JOURNAL OF NUMBER THEORY 8, 1–11 (1976)

# Hadamard Matrices of Order $4(2p + 1)$

ALBERT LEON WHITEMAN*

*Department of Mathematics, University of Southern California, Los Angeles, California 90007*

*Communicated by Olga Taussky-Todd*

Received July 24, 1972

DEDICATED TO THE MEMORY OF NORMAN LEVINSON

It is shown in this paper that if $p$ is a prime and $q = 2p - 1$ is a prime power, then there exists an Hadamard matrix of order $4(2p + 1)$.

## 1. INTRODUCTION

An Hadamard matrix $H$ is a matrix of order $n$ all of whose elements are $+1$ or $-1$ and that satisfies $HH^T = nI$, 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. Many classes of Hadamard matrices are known; pertinent references may be found in [3, 6, 7]. The smallest order $n$ for which the existence of an Hadamard matrix is unsettled is $n = 268$.

Let $D_1, D_2, \ldots, D_n$ be subsets of $V$, the set of residues modulo a positive integer $v$, containing $k_1, k_2, \ldots, k_n$ elements, respectively. Write $T_i$ for the totality of all differences modulo $v$ (with repetitions) between elements of $D_i$, and $T$ for the totality of elements of all the $T_i$. If $T$ contains each nonzero residue of $V$ a fixed number of times, $\lambda$, say, then the sets $D_1, D_2, \ldots, D_n$ are called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets. Supplementary difference sets are useful in constructing Hadamard matrices (see [6]). In Sections 2 and 3 of this paper we show that $4 - \{2t; t - 1, t, t, t; 2(t - 1)\}$ supplementary difference sets can be used to construct an Hadamard matrix of order $4(2t + 1)$. Let $p$ be a prime and $q = 2p - 1$ a prime power. In Section 6 a construction is given of

* The research of this paper was partially supported by National Science Foundation Grant GP-25735X1.

$4 - \{2p; p - 1, p, p, p; 2(p - 1)\}$ supplementary difference sets. This is accomplished by suitably combining the residue sets in Lemma 2 of Section 4 and Lemma 3 of Section 5. The construction yields an Hadamard matrix of order $4(2p + 1)$. Two interesting examples may be cited. An Hadamard matrix of order 156 was first constructed by Baumert and Hall [1] in 1965. The case $p = 19$, $q = 37$ of the present construction furnishes a new matrix of this order. The case $p = 439$, $q = 877$ leads to an Hadamard matrix of order 3516. This order seems to be new.

The method of this paper was suggested by the results of a computer search for $4 - \{2t; t - 1, t, t, t; 2(t - 1)\}$ supplementary difference sets. Indeed, in the case $t = 19$ an Hadamard matrix of order 156 was originally constructed in this manner.

## 2. Supplementary Difference Sets

Let $D = (x_1, x_2, ..., x_k)$ denote a set of $k$ distinct residues modulo a positive integer $v$. For each residue $r \not\equiv 0 \pmod{v}$ let $\lambda(r)$ denote the number of solution pairs $(x_i, x_j)$ of the congruence $x_i - x_j \equiv r \pmod{v}$ with $x_i$ and $x_j$ in $D$. If $\lambda(r) = \lambda$ for each $r \not\equiv 0 \pmod{v}$, then $D$ is said to be a $(v, k, \lambda)$ difference set. In this case the relation $k(k - 1) = \lambda(v - 1)$ evidently holds. A familiar example of a difference set is incorporated into the following lemma.

Lemma 1. *Suppose that the set $D$ consists of the $(p - 1)/2$ quadratic residues modulo an odd prime $p$. If $p \equiv 3 \pmod 4$, then $\lambda(r) = (p - 3)/4$ for each $r \not\equiv 0 \pmod p$. If $p \equiv 1 \pmod 4$, then $\lambda(r) = (p - 5)/4$ when $(r \mid p) = 1$ and $\lambda(r) = (p - 1)/4$ when $(r \mid p) = -1$. The symbol $(r \mid p)$ is the Legendre symbol.*

This lemma is well known and is proved implicitly in [4, p. 30].

The elements in $D = (x_1, x_2, ..., x_k)$ generate the circulant $(1, -1)$ matrix $A = [a_{ij}](i, j = 0, 1, ..., v - 1)$ of order $v$; $a_{ij} = a_{0,j-i} = 1$ when $j - i \in D$ (all numbers modulo $v$) and $-1$ otherwise. Conversely, if $A$ is a circulant $(1, -1)$ matrix of order $v$ with $+1$ appearing $k$ times in the top row and $-1$ appearing $v - k$ times, then the set $D = (x_1, x_2, ..., x_k)$ of $k$ residues modulo $v$ that generate $A$ can be reconstructed.

