University of Wollongong
Research Online

# Some classes of Hadamard matrices with constant diagonal 

Jennifer Seberry<br>University of Wollongong, jennie@uow.edu.au<br>Albert Leon Whiteman

Follow this and additional works at: https://ro.uow.edu.au/infopapers
Part of the Physical Sciences and Mathematics Commons

## Recommended Citation

Seberry, Jennifer and Whiteman, Albert Leon: Some classes of Hadamard matrices with constant diagonal 1972.
https://ro.uow.edu.au/infopapers/942

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

## Some classes of Hadamard matrices with constant diagonal


#### Abstract

The concepts of circulant and back circulant matrices are generalized to obtain incidence matrices of subsets of finite additive abelian groups. These results are then used to show the existence of skewHadamard matrices of order $8(4 f+I)$ when $f$ is odd and $8 f+1$ is a prime power. This shows the existence of skew-Hadamard matrices of orders 296, 592, 1184, 1640, 2280, 2368 which were previously unknown.

\section*{Disciplines}

Physical Sciences and Mathematics

\section*{Publication Details}

Jennifer Seberry Wallis and Albert Leon Whiteman, Some classes of Hadamard matrices with constant diagonal, Bulletin of the Australian Mathematical Society, 7, (1972), 233-249.


# Some classes of Hadamard matrices with constant diagonal 

## Jennifer Wallis and Albert Leon Whiteman

```
The concepts of circulant and backcirculant matrices are generalized to obtain incidence matrices of subsets of finite additive abelian groups. These results are then used to show the existence of skew-Hadamard matrices of order \(8(4 f+1)\) when \(f\) is odd and \(8 f+1\) is a prime power. This shows the existence of skew-Hadamard matrices of orders 296, 592, 1184, 1640, 2280, 2368 which were previously unknown.
A construction is given for regular symmetric Hadamard matrices with constant diagonal of order \(4(2 m+1)^{2}\) when a symmetric conference matrix of order \(4 m+2\) exists and there are Szekeres difference sets, \(X\) and \(Y\), of size \(m\) satisfying \(x \in X \Rightarrow-x \notin X, y \in Y \Rightarrow-y \in Y\).
```

Suppose $V$ is a finite abelian group with $v$ elements, written in additive notation. A difference set $D$ with parameters ( $v, k, \lambda$ ) is a subset of $V$ with $k$ elements and such that in the totality of all the possible differences of elements from $D$ each non-zero element of $V$ occurs $\lambda$ times.

If $V$ is the set of integers modulo $v$ then $D$ is called a cyclic difference set: these are extensively discussed in Baumert [1].

A circulont matrix $B=\left(b_{i j}\right)$ of order $v$ satisfies $b_{i j}=b_{1, j-i+1}$ $(j-i+1$ reduced modulo $v)$, while $B$ is back-circuzont if its elements

[^0]satisfy $b_{i j}=b_{1, i+j-1}(i+j-1$ reduced modulo $v)$.
Throughout the remainder of this paper $I$ will always mean the identity matrix and $J$ the matrix with every element +1 , where the order, unless specifically stated, is determined by the context.

Let $S_{1}, S_{2}, \ldots, S_{n}$ be subsets of $V$, a finite abelian group, $|V|=v$, containing $k_{1}, k_{2}, \ldots, k_{n}$ elements respectively. Write $T_{i}$ for the totality of all differences between elements of $S_{i}$ (with repetitions), and $T$ for the totality of elements of all the $T_{i}$. If $T$ contains each non-zero element of $V$ a fixed number of times, $\lambda$ say, then the sets $S_{1}, S_{2}, \ldots, S_{n}$ will be called $n-\left\{v ; k_{1}, k_{2}, \ldots, k_{n} ; \lambda\right\}$ supplementary difference sets.

The parameters of $n-\left\{v ; k_{1}, k_{2}, \ldots, k_{n} ; \lambda\right\}$ supplementary
difference sets satisfy

$$
\begin{equation*}
\lambda(v-1)=\sum_{i=1}^{n} k_{i}\left(k_{i}-1\right) \tag{I}
\end{equation*}
$$

If $k_{1}=k_{2}=\ldots=k_{n}=k$ we will write $n-\{v ; k ; \lambda\}$ to denote the $n$ supplementary difference sets and (I) becomes

$$
\begin{equation*}
\lambda(v-1)=n k(k-1) \tag{2}
\end{equation*}
$$

See [14] and [15] for more details.
We shall be concerned with collections, (denoted by square brackets
[ ] ) in which repeated elements are counted multiply, rather than with sets (denoted by braces \{ \} ). If $T_{1}$ and $T_{2}$ are two collections then $T_{1} \& T_{2}$ will denote the result of adjoining the elements of $T_{1}$ to $T_{2}$ with total multiplicities retained.

