On supplementary difference sets

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

On supplementary difference sets

Abstract

Given a finite abelian group V and subsets $S_1, S_2, \ldots, S_n$ of V, write T_i for the totality of all the possible differences between elements of S_i (with repetitions counted multiply) and T for the totality of members of all the T_i. If T contains each non-zero element of V the same number of times, then the sets $S_1, S_2, \ldots, S_n$ will be called supplementary difference sets.

We discuss some properties for such sets, give some existence theorems and observe their use in the construction of Hadamard matrices and balanced incomplete block designs.

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, On supplementary difference sets, Aequationes Mathematicae, 8, (1972), 242-257.

Reprint from
aequationes mathematicae
Vol. 8, fasc. 3, 1972 BIRKHÄUSER VERLAG BASEL pages 242–257

On Supplementary Difference Sets

JENNIFER WALLIS (New South Wales, Australia)

Given a finite abelian group V and subsets $S_1, S_2, \ldots, S_n$ of V, write T_i for the totality of all the possible differences between elements of S_i (with repetitions counted multiply) and T for the totality of members of all the T_i. If T contains each non-zero element of V the same number of times, then the sets $S_1, S_2, \ldots, S_n$ will be called *supplementary difference sets.*

We discuss some properties for such sets, give some existence theorems and observe their use in the construction of Hadamard matrices and balanced incomplete block designs.

1. Definitions

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 may be called a *cyclic difference set*: these are extensively discussed in Baumert [1].

It is often easier to discuss a subset D of an abelian group in terms of its *incidence matrix* $A=(a_{ij})$ which is obtained by ordering the elements of V as $v_1, v_2, \ldots, v_v$ in some way and then choosing

$$a_{ij} = \begin{cases} 0 & i=j \\ +1 & (v_j - v_i) \in D \\ 0 & \text{otherwise} \end{cases}$$

For a *cyclic difference set* if we order the elements of V as $0, 1, \ldots, v-1$ we will obtain a *cyclic* or *circulant incidence matrix*: a *circulant matrix* $B=(b_{ij})$ 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 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.

Although there are many equivalent definitions, we define a (v, k, λ)-*configuration* to be a $(0, 1)$-matrix A of order v, with row and column sum k, such that the inner product of any two row vectors is λ. Hence A satisfies

$$AA^T = (k-\lambda) I + \lambda J .$$

Received April 21, 1971 and in revised form August 16, 1971

A (v, b, r, k, λ)-*configuration* or *BIBD* is a (0, 1) matrix B of size $v \times b$, with row sum r and column sum k, such that the inner product of any two row vectors is λ. That is, B satisfies

$$BB^T = (r - \lambda) I + \lambda J.$$

The reader is referred to Marshall Hall Jr. [7] for further discussion of these configurations.

Let $S_1, S_2, \ldots, S_n$ be subsets of V, a finite abelian group, 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 incidence matrix for each individual set may be determined as described above.

Examples

In all the following cases the numbers are residues modulo 13:

1. $\{5, 6, 7, 8, 11\}$, $\{1, 4, 9, 10, 12\}$, $\{1, 9, 10\}$, $\{1, 5, 7\}$, $\{1, 4, 10\}$, $\{1, 7\}$ are $6-\{13; 5, 5, 3, 3, 2; 5\}$ supplementary difference sets;
2. $\{1, 4, 10\}$, $\{1, 3, 4\}$, $\{3, 4, 12\}$, $\{6, 8, 11\}$, $\{1, 7\}$ are $5-\{13; 4{:}3, 2; 2\}$ supplementary difference sets;
3. $\{1, 4, 9, 12\}$, $\{2, 5, 6, 11\}$, $\{1, 3, 10, 12\}$, $\{2, 5, 6, 7\}$, $\{3, 4, 9, 10\}$, $\{2, 5, 6, 8\}$ are $6-\{13; 4; 6\}$ supplementary difference sets;
4. $\{1, 4, 10\}$, $\{3, 4, 12\}$, $\{0, 5, 7\}$, $\{5, 6, 8\}$ are $4-\{13; 3; 2\}$ supplementary difference sets.

These examples indicate the existence of supplementary difference sets which have a range of k-values.

NOTATION. Although G. Szekeres [12], [13] and A. L. Whiteman [16] have used the word 'complementary' for what we call $2-\{v; k_1, k_2; \lambda)$ supplementary difference sets, we will follow the convention of using *complementary difference sets* for the case when S is a (v, k, λ)-difference set and $R = \{r : r \in V, r \notin S\}$ is its *complementary* $(v, v-k, v-2k+\lambda)$ difference set (see Baumert [1], Chapter IB).

NOTATION. If $k_1 = k_2 = \cdots = k_n = k$ we will write $n-\{v; k; \lambda\}$ to denote the n supplementary difference sets. If

$$k_1 = k_2 = \cdots = k_i, \quad k_{i+1} = k_{i+2} = \cdots = k_{i+j}, \ldots, k_l = \cdots = k_n$$

then we sometimes write $n-\{v; i{:}k_1, j{:}k_{i+1}, \ldots; \lambda\}$. A (v, k, λ) difference set repeated n-times will be denoted $n-(v, k, \lambda)$.

NOTATION. We shall frequently be concerned with collections in which repeated elements are counted multiply, rather than with sets. If T_1 and T_2 are two such 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, 476. Skew-Hadamard matrices are as yet unknown for the following orders <300: 100, 116, 148, 156, 172, 188, 196, 232, 236, 260, 268, 276, 292, 296.

2. Preliminary Results

LEMMA 1. *The parameters of $n-\{v; k_1, k_2, \ldots, k_n; \lambda\}$ supplementary difference sets satisfy*

$$\lambda(v-1)=\sum_{j=1}^{n} k_j(k_j-1). \tag{1}$$

Proof. This follows immediately from the definition by counting the differences.

