COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
10. INFINITE AND FINITE SETS, KESZTHELY (HUNGARY), 1973.

SOME REMARKS ON SUPPLEMENTARY DIFFERENCE SETS

JENNIFER SEBERRY WALLIS

1. INTRODUCTION AND DEFINITIONS

Let $S_1, S_2, \ldots, S_n$ be subsets of V, a finite abelian group of order v written in additive notation, 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.* Throughout this paper this will be abbreviated as sds.

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

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

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

We shall be concerned with collections, (denoted by square brackets [ ]) defined on a fixed group V of order v, 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 and T_2 will denote the result of adjoining the elements of T_1 to T_2 with total multiplicities retained. For example: $x_1, x_2, x_3 \in V$ and $T_1 = [x_1, x_2, x_3, x_3]$, $T_2 = [x_1, x_2, x_4]$ then

(3) $T_1 + T_2 = [x_1, x_1, x_2, x_2, x_2, x_3, x_4]$.

Suppose $x_1, x_2, \ldots, x_v$ are the elements of V ordered in some fixed way. Let X be a subset of V. Further let φ and ψ be two maps from V into a commutative ring with unity (1). Then the matrix $M = [m_{ij}]$ of order v defined by

(4) $m_{ij} = \psi(x_j - x_i)$

will be called *type* 1 and the matrix $N = [n_{ij}]$ of order v defined by

(5) $n_{ij} = \varphi(x_j + x_i)$

will be called *type* 2.

If φ and ψ are defined by

(6) $$\varphi(x) = \psi(x) = \begin{cases} 1 & x \in X, \\ 0 & x \notin X, \end{cases}$$

then M and N will be called the *type* 1 *incidence matrix of* X *(in* V*)* and the *type* 2 *incidence matrix of* X *(in* V*)*, respectively. These are discussed further in [10].

Notation. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a k-set then we will use ΔA for the collection of differences between distinct elements of A, i.e.,

$$\Delta A = [a_i - a_j : i \neq j,\ 1 \leqslant i, j \leqslant k].$$

Notation. If $k_1 = k_2 = \ldots = k_n = k$ we will write $n - \{v; k; \lambda\}$ to denote $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ sds. If $k_1 = k_2 = \ldots = k_i, k_{i+1} =$

$= k_{i+2} = \ldots = k_{i+j}, \ldots, k_l = \ldots = k_n$ then we will sometimes write $n - \{v;\ i\colon k_1,\ j\colon k_{i+1}, \ldots;\ \lambda\}$. A (v, k, λ) difference set repeated n-times will be denoted $n - (v, k, \lambda)$.

A *balanced incomplete block design* or BIBD (v, b, r, k, λ) may be considered to be 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 pair of distinct row vectors is λ. B satisfies

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

where I is the identity matrix and J the matrix of all 1's.

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 $R^T = -R$.

2. CYCLOTOMY

We now turn to Storer [2; p. 24-25] for the elementary theory of cyclotomy:

Let x by a primitive root of $F = GF(q)$ where $q = q^\alpha = ef + 1$ is a prime power. Write $G = \langle x\rangle \setminus \{0\}$. The *cyclotomic classes* C_i in F are:

$$C_i = \{x^{es+i}\colon s = 0, 1, \ldots, f-1\} \quad i = 0, 1, \ldots, e-1\ .$$

We note that C_i are pairwise disjoint and their union is G.

