Some classes of Hadamard matrices with constant diagonal

Jennifer Wallis and Albert Leon Whiteman

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 skew-Hadamard matrices of order $8(f^2+1)$ when $f$ is odd and $8f+1$ 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 $4(2m+1)^2$ when a symmetric conference matrix of order $4m+2$ exists and there are Szekeres difference sets, $X$ and $Y$, of size $m$ satisfying $x \in X \Rightarrow -x \notin X$, $y \in Y \Rightarrow -y \notin Y$.

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 circulant matrix $B = (b_{i,j})$ of order $v$ satisfies $b_{i,j} = b_{l,j-i+1}$ ($j-i+1$ reduced modulo $v$), while $B$ is back-circulant if its elements

Received 3 May 1972. The authors wish to thank Dr W.O. Wallis for helpful discussions and for pointing out the regularity in Theorem 16.
satisfy \( b_{i,j} = b_{i \equiv j \pmod{\nu}} \) (i+j-1 reduced modulo \( \nu \)).

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, \( |V| = \nu \), containing \( k_1, k_2, \ldots, k_n \) elements respectively. Write \( T_\nu \) for the totality of all differences between elements of \( S_\nu \) (with repetitions), and \( T \) for the totality of elements of all the \( T_\nu \). 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 \( \nu \)-\{\( k_1, k_2, \ldots, k_n; \lambda \)\} supplementary difference sets.

The parameters of \( \nu \)-\{\( k_1, k_2, \ldots, k_n; \lambda \)\} supplementary difference sets satisfy

\[
\lambda(\nu-1) = \sum_{i=1}^{n} k_i(k_i-1).
\]

If \( k_1 = k_2 = \ldots = k_n = k \) we will write \( \nu \)-\{\( k; \lambda \)\} to denote the \( \nu \) supplementary difference sets and (1) becomes

\[
\lambda(\nu-1) = \lambda(k-1).
\]


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 \( T_1 \cup T_2 \) will denote the result of adjoining the elements of \( T_1 \) to \( T_2 \) with total multiplicities retained.

An Hadamard matrix \( H \) of order \( \nu \) has every element \(+1\) or \(-1\) and satisfies \( H^T H = \nu I \) \( H \). A skew-Hadamard matrix \( H = I + R \) is an Hadamard matrix with \( H^T = -R \). 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 \(HJ = JW\) for some integer \(k\) is regular.

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

\[
CC^T = (n-1)I_n, \quad C^T = C.
\]

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

\[
\begin{bmatrix}
0 & 1 & \ldots & 1 \\
1 & & & \\
\vdots & & W & \\
1 & & & 
\end{bmatrix}
\]

may be obtained and \(WW^T\) satisfies

\[
WW^T = (n-1)I - J, \quad WW = 0, \quad W^T = W.
\]

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

1. Preliminary results

**Lemma 1.** If there exist \(k = \{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i = \nu - 1\}\) supplementary difference sets then each \(k_i = m\) or \(m - 1\) for \(v = 2m + 1\) and \(k_1 = m + 1\), \(k_2 = k_3 = k_4 = m\) for \(v = 2m\).

**Proof.** By (1),

\[
\left(\sum_{i=1}^{4} k_i - \nu - 1\right)\left(\nu - 1\right) = \sum_{i=1}^{4} k_i(k_i - 1),
\]

so

\[
4 \sum_{i=1}^{4} k_i^2 - 4\nu \sum_{i=1}^{4} k_i + 4(\nu^2 - 1) = 0,
\]
\[
\sum_{t=1}^{h} (2k_t - \nu)^2 = \lambda \\
= \begin{cases} 
2^{2} + 0 + 0 + 0 & , \nu \text{ even,} \\
1^{2} + 1^{2} + 1^{2} + 1^{2} & , \nu \text{ odd.}
\end{cases}
\]

If \( \nu \equiv 0 (\text{mod } 2) \), \( k_{1} = \frac{1}{2}(\nu+2) \), \( k_{2} = k_{3} = k_{4} = \frac{1}{4}\nu \), but if \( \nu \equiv 1 (\text{mod } 2) \), \( k_{1} = \frac{1}{2}(\nu+1) \).

