SKEW HADAMARD MATRICES OF GOETHALS--SEIDEL TYPE

Albert Leon Whitman*

University of Southern California, Los Angeles, Calif 90007, U.S.A.

Received 15 September 1971**

Abstract. Goethals and Seidel have recently demonstrated the existence of skew Hadamard matrices of orders 36 and 52 by means of a new type of construction. Jennifer Walls has obtained additional matrices of this type for all orders $4^r$, $3 \leq n \leq 25$ and $n$ odd. In the present paper, an infinite family of such matrices is derived. The main result states that if $q$ is a prime power $\equiv 3 \pmod{8}$, then there exists a skew Hadamard matrix of order $4n = q + 1$ that is of the Goethals--Seidel type.

§ 1. Introduction

An Hadamard matrix $H$ is a matrix of order $n$, all of whose elements are $+1$ and $-1$ and which satisfies $HH^T = nl$, where $H^T$ is the transpose of $H$ and $I$ is the unit matrix of order $n$. The order $n$ of $H$ is necessarily 1, 2 or is divisible by 4. It is an outstanding conjecture that Hadamard matrices of order $n$ always exist when $n$ is divisible by 4. The smallest order for which the existence of an Hadamard matrix is not yet known is $n = 188$.

An Hadamard matrix $H = S + I$ is said to be skew Hadamard if $S^T = -S$. It is conjectured that whenever there exists an Hadamard matrix of order $n$ there exists a skew Hadamard matrix of the same order. The smallest order for which a skew Hadamard matrix is not known is $n = 116$.

Many families of Hadamard and skew Hadamard matrices are known. For example, Szekeres [4] recently constructed skew Hadamard matrices of all orders $n = 2(p^t + 1)$, where $p$ is a prime and $p^t \equiv 5 \pmod{8}$. Relevant references may be found in [2, 6, 7 and 8].

* Supported in part by National Science Foundation grant no GP-25735 X.

** Original version received 10 June 1971.
In order to demonstrate the existence of skew Hadamard matrices of orders 36 and 54, Goethals and Seidel [1] devised a new type of construction. Let the square matrices $Q$ and $R$ of order $n$ be defined by their only non-zero elements

$$q_{k, i+1} = q_{n-1, 0} = 1, \quad r_{i, n-2-i} = r_{n-1, n-1} = 1, \quad i = 0, 1, \ldots, n-2.$$ 

Then we have

$$Q^n = I, \quad R^2 = I, \quad RQ = Q^TR.$$ 

Any square matrix $A$ of order $n$ is symmetric if $A = A^T$, skew if $A + A^T = 0$, circulant if $AQ = QA$ and back-circulant if $AQ^T = QA^T$. In particular, for a circulant $A$ we have

$$A = \sum_{i=0}^{n-1} a_i Q^i, \quad RA = A^TR.$$ 

If $A$ is a square circulant matrix of order $n$, then $AR$ and $A^TR$ are back-circulants of order $n$. If the numbers $a_0, a_1, \ldots, a_{n-1}$ comprise the first row of $A$, then the numbers $a_{n-2}, a_{n-3}, \ldots, a_0, a_{n-1}$ comprise the first row of $AR$, and the numbers $a_2, a_3, \ldots, a_0, a_1$ comprise the first row of $A^TR$. By means of a straightforward verification, Goethals and Seidel [1] established the following theorem:

**Theorem 1.** If $A, B, C, D$ are square circulant matrices of order $n$, if $A$ is skew, and if

$$AA^T + BB^T + CC^T + DD^T = (4n-1)I,$$

then

$$H = \begin{bmatrix} A+i & BR & CR & DR \\ -BR & A+i & -D^TR & C^TR \\ -CR & D^TR & A+i & -B^TR \\ -DR & -C^TR & B^TR & A+i \end{bmatrix}$$

satisfies $HH^T = 4nI$, $H + H^T = 2I$. 
Skew Hadamard matrices of type (2) have been constructed by Goethals and Seidel [1] for orders $4n = 36$ and 52, and by Jennifer Wallis [6, 8, 9] for orders $4n = 12, 20, 28, 36, 44, 52, 60, 76, 92$ and 100. In the present paper we exhibit an infinite family of skew Hadamard matrices of Goethals--Seidel type. Our main result states that if $q$ is a prime power $\equiv 3 \pmod{8}$, then there exists a skew Hadamard matrix $H$ of order $4n = q + 1$ that is of the form (2).