An Hadamard matrix $H$ of order $h$ has every element +1 or -1 and satisfies $H H^{T}=h I_{h}$. A skew-Hadomard matrix $H=I+R$ is an Hadamerd matrix with $R^{T}=-R$. A square matrix $K= \pm I+Q$, where $Q$ has zero diagonal, is skew-type if $Q^{T}=-Q$. Hadamard matrices are not yet known
for the following orders < 500: 188, 236, 268, 292, 356, 376, 404, 412, 428, 436, 472. Skew-Hadamard matrices are as yet unknown for the following orders < 300: 116, 148, $156,172,188,196,232,236,260$, 268, 276, 292 .

An Hadamard matrix satisfying $H J=k_{J} J$ for some integer $k$ is reguzar.

A symmetric conference matrix $C+I$ of order $n \equiv 2(\bmod 4)$ is a
( $1,-1$ ) matrix satisfying

$$
C C^{T}=(n-1) I_{n}, \quad C^{T}=C
$$

By suitably multiplying the rows and columns of $C$ by -1 a matrix
(3)

$$
\left[\begin{array}{cccc}
0 & 1 & \ldots & 1 \\
1 & & & \\
\vdots & & W & \\
1 & & &
\end{array}\right]
$$

may be obtained and $W$ satisfies

$$
W W^{T}=(n-1) I-J, \quad W J=0, \quad W^{T}=W
$$

These matrices are studied in [3], [6], [10], [11], [13].

## 1. Preliminary results

LEMMA 1. If there exist $4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{4} ; \sum_{i=1}^{4} k_{i}-v-1\right\}$
supplementary difference sets then each $k_{i}=m$ or $m-1$ for $v=2 m+1$ and $k_{1}=m \pm 1, k_{2}=k_{3}=k_{4}=m$ for $v=2 m$.

Proof. By (I),

$$
\left(\sum_{i=1}^{4} k_{i}-v-1\right)(v-1)=\sum_{i=1}^{4} k_{i}\left(k_{i}-1\right)
$$

so

$$
4 \sum_{i=1}^{4} k_{i}^{2}-4 v \sum_{i=1}^{4} k_{i}+4\left(v^{2}-1\right)=0
$$

$$
\begin{aligned}
& \sum_{i=1}^{4}\left(2 k_{i}-v\right)^{2}=4 \\
&=\left\{\begin{array}{l}
2^{2}+0+0+0, \\
1^{2}+1^{2}+1^{2}+1^{2}, \\
\text { If } \quad v \text { odd. }
\end{array}\right. \\
& \text { If } v \equiv 0(\bmod 2), \quad k_{1} \doteq \frac{1}{2}(v \pm 2), \quad k_{2}=k_{3}=k_{4}=\frac{1}{2} v, \text { but if }
\end{aligned}
$$

$$
v \equiv 1(\bmod 2), \quad k_{i}=\frac{2}{2}(v \pm 1) .
$$

DEFINITION. Let $G$ be an additive abelian group of order $v$ with elements $z_{1}, z_{2}, \ldots, z_{v}$ ordered in some fixed way. Let $X$ be a subset of $G$. Further let $\phi$ and $\psi$ be maps from $G$ into a commutative ring. Then $M=\left(m_{i j}\right)$ defined by
(4)

$$
m_{i j}=\psi\left(z_{j}-z_{i}\right)
$$

will be called type $I$ and $N=\left(n_{i j}\right)$ defined by

$$
\begin{equation*}
n_{i j}=\phi\left(z_{j}+z_{i}\right) \tag{5}
\end{equation*}
$$

will be called type 2 .
If $\phi$ and $\psi$ are defined by

$$
\phi(z)=\psi(z)=\left\{\begin{array}{ll}
1 & z \in X  \tag{6}\\
0 & z k X
\end{array},\right.
$$

then $M$ and $N$ will be called the type 1 incidence matmix of $X$ in $G$ and the type 2 incidence matrix of $X$ in $G$, respectively. While if $\phi$ and $\psi$ are defined by

$$
\phi(z)=\psi(z)=\left\{\begin{array}{rr}
1 & z \in X,  \tag{7}\\
-1 & z
\end{array} \in X,\right.
$$

$M$ and $N$ will be called the type $1(1,-1)$-matrix of $X$ and the type 2 (1, -1)-matrix of $X$ respectively.

