BULL. AUSTRAL. MATH. SOC. 05B05. 05B20
VOL. 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 $8(4f+1)$ 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 $x \in X \Rightarrow -x \notin X$, $y \in Y \Rightarrow -y \in Y$.

Suppose V is a finite abelian group with v elements, written in additive notation. A *difference set* D with parameters (v, k, λ) 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 λ 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* $B = \left(b_{ij}\right)$ of order v satisfies $b_{ij} = b_{1,j-i+1}$ ($j-i+1$ reduced modulo v), while B is *back-circulant* if its elements

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

satisfy $b_{ij} = b_{1,i+j-1}$ ($i+j-1$ 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, λ say, then the sets $S_1, S_2, \ldots, S_n$ will be called $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ *supplementary difference sets*.

The parameters of $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets satisfy

$$(1) \qquad \lambda(v-1) = \sum_{i=1}^{n} k_i(k_i-1) .$$

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

$$(2) \qquad \lambda(v-1) = nk(k-1) .$$

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 $HH^T = hI_h$. A *skew-Hadamard matrix* $H = I + R$ is an Hadamard 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 $HJ = kJ$ for some integer k is *regular*.

A *symmetric conference matrix* $C + I$ of order $n \equiv 2 (\mathrm{mod}\ 4)$ 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

$$\text{(3)} \qquad \begin{bmatrix} 0 & 1 \ldots 1 \\ 1 & \\ \vdots & W \\ 1 & \end{bmatrix}$$

may be obtained and W satisfies

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

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* $v = 2m + 1$ *and* $k_1 = m \pm 1$, $k_2 = k_3 = k_4 = m$ *for* $v = 2m$.

Proof. By (1),

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

so

$$4 \sum_{i=1}^{4} k_i^2 - 4v \sum_{i=1}^{4} k_i + 4(v^2 - 1) = 0 \ ,$$

$$\sum_{i=1}^{4} (2k_i-v)^2 = 4$$

$$= \begin{cases} 2^2+0+0+0 & , \quad v \text{ even}, \\ 1^2+1^2+1^2+1^2 & , \quad v \text{ odd}. \end{cases}$$

If $v \equiv 0 \pmod 2$, $k_1 \doteq \frac{1}{2}(v\pm 2)$, $k_2 = k_3 = k_4 = \frac{1}{2}v$, but if $v \equiv 1 \pmod 2$, $k_i = \frac{1}{2}(v\pm 1)$.

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 ϕ and ψ be maps from G into a commutative ring. Then $M = (m_{ij})$ defined by

$$m_{ij} = \psi(z_j - z_i) \tag{4}$$

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

$$n_{ij} = \phi(z_j + z_i) \tag{5}$$

will be called *type* 2.

If ϕ and ψ are defined by

$$\phi(z) = \psi(z) = \begin{cases} 1 & z \in X , \\ 0 & z \notin X , \end{cases} \tag{6}$$

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 ϕ and ψ are defined by

$$\phi(z) = \psi(z) = \begin{cases} 1 & z \in X , \\ -1 & z \notin X , \end{cases} \tag{7}$$

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* $X = \{x_j\}$ *of an additive abelian group* $G = \{z_i\}$. *Then*

$$MM^T = NN^T .$$

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

$$\sum_{z_j \in G} \psi(z_j - z_i)\psi(z_j - z_k)$$

$$= \sum_{g \in G} \psi(g)\psi(g + z_i - z_k)$$

since as z_j runs through G so does $z_j - z_i = g$

$$= \sum_{x \in X} \psi(x + z_i - z_k)$$

= number of times $x + z_i - z_k \in X$ as x runs through X.

$$\sum_{z_j \in G} \phi(z_j + z_i)\phi(z_j + z_k)$$

$$= \sum_{h \in G} \phi(h + z_i - z_k)\phi(h)$$

since as z_j runs through G so does $z_j + z_k = h$

$$= \sum_{x \in X} \phi(x + z_i - z_k)$$

= number of times $x + z_i - z_k \in X$ as x runs through X.

