A SKEW HADAMARD MATRIX OF ORDER 52

D. BLATT AND G. SZEKERES

1. A Hadamard (H-) matrix $H = (h_{ij})$ of order n is an $n \times n$ square matrix satisfying the conditions

$$h_{ij} = +1 \text{ or } -1, \qquad \sum_{k=1}^{n} h_{ik}h_{jk} = n\delta_{ij}$$

for all $i, j \leqq n$. A skew H-matrix is an H-matrix of the form

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

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

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

Skew H-matrices have applications in the theory of finite projective planes (**2**) and tournaments (**4**), also in the construction of H-matrices of certain orders. For example, if there is a skew H-matrix of order n, then there is an H-matrix of order $n(n-1)$ (Williamson, see (**1**, p. 213)).

It is known from constructions of Paley (**3**) and Williamson (**5**) that there exist skew H-matrices of orders $2^t \prod_{i=1}^{r} (p_i^{\alpha_i} + 1)$, where the p_i are distinct primes, $t \geqq 0$, $r \geqq 0$, and $p_i^{\alpha_i} + 1 \equiv 0 \pmod 4$ for each i. Furthermore, if n is an order of a skew H-matrix, then there exists one of order $(n-1)^3 + 1$ (Goldberg (**1**, p. 221)). Until quite recently these were the only known constructions of skew H-matrices. In a recent paper (**4**, p. 277, Theorem 6), skew H-matrices of all orders $n = 2(p^t + 1)$ were constructed, where p is prime and $p^t \equiv 5 \pmod 8$. The following is a summary of the construction.

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) $\alpha \in A \Rightarrow -\alpha \notin A$, and

(ii) for each $\delta \in G$, $\delta \neq 0$, the total number of solutions $(\alpha_1, \alpha_2) \in A \times A$, $(\beta_1, \beta_2) \in B \times B$ of the equations

$$\delta = \alpha_1 - \alpha_2, \qquad \delta = \beta_1 - \beta_2$$

is $n - 1$.

Then the following results are true.

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* $4(m + 1)$.

Received May 22, 1968.

https://doi.org/10.4153/CJM-1969-144-2 Published online by Cambridge University Press

THEOREM 2. *Let* $2m + 1 = p^t \equiv 5 \pmod 8$ *and* G *the additive group of* $\mathrm{GF}(p^t)$. *Let* ρ *be a primitive root of* $\mathrm{GF}(p^t)$, H_0 *the multiplicative subgroup of index* 4 *generated by* ρ^4, *and* H_i, $i = 1, 2, 3$, *the coset of* H_0 *represented by* ρ^i. *Then*

$$A = H_0 \cup H_1 \quad \textit{and} \quad B = H_0 \cup H_3$$

are complementary difference sets in G.

These two theorems clearly imply the existence of a skew H-matrix of order $2(p^t + 1) \equiv 12 \pmod{16}$. The construction of a skew H-matrix from complementary difference sets A and B is as follows (see **4**).

Let $\gamma_1, \ldots, \gamma_{2m+1}$ be the elements of G. Define, for $1 \leqq i, j \leqq 2m + 1$,

$$-s_{2m+1+i,2m+1+j} = s_{ij} = \begin{cases} +1 & \text{if } \gamma_j - \gamma_i \in A, \\ -1 & \text{if } \gamma_i - \gamma_j \in A, \end{cases}$$

$$-s_{2m+1+j,i} = s_{i,2m+1+j} = \begin{cases} +1 & \text{if } \gamma_j - \gamma_i \in B, \\ -1 & \text{if } \gamma_j - \gamma_i \notin B, \end{cases}$$

and

$$-s_{4m+3,i} = s_{i,4m+3} = \begin{cases} 1 & \text{for } 1 \leqq i \leqq 2m+1, \\ -1 & \text{for } 2m+2 \leqq i \leqq 4m+2, \end{cases}$$

$$s_{4m+4,i} = -s_{i,4m+4} = 1 \quad \text{for } 1 \leqq i \leqq 4m+3,$$

$$s_{ii} = 0 \quad \text{for } 1 \leqq i \leqq 4m+4.$$

Then $H = I + S = (\delta_{ij} + s_{ij})$ is a skew H-matrix.

2. The only orders divisible by four and less than or equal to 100 not covered by these constructions are 36, 52, 96, and 100. A machine search has shown that there are no complementary difference sets in the cyclic group of order 17, hence no skew H-matrix of order 36 can be obtained by this construction. Similarly, there are no complementary difference sets in the cyclic group of order 25.

On the other hand, a complete machine search of the elementary abelian group of order 25 and type (5, 5) has produced 480 different pairs of complementary difference sets. Examination of these difference sets has shown that the corresponding H-matrices are all equivalent under permutation and multiplication by ± 1 of rows and columns. One of the pairs of sets A and B can be obtained as follows.