LEMMA 2. Suppose $M$ and $N$ are type 1 and type 2 incidence matrices of a subset $X=\left\{x_{j}\right\}$ of an additive abetian group $G=\left\{z_{i}\right\}$. Then

$$
M M^{T}=N N^{T}
$$

Proof. The inner products of distinct rows $i$ and $k$ in $M$ and $N$ respectively are given by

$$
\begin{array}{ll}
\sum_{z_{j} \in G} \psi\left(z_{j}-z_{i}\right) \psi\left(z_{j}-z_{k}\right) & \sum_{j \in G} \phi\left(z_{j}+z_{i}\right) \phi\left(z_{j}+z_{k}\right) \\
=\sum_{g \in G} \psi(g) \psi\left(g+z_{i}-z_{k}\right) & =\sum_{h \in G} \phi\left(h+z_{i}-z_{k}\right) \phi(h) \\
\text { since as } z_{j} \text { runs through } G & \text { since as } z_{j} \text { runs through } G \\
\text { so does } z_{j}-z_{i}=g & \text { so does } z_{j}+z_{k}=h \\
=\sum_{x \in X} \psi\left(x+z_{i}-z_{k}\right) & =\sum_{x \in X} \phi\left(x+z_{i}-z_{k}\right) \\
=\text { number of times } x+z_{i}-z_{k} \in X & =\text { number of times } x+z_{i}-z_{k} \in X \\
\text { as } x \text { runs through } X . & \text { as } x \text { runs through } X .
\end{array}
$$

For the inner product of row $i$ with itself we have

$$
\begin{aligned}
& \sum_{z_{j} \in G}\left[\psi\left(z_{j}-z_{i}\right)\right]^{2} \\
& =\sum_{g \in G}[\psi(g)]^{2} \\
& =\sum_{x \in X}[\psi(x)]^{2} \\
& =\text { number of elements in } X .
\end{aligned}
$$

$$
\sum_{z_{j} \in G}\left[\phi\left(z_{j}+z_{i}\right)\right]^{2}
$$

$$
=\sum_{h \in G}[\phi(h)]^{2}
$$

$$
=\sum_{x \in X}[\phi(x)]^{2}
$$

So $M M^{T}=N N^{T}$.
LEMMA 3. Suppose $G$ is an additive abetion group of order $v$ with elements $z_{1}, z_{2}, \ldots, z_{v}$. Let $\phi, \psi$ and $\mu$ be maps from $G$ to a commutative ring $R$. Define

$$
\begin{array}{ll}
A=\left(a_{i j}\right), & a_{i j}=\phi\left(z_{j}-z_{i}\right), \\
B=\left(b_{i j}\right), & b_{i j}=\psi\left(z_{j}-z_{i}\right), \\
C=\left(c_{i j}\right), & c_{i j}=\mu\left(z_{j}+z_{i}\right),
\end{array}
$$

that is, $A$ and $B$ are type lwhile $C$ is type 2. Then (independently of the ordering of $z_{1}, z_{2}, \ldots, z_{v}$ save on iy that it is fixed)

$$
\begin{aligned}
\text { (i) } \quad C^{T} & =C \\
\text { (ii) } \quad A B & =B A \\
\text { (iii) } A C^{T} & =C A^{T}
\end{aligned}
$$

Proof. (i) $c_{i j}=\mu\left(z_{j}+z_{i}\right)=\mu\left(z_{i}+z_{j}\right)=c_{j i}$.
(ii) $\quad(A B)_{i j}=\sum_{g \in G} \phi\left(g-z_{i}\right) \psi\left(z_{j}-g\right)$; putting $h=z_{i}+z_{j}-g$, it is clear that as $g$ ranges through $G$ so does $h$, and the above expression becomes

$$
\begin{aligned}
\sum_{h \in G} \phi\left(z_{j}-h\right) \psi\left(h-z_{i}\right) & =\sum_{h \in G} \psi\left(h-z_{i}\right) \phi\left(z_{j}-h\right) \\
& =(B A)_{i j} .
\end{aligned}
$$

(iii)

$$
\begin{aligned}
\left(A C^{T}\right)_{i j} & =\sum_{g \in G} \phi\left(g-z_{i}\right) \mu\left(z_{j}+g\right) \\
& =\sum_{h \in G} \phi\left(h-z_{j}\right) \mu\left(z_{i}+h\right) \quad\left(h=z_{j}-z_{i}+g\right) \\
& =\sum_{h \in G} \mu\left(z_{i}+h\right) \phi\left(h-z_{j}\right) \\
& =\left(C A^{T}\right)_{i j} .
\end{aligned}
$$

COROLLARY 4. If $X$ and $Y$ are type 1 incidence matrices (or type 1 ( $1,-1$ )-matrices) and $z$ is a type 2 incidence matrix (or type 2 ( $1,-1$ )-matmix) then

$$
\begin{gathered}
X Y=Y X \\
X Z^{T}=Z X^{T} .
\end{gathered}
$$

LEMMA 5. If $X$ is type $i$, $i=1,2$, then $X^{T}$ is type $i$.
Proof. (i) If $X=\left(x_{i, j}\right)=\phi\left(z_{j}+z_{i}\right)$ is type 2 then $X^{T}=\left(y_{i j}\right)=\phi\left(z_{i}+z_{j}\right)$ is type 2.
(ii) If $X=\left(x_{i j}\right)=\psi\left(z_{j}-z_{i}\right)$ is type 1 then so is
$X^{T}=\left(y_{i, j}\right)=\mu\left(z_{j}-z_{i}\right)$ where $\mu$ is the $\operatorname{map} \mu(z)=\psi(-z)$.
COROLLARY 6. (i) If $X$ and $Y$ are type 1 matrices then

$$
X Y=Y X, \quad X^{T} Y=Y X^{T}, \quad X Y^{T}=Y^{T} X, \quad X^{T} Y^{T}=Y^{T} X^{T}
$$

(ii) If $P$ is type 1 and $Q$ is type 2 then $P Q^{T}=Q P^{T}, \quad P Q=Q^{T} P^{T}, \quad P_{Q}^{T} Q^{T}=Q P, \quad P_{Q}^{T}=Q^{T} P$.

