1988

# New Hadamard matrices and conference matrices obtained via Mathon's construction

Jennifer Seberry
*University of Wollongong*, jennie@uow.edu.au

Albert L. Whiteman

# New Hadamard matrices and conference matrices obtained via Mathon's construction


## Abstract

We give a formulation, via (1, - 1) matrices, of Mathon's construction for conference matrices and derive a new family of conference matrices of order $5 \cdot 9^{2r+1} + 1$, $t \geq 0$. This family produces a new conference matrix of order 3646 and a new Hadamard matrix of order 7292. In addition we construct new families of Hadamard matrices of orders $6.9^{2r+1} + 2$, $10.9^{2t+1} + 2$, $8 \cdot 49 \cdot 9^{2}$, $t \geq 0$; $q2(q + 3) + 2$ where $q \equiv 3 \pmod 4$ is a prime power and $1/2(q + 5)$ is the order of a skew-Hadamard matrix); $(q + 1)q^{2}.9t$, $t \geq o$ (where $q \equiv 7 \pmod 8$is a prime power and $1/2(q + 1)$ is the order of an Hadamard matrix). We also give new constructions for Hadamard matrices of order $4 \cdot 9' \geq 0$ and $(q + l)q^{2}$ (where $q \equiv 3 \pmod 4$ is a prime power).



## Disciplines

Physical Sciences and Mathematics

## Publication Details

Seberry, J and Whiteman, AL, New Hadamard matrices and conference matrices obtained via Mathon's construction, Graphs and Combinatorics, 4, 1988, 355-377.

Graphs and Combinatorics 4, 355–377 (1988)

Graphs and Combinatorics



# New Hadamard Matrices and Conference Matrices Obtained via Mathon's Construction

Jennifer Seberry[1]* and Albert Leon Whiteman[2]

[1] Department of Computer Science, University College, UNSW, ADFA, Canberra, 2600 Australia

[2] Department of Mathematics, University of Southern California, Los Angeles, CA 90089, USA

*Dedicated to the memory of our esteemed friend Ernst Straus.*

**Abstract.** We give a formulation, via $(1, -1)$ matrices, of Mathon's construction for conference matrices and derive a new family of conference matrices of order $5 \cdot 9^{2t+1} + 1$, $t \geq 0$. This family produces a new conference matrix of order 3646 and a new Hadamard matrix of order 7292. In addition we construct new families of Hadamard matrices of orders $6 \cdot 9^{2t+1} + 2$, $10 \cdot 9^{2t+1} + 2$, $8 \cdot 49 \cdot 9^t$, $t \geq 0$; $q^2(q+3) + 2$ where $q \equiv 3 \pmod 4$ is a prime power and $\frac{1}{2}(q+5)$ is the order of a skew-Hadamard matrix; $(q+1)q^2 \cdot 9^t$, $t \geq 0$ (where $q \equiv 7 \pmod 8$ is a prime power and $\frac{1}{2}(q+1)$ is the order of an Hadamard matrix). We also give new constructions for Hadamard matrices of order $4 \cdot 9^t \geq 0$ and $(q+1)q^2$ (where $q \equiv 3 \pmod 4$ is a prime power).

## 1. Introduction and Some Preliminary Results

For the definitions of *Hadamard matrices, skew-Hadamard matrices, conference matrices, type* 1 and *type* 2 matrices the reader is referred to Wallis (=Seberry) [9].

The theorem of Mathon [3, p. 323] states that there are symmetric conference matrices of order $(q+2)q^2 + 1$ when $q = 4t - 1$ is a prime power and $q + 3$ is the order of a conference matrix. In this paper we study Mathon's construction giving the matrices he uses an alternative formulation directly as $(1, -1)$ matrices. These matrices are then generalized and used to find new constructions for Hadamard matrices and conference matrices. In a paper under preparation we develop a theorem of Mathon's type when $q = 4t + 1$ is a prime power. The ramifications of this construction are also explored.

Throughout this paper we have retained the concepts of Mathon, using both $B_i$ and $B_i^t$, to emphasize our dependence on Mathon's ideas: then $B_i^t$ could be replaced by $B_{n-i}$ just as easily, although $C$ and $C^t$, an ingenious construction of Mathon, would need to be retained.

Let $q = p^r$ be an odd prime power. Let $GF(q)$ be the finite field of $q$ elements. If $r = 1$ the elements of the field may be selected as the complete residue system 0,

* This work was supported by grants from ARGS and ACRB.

$1, \ldots, p-1$. Let $\chi(x)$ be the quadratic character defined on GF$(q)$, where $\chi(0) = 0$, $\chi(x) = 1$ if $x$ is a square and $\chi(x) = -1$ if $x$ is not a square.

Assume now that $n$ is a prime. For $i, j = 0, 1, \ldots, n-1$ we define the shift matrix $T$ and the back-shift matrix $R$ by

$$T = (t_{ij}) \quad \text{where} \quad t_{ij} = \begin{cases} 1 & \text{if } j - i \equiv 1 \pmod{n} \\ 0 & \text{otherwise,} \end{cases} \tag{1.1}$$

$$R = (r_{ij}) \quad \text{where} \quad r_{ij} = \begin{cases} 1 & \text{if } j + i \equiv 1 \pmod{n} \\ 0 & \text{othewise.} \end{cases} \tag{1.2}$$

For $k = 0, 1, \ldots, n-1$ we have

$$T^k = (t_{ij}^{(k)}) \quad \text{where} \quad t_{ij}^{(k)} = \begin{cases} 1 & \text{if } j - i \equiv k \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

The matrices $T$ and $R$ have the following useful properties:

$$\begin{aligned} &T^n = I, \qquad (T^k)^t = T^{n-k}, \qquad I + T + T^2 + \cdots + T^{n-1} = J, \\ &R^2 = I, \qquad RT^k = R^t T^k = T^{n-k} R, \qquad JT^k = JR^k = J. \end{aligned} \tag{1.3}$$

Here $A^t$ denotes the transpose of a matrix $A$. The matrix $J$ is the matrix of 1's of order $n$, and $I$ is the identity matrix of order $n$.

If $n$ is a prime power let $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ denote the elements of GF$(n)$ numbered so that $\gamma_0 = 0, \gamma_1 = 1, \gamma_{n-i} = -\gamma_i \, (i = 0, 1, \ldots, n-1)$. For $i, j, k = 0, 1, \ldots, n-1$ we define the type 1 shift matrix $T$ and the type 2 back-shift matrix $R$ by

$$T_k = T(\gamma_k) = (t_{ij}^{(k)}) \quad \text{where} \quad t_{ij}^{(k)} = \begin{cases} 1 & \text{if } \gamma_j - \gamma_i = \gamma_k \\ 0 & \text{otherwise,} \end{cases} \tag{1.11}$$

$$R = (r_{ij}) \qquad \text{where} \quad r_{ij} = \begin{cases} 1 & \text{if } \gamma_j + \gamma_i = \gamma_0, \\ 0 & \text{othewise.} \end{cases} \tag{1.21}$$

The matrices $T(\gamma_k)$ have the following properties:

(i) $T(\gamma_k)$ are permutation matrices with $T(\gamma_0) = \mathrm{I}$.

(ii) If $k \neq l$ and $t_{ij}^{(k)} = 1$ then $t_{ij}^{(l)} = 0$. Consequently

$$T(\gamma_0) + T(\gamma_1) + \cdots + T(\gamma_{n-1}) = J.$$

(iii)
$$(T(\gamma_k))^t = T(\gamma_{n-k}). \tag{1.31}$$

(iv) The matrices $T(\gamma_k)$ form an abelian group under multiplication:

$$T(\gamma_k)T(\gamma_l) = T(\gamma_m), \qquad \gamma_k + \gamma_l = \gamma_m.$$

To prove (iv) we note that the product $P = T(\gamma_k)T(\gamma_l)$ of two permutation matrices is itself a permutation matrix. Put $P = (p_{ij}) \, (i, j = 0, 1, \ldots, n-1)$. Then

$$p_{ij} = \sum_{s=0}^{n-1} t_{is}^{(k)} t_{sj}^{(l)} = \begin{cases} 1 & \text{if } t_{is}^{(k)} = t_{sj}^{(l)} = 1 \quad \text{for some } s, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $p_{ij} = 1$. From (1.11) we have $\gamma_s - \gamma_i = \gamma_k$, $\gamma_j - \gamma_s = \gamma_l$ so that $\gamma_j - \gamma_i = \gamma_k + \gamma_l = \gamma_m$. Thus $p_{ij} = t_{ij}$.