\textbf{DEFINITION.} Let \( G \) be an additive abelian group of order \( \nu \) with elements \( z_{1}, z_{2}, \ldots, z_{\nu} \) 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 \( M = \{m_{ij}\} \) defined by

\[
m_{ij} = \psi(z_{j}-z_{i})
\]

will be called type 1 and \( N = \{n_{ij}\} \) defined by

\[
n_{ij} = \phi(z_{j}+z_{i})
\]

will be called type 2.

If \( \phi \) and \( \psi \) are defined by

\[
\phi(z) = \psi(z) = \begin{cases} 
1 & z \in X, \\
0 & z \notin X,
\end{cases}
\]

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

\[
\phi(z) = \psi(z) = \begin{cases} 
1 & z \in X, \\
-1 & z \notin X,
\end{cases}
\]

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

\textbf{LEMMA 2.} Suppose \( M \) and \( N \) are type 1 and type 2 incidence matrices of a subset \( X = \{z_{j}\} \) of an additive abelian group \( G = \{z_{1}\} \). Then

\[
M^{T}N = NN^{T}.
\]
Proof. The inner products of distinct rows $i$ and $k$ in $M$ and $N$ respectively are given by

$$\sum_{s_j \in G} \psi(s_j z_i z_k) \psi(s_j z_i z_k) = \sum_{s_j \in G} \phi(s_j z_i z_k) \phi(s_j z_i z_k)$$

since as $z_j$ runs through $G$, so does $z_j - z_k = g$.

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

$$\sum_{s_j \in G} [\psi(s_j z_i z_i)]^2 = \sum_{s_j \in G} [\phi(s_j z_i z_i)]^2$$

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

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

= number of elements in $X$. = number of elements in $X$.

So $MM^T = NN^T$.

**Lemma 3.** Suppose $G$ is an additive abelian 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

$$A = (a_{i,j}), \quad a_{i,j} = \phi(z_j - z_i),$$

$$B = (b_{i,j}), \quad b_{i,j} = \psi(z_j - z_i),$$

$$C = (c_{i,j}), \quad c_{i,j} = \psi(z_j + z_i),$$

that is, $A$ and $B$ are type 1 while $C$ is type 2. Then (independently of the ordering of $z_1, z_2, \ldots, z_v$) save only that it is fixed.
\[(i)\quad C^T = C,\]
\[(ii)\quad AB = BA,\]
\[(iii)\quad AC^T = CA^T.\]

Proof. \((i)\) \(c_{ij} = u(s_j + s_i) = u(s_i + s_j) = c_{ji}.\)

\((ii)\) \[(AB)_{ij} = \sum_{g \in G} \phi(g-s_i) \psi(s_j-g); \text{ putting } h = s_i + s_j - g, \text{ it is clear that as } g \text{ ranges through } G \text{ so does } h, \text{ and the above expression becomes} \]
\[
\sum_{h \in G} \phi(s_i-h) \psi(h-s_j) = \sum_{h \in G} \psi(h-s_j) \phi(s_i-h) = (BA)_{ij}.\]

\((iii)\) \[
(AC^T)_{ij} = \sum_{g \in G} \phi(g-s_i) u(s_j + g)
= \sum_{h \in G} \phi(h-s_j) u(s_i + h) \quad [h = s_j - s_i + g]
= \sum_{h \in G} u(s_i + h) \phi(h-s_i)
= (CA^T)_{ij}.\]

**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 \((1,-1)\)-matrix) then
\[XY = YX\]
\[ZX^T = ZX^T.\]

**LEMMA 5.** If \(X\) is type \(i\), \(i = 1, 2\), then \(X^T\) is type \(i\).

Proof. \((i)\) If \(X = [x_{ij}] = \phi(s_j + s_i)\) is type 2 then \(x^T = [y_{ij}] = \phi(s_i + s_j)\) is type 2.

\[(ii)\] If \(X = [z_{ij}] = \psi(s_j - s_i)\) is type 1 then so is
\(X^T = (y_{i,j}) = u(z_j - z_i)\) where \(u\) is the map \(\mu(a) = \psi(-a)\).