This of course includes the case where $S_1=S_2=\cdots=S_n$ when each S_i is a (v, k, λ') difference set and $\lambda=n\lambda'$. Also immediately we have

LEMMA 2. *For $n-\{v; k; \lambda\}$ supplementary difference sets $\lambda(v-1)=nk(k-1)$.*

Although we cannot have a counterpart of the Bruck-Chowla-Ryser theorem for supplementary difference sets it is clear that the methods of Connor are applicable; see [7] for more details.

LEMMA 3. *Take any set of k elements $S=\{s_1, s_2, \ldots, s_k\}$ from an additive Abelian group V. Let T be the totality of differences of elements from S. Write*

$$T=[s_i-s_j: i\neq j,\ i, j=1\ldots k].$$

Then if we form k sets $S_i=\{s_j: j\neq i,\ s_j\in S\}$ and let T_i be the totality of differences of elements from S_i and if

$$R=T_1 \;\&\; T_2 \;\&\; \ldots \;\&\; T_k$$

(all repetitions remain) then

$$R=(k-2)\,T.$$

Proof. The difference occurring from s_n and s_m, n and m fixed, will occur in every T_i except T_n and T_m and so s_n-s_m will occur $k-2$ times in R.

LEMMA 4. (Das and Kulshreshtha [5]). *If S and T are as in Lemma 3 but the S_i are formed by removing j elements systematically from S (so that each possible subset of j elements is removed exactly once), then there are $\binom{k}{j}$ S_i each of $(k-j)$ elements. The corresponding T_i have $(k-j)(k-j-1)$ elements and*

$$R = \binom{k-2}{j} T,$$

where $\binom{n}{r}$ is the usual binomial coefficient.

3. Some Existence Theorems

We note that while there are no non-trivial difference sets of order 5 there are supplementary difference sets of order 5. There are $2-\{5; 2; 1\}$, $2-\{5; 3, 2; 2\}$ and

Table 1

Ref. No.	Supplementary difference set parameters	Source and conditions for existence; p is a prime power
1	$\binom{k}{j}-\{v; k-j; \lambda\binom{k-2}{j}\}$	(v, k, λ) difference set exists and lemma 4;
2	$2-\{4r+1; 2r+1, 2r; 2r-1\}$	$p=4r+1$; from lemma 6;
3	$2k-\{v; k-1; \lambda(k-2)\}$	$2-\{v; k; \lambda\}$ supplementary difference sets exist and lemma 5 with $j=1$ on both sets;
4	$2(k-1)-\{v; k{:}k-1, (k-2){:}k; \lambda(k-2)\}$	$2-\{v; k; \lambda\}$ supplementary difference sets exist. Apply lemma 5 to one of the sets and repeat the other set $(k-2)$ times then lemma 4 gives the result;
5	$(n(k-1)+k+1)-\{v; k; \lambda(k-1)\}$	$(n+1)-\{v; n{:}k, k+1; \lambda\}$ supplementary difference sets exist. Apply lemma 4;
6	$4r-\{4r+1; 2r; 2r(2r-1)\}$	Number 7 and number 4;
7	$4r-\{4r+1; 2r-1; 2(r-1)(2r-1)\}$	Number 10 with $m=2$, $k=2r$ and lemma 5;
8	$(4r+2)-\{4r+1; 2r; 2r(2r-1)\}$	Number 11 with $m=2$, $k=2r$ and lemma 5;
9	$t-\{6t+1; 3; 1\}$	from Bose [4; series T_2], Peltesohn [20];
10	$m-\{mk+1; k; k-1\}$	$p=mk+1$; from Sprott [9; Series A];
11	$m-\{m(k-1)+1; k; k\}$	$p=m(k-1)+1$; from Sprott [10; Series 1];
12	$m-\{2m(2\lambda+1)+1; 2\lambda+1; \lambda\}$	$p=2m(2\lambda+1)+1$; from Sprott [9; Series B];
13	$m-\{2m(2\lambda-1)+1; 2\lambda; \lambda\}$	$p=2m(2\lambda-1)+1$; from Sprott [9; Series C];
14	$4-\{2k-1; k; 2(k-1)\}$	$p=2k-1$; from Sprott [10; Series 5];
15	$(x+y)-\{4r+1; y{:}2r, x{:}r; k\}$	$p=4r+1$; x, y, k defined in lemma 7;
16	$(\lambda+\mu)-\{4r+1; 2r; k\}$	$p=4r+1$; λ, μ, k defined in lemma 8;
17	$(dq-4k)-\{6q+1; k{:}6, dq-5k{:}3; d\}$	$p=6q+1$; d, k defined in lemma 9;
18	$[n\binom{k+r-2}{r}+m\binom{k+r}{r}]-\{v; k; \binom{k+r-2}{r}\lambda\}$	If $\exists\,(n+m)-\{v; n{:}k, m{:}k+r; \lambda\}$ supplementary difference sets exist. Apply lemma 4.

$2-\{5; 3; 3\}$ supplementary difference sets. It may be that for many orders which have no (v, k, λ) difference set there are supplementary difference sets.

We now consider some constructions and instances of supplementary difference sets. Some results are summarized in table 1.

LEMMA 5. *Let* $(4r+1)$ *(prime power)* $\equiv 1 \pmod 4$. *Then there exist* $2-\{4r+1; 2r+1, 2r; 2r\}$ *supplementary difference sets.*

Proof. If A and B are the incidence matrices of these two supplementary difference sets we wish to show $AA^T+BB^T=(2r+1)I+2rJ$. Define $A-C=Q$ of [7, p. 209], where A and C are $(0, 1)$ matrices. Then $A+C=J-I$ and $Q=2A-J+I$ where Q and hence A is symmetric. Choose $B=A+I$ and since $Q^2=(4r+1)I-J$ and $QJ=0$ we have $A^2+B^2=(2r+1)I+2rJ$ as required.