For the inner product of row i with itself we have

$$\sum_{z_j \in G} [\psi(z_j - z_i)]^2 = \sum_{g \in G} [\psi(g)]^2 = \sum_{x \in X} [\psi(x)]^2$$

= number of elements in X.

$$\sum_{z_j \in G} [\phi(z_j + z_i)]^2 = \sum_{h \in G} [\phi(h)]^2 = \sum_{x \in X} [\phi(x)]^2$$

= 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 ϕ, ψ and μ be maps from G to a commutative ring R. Define*

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

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

$$C = (c_{ij}), \quad c_{ij} = \mu(z_j + z_i),$$

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)

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

(i) $C^T = C$,

(ii) $AB = BA$,

(iii) $AC^T = CA^T$.

Proof. *(i)* $c_{ij} = \mu(z_j+z_i) = \mu(z_i+z_j) = c_{ji}$.

(ii) $(AB)_{ij} = \sum_{g\in G} \phi(g-z_i)\psi(z_j-g)$; putting $h = z_i + z_j - g$, it is clear that as g ranges through G so does h , and the above expression becomes

$$\sum_{h\in G} \phi(z_j-h)\psi(h-z_i) = \sum_{h\in G} \psi(h-z_i)\phi(z_j-h)$$
$$= (BA)_{ij} .$$

(iii)

$$(AC^T)_{ij} = \sum_{g\in G} \phi(g-z_i)\mu(z_j+g)$$
$$= \sum_{h\in G} \phi(h-z_j)\mu(z_i+h) \qquad (h = z_j-z_i+g)$$
$$= \sum_{h\in G} \mu(z_i+h)\phi(h-z_j)$$
$$= (CA^T)_{ij} .$$

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*

$$XY = YX$$
$$XZ^T = ZX^T .$$

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

Proof. (i) If $X = (x_{ij}) = \phi(z_j+z_i)$ is type 2 then $X^T = (y_{ij}) = \phi(z_i+z_j)$ is type 2.

(ii) If $X = (x_{ij}) = \psi(z_j-z_i)$ is type 1 then so is

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

$X^T = (y_{ij}) = \mu(z_j - z_i)$ where μ is the map $\mu(z) = \psi(-z)$.

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

$$XY = YX\ ,\quad X^TY = YX^T\ ,\quad XY^T = Y^TX\ ,\quad X^TY^T = Y^TX^T\ .$$

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

$$PQ^T = QP^T\ ,\quad PQ = Q^TP^T\ ,\quad P^TQ^T = QP\ ,\quad P^TQ = Q^TP\ .$$

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

$$XY = YX \text{ and } XY^T = YX^T\ .$$

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

Suppose $X = (x_{ij})$ and $Y = (y_{ij})$ are defined by

$$x_{ij} = \phi(z_i + z_j)\ ,\quad y_{ij} = \psi(z_i + z_j)\ ,$$

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

$$\begin{aligned}
(XY^T)_{ij} &= \sum_k \phi(z_i + z_k)\psi(z_k + z_j) \\
&= \sum_k \phi(-z_i - z_k)\psi(z_k + z_j) \quad \text{since } a \in A \Rightarrow -a \in A \\
&= \sum_l \phi(z_j + z_l)\psi(-z_l - z_i)\ , \quad z_l = -z_k - z_i - z_j \\
&= \sum_l \phi(z_j + z_l)\psi(z_l + z_i) \quad \text{since } b \in B \Rightarrow -b \in B \\
&= (YX^T)_{ij}\ .
\end{aligned}$$

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

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

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

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

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

LEMMA 8. *Let* $R = (r_{ij})$ *be the permutation matrix of order* v *, defined on an additive abelian group* $G = \{g_k\}$ *of order* v *by*

$$r_{ij} = \begin{cases} 1 & \text{if } g_i + g_j = 0 , \\ 0 & \text{otherwise.} \end{cases}$$

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* v *,* MR *is a back-circulant matrix.*

Proof. Let $M = (m_{ij})$ be defined by $m_{ij} = \psi(g_j-g_i)$ where ψ maps G into a commutative ring. Let μ be the map defined by $\mu(-z) = \psi(z)$. Then

$$\begin{aligned} (MR)_{ij} &= \sum_k m_{ik}r_{kj} = m_{il} \quad \text{where} \quad g_l + g_j = 0 \\ &= \psi(g_l-g_i) \\ &= \psi(-g_j-g_i) \\ &= \mu(g_j+g_i) , \end{aligned}$$

which is a type 2 matrix.