LEMMA 7. Let $X$ and $Y$ be type 2 matrices obtained from two subsets $A$ and $B$ of an additive abelian group $G$ for which

$$
a \in A \Rightarrow-a \in A, \quad b \in B \Rightarrow-b \in B
$$

then

$$
X Y=Y X \quad \text { and } \quad X Y^{T}=Y X^{T}
$$

Proof. Since $X$ and $Y$ are symmetric we only have to prove that $X Y^{T}=Y X^{T}$.

Suppose $X=\left(x_{i j}\right)$ and $Y=\left(y_{i j}\right)$ are defined by

$$
x_{i j}=\phi\left(z_{i}+z_{j}\right), \quad y_{i, j}=\psi\left(z_{i}+z_{j}\right)
$$

where $z_{1}, z_{2}, \ldots$ are the elements of $G$. Then

$$
\begin{aligned}
\left(X Y^{T}\right)_{i j} & =\sum_{k} \phi\left(z_{i}+z_{k}\right) \psi\left(z_{k}+z_{j}\right) \\
& =\sum_{k} \phi\left(-z_{i}-z_{k}\right) \psi\left(z_{k}+z_{j}\right) \text { since } a \in A \Rightarrow-\alpha \in A \\
& =\sum_{Z} \phi\left(z_{j}+z_{\eta}\right) \psi\left(-z_{\eta}-z_{i}\right), \quad z_{\eta}=-z_{k}-z_{i}-z_{j} \\
& =\sum_{\eta} \phi\left(z_{j}+z_{\eta}\right) \psi\left(z_{i}+z_{i}\right) \text { since } b \in B \Rightarrow-b \in B \\
& =\left(Y X^{T}\right)_{i j} .
\end{aligned}
$$

We note if the additive abelian group in the definition of type 1 and type 2 is the integers modulo $p$ with the usual ordering then
(i) the type 1 matrix is circulant since

$$
m_{i, i}=\psi(j-i)=\psi(j-i+1-1)=m_{1 . j-i+1}
$$

(ii) the type 2 matrix is back-circulant since

$$
n_{i j}=(j+i)=(j+i-1+1)=n_{1, j+i-1}
$$

LEMMA 8. Let $R=\left(r_{i j}\right)$ be the permutation matrix of order $v$, defined on an additive abelian group $G=\left\{g_{k}\right\}$ of order $v$ by

$$
r_{i j}=\left\{\begin{array}{l}
1 \quad \text { if } g_{i}+g_{j}=0 \\
0 \quad \text { otherwise }
\end{array}\right.
$$

Let $M$ be a type I matrix of a subset $X$ of $G$. Then $M R$ is a type 2 matrix. In particular if $G$ is the integers moduzo $v, M R$ is a back-circulant matrix.

Proof. Let $M=\left(m_{i j}\right)$ be defined by $m_{i j}=\psi\left(g_{j}-g_{i}\right)$ where $\psi$ maps $G$ into a commutative ring. Let $\mu$ be the map defined by $\mu(-z)=\psi(z)$. Then

$$
\begin{aligned}
(M R)_{i j} & =\sum_{k} m_{i k} r_{k j}=m_{i l} \text { where } g_{\imath}+g_{j}=0 \\
& =\psi\left(g_{\imath}-g_{i}\right) \\
& =\psi\left(-g_{j}-g_{i}\right) \\
& =\mu\left(g_{j}+g_{i}\right)
\end{aligned}
$$

which is a type 2 matrix.
LEMMA 9. Let $X_{1}, X_{2}, \ldots, X_{n}$ be the type 1 incidence matrices of $n-\left\{v ; k_{1}, k_{2}, \ldots, k_{n} ; \lambda\right\}$ supplementary difference sets $S_{1}, \ldots, S_{n}$ defined on $G$ with elements $z_{1}, z_{2}, \ldots, z_{v}$; then

$$
\sum_{i=1}^{n} X_{i} X_{i}^{T}=\left(\sum_{i=1}^{n} k_{i}-\lambda\right) I+\lambda J
$$

If $Y_{1}, Y_{2}, \ldots, Y_{n}$ are the type $1(1,-1)$-matrices of the supplementary difference sets then

$$
\sum_{i=1}^{n} Y_{i} Y_{i}^{T}=4\left(\sum_{i=1}^{n} k_{i}-\lambda\right) I+\left(n v-4 \sum_{i=1}^{n} k_{i}+4 \lambda\right) d
$$