The matrices $T(\gamma_k)$ and $R$ are both defined over the field GF($n$) in which the ordering of the elements has been fixed. $T(\gamma_k)$ is a type 1 matrix and $R$ is a type 2 matrix. Therefore

$$RT(\gamma_k) = (T(\gamma_k))^t R^t = T(\gamma_{n-k})R \tag{1.32}$$

by [2, Corollary 4.19].

Now let $X = (x_{ij})$ $(i,j = 0, 1, \ldots, n-1)$ be a matrix of order $n$. If $n$ is a prime, then

$$(T^k X)_{ij} = x_{i+k,j}$$

and

$$(XT^{-k})_{ij} = x_{i,j+k},$$

where the subscripts $i + k$ and $j + k$ are reduced modulo $n$ whenever necessary. Thus we get

$$(T^k X T^{-k})_{ij} = x_{i+k,j+k}$$

and

$$\left(\sum_{k=0}^{n-1} T^k X T^{-k}\right)_{ij} = \sum_{k=0}^{n-1} x_{i+k,j+k}. \tag{1.4}$$

Similarly if $n$ is a prime power, then

$$(T(\gamma_k)X)_{ij} = x_{uj}, \qquad \gamma_u = \gamma_i + \gamma_k, \qquad u = 0, 1, \ldots, n-1$$

and

$$(XT(\gamma_{n-k}))_{ij} = x_{iv}, \qquad \gamma_v = \gamma_j + \gamma_k, \qquad v = 0, 1, \ldots, n-1.$$

Consequently

$$(T(\gamma_k)XT(\gamma_{n-k}))_{ij} = x_{uv}, \qquad \gamma_u = \gamma_i + \gamma_k, \quad \gamma_v = \gamma_j + \gamma_k$$

and

$$\left(\sum_{k=0}^{n-1} T(\gamma_k)XT(\gamma_{n-k})\right)_{ij} = \sum_{k=0}^{n-1} x_{uv}. \tag{1.41}$$

We note that when $k$ runs over the integers $0, 1, \ldots, n-1$ so do $u$ and $v$ in some order. In particular, if $k = n - i$ then $u = 0$ and $\gamma_v = \gamma_j - \gamma_i$; if $k = n - j$, then $v = 0$ and $\gamma_u = \gamma_i - \gamma_j$.

We use a standard procedure introduced by Scarpis and Paley (as described in Wallis [9, p. 291]) to construct the core of a skew-Hadamard matrix. Let $n = q$ be a prime power. Let the order of the elements $\gamma_0, \gamma_1, \ldots, \gamma_{q-1}$ of GF($q$) be fixed as in the constructions of $T(\gamma_k)$ and $R$ in (1.11) and (1.21). Define the matrix

$$W = (w_{ij}) \qquad (i,j = 0, 1, \ldots, q-1)$$

of order $q$, where

$$w_{ij} = \chi(\gamma_j - \gamma_i) \qquad (i,j = 0,1,\ldots,q-1)$$

and $\chi$ is the quadratic character defined over GF($q$). Then $W$ is a circulant matrix when $q$ is a prime and a type 1 matrix when $q$ is a prime power. In either case $W$ is symmetric for $q \equiv 1 \pmod 4$ and skew-symmetric for $q \equiv 3 \pmod 4$.

Henceforth let $n = q \equiv 3 \pmod 4$ be a prime or prime power. Let $e = e_n = (1,1,\ldots,1)$ be a vector of $n$ 1's. Then the matrix

$$S = \begin{pmatrix} 0 & e \\ -e^t & W \end{pmatrix}$$

is a skew-conference matrix of order $n+1$, and $S + I_{n+1}$ is a skew-Hadamard matrix of order $n+1$. Moreover $W$ is the core of $S$. The matrices $S$ and $W$ satisfy the relations

$$\begin{gathered} S^t = -S, \qquad SS^t = nI_{n+1} \\ W^t = -W, \qquad WW^t = nI_n - J_n, \qquad WJ = 0. \end{gathered} \tag{1.5}$$

The matrices $W$ and $T(\gamma_k)$ are both type 1 matrices over GF($q$) and $R$ is a type 2 matrix. Therefore

$$\begin{gathered} WT(\gamma_k) = T(\gamma_k)W, \\ WR = R^tW^t = RW^t = -RW, \end{gathered} \tag{1.51}$$

by [2, Corollary 4.19].

Next define the matrix

$$M = I + W$$

with top row $(b_0, b_1, \ldots, b_{n-1})$ so that $b_0 = 1, b_i = \chi(\gamma_i)(i = 1,2,\ldots,n-1)$. Then (1.5) implies

$$MM^t = (n+1)I - J, \qquad MJ = M^2J = J. \tag{1.6}$$

Finally define the matrix

$$N = e^t(b_0, b_1, \ldots, b_{n-1}).$$

The matrix $N$ is of order $n$ and each of its rows is the same as the top row of $M$. It follows from (1.6) that

$$NT_kN^t = \begin{cases} nJ & \text{for } k = 0, \\ -J & \text{for } 1 \le k \le n-1. \end{cases} \tag{1.7}$$

The following additional properties of the matrices $M$ and $N$ are useful:

$$\begin{gathered} MN^t = (n+1)E - J, \qquad NJ = J, \qquad JN = nN, \\ WN = 0, \qquad MN = T^kN = R^kN = N. \end{gathered} \tag{1.8}$$

Here the matrix $E$ is the matrix of order $n$ with top row ones and zeros elsewhere.

## 2. Matrices for Mathon's Construction

We shall establish the existence of $n+2$ $(1,-1)$ matrices $A+I, B_i (i=1,2,\ldots,n-1)$, $C$ and $C^t$ of order $n^2$ which satisfy the relations

$$
\begin{aligned}
&\text{(i)} && A = A^t,\ AA^t = n^2 I - J, && \\
&\text{(ii)} && AB_i = -B_i A, && (i = 1,2,\ldots,n-1) \\
&\text{(iii)} && AC = -CA, && \\
&\text{(iv)} && AJ = 0,\ B_i J = CJ = nJ, && (i = 1,2,\ldots,n-1) \\
&\text{(v)} && B_i B_j = B_j B_i = J, && (i,j = 1,2,\ldots,n-1;\ i+j \neq n) \\
&\text{(vi)} && B_i B_j^t = B_j^t B_i = J, && (i,j = 1,2,\ldots,n-1;\ i \neq j) \\
&\text{(vii)} && B_i B_i^t = B_{n-i}^t B_{n-i}, && (i = 1,2,\ldots,n-1) \\
&\text{(viii)} && B_i C = CB_i = B_i^t C = CB_i^t = J, && (i = 1,2,\ldots,n-1) \\
&\text{(ix)} && C^2 = J,\ CC^t = n(n+1)I \times J - nJ \times J,\ C^t C = nJ \times ((n+1)I - J) && \\
&\text{(x)} && \sum_{i=1}^{(r-1)/2} (B_i B_i^t + B_i^t B_i) + CC^t + C^t C = n^2(r+1)I. &&
\end{aligned}
\tag{2.1}
$$

The integer $r$ in (x) is a parameter whose value in the present section is specified in Theorem 1.

The matrices $A$, $B_i$, $C$ are defined as follows:

$$A = W \times W + I \times J - J \times I. \tag{2.2}$$

For $n$ a prime

$$B_j = \sum_{i=0}^{n-1} RT^i \times MT^{ij} \qquad (j = 1,2,\ldots,n-1), \tag{2.3}$$

$$C = N(I, T, T^2, \ldots, T^{n-1})^t e. \tag{2.4}$$

For $n$ a prime power

$$B_j = \sum_{i=0}^{n-1} RT(\gamma_i) \times MT(\gamma_i \gamma_j) \qquad (j = 1,2,\ldots,n-1), \tag{2.31}$$

$$C = N(I, T_1, T_2, \ldots, T_{n-1})^t e, \qquad T_i = T(\gamma_i). \tag{2.41}$$

We now prove that when $n \equiv 3 \pmod 4$ is a prime or prime power the equations in (2.1) are satisfied with $r = n$. The proofs are carried out for the most part when $n$ is a prime. Parallel proofs can be given when $n$ is a prime power with $T^i$ replaced by $T_i = T(\gamma_i)$.

*Proof of (i).* The $(1,-1)$ matrix $A$ defined in (2.2) was first constructed by Belevitch [1]. The meaning of (i) is that $A$ is the core of a symmetric conference matrix of order $n^2+1$. Details of the proof may be found in Wallis [9, p. 309].