For fixed i and j, the *cyclotomic number* (i, j) is defined to be the number of solutions of the equation

$$z_i + 1 = z_j \quad (z_i \in C_i,\ z_j \in C_j)\ ,$$

where $1 = x^0$ is the multiplicative unit of F. That is (i, j) is the number of ordered pairs s, t such that

$$x^{es+i} + 1 = x^{et+j} \quad (0 \leqslant s,\ t \leqslant f-1)\ .$$

Note that the number of times

$$x^{es+i} - x^{et+k} \in C_j$$

is the number of solutions of

$$x^{es+i} - x^{et+k} = x^{er+j}$$

$$x^{et+k} + x^{er+j} = x^{es+i}$$

$$x^{e(t-r)+k-j} + 1 = x^{e(s-r)+i-j}$$

which is the cyclotomic number $(k-j, i-j)$. Using [2, p. 25]

$$(k-j, i-j) = (e-(j-k), (i-k)-(j-k)) = (j-k, i-k) .$$

Hence

$$\begin{aligned}
\Delta C_i &= [x^{es+i} - x^{et+i}:\ s \neq t,\ 0 \leqslant s,\ t \leqslant f-1] = \\
&= [x^{es+i} - x^{et+i}:\ 0 \leqslant s,\ t \leqslant f-1]/f\{0\} = \\
&= (-i, 0)C_0 + (1-i, 0)C_1 + (2-i, 0)C_2 + \ldots \\
\ldots &= (0, 0)C_i + (1, 0)C_{i+1} + (2, 0)C_{i+2} + \ldots
\end{aligned}$$

and

$$\begin{aligned}
\Delta(C_i - C_j) = {} & (-i, 0)C_0 + (1-i, 0)C_1 + \ldots \\
& \ldots + (-j, 0)C_0 + (1-j, 0)C_1 + \ldots \\
& \ldots + (-j, i-j)C_0 + (1-j, i-j)C_1 + \ldots \\
& \ldots + (-i, j-i)C_0 + (1-i, j-i)C_1 + \ldots \\
& = (0, 0)C_j + (1, 0)C_{j+1} + \ldots \\
& \ldots + (0, 0)C_i + (1, 0)C_{i+1} + \ldots \\
& \ldots + (0, i-j)C_j + (1, i-j)C_{j+1} + \ldots \\
& \ldots + (0, j-i)C_i + (1, j-i)C_{i+1} + \ldots
\end{aligned}$$

3. SOME KNOWN APPLICATIONS OF SDS

Perhaps the most important application of *sds* is in constructing BIBD's. Here the module theorems of Bose are used, viz.,

If there exist $m - \{v; k; \lambda\}$ sds then there exists a BIBD $(v, b = mv, r = mk, k, \lambda)$.

If there exist $(t + s) - \{u = kt/s + k - 1;\ t:\ k,\ s:\ (k - 1);\ \lambda = (k - 1)s\}$ sds then there exists a BIBD

$$(kt/s + k, b = u(s + t), r = us, k, \lambda = (k - 1)s)\ .$$

In [6] it is pointed but that

If there exist $(n + m) - \{v; n:\ k, m:\ (k + r); \lambda\}$ sds then there exist $\left[n\binom{k+r-2}{r} + m\binom{k+r}{r}\right] - \left\{v; k; \binom{k+r-2}{r}\lambda\right\}$ sds.

Similarly, if there exist $n - \{v; k_1, k_2, \ldots, k_n; \lambda\}$ sds there exist $n' - \{v; k; \lambda'\}$ sds for some n', λ' and $k \leqslant \min(k_1, k_2, \ldots, k_n)$. Also in [6] and [7] a number of constructions, by various authors, are quoted.

Sds have also proved to be very important in constructing Hadamard matrices. In particular the existence of

(i) $4 - \left\{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i - v\right\}$ sds; or

(ii) $4 - \left\{v; k_1, k_2, k_3, k_4; \sum_{i=1}^{4} k_i - v - 1\right\}$ sds (here necessarily $k_i = \frac{1}{2}(v \pm 1)$ for v odd or $k_1 = \frac{1}{2}(v \pm 2)$, $k_2 = k_3 = k_4 = \frac{1}{2}v$ for v even); or

(iii) $2 - \left\{v; k_1, k_2; k_1 + k_2 - \frac{1}{2}v\right\}$ sds (here v is necessarily even); or

(iv) $2 - \left\{v; k_1, k_2; k_1 + k_2 - \frac{1}{2}(v + 1)\right\}$ sds (here v is necessarily odd)

imply the existence of Hadamard matrices of order

(i) $4v$;

(ii) $4(v+1)$;

(iii) $2v$;

(iv) $2(v+1)$; respectively.