**COROLLARY 6.** (i) If \(X\) and \(Y\) are type 1 matrices then

\[XY = YX, \quad X^T Y = YX^T, \quad X^T X = Y^T Y, \quad X^T X = Y^T Y.\]

(ii) If \(P\) is type 1 and \(Q\) is type 2 then

\[PQ^T = QP^T, \quad PQ = QP^T, \quad P^T Q^T = QP, \quad P^T Q = Q^T P.\]

**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

\[XY = YX\] and \(X^T = YX^T.\]

Proof. Since \(X\) and \(Y\) are symmetric we only have to prove that

\[X^T = YX^T.\]

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

\[x_{i,j} = \phi(z_i + z_j), \quad y_{i,j} = \psi(z_i + z_j),\]

where \(z_1, z_2, \ldots\) are the elements of \(G\). Then

\[(XY^T)_{i,j} = \sum_k \phi(z_i + z_k) \psi(z_k + z_j)\]

\[= \sum_k \phi(-z_i - z_k) \psi(z_k + z_j) \quad \text{since } a \in A \Rightarrow -a \in A\]

\[= \sum_i \phi(z_i + z_j) \psi(-z_i - z_j), \quad z_i = -z_i - z_i - z_j\]

\[= \sum_i \phi(z_i + z_j) \psi(z_i + z_j) \quad \text{since } b \in B \Rightarrow -b \in B\]

\[= (YX^T)_{i,j}.\]

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

\[m_{i,j} = \psi(j - i) = \psi(j - i + 1 - 1) = m_{1, j - i + 1}.\]
(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 \( R = \{ r_{i,j} \} \) be the permutation matrix of order \( \nu \), defined on an additive abelian group \( G = \{ g_i \} \) of order \( \nu \) by
\[ r_{i,j} = \begin{cases} 1 & \text{if } g_i + g_j = 0, \\ 0 & \text{otherwise}. \end{cases} \]
Let \( M \) be a type 1 matrix of a subset \( X \) of \( G \). Then \( MR \) is a type 2 matrix. In particular if \( G \) is the integers modulo \( \nu \), \( MR \) is a back-circulant matrix.

**Proof.** Let \( M = \{ m_{i,j} \} \) be defined by \( m_{i,j} = \psi(g_i - g_j) \) where \( \psi \) maps \( G \) into a commutative ring. Let \( u \) be the map defined by \( u(-z) = \psi(z) \).
Then
\[
(MR)_{i,j} = \sum_k m_{i,k} r_{k,j} = m_{i,j} \text{ where } g_i + g_j = 0 \\
\quad = \psi(g_i - g_j) \\
\quad = \psi(-g_j + g_i) \\
\quad = u(g_i + g_j),
\]
which is a type 2 matrix.

**LEMMA 9.** Let \( X_1, X_2, \ldots, X_N \) be the type 1 incidence matrices of \( n - (\nu; k_1, k_2, \ldots, k_N, \lambda) \) supplementary difference sets \( S_1, \ldots, S_N \) defined on \( G \) with elements \( x_1, x_2, \ldots, x_\nu \); 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
\[
\sum_{i=1}^{N} Y_i Y_i^T = \left( \sum_{i=1}^{N} k_i - \lambda \right) I + \left( \nu - \lambda \right) \sum_{i=1}^{N} k_i^2 + \lambda(j). 
\]
Proof. Let \( X_t = \begin{pmatrix} z_t \\ j_k \end{pmatrix} \) be defined by

\[
  x_{jk}^t = \phi_t(z_k - z_j)
\]

where \( \phi(z) = \begin{cases} 
  1 & \text{if } z \in S_t, \\
  0 & \text{otherwise}.
\end{cases} \)