*Proof of (ii).* From definitions (2.2), (2.3) we have

$$AB_j = (W \times W + I \times J - J \times I) \sum_{i=0}^{n-1} RT^i \times MT^{ij}$$

$$= \sum_{i=0}^{n-1} WRT^i \times WMT^{ij} + \sum_{i=0}^{n-1} (RT^i \times J - J \times MT^{ij}) \qquad \text{(by (1.6))}$$

$$= \sum_{i=0}^{n-1} WRT^i \times WMT^{ij}. \qquad \text{(by (1.3))}$$

In a similar manner we obtain

$$B_jA = \sum_{i=0}^{n-1} RT^iW \times MT^{ij}W.$$

Therefore

$$AB_j + B_jA = (WRT^i + RWT^i) \times \sum_{i=0}^{n-1} WMT^{ij} = 0$$

since $WR = -RW$ by (1.51). This completes the proof.

*Proof of (iii).* From (2.2) and (2.4) we get

$$(AC)_{ij} = ((W \times W)C)_{ij} + ((I \times J)C)_{ij} - ((J \times I)C)_{ij}$$

$$= 0 + JNT^i - NJ = -J + nNT^i. \qquad \text{(by (1.8))}$$

$$(CA)_{ij} = (C(W \times W)_{ij} + (C(I \times J))_{ij} - (C(J \times I))_{ij}$$

$$= 0 + NT^iJ - nNT^i = J - nNT^i. \qquad \text{(by (1.8))}$$

This establishes the formula $AC + CA = 0$.

*Proof of (iv).* The definition of $A$ in (2.2) reveals that the sum of the elements in each row of $A$ is 0. Therefore $AJ = 0$. The definitions (2.3) and (2.4) reveal that the sum of the elements in each row of $B_i$ and in each row of $C$ is $n$. Therefore $B_iJ = CJ = nJ$.

*Proof of (v).* For $j + k \neq n$ we have

$$B_jB_k = \sum_{i=0}^{n-1} \sum_{h=0}^{n-1} RT^iRT^h \times MT^{ij}MT^{hk} \qquad \text{(by (2.3))}$$

$$= \sum_{h=0}^{n-1} \sum_{i=0}^{n-1} T^{n+h-i} \times M^2T^{ij+hk} \qquad \text{(by (1.3))}$$

$$= \sum_{g=0}^{n-1} \sum_{i=0}^{n-1} T^g \times M^2T^{i(j+k)+gk} \qquad (g = h - i)$$

$$= \sum_{g=0}^{n-1} T^g \times M^2J \qquad \text{(by (1.3))}$$

$$= J \times J.$$

The proof of (v) is thus complete. This result includes the corollary

$$B_i^2 = J, \qquad (i = 1, 2, \ldots, n-1).$$

*Proof of (vi).* For $j \neq k$ we have

$$B_jB_k^t = \sum_{i=0}^{n-1}\sum_{h=0}^{n-1} RT^i(RT^h)^t \times MT^{ij}(MT^{hk})^t \qquad \text{(by (2.3))}$$

$$= \sum_{i=0}^{n-1}\sum_{h=0}^{n-1} T^{h-i} \times MM^tT^{ij-hk} \qquad \text{(by (1.3))}$$

$$= \sum_{g=0}^{n-1}\sum_{i=0}^{n-1} T^g \times MM^tT^{i(j-k)-gk} \qquad (g = h - i)$$

$$= \sum_{g=0}^{n-1} T^g \times J \qquad \text{(by (1.6))}$$

$$= J \times J \qquad \text{(by (1.3))}$$

The result for $B_k^tB_j$ is obtained in a similar manner. This completes the proof of (vi).

*Proof of (vii).* In the proof of (vi) assume that $j = k$. Then we get

$$B_jB_j^t = n\sum_{g=0}^{n-1} T^g \times MM^tT^{-gj}. \qquad (2.5)$$

**Similarly we have**

$$B_j^tB_j = n\sum_{g=0}^{n-1} T^g \times MM^tT^{gj}.$$

Thus $B_jB_j^t = B_{n-j}^tB_{n-j}$ and the proof is complete.

*Proof of (viii).* From (2.3) and (2.4) we obtain

$$(B_kC)_{ij} = M\sum_{h=0}^{n-1} T^{(i+h)k}NT^h = MN\sum_{h=0}^{n-1} T^h \qquad \text{(by (1.8))}$$

$$= MNJ = MJ = J. \qquad \text{(by (1.3), (1.6))}$$

$$(CB_k)_{ij} = NT^iM\sum_{h=0}^{n-1} T^{hk} = NT^iMJ \qquad \text{(by (1.3))}$$

$$= NT^iJ = NJ = J. \qquad \text{(by (1.6), (1.8))}$$

The results for $B_k^tC$ and $CB_k^t$ are derived in a similar manner.

*Proof of (ix).* First we prove that $C^2 = J \times J$. This follows from

$$(C^2)_{ij} = NT^iN\sum_{i=0}^{n-1} T^i = NNJ = NJ = J,$$

where we have used (2.4), (1.3) and (1.8).

Next we deduce from (1.7) that

$$(CC^t)_{ij} = nNT^iT^{n-j}N^t = nNT^{i-j}N^t = \begin{cases} n^2J & \text{if } i = j, \\ -nJ & \text{if } i \neq j \end{cases}$$

which is equivalent to

$$CC^t = n(n+1)I \times J - nJ \times J.$$

The evaluation of $C^tC$ is more difficult. When $n$ is a prime we use (1.3) and get

$$C^tC = J \times \sum_{k=0}^{n-1} (NT^k)^t(NT^k) = J \times \sum_{k=0}^{n-1} T^{-k}(N^tN)T^k$$
$$= J \times \sum_{k=0}^{n-1} T^k(N^tN)T^{-k}.$$

Since each row of the matrix $N$ is the vector $(b_0, b_1, \ldots, b_{n-1})$, where $b_0 = 1$ and $b_i = \chi(i)\,(i = 1, 2, \ldots, n-1)$ it follows that

$$(N^tN)_{ij} = nb_ib_j \qquad (i,j = 0, 1, \ldots, n-1).$$

Hence (1.4) yields

$$\left(\sum_{k=0}^{n-1} T^k(N^tN)T^{-k}\right)_{ij} = n\sum_{k=0}^{n-1} b_{i+k}b_{j+k}. \tag{2.6}$$

If $i = j$ then the right member of (2.6) reduces to $n^2$ since $b_{i+k}b_{j+k} = 1$ for each $k$ from 0 to $n-1$. If $i \neq j$ then the right member of (2.6) becomes

$$n(b_0b_{j-i} + b_{i-j}b_0) + n\sum_{k=0}^{n-1} \chi(i+k)\chi(j+k) = -n$$

in view of a lemma of Jacobsthal [9, p. 9, Lemma 5]. Therefore

$$\sum_{k=0}^{n-1} T^k(N^tN)T^{-k} = nMM^t = n(n+1)I - nJ,$$

where we have used (1.6). This establishes the formula

$$C^tC = nJ \times ((n+1)I - J)$$

when $n$ is a prime.

Since the extension of the preceding argument to the prime power case is not straight forward we now turn to the consideration of this case. From the definition of $C$ in (2.4) and the properties of $T(\gamma_k)$ in (1.31) we get

$$C^tC = J \times \sum_{k=0}^{n-1} (NT(\gamma_k))^t(NT(\gamma_k)) = J \times \sum_{k=0}^{n-1} T(\gamma_{n-k})N^tNT(\gamma_k)$$
$$= J \times \sum_{k=0}^{n-1} T(\gamma_k)(N^tN)T(\gamma_{n-k}).$$

Since each row of the matrix $N$ is the vector $(b_0, b_1, \ldots, b_{n-1})$ where $b_0 = 1$ and $b_i = \chi(\gamma_i)\,(i = 1, 2, \ldots, n-1)$ it follows that

$$(N^tN)_{ij} = nb_ib_j \qquad (i,j = 0, 1, \ldots, n-1).$$

Hence (1.41) yields

$$\left(\sum_{k=0}^{n-1} T(\gamma_k)(N^tN)T(\gamma_{n-k})\right)_{ij} = n\sum_{k=0}^{n-1} b_ub_v, \tag{2.61}$$

where for each $k$ the values of $u$ and $v$ are uniquely determined from the relations $\gamma_u = \gamma_i + \gamma_k$ and $\gamma_v = \gamma_j + \gamma_k$. If $i = j$ then the right member of (2.61) reduces to $n^2$

since $b_u b_v = 1$ for each $k$ from 0 to $n-1$. If $i \neq j$ then $b_u = 1$, $b_v = \chi(\gamma_j - \gamma_i)$ for $k = n - i$, and $b_v = 1$, $b_u = \chi(\gamma_i - \gamma_j)$ for $k = n - j$. The right member of (2.61) now becomes

$$n(\chi(\gamma_j - \gamma_i) + \chi(\gamma_i - \gamma_j)) + n \sum_{k=0}^{n-1} \chi(\gamma_i + \gamma_k)\chi(\gamma_j + \gamma_k) = -n$$

in view of the lemma of Jacobsthal [9, p. 9 Lemma 5]. The rest of the proof proceeds as before.