Let $p=2qr+1$ be a prime power and let ϱ be a generator of the cyclic group G of order $2qr$. Define the subgroups L_i and H_i of G by

$$\begin{aligned} H_i &= \{\varrho^{2jq+i} : 0 \leqslant j \leqslant r-1\} \quad & 0 \leqslant i \leqslant 2q-1 \\ L_i &= \{\varrho^{jq+i} : 0 \leqslant j \leqslant 2r-1\} \quad & 0 \leqslant i \leqslant q-1\,. \end{aligned}$$

Now Sprott [1954] shows that $L_0, \ldots, L_{q-1}$ are supplementary difference sets as are $H_0, \ldots, H_{2q-1}$.

We show that a collection such as

$$L_{i_0}, L_{i_1}, \ldots, L_{i_s}, \underbrace{H_{i_1}, H_{i_1}, \ldots, H_{i_1}}_{j_1 \text{ times}}, \ldots, \underbrace{H_{i_t}, H_{i_t}, \ldots, H_{i_t}}_{j_t \text{ times}}$$

where $s<q-1$ and $t<2q-1$ may be supplementary difference sets. Das and Kulshreshtha's result could then be applied to the L_i to form sets with r elements (as have the H_i). These sets with r elements would then be in suitable form for constructing a BIBD.

First we note that the totality of differences from any L_i are

$$\left.\begin{aligned} &[\varrho^{jq+i} - \varrho^{kq+i} : j \neq k, 1 \leqslant j, k \leqslant 2r] \\ &\qquad = \{\varrho^{kq+i} : 1 \leqslant k \leqslant 2r\}\,[\varrho^{jq-kq} - 1 : j \neq k, 1 \leqslant j \leqslant 2r] \\ &\qquad = L_i\,[\text{sundry elements}] \end{aligned}\right\} \tag{2}$$

$$= a_0 L_0 \ \&\ a_1 L_1 \ \&\ \cdots \ \&\ a_{q-1} L_{q-1} \tag{3}$$

where (2) has $2r(2r-1)$ elements and (3) has $2r(a_0+a_1+\cdots+a_{q-1})$ elements so

$$a_0 + a_1 + \cdots + a_{q-1} = 2r - 1\,.$$

Similarly the totality of differences from any H_i are

$$\begin{aligned} &[\varrho^{2jq+i} - \varrho^{2kq+i} : j \neq k, i \leqslant j, k \leqslant r] \\ &\qquad = H_i\,[\text{sundry elements}] \\ &\qquad = b_0 H_0 \ \&\ b_1 H_1 \ \&\ \cdots \ \&\ b_{2q-1} H_{2q-1} \end{aligned}$$

where

$$b_0 + b_1 + \cdots + b_{2q-1} = r - 1.$$

Now

$$-1 = \varrho^{rq} \quad \text{so}$$

$$-H_i = H_{rq(\bmod 2q)+i} = \begin{cases} H_i & r \text{ even} \\ H_{i+q} & r \text{ odd} \end{cases}$$

and hence, for odd r, $b_i = b_{q+i}$.

A construction with r odd and p (prime power) $=4r+1$

Define

$$\left.\begin{array}{ll} H_i = \{\varrho^{4j+i}: 0 \leqslant j \leqslant r-1\} & i = 0, 1, 2, 3, \\ L_i = \{\varrho^{2j+i}: 0 \leqslant j \leqslant 2r-1\} & i = 0, 1. \end{array}\right\} \tag{4}$$

The differences from H_i are

$$b_0 L_i \;\&\; b_1 L_{i+1} \tag{5}$$

where $2(b_0 + b_1) = r - 1$; the differences from L_i are

$$a_0 L_i \;\&\; a_1 L_{i+1} \tag{6}$$

where $a_0 + a_1 = 2r - 1$.

Then we have

LEMMA 6. *Let S be a collection of sets*

$$\underbrace{H_i, \ldots, H_i}_{x \text{ times}}, \underbrace{L_0, \ldots, L_0}_{y \text{ times}} \qquad i = 0 \text{ or } 1$$

where $4r+1$ is a prime power, r is odd, H_i and L_i are defined above, in (4), *b_0 and a_0 are defined in* (5) *and* (6),

$$x = 2(2r - 1 - 2a_0)\, k / [2(2r-1)\, b_0 - (r-1)\, a_0],$$
$$y = -2(2r - 1 - 2b_0)\, k / [2(2r-1)\, b_0 - (r-1)\, a_0],$$

k is an integer chosen so that x and y are integers, and i is chosen by the rule 'if $a_i > a_{j+i}$ and $b_j > b_{j+i}$, choose $i=1$, otherwise choose $i=0$'. Then S is a collection of

$$(x+y) - \{4r+1; y{:}2r, x{:}r; k\}$$

supplementary difference sets.

Example. For the following primes

Prime	Differences from L_0	Differences from H_0	Supplementary difference sets
13	$2L_0$ & $3L_1$	L_1	L_0, H_1 are 2-$\{13; 6, 3; 3\}$
37	$8L_0$ & $9L_1$	$2L_0$ & $2L_1$	H_0
61	$14L_0$ & $15L_1$	$4L_0$ & $3L_1$	L_0, H_0 are 2-$\{61; 30, 15; 18\}$

Another construction with r odd and p (prime power) $=4r+1$

Let L_i and H_i be as defined above. Now for $p=4r+1$ the two L_i have $2r$ elements and the four H_i have r elements.