Then the \((j, k)\) element of \( \sum_{t=1}^N X_t X_t^T \) is

\[
  \left( \sum_{t=1}^N X_t X_t^T \right)_{jk} = \sum_{t=1}^N \left( x_{jk}^t \right)^2 = \sum_{t=1}^N \sum_{t'=1}^N x_{j}^{t'} x_{k}^{t'}
\]

\[
  = \sum_{t=1}^N \sum_{t'=1}^N \phi_t(z_t - z_{t'}) \phi_t(z_j - z_k)
\]

\[
  = \sum_{t=1}^N \sum_{t'=1}^N \phi_t(z_t) \phi_t(z_{t'} + z_j - z_k)
\]

\[
  = \sum_{t=1}^N \left( \text{number of times } z_m \in S_t \text{ and } z_m + z_j \in S_t \right)
\]

\[
  \phi_t(z_j - z_k)
\]

\[
  = \left\{
  \begin{array}{ll}
  \sum_{t=1}^N k_t & (j = k) \\
  \sum_{t=1}^N \text{number of times } z = z_t - z_m \text{ for } z_m, z_t \in S_t & (j \neq k) \\
  \end{array}
\right.
\]

\[
  \lambda
\]

So \( \sum_{t=1}^N X_t X_t^T = \left( \sum_{t=1}^N k_t - \lambda \right) I + \lambda J \).

The type 1 \((-1, -1)\)-matrix \( Y_t \) of a set \( S_t \) is

\[
  Y_t = 2X_t - J
\]

and so
\[
\sum_{\pm=1} Y_{\pm} X_{\pm}^T = \sum_{\pm=1} (2X_{\pm} - \lambda)(2X_{\pm} - \lambda)^T
\]
\[
= \sum_{\pm=1} \left(4X_{\pm} X_{\pm}^T - 4k_{\pm} + \lambda \right)
\]
\[
= \left( \sum_{\pm=1} \left(4k_{\pm} - \lambda \right) \right)I + \left(4n - \sum_{\pm=1} \left(4k_{\pm} + \lambda \right) \right)J.
\]

**COROLLARY 10.** The type 1 (1, -1) incidence matrices $A_i$ and $B_i$, 
$i = 1, 2, 3, 4$ of 
\[
\mu = \left\{v; k_1, k_2, k_3, k_4; \sum_{\pm=1} k_{\pm} - \nu \right\}
\]
and 
\[
\lambda = \left\{v; k_1, k_2, k_3, k_4; \sum_{\pm=1} k_{\pm} - \nu - 1 \right\}
\]
supplementary difference sets satisfy 
\[
\sum_{\pm=1} \mu A_i A_i^T = 4\lambda I
\]
and 
\[
\sum_{\pm=1} \mu B_i B_i^T = 4(\nu + 1)I - 4J
\]
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 $C$ are type 1 (1, -1)-matrices and $D$ is a type 2 (1, -1)-matrix of 
\[
\mu = \left\{v; k_1, k_2, k_3, k_4; \sum_{\pm=1} k_{\pm} - \nu \right\}
\]
supplementary difference sets; then 
\[
H = \begin{bmatrix}
A & B & C & D \\
-B^T & A^T & -D & C \\
-C & D^T & A & -B^T \\
-D^T & -C & B & A^T
\end{bmatrix}
\]
is an Hadamard matrix of order $4v$.

Further, if $A$ is skew-type, then $H$ is a skew-Hadamard matrix.

Proof. The four type 1 $(1, -1)$-matrices $A, B, C, D$ of

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

$$AA^T + BB^T + EE^T + DD^T = 4v I_y,$$

and using Lemma 2 we see $CC^T = EE^T$. So

$$AA^T + BB^T + CC^T + DD^T = 4v I_y.$$

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 $h = \{2m+1; m; 2(m-1)\}$ supplementary difference sets; then with $e$ the $1 \times (2m+1)$ matrix of ones

$$H = \begin{bmatrix}
-1 & +1 & +1 & +1 & e & e & e & e \\
-1 & -1 & -1 & +1 & -e & e & -e & e \\
-1 & +1 & -1 & -1 & -e & e & e & -e \\
-1 & -1 & +1 & -1 & e & -e & e & e \\
-e^T & e^T & e^T & e^T & A & B & C & D \\
e^T & -e^T & e^T & -e^T & A^T & -D & C \\
e^T & -e^T & -e^T & e^T & C & B & A \\
e^T & -e^T & -e^T & -e^T & -C & B & A \\
e^T & -e^T & -e^T & -e^T & -e^T & -e^T & -A & A
\end{bmatrix}$$

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

Proof. By straightforward verification.