We represent G as the additive group of GF (25). Let ρ be a primitive root, H_0 the multiplicative subgroup of index 8 generated by ρ^8, and H_i $(i = 1, \ldots, 7)$ the coset represented by ρ^i. Then

$$A = H_0 \cup H_1 \cup H_2 \cup H_3, \qquad B = H_0 \cup H_1 \cup H_6 \cup H_7,$$

To prove that A and B are complementary difference sets, it is sufficient to verify that

$$1 = \alpha_1 - \alpha_2 \quad \text{and} \quad 1 = \beta_1 - \beta_2,$$

$\alpha_1, \alpha_2 \in A$, $\beta_1, \beta_2 \in B$ have altogether eleven solutions. For the following result is true.

THEOREM 3. *Let ρ be a primitive root of $G = \mathrm{GF}(p^t)$, where $p^t = 8m + 1$, $m \equiv 1 \pmod 2$. Let H_0 be the multiplicative subgroup of index 8 generated by ρ^8, H_i $(i = 1, \ldots, 7)$ the coset of H_0 represented by ρ^i, $A = H_0 \cup H_1 \cup H_2 \cup H_3$, and $B = H_0 \cup H_1 \cup H_6 \cup H_7$. Suppose further that the total number of solution vectors $(\alpha_1, \alpha_2) \in A \times A$, $(\beta_1, \beta_2) \in B \times B$ of*

$$1 = \alpha_1 - \alpha_2, \qquad 1 = \beta_1 - \beta_2$$

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

Proof. Let $\delta \in H_i$ and denote by M_i the number of solutions of $\delta = \alpha_1 - \alpha_2$, $\alpha_1, \alpha_2 \in A$, by M_i' the number of solutions of $\delta = \beta_1 - \beta_2$, $\beta_1, \beta_2 \in B$. Clearly M_i and M_i' are independent of the particular representatives δ of M_i.

Now every solution of $\delta = \alpha_1 - \alpha_2$, $\alpha_1, \alpha_2 \in A$ yields a solution of $-\delta = \alpha_2 - \alpha_1$, and hence, since $-1 \in H_4$, $M_i = M_{4+i}$, $i = 0, 1, 2, 3$. Similarly, $M_i' = M_{4+i}'$, $i = 0, 1, 2, 3$. Furthermore, since $\alpha \in A \Rightarrow \rho^{-2}\alpha \in B$ and $\beta \in B \Rightarrow \rho^2\beta \in A$, we also have $M_{i+2} = M_i'$, $i = 0, 1, 2, 3$; hence

$$M_0 + M_0' = M_2 + M_2' = M_4 + M_4' = M_6 + M_6' = N,$$
$$M_1 + M_1' = M_3 + M_3' = M_5 + M_5' = M_7 + M_7' = N'.$$

However, $(N + N')4m$ is equal to twice the number of pairs $(\alpha_i, \alpha_j) \in A \times A$, i.e. to $8m(4m - 1)$, and thus

$$N + N' = (p^t - 3) = 2(4m - 1).$$

Hence, if $M_0 + M_0' = N = 4m - 1$, then we also have $N' = 4m - 1$, and the statement is proved.

In the case of $p^t = 25$, by using a root of $\rho^2 + \rho + 2 = 0$ as primitive root, we obtain:

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

and the solutions of $1 = \alpha_1 - \alpha_2$ and $1 = \beta_1 - \beta_2$ are

$$(\alpha_1, \alpha_2) = (1 + \rho, \rho), (\rho, 4 + \rho), (1 + 3\rho, 3\rho), (4 + 3\rho, 3 + 3\rho),$$
$$(3\rho, 4 + 3\rho), (3 + 4\rho, 2 + 4\rho),$$

$$(\beta_1, \beta_2) = (2, 1), (1 + \rho, \rho), (2 + \rho, 1 + \rho), (3 + \rho, 2 + \rho), (3 + 2\rho, 2 + 2\rho).$$

Hence A and B are complementary difference sets and we have constructed a skew H-matrix of order 52.

There seems to be no obvious generalization of this construction. J. M. Goethals and J. J. Seidel have recently obtained a skew H-matrix of order 36, by an entirely different method (private communication). Thus the lowest unsettled case is now 92.

References

1. Marshall Hall, Jr., *Combinatorial theory* (Blaisdell, Waltham, Massachusetts, 1967).
2. E. C. Johnsen, *Integral solutions to the incidence equation for finite projective plane cases of orders* $n \equiv 2 \pmod 4$, Pacific J. Math. *17* (1966), 97–120.
3. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. *12* (1933), 311–320.
4. G. Szekeres, *Tournaments and Hadamard matrices*, Enseignement Math. *15* (1969), 269–278.
5. J. Williamson, *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J. *11* (1944), 65–81.

University of Sydney,
Sydney, Australia;
University of New South Wales,
Kensington, New South Wales

https://doi.org/10.4153/CJM-1969-144-2 Published online by Cambridge University Press