Proof. Let $X_{i}=\left(x_{j k}^{i}\right)$ be defined by

$$
x_{j k}^{i}=\phi_{i}\left(z_{k}-z_{j}\right) \text { where } \phi(z)= \begin{cases}1 & \text { if } z \in S_{i} \\ 0 & \text { otherwise }\end{cases}
$$

Then the $(j, k)$ element of $\sum_{i=1}^{n} X_{i} X_{i}^{T}$ is

$$
\text { So } \sum_{i=1}^{n} X_{i} X_{i}^{T}=\left(\sum_{i=1}^{n} k_{i}-\lambda\right) I+\lambda J
$$

The type $1(1,-1)$-matrix $Y_{i}$ of a set $S_{i}$ is

$$
Y_{i}=2 X_{i}-J
$$

and so

$$
\begin{aligned}
& \left\{\sum_{i=1}^{n} X_{i} X_{i}^{T}\right\}_{j k}=\sum_{i=1}^{n}\left(X_{i} X_{i}^{T}\right)_{j k}=\sum_{i=1}^{n} \sum_{l=1}^{n} x_{j l}^{i} x_{k l}^{i} \\
& =\sum_{i=1}^{n} \sum_{i=1}^{n} \phi_{i}\left(z_{i}-z_{j}\right) \phi_{i}\left(z_{i}-z_{k}\right) \\
& =\sum_{i=1}^{n} \sum_{m=1}^{n} \Phi_{i}\left(z_{m}\right) \phi_{i}\left(z_{m}+z_{j}-z_{k}\right) \\
& \left(z_{m}=z_{i}-z_{j}\right) \\
& =\sum_{i=1}^{n} \text { (number of times } z_{m} \in S_{i} \text { and } z_{m}+z \in S_{i} \text { ) } \\
& \left(z=z_{j}-z_{k}\right) \\
& \left\{\sum_{i=1}^{n} k_{i} \quad(j=k)\right. \\
& =\left\{\begin{array}{l}
i=1 \\
\sum_{i=1}^{n} \text { number of times } z=z_{t}-z_{m} \text { for } z_{m}, z_{t} \in S_{i}
\end{array}\right. \\
& (j \neq k) \\
& =\left\{\begin{array}{l}
\sum_{i=1}^{n} k_{i} \\
\lambda
\end{array}\right. \\
& (j=k) \\
& (j \neq k) .
\end{aligned}
$$

$$
\begin{aligned}
\sum_{i=1}^{n} Y_{i} Y_{i}^{T} & =\sum_{i=1}^{n}\left(2 X_{i}-J\right)\left(2 X_{i}-J\right)^{T} \\
& =\sum_{i=1}^{n}\left(4 X_{i} X_{i}^{T}-4 k_{i} J+v J\right) \\
& =4\left(\sum_{i=1}^{n} k_{i}-\lambda\right) I+\left(n v-4 \sum_{i=1}^{n} k_{i}+4 \lambda\right) J
\end{aligned}
$$

COROLLARY 10. The type $1(1,-1)$ incidence matrices $A_{i}$ and $B_{i}$, $i=1,2,3,4$ of
$4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{14} ; \sum_{i=1}^{4} k_{i}-v\right\}$ and $4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{4} ; \sum_{i=1}^{4} k_{i}-v-1\right\}$
supplementary difference sets satisfy

$$
\sum_{i=1}^{4} A_{i} A_{i}^{T}=4 v I
$$

and

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

respectively.

## 2. A construction for skew-Hadamard matrices

We adapt the Goethals-Seidel matrix of [4] to a form that may be used for subsets of any additive abelian group.

THEOREM 11. Suppose $A, B$ and $D$ are type 1 ( $1,-1$ )-matrices and $C$ is a type 2 ( $1,-1$ )-matrix of $4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{4} ; \sum_{i=1}^{4} k_{i}-v\right\}$ supplementary difference sets; then

$$
H=\left[\begin{array}{cccc}
A & B & C & D \\
-B^{T} & A^{T} & -D & C \\
-C & D^{T} & A & -B^{T} \\
-D^{T} & -C & B & A^{T}
\end{array}\right]
$$

is an Hadomard matrix of order $4 v$.
Further, if $A$ is skew-type, then $H$ is a skew-Hadomard matrix.
Proof. The four type $1(1,-1)$-matrices $A, B, E, D$ of
$4-\left\{v ; k_{1}, k_{2}, k_{3}, k_{4} ; \sum_{i=1}^{4} k_{i}-v\right\}$ supplementary difference sets satisfy

$$
A A^{T}+B B^{T}+E E^{T}+D D^{T}=4 v I_{v}
$$

and using Lemma 2 we see $C C^{T}=E E^{T}$. So

$$
A A^{T}+B B^{T}+C C^{T}+D D^{T}=4 v I_{v}
$$

We use Corollary 6 to see that the inner product of distinct rows is zero.
Since $C$ is type $2, C^{T}=C$ and so if $A$ is skew-type $H$ is skew-Hadamard.