Sds which can be used to form Hadamard matrices of various types can be found, using cylotomy, in the following cases:

(i) $2-\{4f+1; 2f; 2f-1\}$ sds when $4f+1$ is a prime power, [10, p. 282];

(ii) $2-\{4f+1; 2f; 2f-1\}$ sds when $4f+1 \equiv 5 \pmod 8 = s^2+4$ is a prime power, [4], [5];

(iii) $4-\{4f+1; 2f; 4f-2\}$ sds when $4f+1 \equiv 5 \pmod 8 = s^2+36$ is a prime power, [5];

(iv) $2-\{2f+1; f; f-1\}$ sds when $2f+1 \equiv 5 \pmod 8$ is a prime power, [10, p. 321];

(v) $2-\{8f+1; 4f; 4f-1\}$ sds when $8f+1 = p^t$ is a prime power, $p \equiv 5 \pmod 8$, $t \equiv 2 \pmod 4$ [10, p. 323];

(vi) $4-\{8f+1; 4f; 2(2f-1)\}$ sds when $8f+1 \equiv 9 \pmod{16}$ is a prime power, [10, p. 334].

4. CONSTRUCTIONS FOR SDS

The case $e = 2$.

The cyclotomic matrices and constraints are:

	0	1	
0	A	B	$2A = f-1$
1	A	A	$A+B=f$

f odd

	0	1	
0	A	B	$2B = f$
1	B	B	$A+B=f-1$

f even

Using these cyclotomic matrices, we have

Lemma 1. *If* $q = 2f + 1$ *(*f *even), then* C_0, C_1 *are* $2 - \{2f + 1; 2 - \{2f + 1; f; f - 1\}$ sds.

Proof.

$$\Delta C_0 + \Delta C_1 = AC_0 + BC_1 + BC_0 + AC_1 = (f - 1)G \setminus \{0\} .$$

Lemma 2. *If* $q = 2f + 1$ *(*f *even), then* C_0, $\{0\} + C_0$ *are* $2 - \{2f + 1; f, f + 1; f\}$ sds.

Proof.

$$\Delta C_0 + \Delta(\{0\} + C_0) = AC_0 + BC_1 + (A + 2)C_0 + BC_1 =$$
$$= fG \setminus \{0\} .$$

The case $e = 4$:

The cyclotomic matrices and constraints are

	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

$$2A + 2E = f - 1$$
$$B + D + 2E = f$$
$$A + B + C + D = f$$

f odd

	0	1	2	3
0	A	B	C	D
1	B	D	E	E
2	C	E	C	E
3	D	E	E	B

$$A + B + C + D = f - 1$$
$$B + D + 2E = f$$
$$2C + 2E = f$$

f even

where for f odd, we have

$$16A = q - 7 + 2s$$
$$16B = q + 1 + 2s - 8t$$
$$16C = q + 1 - 6s$$
$$16D = q + 1 + 2s + 8t$$
$$16E = q - 3 - 2s$$

and for f even

$$16A = q - 11 - 6s$$
$$16B = q - 3 + 2s + 8t$$
$$16C = q - 3 + 2s$$
$$16D = q - 3 + 2s - 8t$$
$$16E = q + 1 - 2s$$

where $q = s^2 + 4t^2$, $s \equiv 1 \pmod 4$ is the proper representation of q if $p \equiv 1 \pmod 4$; the sign of t is ambiguously determined.

Lemma 3. *If $q = 4f + 1$ (f odd), then C_0, C_1 or C_0, C_3 are* $2 - \left\{4f + 1; f; \frac{1}{2}(f - 1)\right\}$ sds.