The matrix $A$ is an incidence matrix. The inner product of its $i$th and $j$th rows $(i \neq j)$ may be computed as follows. Put $j - i = r$. Since

$$(h - i) - r = h - j \qquad (h = 0, 1, ..., v - 1),$$

the number of times that $+1$ appears twice in the same column is $\lambda(r)$, the number of times that opposite signs appear is $2(k - \lambda(r))$, and the

number of times that $-1$ appears twice is $v - 2k + \lambda(r)$. The inner product of the $i$th and $j$th rows is therefore $v - 4k + 4\lambda(r)$. It follows that the $(i, j)$ element of $AA^T$ is given by

$$(AA^T)_{ij} = \begin{cases} v & (i = j), \\ v - 4k + 4\lambda(r) & (i \neq j; j - i = r). \end{cases} \tag{2.1}$$

In particular, if $D$ is a $(v, k, \lambda)$ difference set, then $A$ satisfies the familiar incidence equation

$$AA^T = 4(k - \lambda) I + (v - 4k + 4\lambda) J, \tag{2.2}$$

where $J$ is the matrix of order $v$ with every element $+1$.

Supplementary difference sets have been used by Szekeres [5] and Wallis [6] to construct Hadamard matrices and balanced incomplete block designs. Let $D_1, D_2, \ldots, D_n$ be sets of distinct residues modulo $v$ containing $k_1, k_2, \ldots, k_n$ elements, respectively. For each residue $r \not\equiv 0 \pmod{v}$ let $\lambda_i(r)$ denote the number of solution pairs $(x, y)$ of the congruence $x - y \equiv r \pmod{v}$ with $x$ and $y$ in $D_i$. Put

$$\lambda(r) = \lambda_1(r) + \lambda_2(r) + \cdots + \lambda_n(r).$$

If $\lambda(r) = \lambda$ for each $r \not\equiv 0 \pmod{v}$, then the sets $D_1, D_2, \ldots, D_n$ are called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets. For each individual set $D_i$ the inner product of any two row vectors of the corresponding incidence matrix $A_i$ may be computed by means of formula (2.1). In this manner an extension of the incidence equation (2.2) may be derived. The result is stated in the following theorem.

THEOREM 1. *Let $A_1, A_2, \ldots, A_n$ be the circulant $(1, -1)$ matrices of $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets $D_1, D_2, \ldots, D_n$. Then we have*

$$\sum_{i=1}^{n} A_i A_i^T = 4\left(\sum_{i=1}^{n} k_i - \lambda\right) I + \left(nv - 4\sum_{i=1}^{n} k_i + 4\lambda\right) J.$$

We shall require the following corollary of Theorem 1.

COROLLARY. *The circulant incidence matrices $B_i (i = 1, 2, 3, 4)$ of*

$$4 - \left\{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i - v - 1\right\}$$

*supplementary difference sets satisfy the incidence equation*

$$\sum_{i=1}^{4} B_i B_i^T = 4(v + 1) I - 4J.$$

Supplementary difference sets defined over an Abelian group are treated in [6]. For an extension of Theorem 1 and its corollary from the cyclic case to the Abelian case, see [7, Lemma 9, Corollary 10].

## 3. Hadamard Matrices of Goethals–Seidel Type

A circulant matrix $A = [a_{ij}](i, j = 0, 1,..., v - 1)$ of order $v$ is one in which $a_{ij} = a_{0,j-i}$, where $j - i$ is reduced modulo $v$. A back circulant matrix $A = [a_{ij}](i, j = 0, 1,..., v - 1)$ of order $v$ is one in which $a_{ij} = a_{0,j+i}$, where $j + i$ is reduced modulo $v$. If $A$ and $B$ are two circulant matrices of the same order, then $AB = BA$. If $A$ is circulant and $B$ is back circulant, then $AB = BA^T$.