LEMMA 9. *Let* $X_1, X_2, \ldots, X_n$ *be the type* 1 *incidence matrices of* $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ *supplementary difference sets* $S_1, \ldots, S_n$ *defined on* G *with elements* $z_1, z_2, \ldots, z_v$ *; then*

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

If $Y_1, Y_2, \ldots, Y_n$ *are the type* 1 (1, -1)*-matrices of the supplementary difference sets then*

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

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

Proof. Let $X_i = \left(x^i_{jk}\right)$ be defined by

$$x^i_{jk} = \phi_i\left(z_k - z_j\right) \quad \text{where} \quad \phi(z) = \begin{cases} 1 & \text{if } z \in S_i , \\ 0 & \text{otherwise.} \end{cases}$$

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

$$\left(\sum_{i=1}^{n} X_i X_i^T\right)_{jk} = \sum_{i=1}^{n} \left(X_i X_i^T\right)_{jk} = \sum_{i=1}^{n} \sum_{l=1}^{n} x^i_{jl} x^i_{kl}$$

$$= \sum_{i=1}^{n} \sum_{l=1}^{n} \phi_i\left(z_l - z_j\right) \phi_i\left(z_l - z_k\right)$$

$$= \sum_{i=1}^{n} \sum_{m=1}^{n} \phi_i\left(z_m\right) \phi_i\left(z_m + z_j - z_k\right) \qquad \left(z_m = z_l - z_j\right)$$

$$= \sum_{i=1}^{n} \left(\text{number of times } z_m \in S_i \text{ and } z_m + z \in S_i\right)$$

$$\left(z = z_j - z_k\right)$$

$$= \begin{cases} \sum_{i=1}^{n} k_i & (j = k) \\ \sum_{i=1}^{n} \text{number of times } z = z_t - z_m \text{ for } z_m, z_t \in S_i & (j \neq k) \end{cases}$$

$$= \begin{cases} \sum_{i=1}^{n} k_i & (j = k) \\ \lambda & (j \neq k) . \end{cases}$$

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

$$Y_i = 2X_i - J$$

and so

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

$$\sum_{i=1}^{n} Y_iY_i^T = \sum_{i=1}^{n} (2X_i-J)(2X_i-J)^T$$
$$= \sum_{i=1}^{n} \left(4X_iX_i^T-4k_iJ+vJ\right)$$
$$= 4\left(\sum_{i=1}^{n} k_i-\lambda\right)I + \left(nv-4\sum_{i=1}^{n} k_i+4\lambda\right)J .$$

COROLLARY 10. *The type* 1 (1, -1) *incidence matrices* A_i *and* B_i , $i = 1, 2, 3, 4$ *of*

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

supplementary difference sets satisfy

$$\sum_{i=1}^{4} A_iA_i^T = 4vI$$

and

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

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* 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*

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

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

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, 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

$$AA^T + BB^T + EE^T + DD^T = 4vI_v ,$$

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

$$AA^T + BB^T + CC^T + DD^T = 4vI_v .$$

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* $4 - \{2m+1;\ m;\ 2(m-1)\}$ *supplementary difference sets; then with* e *the* $1 \times (2m+1)$ *matrix of ones*

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

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* $4 - \{2m+1;\ m;\ 2(m-1)\}$ *supplementary difference sets* X_1, X_2, X_3, X_4 *for which* $y \in X_i \Rightarrow -y \notin X_i$, $i = 1, 2, 3, 4$.