THEOREM 13. Let $f$ be odd and $q = 2m + 1 = 8f + 1$ be a prime power; then there exist $h = \{2m+1; m; 2(m-1)\}$ supplementary difference sets $X_1, X_2, X_3, X_4$ for which $y \in X_i = y \perp X_i$, $i = 1, 2, 3, 4$. 
Proof. Let \( x \) be a primitive root of \( GF(q) \) and \( G \) the cyclic group generated by \( x \). Define the sets

\[
C_i^t = \{x^{bt+i} : t = 0, 1, \ldots, f-1\}, \quad i = 0, 1, \ldots, 7,
\]

and choose

\[
\begin{align*}
X_1 &= C_0 \cup C_1 \cup C_2 \cup C_3, \\
X_2 &= C_0 \cup C_1 \cup C_2 \cup C_7, \\
X_3 &= C_0 \cup C_1 \cup C_6 \cup C_7, \\
X_4 &= C_0 \cup C_5 \cup C_6 \cup C_7.
\end{align*}
\]

Write

\[
\sum_{s=0}^{7} a_s C_s \quad \left( \sum_{s=0}^{7} a_s = f-1 \right),
\]

where the \( a_s \) are non-negative integers, for the differences between elements of \( C_0 \). Thus with \( H_s = C_s \cup C_{s+a} \), since \( q = 8f + 1 \) (\( f \) odd),

\(-1 \in C_0 \) and \( x^j \in \text{[differences from } C_0] \) = \(-x^j \in \text{[differences from } C_0] \),

the differences from \( C_0 \) become

\[
\sum_{s=0}^{3} a_s H_s, \quad \sum_{s=0}^{3} a_s = \frac{1}{2}(f-1).
\]

The differences between elements of \( C_i^t \), \( i = 0, 1, \ldots, 7 \) is therefore

\[
\sum_{s=0}^{3} a_s H_{s+i}^t.
\]

Now write

\[
\sum_{s=0}^{3} b_i H_s, \quad \sum_{s=0}^{3} c_i H_s, \quad \sum_{s=0}^{3} d_i H_s
\]

for the differences between

\( C_0 \) and \( C_1 \), \( C_0 \) and \( C_2 \), \( C_0 \) and \( C_3 \),

respectively, that is for
\[ x-y : x \in C_0, y \in C_i \] \& \[ y-x : x \in C_0, y \in C_i \] \quad i = 1, 2, 3,

where

\[
\frac{3}{s=0} b_s = \frac{3}{s=0} c_s = \frac{3}{s=0} d_s = f.
\]

Then the differences from \( X_1 \) become

\[
\frac{3}{s=0} a_s \left( H_{s+1} \cup H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} b_s \left( H_{s+1} \cup H_{s+2} \right)
\]

\[
\& \frac{3}{s=0} c_s \left( H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} d_s \left( H_{s+3} \right).
\]

The differences from \( X_2 \) are

\[
\frac{3}{s=0} a_s \left( H_{s+1} \cup H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} b_s \left( H_{s+1} \cup H_{s+2} \right)
\]

\[
\& \frac{3}{s=0} c_s \left( H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} d_s \left( H_{s+3} \right).
\]

and the differences from \( X_3 \) are

\[
\frac{3}{s=0} a_s \left( H_{s+1} \cup H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} b_s \left( H_{s+1} \cup H_{s+2} \right)
\]

\[
\& \frac{3}{s=0} c_s \left( H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} d_s \left( H_{s+3} \right).
\]