It should be pointed out that Paley [3] in 1933 had already constructed Hadamard matrices of all orders $q + 1$ when $q$ is a prime power $\equiv 3 \pmod{4}$. By making a slight change in Paley's method, Williamson [11] in 1944 constructed skew Hadamard matrices of the same orders. The novel feature of the present paper consists in constructing an infinite class of skew Hadamard matrices that are of type (2). Hadamard matrices equivalent under permutation of rows or columns or change of sign of rows or columns are considered to be in the same class. The referee has kindly inquired if the new family of skew matrices constructed here is equivalent to the skew family of Paley. This interesting question has not been resolved in the present paper.

The matrix (2) is analogous to the Williamson matrix

$$W = \begin{bmatrix}
A & B & C & D \\
B & A & -D & C \\
C & D & A & -B \\
-D & -C & B & A
\end{bmatrix},$$

where each of $A, B, C, D$ is a symmetric circulant $n \times n$ matrix. If the elements of $A, B, C, D$ in (3) are all $+1$ or $-1$ and if

$$A^2 + B^2 + C^2 + D^2 = 4nI,$$

then $W$ is an Hadamard matrix of order $4n$. Turyn [5] proved the remarkable result that if $q$ is a prime power $\equiv 1 \pmod{4}$, then there exists an Hadamard matrix of Williamson type (3) of order $4n = 2(q + 1)$. The proof of Theorem 2 in the present paper is a modification of the author's [10] alternative proof of Turyn's theorem.

The author wishes to thank Professor G. Szekeres for suggesting the problem of this paper to him in a written communication.
§2. A preliminary lemma

Let $GF(q^2)$ denote the finite field of order $q^2$, where $q = p^t$ is a prime power. Let $\gamma$ denote a generator of the cyclic group of non-zero elements of $GF(q^2)$. Then $\gamma^{q+1} = g$ is a generator of the cyclic group of non-zero elements of the finite field $GF(q)$ of order $q$. For arbitrary $\xi \in GF(q^2)$, define

\[ (4) \quad \text{tr}(\xi) = \xi + \xi^q, \]

so that $\text{tr}(\xi) \in GF(q)$. It follows at once from this definition that

\[ (5) \quad \text{tr}(\gamma^k) = \gamma^{(q+1)k} \text{tr}(\gamma^k), \]

where $k$ is any integer.

Suppose henceforth that $q \equiv 3 \pmod{8}$. Then the polynomial $P(x) = x^2 + 1$ is irreducible in the finite field $GF(q)$. Hence the polynomials $ax + b$, $a, b \in GF(q)$, modulo $P(x)$ form a finite field $GF(q^2)$. We shall employ this concrete representation of $GF(q^2)$ in the rest of this paper. For $\xi \in GF(q^2)$, $\xi \neq 0$, let $\text{ind}(\xi)$ be the least non-negative integer $t$ such that $\gamma^t = \xi$. Let $\beta$ denote a primitive eighth root of unity. Then

\[ (6) \quad \chi(\xi) = \begin{cases} \beta^{\text{ind}(\xi)} & \text{if } \xi \neq 0, \\ 0 & \text{if } \xi = 0. \end{cases} \]

defines an eighth power character $\chi$ of $GF(q^2)$. For $a \in GF(q)$, $a \neq 0$, put $g^t = a$. Then (6) implies that $\chi(a) = \beta^{(q+1)t} = (-1)^t$. This means that the character $\chi(a)$ reduces to the ordinary Legendre symbol over $GF(q)$. Thus $\chi(a) = -1, -1$ or $0$ according as $a$ is a non-zero square, a non-square, or zero in $GF(q)$. Accordingly we deduce from (5) that

\[ (7) \quad \chi(\text{tr}(\gamma^k)) \chi(\text{tr}(\gamma^{-k})) = (-1)^k, \text{tr}(\gamma^k) \neq 0. \]