*Proof of (x).* We now establish the validity of (x) with $r = n$. We have

$$\sum_{i=1}^{(n-1)/2} (B_i B_i^t + B_i^t B_i) = \sum_{j=1}^{n-1} B_j B_j^t \qquad \text{(by (vii))}$$

$$= n \sum_{g=0}^{n-1} \sum_{j=1}^{n-1} T^g \times MM^t T^{-gj} \qquad \text{(by (2.5))}$$

$$= n\left( I \times (n-1)MM^t + \sum_{g=1}^{n-1} T^g \times MM^t(J - I) \right) \qquad \text{(by (1.3))}$$

$$= I \times n(n-1)MM^t + (J - I) \times nMM^t(J - I) \qquad \text{(by (1.3))}$$

$$= (I \times MM^t)(n^2 I \times I - nI \times J - nJ \times I + n(J \times J))$$

$$= n^2(n+1)I \times I - n(n+1)J \times I - n(n+1)I \times J + 2nJ \times J. \qquad \text{(by (1.6))}$$

Combining this with the sum of $CC^t + C^tC$ in (ix) we get

$$\sum_{i=1}^{(n-1)/2} (B_i B_i^t + B_i^t B_i) + CC^t + C^tC = n^2(n+1)I,$$

and this is equation (x) with $r = n$.

The results of this section may be summarized in the following theorem:

**Theorem 1.** *Let $n \equiv 3 \pmod 4$ be a prime power. Then there exist matrices of order $n^2$ satisfying equations (2.1) with $r = n$.*

*Remark.* Although we have couched most of the proofs in terms of $T$, the shift matrix, a circulant matrix, the results and proofs we give go straight through with type 1 and type 2 matrices, (see Wallis, [9] for appropriate definitions) as indicated in the case of $n$ a prime power.

It is possible these constructions can be modified to give matrices satisfying (2.1) for other orders (e.g., $2^t - 1$).

*Example 1.* The case $q = 3$.

Mathon's construction makes use of three matrices $A$, $B$, $C$ of order 9.

*Construction of the matrix A.* The matrix $A$ is the core of a symmetric conference matrix of order 10. It may be defined by means of the equation

$$A = W \times W + I \times J + J \times -I,$$

where $W$ is the circulant matrix with first row $[0 + -]$ obtained from the core of a skew-Hadamard matrix of order 4, $I$ is the identity matrix of order 3 and $J$ is the

$3 \times 3$ matrix of ones. We have

$$W^t = -W, \qquad WW^t = 3I - J, \qquad WJ = 0.$$

Note that $A$ is a type 1 matrix defined over GF($3^2$). It is the same matrix $A$ given by Geramita and Seberry [2, p81]. The matrix $A$ can also be written in the form

$$\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$$

where $a, b, c$ are the circulant matrices with first rows

$$[0 + +] \qquad [- + -] \qquad [- - +]$$

respectively. Thus we have

$$c = b^t, \qquad b + c = -2I.$$

*Construction of the matrix B.* The matrix $B$ is

$$\begin{bmatrix} -c & a - I & -b \\ a - I & -b & -c \\ -b & -c & a - I \end{bmatrix}$$

It should be noted that $B$ is a block back circulant matrix whose elements are circulant matrices. Hence $B$ is neither type 1 nor type 2 matrix over GF(9), (Perhaps it should be referred to as a type 3 matrix over GF(9).) but it could still be defined as a group matrix over $Z_3 \times Z_3$.

The matrix $B$ may also be written in the form

$$B = \begin{bmatrix} M & MT & MT^2 \\ MT & MT^2 & M \\ MT^2 & M & MT \end{bmatrix} \quad \text{or} \quad M\begin{bmatrix} I & T & T^2 \\ T & T^2 & I \\ T^2 & I & T \end{bmatrix}$$

where $M = I + W$, $W$ as before, and $T$ is the circulant matrix (shift matrix) with first row $[0 + 0]$. Note that

$$T^2 = T^t, \qquad T^3 = I, \qquad I + T + T^2 = J.$$

*Construction of C.* The matrix $C$ is constructed as follows:

$$\begin{bmatrix} + & + & - & + & + & - & + & + & - \\ + & + & - & + & + & - & + & + & - \\ + & + & - & + & + & - & + & + & - \\ - & + & + & - & + & + & - & + & + \\ - & + & + & - & + & + & - & + & + \\ - & + & + & - & + & + & - & + & + \\ + & - & + & + & - & + & + & - & + \\ + & - & + & + & - & + & + & - & + \\ + & - & + & + & - & + & + & - & + \end{bmatrix}.$$

The construction of the matrix $C$ is an ingenious idea of Mathon. Note that $C$ is *not* composed of circulants or back-circulants.

The matrix $C$ may also be written in the form

$$C = \begin{bmatrix} N & N & N \\ NT & NT & NT \\ NT^2 & NT^2 & NT^2 \end{bmatrix} \quad \text{or} \quad N \begin{bmatrix} I & I & I \\ T & T & T \\ T^2 & T^2 & T^2 \end{bmatrix}$$

where

$$N = \begin{bmatrix} + & + & - \\ + & + & - \\ + & + & - \end{bmatrix}.$$

Note that each row of $N$ is the same as the top row of $M$.

The matrices $A$, $B$, $C$ satisfy equations (2.1) with $r = n = 3$. In this case they are

$$\left.\begin{aligned} &A = A^t, \quad A^2 = 9I - J, \\ &AB = -BA, \quad AC = -CA, \\ &AJ = 0, \quad BJ = CJ = 3J, \\ &B^2 = C^2 = J, \\ &BC = CB = B^tC = CB^t = J \\ &CC^t = 12I \times J - 3J \times J, \quad C^tC = 12J \times I - 3J \times J, \\ &BB^t + B^tB + CC^t + C^tC = 36I. \end{aligned}\right\} \tag{2.7}$$

*Example 2.* The case $q = 7$.

The construction makes use of five matrices $A$, $B_1$, $B_2$, $B_3$, $C$ of order 49.

*Construction of the matrix A.* The matrix $A$ is the core of a symmetric conference matrix of order 50. It may be defined by means of the equation

$$A = W \times W + I \times J + J \times -I,$$

where $W$ is the circulant matrix with first row $[0 + + - + - -]$ obtained from the core of a skew-Hadamard matrix of order 8. We have

$$W^t = -W, \qquad WW^t = 7I - J, \qquad WJ = 0.$$

The matrix $A$ may also be written as a block circulant matrix of circulant matrices. $A$, then, is a circulant matrix with first row $[a\,b\,b\,c\,c\,b\,c\,c]$ where $a, b, c$ are themselves circulant matrices with first rows

$$[0 + + + + + +] \quad [- + + - + - -] \quad [- - - + - + +]$$

respectively. We note that although $A$ has been defined thus it could also have been defined as a type 1 matrix over the group $Z_7 \times Z_7$.

Thus we have

$$c = b^t, \qquad b + c = -2I.$$

*Construction of the matrices* $B_1$, $B_2$, $B_3$. We define $M = I + W$, to be the circulant matrix with first row $[+\ +\ +\ -\ +\ -\ -]$, and $T$ to be the circulant matrix with first row $[0\ +\ 0\ 0\ 0\ 0\ 0]$. Thus $M$ is the core of the skew-Hadamard matrix of order 8 and $T$, the shift matrix, has the properties

$$T^6 = T^t, \qquad T^5 = (T^2)^t, \qquad T^4 = (T^3)^t, \qquad T^7 = I,$$
$$I + T + T^2 + T^3 + T^4 + T^5 + T^6 = J.$$

We now construct the matrices $B_1$, $B_2$, $B_3$ to be block back circulant matrices with first rows

$$B_1 = [M \quad MT \quad MT^2 \quad MT^3 \quad MT^4 \quad MT^5 \quad MT^6]$$
$$B_2 = [M \quad MT^2 \quad MT^4 \quad MT^6 \quad MT \quad MT^3 \quad MT^5]$$
$$B_3 = [M \quad MT^3 \quad MT^6 \quad MT^2 \quad MT^5 \quad MT \quad MT^4]$$

respectively. We note that these matrices, while neither type 1 nor type 2 (as noted before they should be called type 3), they are still group matrices and could be defined on $Z_7 \times Z_7$.