We consider the totality of differences from the set

$$\left.\begin{aligned} H_1 \cup H_3 &= \text{differences between elements of } H_1 \\ &\quad \& \text{ differences between elements of } H_3 \\ &\quad \& \text{ [elements of } H_3 - \text{elements of } H_1] \\ &\quad \& - \text{[elements of } H_3 - \text{elements of } H_1] \\ &= (b_1 L_0 \,\&\, b_0 L_1) \,\&\, (b_1 L_0 \,\&\, b_0 L_1) \\ &\quad \& \, H_1 \text{[sundry elements]} \,\&\, - H_1 \text{[sundry elements]} \\ &= (2b_1 L_0 \,\&\, 2b_0 L_1) \,\&\, (eH_0 \,\&\, fH_1 \,\&\, gH_2 \,\&\, hH_3) \\ &\quad \& \, (gH_0 \,\&\, hH_1 \,\&\, eH_2 \,\&\, fH_3) \\ &= xL_0 \,\&\, (2r-1-x)\, L_1, \end{aligned}\right\} \qquad (7)$$

where counting elements we see that $(b_1+b_0)\,2r=r(r-1)$ and $(e+f+g+h)\,r=r^2$ and x is written for $2b_1+e+g$.

Similarly the totality of differences between elements of $H_0 \cup H_2 = (2r-1-x)\, L_0$ $\&\, xL_1$ and between the elements of

$$\left.\begin{aligned} H_0 \cup H_1 &= (b_0 + b_1 + l + n)\, L_0 \,\&\, (b_0 + b_1 + p + m)\, L_1 \\ &= yL_0 \,\&\, (2r-1-y)\, L_1 \end{aligned}\right\} \qquad (8)$$

where x and b_i are as before and $(p+m+l+n)\, r=r^2$. Then

LEMMA 7. *Let S be a collection of* λ *copies of* $H_0 \cup H_1$ *and* μ *copies of* $H_i \cup H_{i+2}$, *where* $4r+1$ *is a prime power, r is odd,* H_i *is defined above in* (4), *x and y are defined in* (7) *and* (8),

$$\lambda = (2r-1-2y)\, k/(2r-1)(u-y), \qquad \mu = -(2r-1-2u)\, k/(2r-1)(u-y),$$

k is an integer so that λ *and* μ *are both integers and i and u are chosen by the rule 'if* $(x>r-\frac{1}{2}$ *and* $y,>r-\frac{1}{2})$ *or* $(x<r-\frac{1}{2}$ *and* $y<r-\frac{1}{2})$ $i=0$, $u=2r-1-x$, *otherwise choose* $i=1$ *and* $u=x$. *Then S is a collection of*

$$(\lambda + \mu) - \{4r+1; 2r; k\}$$

supplementary difference sets.

Example. For the following primes of the form $p=4(6s+3)+1$

Prime	Differences from $H_0 \cup H_1$	Differences from $H_1 \cup H_3$	Supplementary Difference sets	Parameters
13	$3L_0$ & $2L_1$	$3L_0$ & $2L_1$	$H_0 \cup H_1$, $H_0 \cup H_2$	2-{13; 6; 5}
37	$7L_0$ & $10L_1$	$9L_0$ & $8L_1$	$H_0 \cup H_1$, $3(H_1 \cup H_3)$	4-{37; 18; 34}
61	$13L_0$ & $16L_1$	$15L_0$ & $14L_1$	$H_0 \cup H_1$, $3(H_1 \cup H_3)$	4-{61; 30; 58}

A construction with $r=3$ and p (prime power) $=2qr+1$

Define H_i and L_i as before. Then

$$H_i=\{\varrho^{2jq+i}:0\leqslant j\leqslant 2\}\qquad 0\leqslant i\leqslant 2q-1$$
$$L_i=\{\varrho^{jq+i}:0\leqslant j\leqslant 5\}\qquad 0\leqslant i\leqslant q-1\,.$$

The totality of differences from H_i is

$$b_0H_0\ \&\ b_1H_1\ \&\cdots\&\ b_{2q-1}H_{2q-1}$$

and since r is odd this equals

$$b_0L_0\ \&\ b_1L_1\ \&\cdots\&\ b_{q-1}L_{q-1}\,.$$

Now there are six elements in L_i and three in H_i so

$$6\left(b_0+b_1+\cdots+b_{q-1}\right)=6$$

so only one $b_i\neq 0$. Suppose H_{j_i} is the set whose differences are L_i.

Let $S=\{L_{i_1},L_{i_2},\ldots,L_{i_k}\}$, where a given L_j may occur more than once, but where at least one L_i (of those defined above) is not included. Then the totality of differences from elements in S is

$$c_0L_0\ \&\ c_1L_1\ \&\cdots\&\ c_{q-1}L_{q-1}$$

which has $2r(c_0+c_1+\cdots+c_{q-1})$ elements but there are $2r(2r-1)$ differences from L_i and so if we take k sets we have $2r(2r-1)\,k$ differences. Hence

$$c_0+c_1+\cdots+c_{q-1}=(2r-1)\,k=5k\,.$$

Let $d=\max(c_0,c_1,\ldots,c_{q-1})$. Now form

$$T=\underbrace{H_{j_0},H_{j_0},\ldots,H_{j_0}}_{d-c_0\text{ times}},\underbrace{H_{j_1},H_{j_1},\ldots,H_{j_1}}_{d-c_1\text{ times}},\ldots,\underbrace{H_{j_{q-1}},H_{j_{q-1}},\ldots,H_{j_{q-1}}}_{d-c_{q-1}\text{ times}}\,.$$

Then $W=S\ \&\ T$ is a set of

$$(dq-4k)-\{6q+1;k{:}\,6,dq-5k{:}\,3;d\}$$

supplementary difference sets.