The proof of Theorem 2 in the next section is based upon the following lemma.
Lemma 1 If \( r \) is a non-negative integer, then

\[
\sum_{k=0}^{q} \chi(\text{tr}(\gamma^k)) \chi(\text{tr}(\gamma^{k+r})) = \begin{cases} 
(1)^{q} & \text{if } q + 1 \parallel r \\
0 & \text{otherwise}
\end{cases}
\]

where, in the first case, \( r = j(q+1) \).

This lemma is analogous to formula (9) in [10]. For the sake of completeness we give the following short proof. For fixed \( \eta \in \text{GF}(q^2) \) put \( \eta = cx + d \), \( c, d \in \text{GF}(q) \). Then \( \eta \in \text{GF}(q) \) if \( c = 0 \) and \( \eta \notin \text{GF}(q) \) if \( c \neq 0 \). We first show that

\[
\sum_{\xi} \chi(\text{tr}(\xi)) \chi(\text{tr}(\eta \xi)) = \begin{cases} 
\chi(d)q(q-1) & \text{if } c = 0 \\
0 & \text{if } c \neq 0
\end{cases}
\]

where the summation extends over all \( \xi \in \text{GF}(q^2) \). Put \( \xi = ax + b \), \( a, b \in \text{GF}(q) \). By (4) we have \( \text{tr}(\xi) = 2b \) and \( \text{tr}(\eta \xi) = 2bd - ac \). Therefore

\[
\sum \chi(\text{tr}(\xi)) \chi(\text{tr}(\eta \xi)) = \sum_b \chi(b) \sum_a \chi(bd - ac)
\]

and (9) follows at once.

For \( \eta \neq 0 \) we may put \( \eta = \gamma^r \), \( 0 \leq r \leq q^2 - 2 \), so that \( c = 0 \) if \( q + 1 \mid r \)
and \( c \neq 0 \) if \( q + 1 \nmid r \). If \( c = 0 \), put \( r = j(q+1) \), then we get \( \chi(d) = (1)^j \). The sum in (9) now becomes

\[
\sum_{k=0}^{q^2 - 2} \chi(\text{tr}(\gamma^k)) \chi(\text{tr}(\gamma^{k+r})) = \sum_{h=0}^{q-2} \sum_{k=h(q+1)}^{h(q+1)+q} \chi(\text{tr}(\gamma^k)) \chi(\text{tr}(\gamma^{k+r})).
\]

In view of (9), the double sum on the right has the value 0 if \( q + 1 \nmid r \). Since \( \chi(\text{tr}(\gamma^{k+q+1})) = -\chi(\text{tr}(\gamma^k)) \), the value of the inner sum is the same for each \( h \). In particular for \( h = 0 \) we obtain the result stated in the lemma.
§3. The main theorem

The principal result of this paper is the following theorem:

**Theorem 2.** Let \( q \) be a prime power \( \equiv 3 \pmod{8} \) and put \( n = \frac{1}{2}(q+1) \). Let \( \gamma \) be a primitive element of \( \text{GF}(q^2) \). Put \( \gamma^k = ax + b \), \( a, b \in \text{GF}(q) \), and define

\[
(10) \quad a_k = \chi(a), \quad b_k = \chi(b).
\]

Let \( A, B, C, D \) be square circulant matrices of order \( n \) whose initial rows are given by \( a_0, a_8, a_{16}, \ldots, a_{8(n-1)}; b_0, b_8, b_{16}, \ldots, b_{8(n-1)}; a_1, a_9, a_{17}, \ldots, a_{8n-7}; b_1, b_9, b_{17}, \ldots, b_{8n-7} \) respectively. Then the matrix \( H \) defined by (2) in Theorem 1 is a skew Hadamard matrix of order \( 4n \).