THEOREM 12. Suppose $A, B$ and $D$ are type 1 (1, -1)-matrices and $C$ is a type $2(1,-1)$-matrix of $4-\{2 m+1 ; m ; 2(m-1)\}$ supplementary difference sets; then with $e$ the $1 \times(2 m+1)$ matrix of ones

$$
H=\left[\begin{array}{cccccccc}
-1 & +1 & +1 & +1 & e & e & e & e \\
-1 & -1 & -1 & +1 & -e & e & -e & e \\
-1 & +1 & -1 & -1 & -e & e & e & -e \\
-1 & -1 & +1 & -1 & -e & -e & e & e \\
-e^{T} & e^{T} & e^{T} & e^{T} & A & B & C & D \\
-e^{T} & -e^{T} & -e^{T} & e^{T} & -B^{T} & A^{T} & -D & C \\
-e^{T} & e^{T} & -e^{T} & -e^{T} & -C & D^{T} & A & -B^{T} \\
-e^{T} & -e^{T} & e^{T} & -e^{T} & -D^{T} & -C & B & A^{T}
\end{array}\right]
$$

is an Hadamard matrix of order $8(m+1)$. Further, if $A$ is skew-type, then $H$ is a skew-Hadomard matrix.

Proof. By straightforward verification.
THEOREM 13. Let $f$ be odd and $q=2 m+1=8 f+1$ be a prime power; then there exist $4-\{2 m+1 ; m ; 2(m-1)\}$ supplementary difference sets $X_{1}, X_{2}, X_{3}, X_{4}$ for which $y \in X_{i} \Rightarrow-y k X_{i}, i=1,2,3,4$.

Proof. Let $x$ be a primitive root of $G F(q)$ and $G$ the cyclic group generated by $x$. Define the sets

$$
c_{i}=\left\{x^{8 t+i}: t=0,1, \ldots, f-1\right\}, i=0,1, \ldots, 7
$$

and choose

$$
\begin{aligned}
& x_{1}=c_{0} \cup c_{1} \cup c_{2} \cup c_{3}, \\
& x_{2}=c_{0} \cup C_{1} \cup c_{2} \cup C_{7}, \\
& x_{3}=c_{0} \cup c_{1} \cup C_{6} \cup c_{7}, \\
& x_{4}=c_{0} \cup C_{5} \cup C_{6} \cup C_{7} .
\end{aligned}
$$

Write
where the $a_{i}$ are non-negative integers, for the differences between
elements of $C_{0}$. Thus with $H_{s}=C_{s} \cup C_{s+4}$, since $q=8 f+1(f$ odd $)$, $-1 \in C_{4}$ and $x^{j} \in\left[\right.$ differences from $\left.C_{0}\right] \Rightarrow-x^{\dot{j}} \in\left[\right.$ differences from $\left.C_{0}\right]$, the differences from $C_{0}$ become

$$
\sum_{s=0}^{3} a_{s} H_{s}, \sum_{s=0}^{3} a_{s}=\frac{1}{2}(f-1)
$$

The differences between elements of $C_{i}, i=0,1, \ldots, 7$ is therefore

$$
{\underset{s=0}{3} a_{s} H_{s+i} . . . . . . .}
$$

Now write
for the differences between

$$
C_{0} \text { and } C_{1}, C_{0} \text { and } C_{2}, C_{0} \text { and } C_{3}
$$

respectively, that is for

$$
\left[x-y: x \in C_{0}, y \in C_{i}\right] \&\left[y-x: x \in C_{0}, y \in C_{i}\right] \quad i=1,2,3,
$$

where

$$
\sum_{s=0}^{3} b_{s}=\sum_{s=0}^{3} c_{s}=\sum_{s=0}^{3} d_{s}=f
$$

Then the differences from $X_{1}$ become

$$
\begin{aligned}
& \sum_{s=0}^{3} a_{s}\left(H_{s} \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \& \sum_{s=0}^{3} b_{s}\left(H_{s} \cup H_{s+1} \cup H_{s+2}\right) \\
& \qquad \sum_{s=0}^{3} c_{s}\left(H_{s} \cup H_{s+1}\right) \& \sum_{s=0}^{3} d_{s} H_{s}
\end{aligned}
$$