Summarizing

LEMMA 8. *Let $p=6q+1$ be a prime power and let ϱ be a primitive root of $GF(p)$, define*

$$H_i=\{\varrho^{2jq+s}:0\leqslant j\leqslant 2\}\,,\quad L_i=\{\varrho^{jq+i}:0\leqslant j\leqslant 5\}\quad \begin{array}{l}0\leqslant i\leqslant q-1\\ 0\leqslant s\leqslant 2q-1\,.\end{array}$$

Let S be a collection of k L_i, where repetitions may occur but at least one of the q L_i is not in S. Suppose the differences from the sets of S are $\&_{i=0}^{q-1} c_i L_i$ and $d=\max(c_i)$. Then there exist

$$(dq-4k)-\{6q+1; k:6, dq-5k:3; d\}$$

supplementary difference sets.

4. Supplementary Difference Sets as Used by Paley, Szekeres and Whiteman

Paley [8], Szekeres [12], [13] and Whiteman [16] have been constructing two $(1,-1)$ matrices A and B of order v satisfying

$$AA^T + BB^T = 2(v+1)I - 2J.$$

The results of these papers imply the existence of $2-\{v; k_1, k_2; k_1+k_2-\frac{1}{2}(v+1)\}$ supplementary difference sets where v is odd.

LEMMA 9. *If v is odd $2-\{v; k_1, k_2; k_1+k_2-\frac{1}{2}(v+1)\}$ supplementary difference sets can only exist if*

(i) $k_1=k_2=\frac{1}{2}(v-1)$;
(ii) $k_1=k_2-1=\frac{1}{2}(v-1)$; *or*
(iii) $k_1=k_2=\frac{1}{2}(v+1)$.

Proof. The equation (1) gives

$$[k_1+k_2-\tfrac{1}{2}(v+1)](v-1) = k_1^2+k_2^2-k_1-k_2$$

so

$$(v^2-1) = k_1(v-k_1)+k_2(v-k_2). \tag{9}$$

Elementary calculus tells us the expression $x(v-x)$ is maximum for $x=\frac{1}{2}v$, which is of course not an integer. The maximum integer value of $x(v-x)$ is $\frac{1}{4}(v^2-1)$ which is attained for $x=\frac{1}{2}(v-1)$ or $\frac{1}{2}(v+1)$.

Hence the only times when (9) is satisfied is when

$$k_i = \tfrac{1}{2}(v\pm 1).$$

5. Williamson-Type Hadamard Matrices

An Hadamard matrix of Williamson-type is one of the form

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{bmatrix}. \tag{10}$$

These are discussed by Williamson [18], Marshall Hall Jr. [7], Baumert and Hall [3], Baumert [2], Whiteman [17] and Goethals and Seidel [6].

In [18] and [7] A, B, C, D are circulant symmetric $(1, -1)$ matrices of order v with first rows given by the $(1 \times v)$ vectors (a_{1i}), (a_{2i}), (a_{3i}) and (a_{4i}) respectively where

$$\begin{aligned} a_{j1} &= +1 \qquad & j = 1, 2, 3, 4 \\ a_{ji} &= a_{j,v+2-i} \qquad & 2 \leqslant i \leqslant v. \end{aligned}$$

Let the sets $S_j = \{i : a_{ji} = +1\}$, $j = 1, 2, 3, 4$ be of order k_j respectively. Then if these sets correspond to an Hadamard matrix they are

$$4 - \{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i - v\} \tag{11}$$

supplementary difference sets.

Since the equation

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

must be satisfied, we have

$$v \sum_{i=1}^{4} k_i - v(v-1) = \sum_{i=1}^{4} k_i^2 \tag{12}$$

and so, as was also shown by Williamson [18, p. 71, equation 16], we have

LEMMA 10. *If* $4-\{v; k_1, k_2, k_3, k_4; \sum_{i-1}^{4} k_i - v\}$ *supplementary difference sets which may be used to construct Williamson-type Hadamard matrices exist then*

$$v \mid \sum_{i=1}^{4} k_i^2 .$$

Multiplying through (12) by 4 and rearranging we have

$$\sum_{i=1}^{4} (2k_i - v)^2 = 4v. \tag{13}$$

6. Williamson-Type Skew Hadamard Matrices

Goethals and Seidel [6] have used a construction similar to that we now give, but our more restrictive equations have always given a solution.

LEMMA 11. *Suppose* a_{ij}, $i = 1, 2, 3, 4$ *and* $j = 1, 2, \ldots, v$, *are each* ± 1 *and satisfy*

$$\begin{cases} a_{j1} = +1 & j = 1, 2, 3, 4 \\ a_{1j} = -a_{1,v+2-j} & \left.\begin{matrix} \\ i = 2, 3, 4 \\ \end{matrix}\right\} 1 \leqslant j \leqslant v. \\ a_{ij} = +a_{i,v+2} & \end{cases} \tag{14}$$

Let A, B, C and D be square matrices with first rows (a_{1j}), (a_{2j}), (a_{3j}) and (a_{4j}) respectively, A being circulant and B, C and D back-circulant; that is,

$$\left.\begin{aligned} A &= a_{11}I + a_{12}T + \cdots + a_{1v}T^{v-1} \\ B &= (a_{21}I + a_{22}T + \cdots + a_{2v}T^{v-1})\,R \\ C &= (a_{31}I + a_{32}T + \cdots + a_{3v}T^{v-1})\,R \\ D &= (a_{41}I + a_{42}T + \cdots + a_{4v}T^{v-1})\,R \end{aligned}\right\} \tag{15}$$

where T and R are $v \times v$ matrices defined by

$$T = \begin{bmatrix} 0 & 1 & - & - & - & 0 & 0 \\ 0 & 0 & - & - & - & 0 & 0 \\ - & - & - & - & - & - & - \\ 0 & 0 & - & - & - & 0 & 1 \\ 1 & 0 & - & - & - & 0 & 0 \end{bmatrix}, \quad R = \begin{bmatrix} 0 & 0 & - & - & - & - & 0 & 0 & 1 \\ 0 & 0 & - & - & - & - & 0 & 1 & 0 \\ - & - & - & - & - & - & - & - & - \\ 0 & 1 & - & - & - & - & 0 & 0 & 0 \\ 1 & 0 & - & - & - & - & 0 & 0 & 0 \end{bmatrix}.$$

Then if

$$AA^T + BB^T + CC^T + DD^T = 4vI_v \tag{16}$$

and H is as given by (10) *above, H is a skew-Hadamard matrix of order* $4v$.