Let a square matrix $R$ of order $v$ be defined by its only nonzero elements

$$r_{i,v-2-i} = r_{v-1,v-1} = 1 \qquad (i = 0, 1,..., v - 1).$$

Then $R^T = R$ and $R^2 = I$. If $A$ is a circulant matrix of order $v$, then $AR$ and $A^TR$ are back circulants of order $v$. If the numbers $a_0, a_1,..., a_{v-1}$ are the elements in the first row of $A$, then the numbers $a_{v-2}, a_{v-3},..., a_1, a_0, a_{v-1}$ comprise the first row of $AR$, and the numbers $a_2, a_3,..., a_{v-1}, a_0, a_1$ comprise the first row of $A^TR$. Furthermore, since $R$ is itself a back circulant, $AR = RA^T$.

Let $w$ be the column vector of $v$ 1's. Let $X$, $Y$, $Z$, $W$ be the $v \times 4$ matrices defined by

$$X = [w, w, w, w], \qquad Y = [w, w, -w, -w],$$

$$Z = [w, -w, w, -w], \qquad W = [-w, w, w, -w].$$

Let $K$ be the circulant matrix of order 4 whose top row is the vector $[1, -1, -1, -1]$.

Goethals and Seidel [2] have recently demonstrated the existence of skew Hadamard matrices of orders 36 and 52 by means of a new type of construction. The matrix $H$ in the next theorem is an adaptation of the Goethals–Seidel matrix.

Theorem 2. *Let $v$ be an even integer, and put $v = 2t$. Let $A$, $B$, $C$, $D$ be square circulant matrices of order $v$ with elements $\pm 1$. Suppose that the number of 1's in any row of $A$ is $t - 1$, and the number of 1's in any row of $B$, $C$, or $D$ is $t$. If*

$$AA^T + BB^T + CC^T + DD^T = 4(2t + 1) - 4J,$$

*then the matrix*

$$H = \begin{array}{|c|c|c|c|c|} \hline A & BR & CR & DR & X \\ \hline -BR & A & -D^TR & C^TR & Y \\ \hline -CR & D^TR & A & -B^TR & Z \\ \hline -DR & -C^TR & B^TR & A & W \\ \hline -X^T & Y^T & Z^T & W^T & K \\ \hline \end{array}$$

*is an Hadamard matrix of order* $4(2t + 1)$.

By means of a straightforward verification we may show that the inner product of any two distinct rows of $H$ reduces to the zero matrix.

The idea of associating with a circulant matrix $A$ of order $v$ the polynomial

$$\psi(\zeta) = a_0 + a_1\zeta + \cdots + a_{v-1}\zeta^{v-1},$$

where the coefficients $a_0, a_1, \ldots, a_{v-1}$ comprise the first row of $A$ and $\zeta$ is a $v$th root of unity, has been exploited by Williamson [9]. One may also associate with $\psi(\zeta)$ a finite Parseval relation. For example, if the coefficients of $\psi(\zeta)$ are complex numbers, this relation is given for a fixed integer $r$ by

$$\sum_{i=0}^{v-1} a_i\bar{a}_{i+r} = (1/v) \sum_{j=0}^{v-1} |\psi(\zeta^j)|^2 \zeta^{jr},$$

where $\bar{a}_{i+r}$ is the conjugate of $a_{i+r}$ and $\zeta = \exp(2\pi i/v)$. If $A$ is a symmetric matrix, then $a_i = a_{v-i}$ $(i = 0, 1, \ldots, v-1)$. In this case $\psi(\zeta)$ is actually a real number. If the coefficients $a_i$ $(i = 0, 1, \ldots, v-1)$ are also real, then the identity

$$\sum_{i=0}^{v-1} a_i a_{i+r} = (1/v) \sum_{j=0}^{v-1} \psi^2(\zeta^j) \zeta^{jr} \tag{3.1}$$

holds for each integer $r$. Formula (3.1) will be utilized in the next section to compute the inner product of two row vectors of the circulant matrix $A$.

## 4. The Residue Sets $D_1$ and $D_2$

Let $GF(q)$ denote the Galois field of order $q$, where $q$ is an odd prime power. The Legendre symbol $\chi(a)$ in $GF(q)$ is defined as $+1$, $-1$ or $0$ according as $a$ is a nonzero square, a nonsquare, or zero in $GF(q)$. If $w$ is a nonsquare element in $GF(q)$, then the polynomial $P(x) = x^2 - w$ is irreducible in $GF(q)$, and the polynomials $ax + b (a, b \in GF(q))$ modulo $P(x)$ form a finite field $GF(q^2)$ of order $q^2$. The following theorem is proved in [8].