*Construction of C.* The matrix $C$ may be written in the form

$$C = \begin{bmatrix} N & N & N & N & N & N & N \\ NT & NT & NT & NT & NT & NT & NT \\ NT^2 & NT^2 & NT^2 & NT^2 & NT^2 & NT^2 & NT^2 \\ NT^3 & NT^3 & NT^3 & NT^3 & NT^3 & NT^3 & NT^3 \\ NT^4 & NT^4 & NT^4 & NT^4 & NT^4 & NT^4 & NT^4 \\ NT^5 & NT^5 & NT^5 & NT^5 & NT^5 & NT^5 & NT^5 \\ NT^6 & NT^6 & NT^6 & NT^6 & NT^6 & NT^6 & NT^6 \end{bmatrix}$$

where

$$N = \begin{bmatrix} + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \\ + & + & + & - & + & - & - \end{bmatrix}.$$

Note that each row of $N$ is the same as the top row of $M$.

The matrices $A$, $B_1$, $B_2$, $B_3$, $C$ satisfy equations (2.1) with $r = n = 7$. In this case they are

$$\left.\begin{aligned}
&A = A^t, \quad AA^t = 49I - J,\\
&AB_i = -B_iA, && (i = 1,2,3)\\
&AC = -CA,\\
&AJ = 0, \quad B_iJ = CJ = 7J, && (i = 1,2,3)\\
&B_iB_j = B_jB_i = J, && (i,j = 1,2,3)\\
&B_iB_j^t = B_j^tB_i = J, && (i,j = 1,2,3; i \neq j)\\
&B_iC = CB_i = B_i^tC = CB_i^t = J, && (i = 1,2,3)\\
&C^2 = J, \quad CC^t = 56I \times J - 7J \times J, \quad C^tC = 56J \times I - 7J \times J\\
&B_1B_1^t + B_1^tB_1 + B_2B_2^t + B_2^tB_2 + B_3B_3^t + B_3^tB_3 + CC^t + C^tC = 392I.
\end{aligned}\right\} \quad (2.8)$$

## 3. Further Matrices for Mathon's Construction

In this section we construct matrices of order $n^2$ satisfying the equations (2.1) with $r = 3$ and $n = 3^{2t+1}$, $t \geq 0$.

Suppose $B_i$, $C_i$, $B_j$, $C_j$ are square $(1, -1)$ matrices of orders $b_i$, $b_j$ respectively, which satisfy

$$\left.\begin{aligned}
&B_k^2 = C_k^2 = B_kC_k = C_kB_k = B_kC_k^t = C_k^tB_k = J, && k \in \{i,j\}\\
&B_kJ = C_kJ = a_kJ,\\
&B_kB_k^t + B_k^tB_k + C_kC_k^t + C_k^tC_k = 4b_kI_{b_k}.
\end{aligned}\right\} \quad (3.1)$$

Then $B_m$, $C_m$ where

$$B_m = B_i \times \tfrac{1}{2}(B_j + B_j^t) + C_i \times \tfrac{1}{2}(B_j - B_j^t)$$
$$C_m = -B_i \times \tfrac{1}{2}(C_j - C_j^t) + C_i \times \tfrac{1}{2}(C_j + C_j^t)$$

are square $(1, -1)$ matrices of order $b_ib_j = b_m$ satisfying (3.1) where $a_m = a_ia_j$. So we have

**Lemma 2.** *Suppose there exist two pairs of* $(1, -1)$ *matrices of orders* $b_i$, $b_j$ *respectively satisfying* (3.1). *Then there exists a pair of* $(1, -1)$ *matrices of order* $b_ib_j$ *satisfying* (3.1).

**Corollary 3.** *By* (2.7) *matrices satisfying* (3.1) *exist for order* 9. *Hence by Lemma* 2 *such matrices also exist for orders* $9^s$, $s > 1$.

We now show how to adjoin a matrix $A$ to the matrices $B$, $C$ of Corollary 3 so that the requirements (i), (ii) and (iii) of (2.1) are also satisfied.

Suppose $B_1$, $C_1$ are matrices satisfying (3.1) above. We use Lemma 2 an odd number of times to obtain $(1, -1)$ matrices $B_{2t+1}$ and $C_{2t+1}$ of order $9^{2t+1}$, $t \geq 0$ which also satisfy (3.1) observing that as $B_1J = C_1J = 3J$ we have

$$B_{2t+1}J = C_{2t+1}J = 3^{2t+1}J$$

since each iteration of Lemma 2 only leaves one term without a factor $\pm(B_j - B_j^t)$ or $\pm(C_j - C_j^t)$.

Belevitch [1] observed that if $W$ is the core of a conference matrix of order $p+1$ then

$$W_3 = W \times W \times W + I \times J \times W + J \times W \times I + W \times I \times J$$

is the core of a conference matrix of order $p^3 + 1$. This was also observed by Wallis [8] who noted that if $\sum'$ is used to denote the sum of all the cyclic permutations of a Kronecker product being summed so that

$$\sum' I \times J \times W = I \times J \times W + J \times W \times I + W \times I \times J$$

then

$$W_5 = W \times W \times W \times W \times W + \sum' I \times J \times W \times W \times W + \sum' I \times J \times I \times J \times W$$

and

$$W_7 = W \times W \times W \times W \times W \times W \times W + \sum' I \times J \times W \times W \times W \times W \times W + \sum' I \times J \times I \times J \times W \times W \times W + \sum' I \times J \times W \times W \times I \times J \times W + \sum' I \times J \times I \times J \times I \times J \times W$$

are the cores of conference matrices of orders $p^5 + 1$ and $p^7 + 1$ respectively. Turyn [6] further extended this to obtain cores of conference matrices of order $p^{2s+1} + 1$, $s \geq 0$. This ensures that the matrix $A = A_1$ of equations (2.1) can be extended to a matrix of order $9^{2t+1}$ satisfying

$$A_{2t+1} = A_{2t+1}^t, \qquad A_{2t+1}^2 = 9^{2t+1} I - J.$$

It only remains to show that

$$A_{2t+1}B_{2t+1} + B_{2t+1}A_{2t+1} = 0 \quad \text{and} \quad A_{2t+1}C_{2t+1} + C_{2t+1}A_{2t+1} = 0.$$

Since each term of $A_{2t+1}$ contains an odd number of $A_1$'s in its Kronecker product representation the equation $A_1B_1 = -B_1A_1$ will be used an odd number of times while each other factor in a term in $A_{2t+1}B_{2t+1}$ will either be $\pm B_1$, $\pm C_1$, $3J$ (from $J \cdot \frac{1}{2}(B_1 + B_1^t)$ or $J \cdot \frac{1}{2}(C_1 + C_1^t)$) or $0$ (from $J \cdot \frac{1}{2}(B_1 - B_1^t)$ or $J \cdot \frac{1}{2}(C_1 - C_1^t)$). Since $\pm B_1$, $\pm C_1$, $3J$, $0$ will occur in the same positions in $A_{2t+1}B_{2t+1}$ and $B_{2t+1}A_{2t+1}$ the odd number of occurrences of $A_1B_1$ and $B_1A_1$ respectively ensures

$$A_{2t+1}B_{2t+1} + B_{2t+1}A_{2t+1} = 0$$

and similarly

$$A_{2t+1}C_{2t+1} + C_{2t+1}A_{2t+1} = 0.$$

Thus we can say

**Theorem 4.** *Suppose there exist* $(1, -1)$ *matrices* $A + I$, $B$, $C$ *of order* $q^i$ *satisfying, for* $i = 1$

$$\left.\begin{aligned} &A^t = A, \quad AA^t = q^i I - J, \quad AJ = 0 \\ &AB = -BA, \quad AC = -CA \\ &B^2 = C^2 = J, \quad BJ = CJ = k^i J \qquad (k \text{ constant}) \\ &BC = CB = B^tC = CB^t = J \\ &BB^t + B^tB + CC^t + C^tC = 4q^i I. \end{aligned}\right\} \tag{3.2}$$

*Then such matrices also exist of order* $q^{2t+1}$.