If k_1, k_2, k_3, k_4 are the numbers of positive elements in A, B, C, D respectively, then $k_1 = \frac{1}{2}(v+1)$ and k_2, k_3, k_4 are odd. Then equation (13) may be rewritten

$$\sum_{i=2}^{4} (2k_i - v)^2 = 4v - 1\,; \tag{17}$$

this result was pointed out to us be Professor G. Szekeres.

Now every odd number may be written as the sum of three squares and thus (17), together with k_2, k_3, k_4 being odd, gives the k_i exactly. If in addition we repeat the logic of Williamson's method as given in Marshall Hall, Jr. [7] we get

THEOREM 12. *Suppose v is odd. Let the a_{ij} be given by* (14), *and define P_1, P_2, P_3 and P_4 by*

$$P_1 = \sum_{a_{1j}=1} T^{j-1}, \qquad P_i = \sum_{a_{ij}=1} T^{j-1}R, \quad i = 2, 3, 4.$$

(That is, each P is the sum of those terms of the relevant line of (15) *with positive coefficient.)*

If (16) *is satisfied then we can write*

$$P_1 + P_1^2 = \Sigma g_i T^i$$
$$P_2^2 + P_3^2 + P_4^2 = \Sigma g_i T^i$$

for some integers f_i and g_i, and

$$g_i \equiv f_i \pmod 2 \quad \text{when } i \neq 0\,.$$

Proof. Write the A of (15) as

$$A = P_1 - N_1 \tag{18}$$

where P is as we have defined above; then

$$N_1 = \sum_{a_{1j}=-1} T^{j-1}. \tag{19}$$

In the same way write

$$B = P_2 - N_2, \quad C = P_3 - N_3, \quad D = P_4 - N_4. \tag{20}$$

By (14), $a_{11} = +1$ and $a_{1j} = -a_{1,v+2-j}$ when $2 \leqslant j \leqslant v$, so there are

$$k_1 = \tfrac{1}{2}(v+1) \tag{21}$$

positive summands in A; so the number of summands in P_1 is odd if $v \equiv 1 \pmod 4$ and even if $v \equiv 3 \pmod 4$. For $i=2, 3, 4$, we know by (14) that $a_{i1} = +1$ and $a_{ij} = a_{i,v+2-j}$ for $2 \leqslant j \leqslant v$, so the positive elements (after the first) appear in pairs and their number is odd, so the number k_i of positive summands in P_i is also odd for $i > 1$.

Clearly

$$J = I + T + T^2 + \cdots + T^{v-1} = (I + T + T^2 + \cdots + T^{v-1})R, \tag{22}$$

so

$$P_i + N_i = J, \quad i = 1, 2, 3, 4. \tag{23}$$

Since A is skew-type and B, C and D are symmetric, equation (16) is

$$A(2I - A) + B^2 + C^2 + D^2 = 4vI_v,$$

and using (18), (19), (20), (22) and (23) this becomes

$$(2P_1 - J)(2I - 2P_1 + J) + (2P_2 - J)^2 + (2P_3 - J)^2 + (2P_4 - J)^2 = 4vI.$$

Therefore, since $P_iJ = k_iJ$ and $J^2 = vJ$,

$$4(P_1 - P_1^2 + P_2^2 + P_3^2 + P_4^2) + 4(k_1 - k_2 - k_3 - k_4)J + (2v - 2)J = 4vI. \tag{24}$$

Now from (21)

$$4k_1 + 2v - 2 = 4v$$

so (24) becomes

$$P_1 - P_1^2 + P_2^2 + P_3^2 + P_4^2 = (k_2 + k_3 + k_4 - v)J + vI. \tag{25}$$

Since v, k_2, k_3 and k_4 are all odd, the coefficient of J is always even.

Since P_1 is a polynomial in T with integer coefficients, so is $P_1 - P_1^2$; from (22) the right hand side of (25) is also an integer polynomial in T. So from (25), $P_2^2 + P_3^2 + P_4^2$ is another polynomial in T. If we write

$$\begin{aligned} P_1 + P_1^2 &= \Sigma f_i T^i \\ P_2^2 + P_3^2 + P_4^2 &= \Sigma g_i T^i \\ P_1 - P_1^2 &= \Sigma h_i T^i \end{aligned}$$

then $\Sigma f_i T^i = \Sigma h_i T^i + 2P_1^2$, so $f_i \equiv h_i \pmod 2$ for each i.

Substituting in (25) and comparing coefficients,

$$g_i + h_i = k_2 + k_3 + k_4 - v \quad \text{when } i > 0,$$

so g_i and h_i are congruent (mod 2) when $i>0$. This establishes the Theorem.

