$ and $b_1 - b_2 = 1$ given by

$$(a_1, a_2) = (x + 1, x), (x, x + 4), (3x + 1, 3x), (3x + 4, 3x + 3),$$

$$(3x, 3x + 4), (4x + 3, 4x + 2),$$

$$(b_1, b_2) = (2, 1), (x + 1, x), (x + 2, x + 1), (x + 3, x + 2), (2x + 3, 2x + 2).$$

In view of Theorem 2 A and B are complementary difference sets. Hence Theorem 1 yields a skew H -matrix of order 52.

Blatt and Szekeres state in their paper that there seems to be no obvious generalization of this construction. The purpose of the present note is to prove the following theorem.

THEOREM 3. *Suppose that the prime power p^t in Theorem 2 is such that $p \equiv 5 \pmod{8}$ and $t \equiv 2 \pmod{4}$. Then for each $d \in G$, $d \neq 0$, the total number of solutions $(a_1, a_2) \in A \times A$, $(b_1, b_2) \in B \times B$ of the equations*

$$(1) \quad a_1 - a_2 = d, \quad b_1 - b_2 = d$$

is $4f - 1$. Accordingly A and B are complementary difference sets in G .

Theorem 3 in conjunction with Theorem 1 produces an infinite

class of skew H -matrices. For $p^t = 5^2, 13^2, 29^2, \dots$ the corresponding orders of the skew matrices are 52, 340, 1684, \dots . Except for the first these orders do not seem to have been obtained previously.

2. **Proof of Theorem 3.** Since $p \equiv 5 \pmod{8}$ and $t \equiv 2 \pmod{4}$ the integer f in the equation $p^t = 8f + 1$ is odd. Since $\gamma^{4f} = -1$ it follows that $-1 \in C_4$. Consequently, if $c \in C_i$, then $-c \in C_{i+4}$, and if $a \in A$, then $-a \notin A$. Condition (i) in the definition of complementary difference sets is thereby satisfied.

For fixed i and j the cyclotomic number (i, j) is defined to be the number of solutions of the equation

$$(2) \quad z_i + 1 = z_j \quad (z_i \in C_i, z_j \in C_j),$$

where $1 = \gamma^0$ is the multiplicative unit in G . That is, (i, j) is the number of ordered pairs s, t such that

$$\gamma^{8s+i} + 1 = \gamma^{8t+j} \quad (0 \leq s, t \leq f - 1).$$

For f odd the numbers (i, j) satisfy the relations (see [2], p. 394)

$$(i, j) = (j + 4, i + 4) = (8 - i, j - i).$$

These lead to the following array in which the 64 constants (i, j) , $i, j = 0, 1, \dots, 7 \pmod{8}$ are expressed in terms of 15 where (i, j) is in row i and column j .

		0	1	2	3	4	5	6	7
(3)	0	A	B	C	D	E	F	G	H
	1	I	J	K	L	F	D	L	M
	2	N	O	N	M	G	L	C	K
	3	J	O	O	I	H	M	K	B
	4	A	I	N	J	A	I	N	J
	5	I	H	M	K	B	J	O	O
	6	N	M	G	L	C	K	N	O
	7	J	K	L	F	D	L	M	I

Following the methods of Dickson [2] Emma Lehmer [3] derived explicit formulas for these cyclotomic numbers. The result are summarized in [4, p. 79] as follows.

LEMMA. *The cyclotomic numbers for $e = 8, f$ odd, are given by the array (3), and the relations:*

I. If 2 is a fourth power in G

$$64A = q - 15 - 2x$$

$$64B = q + 1 + 2x - 4a + 16y$$

$$64C = q + 1 + 6x + 8a - 16y$$

$$64D = q + 1 + 2x - 4a - 16y$$

$$64E = q + 1 - 18x$$

$$64F = q + 1 + 2x - 4a + 16y$$

$$64G = q + 1 + 6x + 8a + 16y$$

$$64H = q + 1 + 2x - 4a - 16y$$

$$64I = q - 7 + 2x + 4a$$

$$64J = q - 7 + 2x + 4a$$

$$64K = q + 1 - 6x + 4a + 16b$$

$$64L = q + 1 + 2x - 4a$$

$$64M = q + 1 - 6x + 4a - 16b$$

$$64N = q - 7 - 2x - 8a$$

$$64O = q + 1 + 2x - 4a$$

II. If 2 is not a fourth power in G

$$64A = q - 15 - 10x - 8a$$

$$64B = q + 1 + 2x - 4a - 16b$$

$$64C = q + 1 - 2x + 16y$$

$$64D = q + 1 + 2x - 4a - 16b$$

$$64E = q + 1 + 6x + 24a$$

$$64F = q + 1 + 2x - 4a + 16b$$

$$64G = q + 1 - 2x - 16y$$

$$64H = q + 1 + 2x - 4a + 16b$$

$$64I = q - 7 + 2x + 4a + 16y$$

$$64J = q - 7 + 2x + 4a - 16y$$

$$64K = q + 1 + 2x - 4a$$

$$64L = q + 1 - 6x + 4a$$

$$64M = q + 1 + 2x - 4a$$

$$64N = q - 7 + 6x$$

$$64O = q + 1 - 6x + 4a$$

where x, y, a and b are specified by:

(i) $q = x^2 + 4y^2$, $x \equiv 1 \pmod{4}$ is the unique proper representation of $q = p^t$ if $p \equiv 1 \pmod{4}$; otherwise

$$q = (\pm p^{t/2})^2 + 4 \cdot 0^2; \text{ i.e., } x = \pm p^{t/2}, y = 0.$$

(ii) $q = a^2 + 2b^2$, $a \equiv 1 \pmod{4}$ is the unique proper representation of $q = p^t$ if $p \equiv 1$ or $3 \pmod{8}$; otherwise

$$q = (\pm p^{t/2})^2 + 2 \cdot 0^2; \text{ i.e., } a = \pm p^{t/2}, b = 0.$$

The signs of y and b are ambiguously determined.

In view of (2) the cyclotomic number (i, j) may be expressed as the number of solutions of the equation

$$(4) \quad y - x = 1 \quad (y \in C_j, x \in C_i).$$

If $d \in C_k$, then each solution of (4) yields a solution of

$$y_1 - x_1 = d \quad (y_1 \in C_{j+k}, x_1 \in C_{i+k}).$$

It follows that if $d \in C_k$, then there are $(i - k, j - k)$ solutions of the equation

$$y - x = d \quad (y \in C_j, x \in C_i).$$

This enables us to determine how often each difference arises from sets composed of given cyclotomic classes. The set A of Theorem 3 is the union of the classes C_0, C_1, C_2, C_3 . Here we find that the number N_k of solutions of $y - x = d$ with $y, x \in A$ and $d \in C_k$ is given by

$$\begin{aligned}
 N_k &= (-k, -k) + (1 - k, -k) + (2 - k, -k) + (3 - k, -k) \\
 (5) \quad &+ (-k, 1-k) + (1-k, 1-k) + (2-k, 1-k) + (3-k, 1-k) \\
 &+ (-k, 2-k) + (1-k, 2-k) + (2-k, 2-k) + (3-k, 2-k) \\
 &+ (-k, 3-k) + (1-k, 3-k) + (2-k, 3-k) + (3-k, 3-k) .
 \end{aligned}$$

The set B is the union of the classes C_0, C_1, C_6, C_7 . The corresponding number N'_k of solutions of $y - x = d$ with $y, x \in B$ and $d \in C_k$ is

$$\begin{aligned}
 N'_k &= (-k, -k) + (1 - k, -k) + (6 - k, -k) + (7 - k, -k) \\
 (6) \quad &+ (-k, 1-k) + (1-k, 1-k) + (6-k, 1-k) + (7-k, 1-k) \\
 &+ (-k, 6-k) + (1-k, 6-k) + (6-k, 6-k) + (7-k, 6-k) \\
 &+ (-x, 7-k) + (1-k, 7-k) + (6-k, 7-k) + (7-k, 7-k) .
 \end{aligned}$$

Since every solution of $y - x = d$ with $y, x \in A$ and $d \in C_k$ yields a solution of $x - y = -d$, and since $-1 \in C_4$, it follows that $N_k = N_{k+4} (k = 0, 1, 2, 3)$. Similarly, $N'_k = N'_{k+4} (k = 0, 1, 2, 3)$. Furthermore, since $a \in A \Rightarrow \gamma^6 a \in B$ and $b \in B \Rightarrow \gamma^2 b \in A$, we have also $N_{k+2} = N'_k (k = 0, 1, 2, 3)$. Hence we find that

$$\begin{aligned}
 (7) \quad N_0 + N'_0 &= N_2 + N'_2 = N_4 + N'_4 = N_6 + N'_6 , \\
 N_1 + N'_1 &= N_3 + N'_3 = N_5 + N'_5 = N_7 + N'_7 .
 \end{aligned}$$

The application of the lemma to the evaluation of N_k and N'_k depends upon whether or not 2 is a fourth power in G . We now show that 2 is not a fourth power in G when $p \equiv 5 \pmod{8}$ and $t \equiv 2 \pmod{4}$. It is convenient to put $r = (p^t - 1)/(p - 1)$. The number γ is a generator of the cyclic group of nonzero elements of $GF(p^t)$, and hence $\gamma^r = g$ is a generator of the cyclic group of nonzero elements of $GF(p)$. Since $(2|p) = -1$ the exponent k in the equation $g^k = 2$ is odd. Furthermore, since $r = p^{t-1} + p^{t-2} + \dots + 1 \equiv t \pmod{4}$, the exponent rk in the equation $\gamma^{rk} = 2$ is $\equiv 2 \pmod{4}$. Therefore 2 is not a fourth power in G .