**Corollary 5.** *There exist* $(1, -1)$ *matrices* $A + I, B, C$ *of order* $9^{2t+1}$, $t \geq 0$ *satisfying* (3.2).

*Example 3.* Lemma 2 gives the following matrices of order $q^3$ (writing $A, B, C$ for $A_1$, $B_1$, $C_1$).

$$\begin{aligned} B_3 &= B \times \tfrac{1}{2}(B + B^t) \times \tfrac{1}{2}(B + B^t) + C \times \tfrac{1}{2}(B - B^t) \times \tfrac{1}{2}(B + B^t) \\ &\quad - B \times \tfrac{1}{2}(C - C^t) \times \tfrac{1}{2}(B - B^t) + C \times \tfrac{1}{2}(C + C^t) \times \tfrac{1}{2}(C + C^t) \\ C_3 &= -B \times \tfrac{1}{2}(B + B^t) \times \tfrac{1}{2}(C - C^t) - C \times \tfrac{1}{2}(B - B^t) \times \tfrac{1}{2}(C - C^t) \\ &\quad - B \times \tfrac{1}{2}(C - C^t) \times \tfrac{1}{2}(C + C^t) + C \times \tfrac{1}{2}(C + C^t) \times \tfrac{1}{2}(C + C^t) \\ A_3 &= A \times A \times A + A \times I \times J + I \times J \times A + J \times A \times I. \end{aligned}$$

Now $BJ = CJ = 3J$ (see (2.7)) and $AB = -BA$, $AC = -CA$ so

$$\begin{aligned} A_3B_3 &= (A \times A \times A)B_3 + AB \times \tfrac{1}{2}(B + B^t) \times 3J + AC \times \tfrac{1}{2}(B - B^t) \times 3J \\ &\quad + AC \times \tfrac{1}{2}(C + C^t) \times 3J + B \times 3J \times \tfrac{1}{2}A(B + B^t) \\ &\quad + C \times 3J \times \tfrac{1}{2}A(C + C^t) + 3J \times \tfrac{1}{2}A(B + B^t) \times \tfrac{1}{2}(B + B^t) \\ &\quad + 3J \times \tfrac{1}{2}A(B - B^t) \times \tfrac{1}{2}(B + B^t) - 3J \times \tfrac{1}{2}A(C - C^t) \times \tfrac{1}{2}(B - B^t) \\ &\quad + 3J \times \tfrac{1}{2}A(C + C^t) \times \tfrac{1}{2}(C + C^t) \\ &= -B_3A_3. \end{aligned}$$

Similarly for $A_3C_3$. The results for $B_3C_3$, $B^tC_3$, $C_3B_3$, $C_3B_3^t$ follow by similar simple calculation. □

## 4. Mathon's Construction for Conference Matrices

The theorem of Mathon cited in the introduction is an immediate consequence of the following result.

**Theorem 6.** *Suppose there exist* $(1, -1)$ *matrices* $A + I, B_1, \ldots, B_{(n-1)/2}, C$ *of order* $n^2$ *satisfying equations* (2.1) *with* $r = n$. *Further suppose there is a symmetric conference matrix of order* $n + 3$. *Then there exists a conference matrix of order* $n^2(n + 2) + 1$.

*Proof.* Form the circulant matrix $Z$ with first row

$$A, B_1, B_2, \ldots, B_{(n-1)/2}, C, C^t, B^t_{(n-1)/2}, \ldots, B^t_2, B^t_1.$$

Form the symmetric core of order $n+2$ of the given symmetric conference matrix. The inner product of two rows of the core is $-1$. Attach to each off diagonal element in $Z$ the same sign as the corresponding element in the core. Denote the resulting matrix by $V$.

We now prove that the matrix

$$\begin{bmatrix} 0 & e \\ e^t & V \end{bmatrix}$$

is the required conference matrix of order $n^2(n+2)$. Here $e$ is the row vector composed of $n^2(n+2)-1$ ones.

Let $\delta_{ij}$ denote the inner product of the $i$th row of $V$ with the $j$th column of $V^t$. From (i) and (x) of (2.1) we get

$$\delta_{ii} = n^2(n+2)I - J.$$

If $i \neq j$ the contribution to $\delta_{ij}$ from the diagonal elements is of the form $AB_i + B_iA = 0$ or $AC + CA = 0$ in view of (ii) and (iii). The contribution from the off diagonal elements is $-J$ in view of (v), (vi) and (viii). Hence $\delta_{ij} = -J$, $i \neq j$. This proves

$$VV^t = n^2(n+2)I - J \times J.$$

Theorem 6 follows at once. □

*Remark.* In [3] Mathon investigates a method for constructing classes of inequivalent conference matrices by means of skew latin squares. We shall not pursue this subject in the present paper but the reader can see from Example 5 that skew latin squares are implicitly used. It is quite possible that using inequivalent skew latin squares here will lead to inequivalent conference matrices.

*Example 4.* Construction of $C_{46}$ in the case $q = 3$. We first form the matrix $Z$ and the core of the symmetric conference matrix of order 6.

$$Z = \begin{bmatrix} A & B_1 & C & C^t & B_1^t \\ B_1^t & A & B_1 & C & C^t \\ C^t & B_1^t & A & B_1 & C \\ C & C^t & B_1^t & A & B_1 \\ B_1 & C & C^t & B_1^t & A \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{bmatrix}.$$

Hence

$$U = \begin{bmatrix} A & B_1 & -C & -C^t & B_1^t \\ B_1^t & A & B_1 & -C & -C^t \\ -C^t & B_1^t & A & B_1 & -C \\ -C & -C & B_1^t & A & B_1 \\ B_1 & -C & -C^t & B_1^t & A \end{bmatrix}$$

gives the conference matrix of order 46:

$$C_{46} = \begin{bmatrix} 0 & 1 \ldots 1 \\ 1 & \\ \vdots & U \\ 1 & \end{bmatrix}.$$

*Example 5.* Using the core of $C_{10}$ given in Example 1 we have for $q = 7$ that the core, $U$, of the conference matrix of order 442 is

$$\begin{bmatrix} A & B_1 & B_2 & -B_3 & C & -C^t & -B_3^t & -B_2^t & B_1^t \\ B_1^t & A & B_1 & -B_2 & -B_3 & C & C^t & -B_3^t & -B_2^t \\ B_2^t & B_1^t & A & B_1 & -B_2 & -B_3 & -C & C^t & -B_3^t \\ -B_3^t & -B_2^t & B_1^t & A & B_1 & B_2 & -B_3 & C & -C^t \\ C^t & -B_3^t & -B_2^t & B_1^t & A & B_1 & -B_2 & -B_3 & C \\ -C & C^t & -B_3^t & B_2^t & B_1^t & A & B_1 & -B_2 & -B_3 \\ -B_3 & C & -C^t & -B_3^t & -B_2^t & B_1^t & A & B_1 & B_2 \\ -B_2 & -B_3 & C & C^t & -B_3^t & -B_2^t & B_1^t & A & B_1 \\ B_1 & -B_2 & -B_3 & -C & C^t & -B_3^t & B_2^t & B_1^t & A \end{bmatrix}.$$

## 5. A New Family of Conference Matrices

The technique used to prove Mathon's theorem may also be used to construct a new family of conference matrices. This time we utilize Corollary 5 instead of Theorem 1.

**Theorem 7.** *There exist symmetric conference matrices of order* $5 \cdot 9^{2t+1} + 1, t \geq 0$.

*Proof.* Let $A$, $B$, $C$ be the matrices of Corollary 5, and let $e$ be the row vector composed of $9^{2t+1}$ ones. Then

$$\begin{bmatrix} 0 & e & e & e & e & e \\ e & A & B & -C & -C & B \\ e & B & A & B & -C & -C \\ e & -C & B & A & B & -C \\ e & -C & -C & B & A & B \\ e & B & -C & -C & B & A \end{bmatrix}$$

is the required conference matrix of order $5 \cdot 9^{2t+1} + 1, t \geq 0$. □

Theorem 7 implies

**Corollary 8.** *There exist symmetric Hadamard matrices of order* $10 \cdot 9^{2t+1} + 2, t \geq 0$.

*Proof.* Lemma 5.2 of [9] states that the existence of a symmetric conference matrix of order $n$ implies the existence of a symmetric Hadamard matrix of order $2n$. This proves the corollary. □

*Remark.* Theorem 7 produces a new conference matrix of order $3646 = 5 \cdot 9^3 + 1$. Corollary 8 produces a new Hadamard matrix of order $7292 = 10 \cdot 9^3 + 2$.

## 6. A New Construction for Hadamard Matrices

The constructions of this section are variations of the constructions of Section 4.

**Theorem 9.** *Suppose there exist* $r + 2$ matrices $A, B_1, \ldots, B_{(r-1)/2}, B_1^t, \ldots, B_{(r-1)/2}^t, C, C^t$ *of order* $n^2$ *satisfying* (2.1). *If there also exists a skew-Hadamard matrix or a symmetric conference matrix of order*
(i) $\frac{1}{2}(r + 5)$, *then there is an Hadamard matrix of order* $n^2(r + 3) + 2$,
(ii) $r + 3$, *then there is an Hadamard matrix of order* $2n^2(r + 2) + 2$.

*Proof of (i).* Since $\frac{1}{2}(r + 5)$ is even it follows that $r \equiv 3 \pmod 4$. Form two circulant matrices $U$ and $V$ with initial rows

$$A + I, B_1, B_2, \ldots, B_{(r-1)/2}, C \quad \text{and} \quad (-1)^{(r+1)/2}(A - I), C^t, B_{(r-1)/2}^t, \ldots, B_2^t, B_1^t$$

respectively. Also form the core of order $\frac{1}{2}(r + 3)$ of the skew-Hadamard matrix or conference matrix. The inner product of any two rows of this core is of course $-1$. Attach to each off diagonal element in $U$ and $V$ the same sign as the corresponding element in the core. Denote the resulting matrices by $X$ and $Y$ respectively. We now prove that the matrix

$$H = \begin{bmatrix} 1 & 1 & e & e \\ 1 & -1 & -e & e \\ e^t & -e^t & X & Y \\ e^t & e^t & Y & -X \end{bmatrix} \tag{6.1}$$

is the required Hadamard matrix of order $n^2(r + 3) + 2$.