The differences from $X_{2}$ are

$$
\begin{aligned}
& {\underset{s=0}{3} a_{s}\left(H_{s} \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \& \sum_{s=0}^{3} b_{s}\left(H_{s} \cup H_{s+1} \cup H_{s+3}\right)}^{\qquad \sum_{s=0}^{3} c_{s}\left(H_{s} \cup H_{s+3}\right) \& \sum_{s=0}^{3} d_{s} H_{s+3}},
\end{aligned}
$$

and the differences from $X_{3}$ are

$$
\begin{array}{r}
\sum_{s=0}^{3} a_{s}\left(H_{s} \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \& \sum_{s=0}^{3} b_{s}\left(H_{s} \cup H_{s+2} \cup H_{s+3}\right) \\
\qquad \begin{array}{l}
\& \\
\&_{s=0} c_{s}\left(H_{s+2} u H_{s+3}\right) \& \sum_{s=0}^{3} d_{s} H_{s+2}
\end{array}
\end{array}
$$

Finally the differences from $X_{4}$ are

$$
\begin{array}{r}
{\underset{s=0}{3} a_{s}\left(H_{s} \cup H_{s+1} U H_{s+2} \cup H_{s+3}\right) \& \sum_{s=0}^{3} b_{s}\left(H_{s+1} U H_{s+2} \cup H_{s+3}\right)}^{\& \sum_{s=0}^{3} e_{s}\left(H_{s+1} \cup H_{s+2}\right) \& \sum_{s=0}^{3} d_{s} H_{s+1}} .
\end{array}
$$

Now $G=H_{s} \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}$. So the totality of differences from $X_{1}, X_{2}, X_{3}$ and $X_{4}$ is

$$
\begin{aligned}
4 \sum_{s=0}^{3} a_{s} G \& 3 \sum_{s=0}^{3} b_{s} G \& 2 \sum_{s=0}^{3} c_{s} G \& \sum_{s=0}^{3} d_{s} G & =(2(f-1)+6 f) G \\
& =(8 f-2) G
\end{aligned}
$$ difference sets.

Clearly since $y \in C_{s} \Rightarrow-y \in C_{s+4}, X_{1}, X_{2}, X_{3}, X_{4}$ all satisfy $y \in X_{i} \Rightarrow-y \notin X_{i}$.

COROLLARY 14. If $f$ is odd and $p=8 f+1$ is a prime power then there exists a skew-Hadomard matrix of order $8(4 f+1)$.

This corollary shows the existence of the following skew-Hadamard matrices of order < 4000 which were previously unknown 296, 592 , $1184,1640,2280,2368,2408,2472,3432,3752$.
3. A construction for a symmetric Hadamard matrix with constant diagonal

DEFINITION. $2-\{2 m+1 ; m ; m-1\}$ supplementary difference sets $S_{1}$ and $S_{2}$ will be called Szekeres difference sets of size $m$ if $x \in S_{1} \Rightarrow-x \notin S_{1}$.

These sets have been used, as in the next lemma, to construct skew-Hadamard matrices.

LEMMA 15. Suppose there exist Szekeres difference sets $S_{1}, S_{2}$ in an additive abelian group $G$ of order $2 m+1$. Let $A$ and $B$ be the type $1(1,-1)$-matrices of $S_{1}$ and $S_{2}$ respectively; then

$$
H=\left[\begin{array}{cccc}
-1 & 1 & e & e \\
-1 & -1 & -e & e \\
-e^{T} & e^{T} & A & B \\
-e^{T} & -e^{T} & -B^{T} & A^{T}
\end{array}\right]
$$

where $e$ is the $1 \times(2 m+1)$ matrix of 1 's, is a skew-Hadamard matrix of order $4(m+1)$.

Szekeres difference sets of size $m$ are known to exist when
(i) $4 m+3$ is a prime power; from [8],
(ii) $2 m+1$ is a prime power $\equiv 5(\bmod 8)$; from [8],
(iii) $2 m+1$ is a prime power $=p^{t}$ where $p \equiv 5(\bmod 8)$ and $t \equiv 2(\bmod 4) ;$ from [9] and [16].

We now generalize an example in [5] to construct symmetric Hadamard matrices with constant diagonal. The Szekeres difference sets of the next theorem were also used in [12].

THEOREM 16. Let $X$ and $Y$ be Szekeres difference sets of size $m$ in an additive abelian group of order $2 m+1$ with $x \in X \Rightarrow-x \neq X$ and further suppose $y \in Y \Rightarrow-y \in Y$. Suppose there exists a symmetric conference matrix $C+I$ or order $4 m+2$. Then there is a regular symmetric Hadomard matrix of order $4(2 m+1)^{2}$ with constant diagonal.