THEOREM 3. *Let $q$ be a prime power $\equiv 1 \pmod 4$ and put $n = (q+1)/2$. Let $\gamma$ be a primitive element of $GF(q^2)$. Put $\gamma^i = ax + b (a, b \in GF(q))$ and define*

$$a_i = \chi(a), \qquad b_i = \chi(b),$$

*where $\chi(a)$ is the Legendre symbol in $GF(q)$. Then the sums*

$$f(\zeta) = \sum_{i=0}^{n-1} a_{4i}\zeta^i, \qquad g(\zeta) = \sum_{i=0}^{n-1} b_{4i}\zeta^i \tag{4.1}$$

*satisfy the identity*

$$f^2(\zeta) + g^2(\zeta) = q, \tag{4.2}$$

*for each $n$-th root of unity $\zeta$ including $\zeta = 1$.*

It is interesting to note that when $q$ is a prime $\equiv 1 \pmod 4$ and $\zeta = 1$, the identity (4.2) reduces to the classical result that every prime $p \equiv 1 \pmod 4$ is representable as the sum of two squares of integers.

We proceed to make the following application of Theorem 3. Put $v = 2n$ so that $v = q + 1$. We construct two polynomials $\psi_1(\zeta)$, $\psi_2(\zeta)$ of degree $v - 1$ as follows:

$$\psi_1(\zeta) = -1 + \sum_{i=1}^{n-1} (-1)^i a_{4i}\zeta^i - \zeta^n + \sum_{i=1}^{n-1} (-1)^{i+1} a_{4i}\zeta^{i+n}, \tag{4.3}$$

$$\psi_2(\zeta) = \sum_{i=0}^{n-1} (-1)^i b_{4i}\zeta^i + \sum_{i=0}^{n-1} (-1)^{i+1} b_{4i}\zeta^{i+n}, \tag{4.4}$$

where $a_{4i}$, $b_{4i}$ are the coefficients appearing in (4.1), and $\zeta$ is a $v$th root of unity. Note that $a_0 = 0$, $b_0 = 1$. Furthermore, exactly $n - 1$ of the coefficients in $\psi_1(\zeta)$ are equal to $+1$, and exactly $n$ of the coefficients in $\psi_2(\zeta)$ are equal to $+1$. The remaining coefficients are equal to $-1$. We

next associate circulant $(1, -1)$ matrices $A$ and $B$ of order $v$ with $\psi_1(\zeta)$ and $\psi_2(\zeta)$, respectively. The elements in the top row of $A$ are the consecutive coefficients of the powers of $\zeta$ in $\psi_1(\zeta)$. The elements in the top row of $B$ are the consecutive coefficients of the powers of $\zeta$ in $\psi_2(\zeta)$. Finally, we construct (see the fourth paragraph in Section 2) two sets of residues

$$D_1 = (x_1, x_2, \ldots, x_{n-1}), \qquad D_2 = (y_1, y_2, \ldots, y_n), \tag{4.5}$$

modulo $v$, that can be used to generate the circulants $A$ and $B$. As in Section 2 let $\lambda_i(r)$ denote for each $r \not\equiv 0 \pmod{v}$ the number of solution pairs $(x, y)$ of the congruence $x - y \equiv r \pmod{v}$ with $x$ and $y$ in $D_i$.

The main result of this section is the following lemma.

LEMMA 2. *For the sets $D_1$ and $D_2$ in* (4.5) *we have*

$$\lambda_1(r) + \lambda_2(r) = \begin{cases} 0 & (r = n), \\ n - 1 & (r \neq n), \end{cases}$$

*with* $1 \leqslant r \leqslant v - 1$.

*Proof.* We return to (4.3) and (4.4). Since $\zeta^v = 1$, we get $\zeta^n = \pm 1$. Clearly, if $\zeta^n = 1$, then $\psi_1(\zeta) = -2$ and $\psi_2(\zeta) = 0$. But if $\zeta^n = -1$, then $\psi_1(\zeta) = 2f(-\zeta)$ and $\psi_2(\zeta) = 2g(-\zeta)$. Note also that $-\zeta$ is an $n$th root of unity when $\zeta^n = -1$. The identity (4.2) is thus transformed into

$$\psi_1^2(\zeta) + \psi_2^2(\zeta) = \begin{cases} 4 & (\zeta^n = 1), \\ 4q & (\zeta^n = -1). \end{cases} \tag{4.6}$$

It is proved in [8, formula (18)] that the coefficients $a_{4i}$, $b_{4i}$ in (4.1) satisfy

$$a_{4i} = a_{4(n-i)}, \; b_{4i} = b_{4(n-i)} \qquad (i = 0, 1, \ldots, n - 1).$$

Consequently the sums $f(\zeta)$ and $g(\zeta)$ are real when $\zeta^n = 1$. It follows that the sums $\psi_1(\zeta)$ and $\psi_2(\zeta)$ are also real when $\zeta^v = 1$.