It suffices to establish that

$$XY^t = YX^t, \tag{6.2}$$

and

$$XX^t + YY^t = n^2(r + 3)I + 2I - 2J. \tag{6.3}$$

Equation (6.2) asserts that the inner product $\delta_{ij}$ of the $i$th row of the matrix $[X\ Y]$ with the $j$th column of the matrix $[Y - X]^t$ is equal to 0. We therefore evaluate $\delta_{ij}$. If $i = j$ the contribution to $\delta_{ij}$ from the diagonal element is

$$(A + I)(A - I) - (A - I)(A + I) = 0.$$

The contribution from the off diagonal elements is $\frac{1}{2}(r + 1)J - \frac{1}{2}(r + 1)J = 0$. Thus $\delta_{ii} = 0$. If $i \neq j$ the contribution to a typical $\delta_{ij}$ from the diagonal elements is of the form $(A + I)B_i + B_i(A - I) - (A - I)B_j - B_j(A + I)$. The contribution from the off diagonal elements is $J - J$. Again, $\delta_{ij} = 0$, $i \neq j$. This proves (6.2).

We now prove (6.3). This time let $\delta_{ij}$ denote the inner product of the $i$th row of

the matrix $[X\ Y]$ with the $j$th column of its transpose. By (i) and (x) of (2.1) we have

$$\begin{aligned}\delta_{ii} &= (A+I)^2 + (A-I)^2 + \sum_{i=1}^{(r-1)/2} (B_iB_i^t + B_i^tB_i) + CC^t + C^tC \\ &= 2A^2 + 2I + n^2(r+1)I \\ &= n^2(r+3)I + 2I - 2J.\end{aligned}$$

If $i \neq j$ the contribution to a typical $\delta_{ij}$ from the diagonal elements is of the form $(A+I)B_i + B_i(A-I) + (A-I)B_j + B_j(A+I)$. The contribution from the off diagonal elements is $-J - J$. Thus $\delta_{ij} = -2J$, $i \neq j$. This completes the proof of (6.3).

*Proof of (ii).* This time form two circulant matrices $U$ and $V$ with initial rows

$$A + I, B_1, B_2, \ldots, B_{(r-1)/2}, C, C^t, B_{(r-1)/2}^t, \ldots, B_2^t, B_1^t,$$

and

$$(-1)^{(r+1)/2}(A-I), B_1, B_2, \ldots, B_{(r-1)/2}, C, C^t, B_{(r-1)/2}^t, \ldots, B_2^t, B_1^t,$$

respectively. Also form the core of order $r+2$ of the skew-Hadamard matrix or conference matrix. Attach to each off diagonal element in $U$ and $V$ the same sign as in the corresponding element of the core. Denote the resulting matrices by $X$ and $Y$ respectively.

The rest of the proof consists in showing that a matrix $H$ defined as in (6.1) is the required Hadamard matrix of order $2n^2(r+2)+2$. The argument is similar to that used in the preceding proof. There is no need to include the details here. □

**Corollary 10.** *Let $q \equiv 3 \pmod 4$ be a prime power. Then if there is a skew-Hadamard matrix of order $\frac{1}{2}(q+5)$ there is an Hadamard matrix of order $q^2(q+3)+2$. Further if there is a symmetric conference matrix of order $q+3$ then there is an Hadamard matrix of order $2q^2(q+2)+2$.*

***Proof.*** Use the matrices constructed above satisfying Theorem 1 with $q = r = n$.

□

***Remark.*** The first part of Corollary 10 gives a new construction for the Hadamard matrix of order $27^2 \cdot 30 + 2 = 2^4 \cdot 1367$. Hadamard matrices of order $2^2 \cdot 1367$ and $2^3 \cdot 1367$ are as yet unknown. The matrices of order $2q^2(q+2)+2$ in the second part can also be constructed from the conference matrices of order $q^2(q+2)+1$ found by Mathon.

**Corollary 11.** *Suppose there exist matrices of order $q^i$ satisfying (3.2). Then there are Hadamard matrices of order $6 \cdot q^i + 2$ and $10 \cdot q^i + 2$. In particular there exist Hadamard matrices of order $6 \cdot 9^{2t+1} + 2$ and $10 \cdot 9^{2t+1} + 2$, $t \geq 0$.*

*Proof.* Use the matrices of Corollary 5 with $r = 3$, $n = 3^{2t+1}$, $t \geq 0$.

*Remark.* Corollary 11 gives new constructions for Hadamard, atrices of orders $56 = 6 \cdot 9 + 2$ and $92 = 10 \cdot 9 + 2$. Corollary 8 is included as a special case.

## 7. Another Proof of a Theorem of Seberry

We now utilize Theorem 1 to construct another family of Hadamard matrices. The matrix $A$ of (2.1) is not included in this construction.

**Theorem 12.** *Suppose there exist* $(1, -1)$ *matrices* $B_1, \ldots, B_{(r-1)/2}$, $C$ *of order* $n^2$ *satisfying* (2.1). *Further suppose that there exists an Hadamard matrix of order* $r + 1$. *Then there is an Hadamard matrix of order* $n^2(r + 1)$.

*Proof.* Let $G$ be the Hadamard matrix of order $r + 1$ and $U$ the circulant matrix of order $r + 1$ with first row

$$B_1, B_2, \ldots, B_{(r-1)/2}, C, C^t, B_{(r-1)/2}^t, \ldots, B_2^t, B_1^t.$$

Construct a matrix $H$ by attaching to each element of $U$ the same sign as the corresponding element in $G$. We now show the $H$ is the required Hadamard matrix of order $n^2(r + 1)$. Let $\delta_{ij}$ denote the inner product of the $i$th row of $H$ and the $j$th column of $H^t$. Since any two rows of $G$ are orthogonal it follows from (v), (vi) and (viii) of (2.1) that $\delta_{ij} = 0$, $i \neq j$. Moreover, from (x) of (2.1) we have $\delta_{ii} = n^2(r + 1)I$. This proves that $H$ is an Hadamard matrix of order $n^2(r + 1)$. □

**Corollary 13.** *Let* $q \equiv 3 \pmod 4$ *be a prime power. Then there exists an Hadamard matrix of order* $q^2(q + 1)$.

*Proof.* Use the matrices $B_i$, $B_i^t$, $C$, $C^t$ of Theorem 1 with $q = r = n$.

**Corollary 14.** *There exist Hadamard matrices of order* $4.9^s$, $s \geq 0$.

*Proof.* Use the matrices $B$, $B^t$, $C$, $C^t$ of Corollary 3 with $r = 3$, $n = 3^s$, $s \geq 1$. The required Hadamard matrix is

$$H = \begin{bmatrix} -B & B^t & C & C^t \\ C^t & -B & B^t & C \\ C & C^t & -B & B^t \\ B^t & C & C^t & -B \end{bmatrix}.$$

*Remark.* Corollary 13 is due to Seberry [5]. Corollary 14 is due to A.C. Mukhopadhyay [4] and R.J. Turyn [7]. However, the approach to these corollaries in the present paper is conceptually different.

*Remark.* We also note the following $4.9^s \times (4.9^s + 2)$ $(1, -1)$ matrix $D$ (where $e$ is an $9^s \times 1$ column of ones)

$$D = \begin{bmatrix} e & e & B & B^t & C & C^t \\ e & -e & B^t & B & C^t & -C \\ e & -e & C & C^t & -B & B^t \\ e & e & C^t & C & -B^t & -B \end{bmatrix}$$

which satisfies

$$DD^t = 4.9^s I + 2J. \qquad \square$$

## 8. Another New Construction for Hadamard Matrices

In this section we construct one more family of Hadamard matrices. The method has already been used in Section 3.