**Proof.** In view of Theorem 1 we must show that \( A \) is skew and that the condition (1) is satisfied. We first demonstrate that \( A \) is skew. Since \( \gamma \) is a primitive element of \( \text{GF}(q^2) \), the integer \( k = \frac{1}{2}(q+1) = 2n \) is the only value of \( k \) in the interval \( 0 < k < q \) for which \( \text{tr}(\gamma^k) = 0 \). Put \( \gamma^{2n} = wx, w \in \text{GF}(q) \), so that \(-w^2 = g\). Then the numbers \( a_k, b_k \) in (10) satisfy the relations

\[
(11) \quad a_k = -a_{k+4n} = a_{k+8n}, \quad b_k = -b_{k+4n} = b_{k+8n},
\]

\[
a_{k+2n} = -a_{k+6n} = \chi(w)b_k, \quad b_{k+2n} = -b_{k+6n} = \chi(w)a_k.
\]

From relation (7) we deduce also the second of the two relations

\[
(12) \quad a_k = (-1)^{k+1}a_{8n-k}, \quad b_k = (-1)^{k}b_{8n-k}.
\]

The first relation in (12) follows from the second by replacing \( k \) by \( k + 2n \) and then applying (11). For \( k = 8i \), we get in particular

\[
(13) \quad a_{8i} = -a_{8(n-i)}, \quad i = 0, 1, \ldots, n-1.
\]

Relation (13) expresses the skew property of the matrix \( A \).
It remains to prove that the matrices $A, B, C, D$ satisfy the orthogonality condition (1). We shall employ an alternative formulation of this condition. Put

\begin{equation}
F(8r) = \sum_{j=0}^{n-1} a_{8j}a_{8j+8r} + \sum_{j=0}^{n-1} b_{8j}b_{8j+8r} + \sum_{j=0}^{n-1} a_{8j+1}a_{8j+1+8r} + \sum_{j=0}^{n-1} b_{8j+1}b_{8j+1+8r},
\end{equation}

where the subscripts are reduced modulo $8n$. Then we may verify directly that condition (1) is equivalent to the condition

\begin{equation}
F(8r) = \begin{cases} 4n-1, & \text{if } r = 0, \\ 0, & \text{if } 1 \leq r \leq n-1. \end{cases}
\end{equation}

We also put

\begin{equation}
G(8r) = \sum_{k=0}^{q} b_k b_{k+8r}.
\end{equation}

Since $n$ is an odd integer, it follows that $q + 1 \not| 8r$ for $1 \leq r \leq n-1$. Hence Lemma 1 in § 2 yields

\begin{equation}
G(8r) = \begin{cases} 4n-1, & \text{if } r = 0, \\ 0, & \text{if } 1 \leq r \leq n-1. \end{cases}
\end{equation}

The right members of (15) and (17) are identical. Accordingly, we shall complete the proof by transforming the right member of (16) into the right member of (14).

We first rewrite (16) in the form
Put $n = 2f + 1$. Then for each fixed $t$ we have

$$G(8r) = \sum_{t=0}^{3} \sum_{i=0}^{n-1} b_{4i+t} b_{4i+t+8r}.$$  \hfill (18)

where we have made use of the periodicity relation $b_k = -b_{k+4n}$ given in (11). Hence (18) becomes

$$G(8r) = \sum_{t=0}^{3} \sum_{j=0}^{n-1} b_{8j+t} b_{8j+t+8r}.$$  \hfill (19)

Thus for $t = 0$ we get the second sum in (14), and for $t = 1$ we get the fourth.

We proceed to consider the summands $t = 2$ and $t = 3$. From the periodicity relation $b_{k+8n} = b_k$ in (11), it is evident that

$$\sum_{j=0}^{n-1} b_{8j+t} b_{8j+t+8r} = \sum_{j=0}^{n-1} b_{8j+u} b_{8j+u+8r}$$

whenever $t \equiv u \pmod{8}$. Since $2 = \pm 2n \pmod{8}$ according as $n \equiv \pm 1 \pmod{4}$, we find in particular for $t = 2$ that
Thus for $t = 3$ the inner sum in (19) is carried into the third sum in (14). This completes the proof of Theorem 2.

References