Proof. Let $B$ and $-A$ be the type 1 ( $1,-1$ ) incidence matrices of $X$ and $Y$. Then using Lemmas 3 and 9 , we see

$$
\begin{gathered}
B^{T}+B=-2 I, A^{T}=A, A B=B A, \quad A J=J, \quad B J=-J \\
A A^{T}+B B^{T}=4(m+1) I-2 J
\end{gathered}
$$

Also forming $W$ from $C$ as described above in (3),

$$
W^{T}=W, \quad W J=0, \quad W W^{T}=(4 m+1) I-J
$$

Write $e$ for the $1 \times(2 m+1)$ matrix of ones and $f$ for the $1 \times(4 m+1)$ matrix of ones. Then

$$
H=\left[\begin{array}{cccc}
I & f & e \times f & -e \times f \\
f^{T} & J & e \times(W-I) & e \times(W+I) \\
e^{T} \times f^{T} & e^{T} \times(W-I) & A \times W+J \times I & -(B+I) \times W+I \times J+(I-J) \times I \\
-e^{T} \times f^{T} & e^{T} \times(W+I) & -(B+I)^{T} \times W+I \times J+(I-J) \times I & A^{T} \times W+J \times I
\end{array}\right]
$$

where $\times$ is the Kronecker product, is the required matrix.
Szekeres difference sets satisfying the conditions of the theorem exist for

$$
\begin{aligned}
& m=2,6,14,26 \\
& m=\frac{1}{4}(p-3), \quad p \text { a prime power }
\end{aligned}
$$

see [8] and [12]. So we have
COROLLARY 17. If $p$ is a prime power and $p-1$ is the order of $a$ symmetric conference matrix, there is a regular symmetric Hadamard matrix with constant diagonal of order $(p-1)^{2}$.

We note that this corollary (barring the constant diagonal) essentially appears in Shrikhande [7].

Thus we have also shown
COROLLARY 18. If $8 f+1$ ( $f$ odd) is a prime power, there exist BIBDs with parcmeters

$$
v=(8 f+1), \quad b=4(8 f+1), \quad r=16 f, \quad k=4 f, \quad \lambda=2(4 f-1)
$$

and

$$
v=b=32 f+7, \quad r=k=16 f+3, \quad \lambda=8 f+1 ;
$$

and also
COROLLARY 19. Suppose there exist Szekeres difference sets $X$ and $Y$ of size $m$ in an additive abelian group of order $2 m+1$, and

$$
x \in X \Rightarrow-x \in X, \quad y \in Y \Rightarrow-y \in Y .
$$

Further suppose there exists a symmetric conference matrix $C+I$ of order $4 m+1$. Then there exists a BIBD with parcometers

$$
v=b=4(2 m+1)^{2}, \quad r=k=2(2 m+1)^{2}+(2 m+1), \quad \lambda=(2 m+1)^{2}+(2 m+1) .
$$

## References

[1] Leonard D. Baumert, Cyclic difference sets (Lecture Notes in Mathematics, 182. Springer-Verlag, Berlin, Heidelberg, New York, 1971).
[2] D. Blatt and G. Szekeres, "A skew Hadamard matrix of order 52 ", Canad. J. Math. 21 (1969), 1319-1322.
[3] J.M. Goethals and J.J. Seidel, "Orthogonal matrices with zero diagonal", Canad. J. Math. 19 (1967), 1001-1010.
[4] J.M. Goethals and J.J. Seidel, "A skew Hadamard matrix of order 36 ", J. AustraZ. Math. Soc. 11 (1970), 343-344.
[5] J.M. Goethals and J.J. Seidel, "Strongly regular graphs derived from combinatorial designs", Canad. J. Math. 22 (1970), 597-614.
[6] J.H. van Lint and J.J. Seidel, "Equilateral point sets in elliptic geometry", K. Nederl. Akad. Wetensch. Proc. Ser. A 69 (1966), 335-348.
[7] S.S. Shrikhande, "On a two-parameter family of balanced incomplete block designs", Sankhyä Ser. A 24 (1962), 33-40.
[8] G. Szekeres, "Tournaments and Hadamard matrices", Enseignement Math. (2) 15 (1969), 269-278.
[9] G. Szekeres, "Cyclotomy and complementary difference sets", Acta Amith. 18 (1971), 349-353.
[10] Richard J. Turyn, "On C-matrices of arbitrary powers", Canad. J. Math. 23 (1971), 531-535.
[11] Jennifer Wallis, "Some (1, -1) matrices", J. Combinatorial Theory Ser. B 10 (1971), 1-11.
[12] Jennifer Wallis, "Amicable Hadamard matrices", J. Combinatomal Theory Ser. A 11 (1971), 296-298.
[13] Jennifer Wallis, "Complex Hadamard matrices", University of Newcastle, Mathematics Research Report No. 63, 1972.
[14] Jennifer Wallis, "On supplementary difference sets", Aequationes Math. (to appear).
[15] Jennifer Wallis, "A note on BIBDs", J. Austral. Math. Soc. (to appear).
[16] Albert Leon Whiteman, "An infinite family of skew Hadamard matrices", Pacific J. Math. 38 (1971), 817-822.
[17] Albert Leon Whiteman, "Skew Hadamard matrices of Goethals-Seidel type", (to appear).
University of Newcastle, University of Southern California,

Newcastle,
New South Wales; and

Los Angeles, California, USA.


[^0]:    Received 3 May 1972. The authors wish to thank Dr W.D. Wallis for helpful discussions and for pointing out the regularity in Theorem 16.