Proof.

$$\Delta C_0 + \Delta C_1 = \Delta C_0 + \Delta C_3 =$$
$$= AC_0 + EC_1 + AC_2 + EC_3 +$$
$$+ EC_0 + AC_1 + EC_2 + AC_3 =$$
$$= \frac{1}{2}(f - 1)G \setminus \{0\}.$$

Lemma 4. *If $q = 4f + 1$ (f odd), then $\{0\} + C_0$, $\{0\} + C_1$ are* $2 - \left\{4f + 1; f + 1; \frac{1}{2}(f + 1)\right\}$ sds.

Proof.

$$\Delta(\{0\} + C_0) + \Delta(\{0\} + C_1) = (A + 1)C_0 + EC_1 +$$
$$+ (A + 1)C_2 + EC_3 + EC_0 +$$
$$+ (A + 1)C_1 + EC_2 + (A + 1)C_3$$

Lemma 5. *If* $q = 4f + 1$ *(*f *odd), then* $A_1 = C_0 + C_1$ *and* $A_2 = C_0 + C_3$ *are* $2 - \{4f + 1; 2f; 2f - 1\}$ sds *with the property that* $a \in A_i \Rightarrow -a \notin A_i$, $i = 1, 2$.

Proof.

$$\Delta(C_0 + C_1) + \Delta(C_0 + C_3) = AC_0 + EC_1 + AC_2 + EC_3 +$$
$$+ EC_0 + AC_1 + EC_2 + AC_3 +$$
$$+ BC_0 + EC_1 + EC_2 + DC_3 +$$
$$+ EC_0 + DC_1 + BC_2 + EC_3 +$$
$$+ AC_0 + EC_1 + AC_2 + EC_3 +$$
$$+ EC_0 + AC_1 + EC_2 + AC_3 +$$
$$+ DC_0 + BC_1 + EC_2 + EC_3 +$$
$$+ EC_0 + EC_1 + DC_2 + BC_3 =$$
$$= (2f - 1)G \setminus \{0\}.$$

Since f is odd, $-1 \in C_2$, and we have the result.

Lemma 6. *If* $q = s^2 + 4t^2 = 4f + 1$ *(*f *odd), then* $A = C_0 + C_1$ *and* $|t|$ *copies of* $B = C_0 + C_2$ *are* $(|t| + 1) - \left\{4f + 1; 2f; \frac{1}{2}(|t| + 1)(2f - 1)\right\}$ sds *with the properties* $a \in A \Rightarrow -a \notin A$, $b \in B \Rightarrow$ $\Rightarrow -b \in B$.

Proof. $a \in A \Rightarrow -a \notin A$, $b \in B \Rightarrow -b \in B$ follows because f is odd and $-1 \in C_2$. We choose our primitive root so that t is negative, i.e., $|t| = -t$.

$$\Delta(C_0 + C_1) + |t|\Delta(C_0 + C_2) = AC_0 + EC_1 + AC_2 + EC_3 +$$
$$+ EC_0 + AC_1 + EC_2 + AC_3 +$$
$$+ BC_0 + EC_1 + AC_2 + DC_3 +$$
$$+ EC_0 + DC_1 + BC_2 + EC_3 +$$
$$+ |t|\{2AC_0 + 2EC_1 + 2AC_2 + 2EC_3 +$$
$$+ \quad CC_0 + DC_1 + AC_2 + BC_3 +$$
$$+ \quad AC_0 + BC_1 + CC_2 + DC_3\} =$$
$$= \frac{1}{16}[(4q - 12 - 8t)(C_0 + C_2) +$$
$$+ (4q - 12 + 8t)(C_1 + C_3) +$$
$$+ |t|(4q - 20)(C_0 + C_2) +$$
$$+ |t|(4q - 4)(C_1 + C_3)] =$$
$$= \frac{1}{16}[(4q(1 - t) - 12 + 12t)G \setminus \{0\}] =$$
$$= \frac{1}{2}(2f - 1)(|t| + 1)G \setminus \{0\}.$$

Lemma 7. *If* $q = 25 + 4t^2 = 4f + 1$ *(f odd), then* $C_0 + C_2$, C_0 *are* $2 - \left\{4f + 1; 2f, f; \frac{1}{4}(5f - 3)\right\}$ sds.