We are now in the position to apply the finite Parseval relation (3.1) to $\psi_1(\zeta)$ and $\psi_2(\zeta)$. For this purpose it is convenient to write

$$\psi_1(\zeta) = a'_0 + a'_1 \zeta + \cdots + a'_{v-1}\zeta^{v-1}, \tag{4.7}$$

$$\psi_2(\zeta) = b'_0 + b'_1 \zeta + \cdots + b'_{v-1}\zeta^{v-1}, \tag{4.8}$$

where the coefficients in (4.7) and (4.8) are the same as the corresponding coefficients in (4.3) and (4.4), respectively.

If $\zeta = \exp(2\pi i/v)$, then formula (3.1) yields

$$\sum_{i=0}^{v-1} (a_i'a_{i+r}' + b_i'b_{i+r}') = (1/v) \sum_{j=0}^{v-1} (\psi_1^2(\zeta^j) + \psi_2^2(\zeta^j))\, \zeta^{jr} \tag{4.9}$$

for each integer $r$.

In order to evaluate the right member of (4.9) we employ (4.6). Suppose that $1 \leqslant r \leqslant v - 1$. In the last sum we separate the even values of $j$ from the odd. Since $\zeta^n = -1$, the coefficient of $\zeta^{jr}$ reduces to 4 when $j$ is even and to $4q$ when $j$ is odd. For $r = n$ we have $\zeta^{jr} = (-1)^j$, and the right side of (4.9) reduces to $-4(n-1)$. For $r \neq n$ the sum over even values of $j$ reduces to 0 and so does the sum over odd values of $j$. Thus we have established for $1 \leqslant r \leqslant v - 1$ that

$$\sum_{i=0}^{v-1} (a_i'a_{i+r}' + b_i'b_{i+r}') = \begin{cases} -4(n-1) & (r = n), \\ 0 & (r \neq n). \end{cases} \tag{4.10}$$

The sum in the left member of (4.10) is the inner product of two row vectors of the circulant $A$ plus the inner product of the corresponding two row vectors of the circulant $B$. By means of (2.1) this sum may also be expressed as

$$\begin{aligned} &(v - 4(n-1) + 4\lambda_1(r)) + (v - 4n + 4\lambda_2(r)) \\ &\quad = -4(n-1) + 4(\lambda_1(r) + \lambda_2(r)). \end{aligned} \tag{4.11}$$

Comparing (4.10) and (4.11), we obtain the result stated in Lemma 2.

## 5. The Residue Set $D_3$

For a prime $p = 2m + 1$ let $D = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ denote the set of $m$ quadratic residues of $p$ that are between 0 and $p$. For $r \not\equiv 0 \pmod p$ let $\lambda(r)$ denote the number of solution pairs $(x, y)$ of the congruence

$$x - y \equiv r \pmod p \tag{5.1}$$

with $x, y$ in $D$. The number $\lambda(r)$ is evaluated in Lemma 1.

The $p$ residues in the set

$$D_3 = (0, \alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_1 + p, \alpha_2 + p, \ldots, \alpha_m + p) \tag{5.2}$$

are in different residue classes with respect to the modulus $2p$. For $r \not\equiv 0$

(mod $2p$) let $\lambda_3(r)$ denote the number of solution pairs $(z, w)$ of the congruence

$$z - w \equiv r \pmod{2p} \tag{5.3}$$

with $z, w$ in $D_3$.

We shall prove the following lemma.

LEMMA 3. *For the set $D_3$ in* (5.2) *we have*

$$\lambda_3(r) = \begin{cases} p-1 & (r = p), \\ (p-1)/2 & (r \neq p), \end{cases}$$

*with* $1 \leqslant r \leqslant 2p-1$.

*Proof.* The structure of $D_3$ reveals at once that $\lambda_3(p) = p - 1$. Any solution pair $(z, w)$ of the congruence (5.3) is such that $w - z \equiv -r \pmod{2p}$. Thus $\lambda_3(r) = \lambda_3(2p - r)$, and we may suppose in the rest of the proof that $1 \leqslant r \leqslant p - 1$.