We have proved more than was stated in Theorem 12, but the form in the enunciation is that which proves most useful in calculation. Using the techniques outlined in this section we have found for the following orders that the four supplementary difference sets given yield a skew-Hadamard matrix of Williamson-type:

$v = 3: \{1, 3\},\ \{1, 2, 3\},\ \{1\},\ \{1\}$
$v = 5: \{1, 4, 5\},\ \{1, 3, 4\},\ \{1\},\ \{1\}$
$v = 7: \{1, 5, 6, 7\},\ \{1, 4, 5\},\ \{1, 3, 6\},\ \{1\}$
$v = 9: \{1, 5, 7, 8, 9\},\ \{1, 2, 3, 5, 6, 8, 9\},\ \{1, 5, 6\},\ \{1, 2, 4, 7, 9\}$
$v = 11: \{1, 6, 8, 9, 10, 11\},\ \{1, 2, 4, 6, 7, 9, 11\},\ \{1, 2, 4, 5, 8, 9, 11\},\ \{1, 6, 7\}$
$v = 13: \{1, 6, 8, 10, 11, 12, 13\},\ \{1, 2, 3, 4, 7, 8, 11, 12, 13\},$
$\quad \{1, 3, 4, 5, 7, 8, 10, 11, 12\},\ \{1, 2, 5, 7, 8, 10, 13\}$
$v = 15: \{1, 7, 9, 11, 12, 13, 14, 15\},\ \{1, 2, 4, 5, 6, 7, 10, 11, 12, 13, 15\},$
$\quad \{1, 2, 3, 6, 8, 9, 11, 14, 15\},\ \{1, 3, 6, 7, 10, 11, 14\}$
$v = 17: \{1, 7, 10, 11, 13, 14, 15, 16, 17\},\ \{1, 2, 6, 9, 10, 13, 17\},$
$\quad \{1, 2, 6, 8, 11, 13, 17\},\ \{1, 4, 6, 13, 15\}$
$v = 19: \{1, 2, 5, 6, 7, 8, 10, 17, 18\},\ \{1, 2, 8, 9, 12, 13, 19\},$
$\quad \{1, 3, 4, 6, 15, 17, 18\},\ \{1, 5, 7, 10, 11, 14, 16\}.$

7. Using Supplementary Difference Sets to form BIBD's

Suppose the incidence matrices $A_1, \ldots, A_n$ of $n-\{v:k_1, \ldots, k_n; \lambda\}$ supplementary difference sets are placed together thus:

$$B = [A_1 A_2 \ldots A_n].$$

Then B is of order $v \times vn$, each row has constant number of non-zero elements $\sum_{i=1}^{n} k_i$ and the inner product of any two rows is λ. In fact, the only hindrance to B being a BIBD is that B does not have constant column sum.

Readers of Bose [4] and Sprott [9], [10] will see the similarity between the constructions described there and this construction. In fact, Bose's Module Theorems for pure differences may be stated as:

FIRST MODULE THEOREM OF BOSE (FOR PURE DIFFERENCES). *If there are $m-\{v; k; \lambda\}$ supplementary difference sets then there is a BIBD with parameters*

$$(v, b = mv, r = mk, k, \lambda).$$

SECOND MODULE THEOREM OF BOSE (FOR PURE DIFFERENCES). *If there are* $(t+s)-\{v;\, t{:}k,\, s{:}(k-1);\, \lambda\}$ *supplementary difference sets, where* $kt=vs-\lambda$ *and* $(k-1)\,s=\lambda$, *then there is a BIBD with parameters*

$$(v+1,\, b=v(s+t),\, r=vs,\, k,\, \lambda).$$

Using the examples after Lemma 7 we now have that there exist a (37, 148, 72, 18, 34) and a (61, 244, 120, 30, 58) configuration.

COROLLARY 13. *If there exist* $(n+1)-\{v;\, n{:}(k+1),\, k;\, k\}$ *supplementary difference sets and* $v=(n+1)\,k+n$, *then there exists a BIBD with parameters*

$$(v+1,\, (n+1)\,v,\, v,\, k+1,\, k).$$

Bose's First Module Theorem and Lemma 5 ensure

THEOREM 14. *If there is a* (v, k, λ) *difference set and* $r<k$ *then there is a BIBD with parameters*

$$\left(v, \binom{k}{r} v, \binom{k}{r}(k-r), (k-r), \lambda\binom{k-2}{r}\right).$$

In particular for $r=1$

$$(v,\, kv,\, k(k-1),\, k-1,\, \lambda(k-2)).$$

With $r=1$ in Theorem 14 we get from the difference sets (21, 5, 1) and (11, 5, 2) the BIBD's with parameters (21, 105, 20, 4, 2), (11, 55, 20, 4, 6) which are listed as unknown by Sprott [11] but were found by Das and Kulshreshtha [5].

COROLLARY 15. *If there exist* 12-$\{v;\, k;\, \lambda\}$ *supplementary difference sets then there exist a*

(i) $(v,\, 2kv,\, 2k(k-1),\, k-1,\, \lambda(k-2))$-*configuration;*

(ii) $(v+1,\, 2v(k-1),\, kv,\, k,\, \lambda(k-2))$-*configuration, when* $\lambda(k-2)=k(k-1)$ *and* $v=2k-3$ *are also satisfied.*

Proof. This follows using Bose's Module Theorems for Pure Differences and numbers 3 and 4 from table 1.

COROLLARY 16. *If there exist* $(n+m)-\{v;\, n{:}k,\, m{:}k+r;\, \lambda\}$ *supplementary difference sets then there exists a*

$$\left(v,\, sv,\, sk,\, k,\, \binom{k+r-2}{r}\lambda\right)\text{-configuration}$$

where

$$s=n\binom{k+r-2}{r}+m\binom{k+r}{r}.$$

Proof. Use number 20 from table 1, Lemma 5 and Bose's First Module Theorem for Pure Differences.