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

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

$$C_i = \{x^{8t+i} : t = 0, 1, \ldots, f-1\} , \quad i = 0, 1, \ldots, 7 ,$$

and choose

$$X_1 = C_0 \cup C_1 \cup C_2 \cup C_3 ,$$
$$X_2 = C_0 \cup C_1 \cup C_2 \cup C_7 ,$$
$$X_3 = C_0 \cup C_1 \cup C_6 \cup C_7 ,$$
$$X_4 = C_0 \cup C_5 \cup C_6 \cup C_7 .$$

Write

$$\mathop{\&}_{s=0}^{7} a_s C_s \quad \left(\sum_{s=0}^{7} a_s = f-1 \right) ,$$

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 $q = 8f + 1$ (f odd), $-1 \in C_4$ and $x^j \in$ [differences from C_0] $\Rightarrow -x^j \in$ [differences from C_0], the differences from C_0 become

$$\mathop{\&}_{s=0}^{3} a_s H_s , \quad \sum_{s=0}^{3} a_s = \tfrac{1}{2}(f-1) .$$

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

$$\mathop{\&}_{s=0}^{3} a_s H_{s+i} .$$

Now write

$$\mathop{\&}_{s=0}^{3} b_s H_s , \quad \mathop{\&}_{s=0}^{3} c_s H_s , \quad \mathop{\&}_{s=0}^{3} d_s H_s$$

for the differences between

$$C_0 \text{ and } C_1 , \quad C_0 \text{ and } C_2 , \quad C_0 \text{ and } C_3$$

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

$$\sum_{s=0}^{3} b_s = \sum_{s=0}^{3} c_s = \sum_{s=0}^{3} d_s = f \,.$$

Then the differences from X_1 become

$$\mathop{\&}_{s=0}^{3} a_s\left(H_s \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} b_s\left(H_s \cup H_{s+1} \cup H_{s+2}\right) \;\&\; \mathop{\&}_{s=0}^{3} c_s\left(H_s \cup H_{s+1}\right) \;\&\; \mathop{\&}_{s=0}^{3} d_s H_s \,.$$

The differences from X_2 are

$$\mathop{\&}_{s=0}^{3} a_s\left(H_s \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} b_s\left(H_s \cup H_{s+1} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} c_s\left(H_s \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} d_s H_{s+3} \,,$$

and the differences from X_3 are

$$\mathop{\&}_{s=0}^{3} a_s\left(H_s \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} b_s\left(H_s \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} c_s\left(H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} d_s H_{s+2} \,.$$

Finally the differences from X_4 are

$$\mathop{\&}_{s=0}^{3} a_s\left(H_s \cup H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} b_s\left(H_{s+1} \cup H_{s+2} \cup H_{s+3}\right) \;\&\; \mathop{\&}_{s=0}^{3} c_s\left(H_{s+1} \cup H_{s+2}\right) \;\&\; \mathop{\&}_{s=0}^{3} d_s H_{s+1} \,.$$

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

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

$$4\sum_{s=0}^{3} a_s G \,\&\, 3\sum_{s=0}^{3} b_s G \,\&\, 2\sum_{s=0}^{3} c_s G \,\&\, \sum_{s=0}^{3} d_s G = \big(2(f-1)+6f\big)G$$
$$= (8f-2)G \; .$$

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

Clearly since $y \in C_s \Rightarrow -y \in C_{s+4}$, 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 $p = 8f + 1$ is a prime power then there exists a skew-Hadamard matrix of order* $8(4f+1)$.

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*

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

where e is the $1 \times (2m+1)$ 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

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

(i) $4m + 3$ 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 [12].

THEOREM 16. *Let X and Y be Szekeres difference sets of size m in an additive abelian group of order $2m + 1$ with $x \in X \Rightarrow -x \notin X$ and further suppose $y \in Y \Rightarrow -y \in Y$. 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

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

where $\times$ is the Kronecker product, is the required matrix.

Szekeres difference sets satisfying the conditions of the theorem exist for

$$m = 2,\ 6,\ 14,\ 26\ ,$$
$$m = \tfrac{1}{4}(p-3)\ , \quad p \text{ a prime power},$$

https://doi.org/10.1017/S0004972700044993 Published online by Cambridge University Press

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* $8f + 1$ *(*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*

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

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

[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. Austral. 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", *Sankhyā 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 Arith.* 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. Combinatorial 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,
Newcastle,
New South Wales; and

University of Southern California,
Los Angeles, California,
USA.