We first note that each solution pair $(x, y)$ of the congruence (5.1) produces two solution pairs $(z, w)$ of the congruence (5.3). If $x > y$, the two solutions are given by

$$x - y \equiv r \pmod{2p} \qquad \text{and} \qquad (x + p) - (y + p) \equiv r \pmod{2p}.$$

If $x < y$, the two solutions are given by

$$(x + p) - y \equiv r \pmod{2p} \qquad \text{and} \qquad x - (y + p) \equiv r \pmod{2p}.$$

For each fixed $r$ such that $1 \leqslant r \leqslant p - 1$ we next seek solutions of (5.3) in which either $z = 0$ or $w = 0$. If $p \equiv 3 \pmod 4$, there is exactly one such solution. If $r \in D_3$, this solution is given by $r - 0 \equiv r \pmod{2p}$. If $r \notin D_3$, then $p - r \in D_3$ and the solution is given by $0 - (2p - r) \equiv r \pmod{2p}$. If $p \equiv 1 \pmod 4$ and $r \in D_3$, there are exactly two such solutions. In this case it is also true that $p - r \in D_3$ so that the two solutions are given by $r - 0 \equiv r \pmod{2p}$ and $0 - (2p - r) \equiv r \pmod{2p}$. If $p \equiv 1 \pmod 4$ and $r \notin D_3$, there are no solutions of the type under consideration.

In summary, we have shown the following. If $p \equiv 3 \pmod 4$, then $\lambda_3(r) = 2\lambda(r) + 1$. If $p \equiv 1 \pmod 4$ and $r \in D_3$, then $\lambda_3(r) = 2\lambda(r) + 2$. If $p \equiv 1 \pmod 4$ and $r \notin D_3$, then $\lambda_3(r) = 2\lambda(r)$. Substituting the value of $\lambda(r)$ given in Lemma 1, we find in any event that $\lambda_3(r) = (p - 1)/2$. This completes the proof of Lemma 3.

## 6. The Main Theorems

Let $p$ be an odd prime and $q = 2p - 1$ a prime power. Since $q \equiv 1 \pmod 4$, the hypothesis of Theorem 3 is satisfied. This enables us to apply Lemma 2 with $n = p$ and modulus $v = 2p$. We may also apply Lemma 3 with the same modulus.

The two sets $D_1$ and $D_2$ of Lemma 2 together with the two sets $D_3$ and $D_4$ (with $D_3 = D_4$) of Lemma 3 constitute four supplementary difference sets in which

$$\lambda(r) = \lambda_1(r) + \lambda_2(r) + \lambda_3(r) + \lambda_4(r) = 2(p - 1)$$

for each $r \not\equiv 0 \pmod{2p}$. We have therefore proved the following theorem.

THEOREM 4. *If $p$ is an odd prime and $q = 2p - 1$ is a prime power, then there exist $4 - \{2p; p - 1, p, p, p; 2(p - 1)\}$ supplementary difference sets.*

By the corollary of Theorem 1 the circulant incidence matrices $A$, $B$, $C$, $D$ of the four supplementary difference sets $D_1, D_2, D_3, D_4$ of Theorem 4 satisfy the incidence equation

$$AA^T + BB^T + CC^T + DD^T = 4(2p + 1) - 4J.$$

Hence Theorem 2 yields the main theorem of this paper

THEOREM 5. *If $p$ is a prime and $q = 2p - 1$ is a prime power, then there exists an Hadamard matrix of order $4(2p + 1)$.*

## Acknowledgment

The author wishes to thank Dr. Howard C. Rumsey, Jr., and Dr. Leonard D. Baumert for providing him with some of the ideas used in the present paper. He is especially grateful to Dr. Rumsey for conducting the preliminary computer search for supplementary difference sets.

## References

1. L. D. Baumert and M. Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169–170.
2. J. M. Goethals and J. J. Seidel, A skew Hadamard matrix of order 36, *J. Austral. Math. Soc.* **11** (1970), 343–344.
3. M. Hall, Jr., "Combinatorial Theory," Blaisdell, Waltham, Mass., 1967.
4. T. Storer, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.

5. G. SZEKERES, Tournaments and Hadamard matrices, *Enseignement Math.* **15** (1969), 269–278.
6. J. WALLIS, On supplementary difference sets, *Aequationes Math.* **8** (1972), 242–257.
7. J. WALLIS AND A. L. WHITEMAN, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.* **7** (1972), 233–249.
8. A. L. WHITEMAN, An infinite family of Hadamard matrices of Williamson type, *J. Combinatorial Theory* **14** (1973), 334–340.
9. J. WILLIAMSON, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65–81.