Suppose that we have two $(1, -1)$ matrices $B$, $C$ of order $m^2$ satisfying the equations of (2.1) with $r = 3$. Then equation (x) becomes

$$BB^t + B^tB + CC^t + C^tC = 4m^2I. \tag{8.1}$$

In addition suppose that we have four $(1, -1)$ matrices $B_1, B_2, B_3, C_1$ of order $n^2$ satisfying the equations of (2.1) with $r = 7$. Then equation (x) becomes

$$\sum_{i=1}^{3} (B_iB_i^t + B_i^tB_i) + C_1C_1^t + C_1^tC_1 = 8n^2I. \tag{8.2}$$

Define four matrices $E_1, E_2, E_3, E_4$ of order $m^2n^2$ as follows:

$$E_1 = B_1 \times \tfrac{1}{2}(B + B^t) + B_2 \times \tfrac{1}{2}(B - B^t),$$
$$E_2 = B_1 \times \tfrac{1}{2}(C - C^t) + B_2 \times \tfrac{1}{2}(C + C^t),$$
$$E_3 = B_3 \times \tfrac{1}{2}(C + C^t) + C_1 \times \tfrac{1}{2}(C - C^t),$$
$$E_4 = B_3 \times \tfrac{1}{2}(B - B^t) + C_1 \times \tfrac{1}{2}(B + B^t).$$

These matrices satisfy the relations

$$E_iE_j = E_k^2 = J \qquad i, j, k \in \{1, 2, 3, 4\}$$
$$E_1E_4^t = E_4E_1^t, \qquad E_1^tE_4 = E_4^tE_1,$$
$$E_2E_3^t = E_3E_2^t, \qquad E_2^tE_3 = E_3^tE_2,$$
$$E_iE_j^t = E_j^tE_i = J, \qquad (i,j) \neq (1,4) \text{ or } (2,3), \qquad i \neq j,$$
$$\sum_{i=1}^{4} (E_iE_i^t + E_i^tE_i) = 8m^2n^2I.$$

Finally construct the matrices

$$F_1 = \begin{bmatrix} E_1 & E_4 \\ E_4 & -E_1 \end{bmatrix} \qquad F_2 = \begin{bmatrix} E_2 & E_3 \\ E_3 & -E_2 \end{bmatrix}$$

then

$$F_1^2 = F_2^2 = F_1F_2 = F_2F_1 = F_1F_2^t = F_2^tF_1 = I_2 \times 2J,$$
$$F_1F_1^t + F_1^tF_1 + F_2F_2^t + F_2^tF_2 = 8m^2n^2I.$$

A direct verification now shows that

$$H = \begin{bmatrix} -F_1 & F_2 & F_2^t & F_1^t \\ F_1^t & -F_1 & F_2 & F_2^t \\ F_2^t & F_1^t & -F_1 & F_2 \\ F_2 & F_2^t & F_1^t & -F_1 \end{bmatrix}$$

is an Hadamard matrix of order $8m^2n^2$.

This proves

**Theorem 15.** *Suppose that there are two* $(1,-1)$ *matrices* $B, C$ *of order* $m^2$ *and four* $(1,-1)$ *matrices* $B_1, B_2, B_3, C_1$ *of order* $n^2$ *satisfying* (2.1). *Then there exists an Hadamard matrix of order* $8m^2n^2$.

**Corollary 16.** *There exist Hadamard matrices of orders* $8 \cdot 49 \cdot 9^s$, $s \geq 1$.

*Proof.* We use the two matrices of order $9^s$, $s \geq 1$ of Corollary 3 and the four matrices of order 49 of Theorem 1. □

*Remark.* Theorem 15 may easily be generalised. We present the argument briefly. Let two $(1,-1)$ matrices $B, C$ of order $m^2$ be defined as in (8.1). In addition suppose that $B_1, B_2, \ldots, B_{4s-1}, C_1$ are $4s$ $(1,-1)$ matrices of order $n^2$ satisfying (2.1) with $r = 8s-1$. Then equation (x) becomes

$$\sum_{i=1}^{4s} (B_i B_i^t + B_i^t B_i) = 8sn^2 I, \tag{8.21}$$

where we have written $B_{4s}$ in place of $C_1$. The equation (8.21) reduces to (8.2) when $s = 1$.

Define $4s$ $(1,-1)$ matrices of order $m^2n^2$ as follows:

$$\begin{aligned}
E_{4u+1} &= B_{4u+1} \times \tfrac{1}{2}(B + B^t) + B_{4u+2} \times \tfrac{1}{2}(B - B^t),\\
E_{4u+2} &= B_{4u+1} \times \tfrac{1}{2}(C - C^t) + B_{4u+2} \times \tfrac{1}{2}(C + C^t),\\
E_{4u+3} &= B_{4u+3} \times \tfrac{1}{2}(C + C^t) + B_{4u+4} \times \tfrac{1}{2}(C - C^t),\\
E_{4u+4} &= B_{4u+3} \times \tfrac{1}{2}(B - B^t) + B_{4u+4} \times \tfrac{1}{2}(B + B^t),
\end{aligned}$$

where $u = 0, 1, \ldots, s-1$. Then the matrices

$$F_{4u+1} = \begin{array}{|c|c|}\hline E_{4u+1} & E_{4u+4} \\ \hline E_{4u+4} & -E_{4u+1} \\ \hline \end{array}, \quad F_{4u+2} = \begin{array}{|c|c|}\hline E_{4u+2} & E_{4u+3} \\ \hline E_{4u+3} & -E_{4u+2} \\ \hline \end{array}, \quad u = 0, 1, \ldots, s-1,$$

satisfy the relations

$$\begin{aligned}
F_i^2 &= F_i F_j = F_j F_i = I_2 \times 2J,\\
F_i F_j^t &= F_j^t F_i = I_2 \times 2J, \qquad i \neq j,\\
\sum_i (F_i F_i^t + F_i^t F_i) &= 8sm^2 n^2 I,
\end{aligned}$$

where both $i$ and $j$ extend over the values $4u+1$ and $4u+2$, $u = 0, 1, \ldots, s-1$.

Next suppose there is an Hadamard matrix $G$ of orders $4s$. Let $U$ be the circulant matrix of order $4s$ with first row

$$F_1, F_2, F_5, F_6, \ldots, F_{4s-3}, F_{4s-2}, F_{4s-2}^t, F_{4s-3}^t, \ldots, F_6^t, F_5^t, F_2^t, F_1^t.$$

Construct a matrix $H$ by attaching to each element of $U$ the same sign as the corresponding element in $G$. We may now check the row inner products of $H$ and verify that the requirements for an Hadamard matrix of order $8sm^2n^2$ are fulfilled. Thus we obtain

**Theorem 17.** *Suppose there exist two* $(1, -1)$ *matrices* $B, C$ *of order* $m^2$ *and* $4s$ $(1, -1)$ *matrices* $B_1, B_2, \ldots, B_{4s-1}, C_1$ *of order* $n^2$ *satisfying* (2.1). *Suppose also that there exists an Hadamard matrix of order* $4s$. *Then there exists an Hadamard matrix of order* $8sm^2n^2$.

The following corollary is complementary to Corollary 13.

**Corollary 18.** *Let* $q \equiv 7 \pmod 8$ *be a prime power. Then if there is an Hadamard matrix of order* $\frac{1}{2}(q+1)$, *there is also an Hadamard matrix of order* $q^2(q+1)9^s$, $s \geqq 0$.

*Proof.* From Corollary 3 we have two matrices of order $9^s$, $s \geqq 1$ satisfying (3.1). From Theorem 1 with $q = r = n = 8s - 1$ we have $4s = (q+1)/2$ matrices of order $q^2$ satisfying (2.1). Assume that an Hadamard matrix of order $\frac{1}{2}(q+1)$ exists. Then Corollary 18 is an immediate consequence of Theorem 17. □

## References


1. **Belevitch, V.:** Theory of $2n$-terminal networks with applications to conference telephony. **Electr. Commun. 27, 3,** 231–244 (1950)
2. **Geramita, A.V., Seberry,** J.: Orthogonal Designs: quadratic forms and Hadamard matrices, **New York – Basel:** Marcel Dekker 1979
3. **Mathon, R.:** Symmetric conference matrices of order $pq^2 + 1$. Canad. J. Math. **30,** 321–331 (1978)
4. Mukhopadhyay, A.C.: Some infinite classes of Hadamard matrices. J. Comb. Theory (A) **25,** 128–141 (1978)
5. Seberry, J.: Some infinite classes of Hadamard matrices. J. Aust. Math. Soc. (A) **29,** 235–242 (1980)
6. Turyn, R.J.: On $C$-matrices of arbitrary powers. Bull. Canad. Math. Soc. **23,** 531–535 (1971)
7. Turyn, R.J.: A special class of Williamson matrices and difference sets. J. Comb. Theory (A) **36,** 111–115 (1984)
8. Wallis, J.: On integer matrices obeying certain matrix equations. J. Comb. Theory (A) **12,** 112–118 (1972)
9. **Wallis, J.: Hadamard Matrices.** In: Lecture Notes in Mathematics, Vol. 292: Combinatories: **Room Squares, sum-free sets, Hadamard matrices, pp.** 273–490. Berlin: Springer-Verlag 1972


Received: November 20, 1986
Revised: January 12, 1988