Finally the differences from \( X_4 \) are

\[
\frac{3}{s=0} a_s \left( H_{s+1} \cup H_{s+2} \cup H_{s+3} \right) \& \frac{3}{s=0} b_s \left( H_{s+1} \cup H_{s+2} \right)
\]

\[
\& \frac{3}{s=0} c_s \left( H_{s+1} \cup H_{s+2} \right) \& \frac{3}{s=0} d_s \left( H_{s+1} \right).
\]

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
\[ \begin{align*}
\frac{4}{a_0} \left( \sum_{s=0}^3 a_s \right) &+ \frac{3}{a_0} \left( \sum_{s=0}^3 b_s \right) &+ \frac{3}{a_0} \left( \sum_{s=0}^3 c_s \right) &+ \frac{3}{a_0} \left( \sum_{s=0}^3 d_s \right) G = &\left( 2(f-1)+6f \right) G \\
= &\left( 8f-2 \right) G.
\end{align*} \]

Hence \(X_1, X_2, X_3, X_4\) are \(4 - \{2m+1; m; 2(m-1)\}\) supplementary difference sets.

Clearly since \(y \in C_{\alpha} \Rightarrow y \in C_{\alpha+4}\), \(X_1, X_2, X_3, X_4\) all satisfy \(y \in X_i \Rightarrow -y \notin X_i\).

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

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.** \(2 - \{2m+1; m; m-1\}\) 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 \(2m+1\). Let \(A\) and \(B\) be the type 1 \((1,-1)\)-matrices of \(S_1\) and \(S_2\) respectively; then

\[
H = \begin{bmatrix}
-1 & 1 & e & e \\
-1 & -1 & -e & e \\
-e & e & A & B \\
e & -e & -B & A
\end{bmatrix},
\]

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

Szekeres difference sets of size \(m\) are known to exist when
Hadamard matrices

(1) \(4m + 3\) is a prime power; from [8],

(ii) \(2m + 1\) is a prime power \(\equiv 5 \pmod{8}\); from [8],

(iii) \(2m + 1\) is a prime power \(= p^t\) where \(p \equiv 5 \pmod{8}\) and \(t \equiv 2 \pmod{4}\); 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 [10].

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

\[
B^T + B = -2I, \quad A^T = A, \quad AB = BA, \quad AJ = J, \quad BJ = -J,
\]

\[AA^T + BB^T = 4(m+1)I - 2J.
\]

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

\[W^T = W, \quad WJ = 0, \quad WW^T = (4m+1)I - J.
\]

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

\[
H = \begin{bmatrix}
1 & f & e \times f & -e \times f \\
\bar{f} & J & e \times (W-I) & e \times (W+I) \\
e \times \bar{f} & e \times (W-I) & A \times W + J \times I & -(B+I) \times W + J \times (I-J) \times I \\
e \times \bar{f} & e \times (W+I) & -(B+I) \times W + J \times (I-J) \times I & A^T \times W + J \times I
\end{bmatrix},
\]

where \(\times\) is the Kronecker product, is the required matrix.

Szekeres difference sets satisfying the conditions of the theorem exist for

\[m = 2, 6, 14, 26,\]

\[m = \frac{p}{2}(p-3), \quad p \text{ a prime power},\]
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 Shrikande [7].

Thus we have also shown

**COROLLARY 18.** If \( 8f + 1 \) (\( f \) odd) is a prime power, there exist BIBDs with parameters

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

and

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

and also

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

\[
x \in X \implies -x \notin X, \quad y \in Y \implies -y \notin Y.
\]

Further suppose there exists a symmetric conference matrix \( C + I \) of order \( 4m + 1 \). Then there exists a BIBD with parameters

\[
v = b = 4(2m+1)^2, \quad r = k = 2(2m+1)^2 + (2m+1), \quad \lambda = (2m+1)^2 + (2m+1).
\]

**References**


University of Newcastle, University of Southern California,
Newcastle, Los Angeles, California,
New South Wales; and USA.