In view of (7) it suffices to evaluate N_0, N'_0 and N_1, N'_1 . From (5), (6) and the array (3) we get

$$\begin{aligned}
 N_0 &= \text{AINJBJOOCKNODLMI} , \\
 N'_0 &= \text{AINJBJMKGLNMHMOI} , \\
 N_1 &= \text{JAINKBJOLCKNIHMK} , \\
 N'_1 &= \text{JAINLFJKMGONIHOO} ,
 \end{aligned}$$

where, for brevity, we have omitted the plus signs between adjacent letters. Applying Case II of the lemma we may now derive the following formulas

$$64N_0 = 16q - 48 - 8x + 8a + 16y - 32b ,$$

$$64N'_0 = 16q - 48 + 8x - 8a - 16y ,$$

$$64N_1 = 16q - 48 + 8x - 8a + 16y ,$$

$$64N'_1 = 16q - 48 - 8x + 8a - 16y + 32b .$$

Consequently

$$64(N_0 + N'_0) = 32q - 96 - 32b, 64(N_1 + N'_1) = 32q - 96 + 32b .$$

Thus $N_0 + N'_0$ and $N_1 + N'_1$ are equal if and only if $b = 0$. Statement (ii) at the end of the lemma guarantees that $b = 0$ when $p \equiv 5 \pmod{8}$. It follows that for each $d \in G$, $d \neq 0$, the total number of solutions of the equations (1) in Theorem 3 is $(q - 3)/2 = 4f - 1$. The proof of Theorem 3 is thus complete.

REFERENCES

1. D. Blatt and G. Szekeres, *A skew Hadamard matrix of order 52*, *Canad. J. Math.*, **21** (1969), 1319-1322.
2. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, *Amer. J. Math.*, **57** (1935), 391-424.
3. E. Lehmer, *On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$* , *Pacific J. Math.*, **5** (1955), 103-118.
4. T. Storer, *Cyclotomy and difference sets*, Markham Publishing Company, Chicago, 1967.

Received October 12, 1970. This research was partially supported by National Science Foundation Grant GP-14180.

UNIVERSITY OF SOUTHERN CALIFORNIA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON
Stanford University
Stanford, California 94305

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

C. R. HOBBY
University of Washington
Seattle, Washington 98105

RICHARD ARENS
University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CHEVRON RESEARCH CORPORATION
NAVAL WEAPONS CENTER

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. 39. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$8.00; single issues, \$3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues \$1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

J. T. Borrego, Haskell Cohen and Esmond Ernest Devun, <i>Uniquely representable semigroups on the two-cell</i>	565
Glen Eugene Bredon, <i>Some examples for the fixed point property</i>	571
William Lee Bynum, <i>Characterizations of uniform convexity</i>	577
Douglas Derry, <i>The convex hulls of the vertices of a polygon of order n</i>	583
Edwin Duda and Jack Warren Smith, <i>Reflexive open mappings</i>	597
Y. K. Feng and M. V. Subba Rao, <i>On the density of (k, r) integers</i>	613
Irving Leonard Glicksberg and Ingemar Wik, <i>Multipliers of quotients of L_1</i>	619
John William Green, <i>Separating certain plane-like spaces by Peano continua</i>	625
Lawrence Albert Harris, <i>A continuous form of Schwarz's lemma in normed linear spaces</i>	635
Richard Earl Hodel, <i>Moore spaces and w Δ-spaces</i>	641
Lawrence Stanislaus Husch, Jr., <i>Homotopy groups of PL-embedding spaces. II</i>	653
Yoshinori Isomichi, <i>New concepts in the theory of topological space—supercondensed set, subcondensed set, and condensed set</i>	657
J. E. Kerlin, <i>On algebra actions on a group algebra</i>	669
Keizō Kikuchi, <i>Canonical domains and their geometry in C^n</i>	681
Ralph David McWilliams, <i>On iterated w^*-sequential closure of cones</i>	697
C. Robert Miers, <i>Lie homomorphisms of operator algebras</i>	717
Louise Elizabeth Moser, <i>Elementary surgery along a torus knot</i>	737
Hiroshi Onose, <i>Oscillatory properties of solutions of even order differential equations</i>	747
Wellington Ham Ow, <i>Wiener's compactification and Φ-bounded harmonic functions in the classification of harmonic spaces</i>	759
Zalman Rubinstein, <i>On the multivalence of a class of meromorphic functions</i>	771
Hans H. Storrer, <i>Rational extensions of modules</i>	785
Albert Robert Stralka, <i>The congruence extension property for compact topological lattices</i>	795
Robert Evert Stong, <i>On the cobordism of pairs</i>	803
Albert Leon Whiteman, <i>An infinite family of skew Hadamard matrices</i>	817
Lynn Roy Williams, <i>Generalized Hausdorff-Young inequalities and mixed norm spaces</i>	823