Then using the 2-$\{61; 30, 15; 18\}$ supplementary difference sets described before we have a $(61, 61(s+t), 15(s+t), 15, 18t)$ configuration where

$$s = \binom{30}{15} \quad \text{and} \quad t = \binom{28}{15}.$$

8. Using Sprott's Series

If $v=2m(2\lambda-1)+1$ in Sprott [9] series B and C then we have $m-\{v; 2\lambda-1; \lambda-1\}$ and $m-\{v; 2\lambda; \lambda\}$ supplementary difference sets respectively. Then applying Bose's Second Module Theorem with the $m-\{v; 2\lambda-1; \lambda-1\}$ sets repeated α times and the $m-\{v; 2\lambda; \lambda\}$ sets repeated β times we have

LEMMA 17. *If* $v=2m(2\lambda-1)+1$ *is a prime power and*

$$m = \frac{(\alpha+\beta)\,\lambda - \alpha}{(2\lambda-1)\,\alpha}$$

then there exists a

$$(v+1, v(\alpha+\beta)\,m, r = \alpha v m, 2\lambda, (2\lambda-1)\,\alpha m)\text{-}configuration.$$

If $v=mk+1$ is a prime power and the supplementary difference sets $m-\{v; k; k-1\}$ from Series A of [9] are repeated α times and the $m-\{v; k+1; k+1\}$ sets from Series 1 of [10] are repeated β times then

LEMMA 18. *If* $v=mk+1$ *is a prime power and*

$$m = \frac{(\alpha+\beta)\,k + (\beta-\alpha)}{\alpha k}$$

then there exists a

$$(v+1, v(\alpha+\beta)\,m, \alpha v m, k+1, \alpha k m)\text{-}configuration.$$

$\alpha=\beta=1, k=2$ gives a (6, 20, 10, 3, 4)-configuration. (A configuration of these parameters can be found by duplicating a (6, 10, 5, 3, 2)-configuration; however, that is not isomorphic to the one we find here.)

Now we examine Sprott's Series A, B, C of [9] and Series 1 of [10] to find when they may be useful in constructing Hadamard matrices.

We use $m=2$ and Sprott's Series of [9] and [10] in the block matrix H of Goethals and Seidel [6], and find

THEOREM 19. *Suppose there exist*

(i) $2-\{2k+1;\, t, u;\, t+u-k\}$ *supplementary difference sets; or*

(ii) $2-\{2k+1;\, t;\, 2t-k\}$ *supplementary difference sets where* $k=t\pm 1$; *or*

(iii) $2-\{2\lambda-1;\, t, u;\, t+u+1-\lambda\}$ *supplementary difference sets; or*

(iv) $2-\{2\lambda-1;\, t;\, 2t+1-\lambda\}$ *supplementary difference sets where* $\lambda=1+t\pm\sqrt{2t}$; *or*

(v) $2-\{8t+t;\, t, u;\, t+u-5\lambda-3\}$ *supplementary difference sets, where the first parameter, v say, is always a prime. Associate with these the two* (2) *supplementary difference sets of Sprott's Series of size v as follows: Series A of* [9] *in cases* (i) *and* (ii), *Series* 1 *of* [10] *in cases* (iii) *and* (iv), *Series B of* [9] *in the case* (v). *If the four incidence matrices in the particular case are circulant then there is an Hadamard matrix of order* $4v$. *If one of the matrices is circulant and skew-type and the other three are circulant then there is a skew-Hadamard matrix of order* $4v$.

REFERENCES

[1] BAUMERT, L. D., *Cyclic Difference Sets* (Springer-Verlag, Berlin–New York, 1971).

[2] BAUMERT, L. D. and HALL, M. JR., *Hadamard Matrices of the Williamson Type*, Math. Comp. *19*, 442–447 (1965).

[3] BAUMERT, L. D. and HALL, M. JR., *A New Construction for Hadamard Matrices*, Bull. Amer. Math. Soc. *71*, 169–170 (1965).

[4] BOSE, R. C., *On the Construction of Balanced Incomplete Block Designs*, Ann. Eugenics *9*, 353–399 (1939).

[5] DAS, M. N. and KULSHRESHTHA, A. C., *On Derivation of Initial Blocks of B.I.B. Designs with More Than One Block*, Austral. J. Statist. *10* (2), 75–82 (1968).

[6] GOETHALS, J. M. and SEIDEL, J. J., *A Skew Hadamard Matrix of Order 36*, J. Austral. Math. Soc. *11*, 343–344 (1970).

[7] HALL, M. JR., *Combinatorial Theory* (Blaisdell, Waltham, Mass., 1967).

[8] PALEY, R. E. A. C., *On Orthogonal Matrices*, J. Math. and Phys. *12*, 311–320 (1933).

[9] SPROTT, D. A., *A Note on Balanced Incomplete Block Designs*, Canad. J. Math. *6*, 341–346 (1954).

[10] SPROTT, D. A., *Some Series of Balanced Incomplete Block Designs*, Sankhya Ser. A *17*, 185–192 (1956).

[11] SPROTT, D. A., *Listing of BIB Designs from r=16 to 20*, Sankhya Ser. A *24* 203–204 (1962).

[12] SZEKERES, G., *Tournaments and Hadamard Matrices*, Enseignement Math. *15*, 269–278 (1969).

[13] BLATT, D. and SZEKERES, G., *A Skew-Hadamard Matrix of Order 52*, Canad. J. Math. *22*, 1319–1322 (1970).

[14] TURYN, R., *An Infinite Class of Williamson Matrices*, J. Combinatorial Theory (to appear).

[15] LINT, J. H. and SEIDEL, J. J., *Equilateral Point Sets in Elliptic Geometry*, Indag. Math. *28*, 335–348 (1969).

[16] WHITEMAN, A. L., *An Infinite Family of Skew-Hadamard Matrices*, (to appear).

[17] WHITEMAN, A. L., *An Infinite Family of Hadamard Matrices of Williamson Type*, (to appear).

[18] WILLIAMSON, J., *Hadamard's Determinant Theorem and the Sum of Four Squares*, Duke Math. J. *11*, 65–81 (1944).

[19] RAO, C. RADHAKRISHNA, *A Study of BIB Designs with Replications 11 to 15*, Sankhya *23*, 117–127 (1961).

[20] PELTESOHN, R., *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math. *6*, 251–257 (1939).

University of Newcastle