Proof.

$$\Delta(C_0 + C_2) + \Delta C_0 = \frac{1}{16}((4q - 20)(C_0 + C_2) + (4q - 4)(C_1 + C_3) +$$
$$+ A(C_0 + C_2) + E(C_1 + C_3)) =$$
$$= \frac{1}{16}((5q - 27 + 2s)(C_0 + C_2) +$$
$$+ (5q - 7 - 2s)(C_1 + C_3)) =$$

$$= \frac{1}{16}((5q - 17)G \setminus \{0\}) =$$

$$= \frac{1}{4}(5f - 3)G \setminus \{0\}, \quad \text{where} \quad s = 5.$$

Lemma 8. *If* $q = 9 + 4t^2 = 4f + 1$ *(f odd) then* $C_0 + C_2$, C_1 *are* $2 - \left\{4f + 1; 2f, f; \frac{1}{4}(5f - 3)\right\}$ sds.

Proof.

$$\Delta(C_0 + C_2) + \Delta C_1 = (5q - 23 - 2s)(C_0 + C_2) +$$

$$= (5q - 11 + 2s)(C_1 + C_3) =$$

$$= \frac{1}{16}((5q - 17)G \setminus \{0\}) =$$

$$= \frac{1}{4}(5f - 3)G \setminus \{0\}, \quad \text{where} \quad s = -3.$$

Lemma 9. *If* $q = s^2 + 4t^2 = 4f + 1$ *(f odd), then* $|s - 1|$ *copies of* $(C_0 + C_1)$ *and*

(i) for $s > 0$ $4|t|$ *copies of* C_0,

(ii) *for* $s < 0$ $4|t|$ *copies of* C_1,

are $(|s - 1| + 4|t|) - \left\{4f + 1; |s - 1|: 2f, |t|: f; \frac{1}{2}((2f - 1)(|s - 1| + |t|)\right\}$ sds.

Proof. We choose the primitive root so that $t = |t|$. Now

$$|s - 1|\Delta(C_0 + C_1) = \frac{1}{16}(|s - 1|(4q - 12 - 8t)(C_0 + C_2) +$$

$$+ |s - 1|(4q - 12 + 8t)(C_1 + C_3))$$

$$4t\Delta C_0 = \frac{1}{16}(4t(q - 7 + 2s)(C_0 + C_2) +$$

$$+ 4t(q - 3 - 2s)(C_1 + C_3))$$

$$4t\Delta C_1 = \frac{1}{16}(4t(q-3-2s)(C_0+C_2)+$$

$$+4t(q-7+2s)(C_1+C_3))\,,$$

so for $s>0$, $|s-1|=s-1$ and

$$|s-1|\Delta(C_0+C_1)+4t\Delta C_0 = \frac{1}{4}((q-3)(s-1+t)-2t)G/\{0\};$$

while for $s<0$, $|s-1|=1-s$ and

$$|s-1|\Delta(C_0+C_1)+4t\Delta C_1 = \frac{1}{4}((q-3)(1-s+t)-2t)G/\{0\},$$

which gives the result.

Lemma 10. *If* $q=4f+1$ *(*f *even), then* C_0, C_1, C_2, C_3 *are* $4-\{4f+1; f; f-1\}$ sds *and* $\{0\}+C_0$, $\{0\}+C_1$, $\{0\}+C_2$, $\{0\}+C_3$ *are* $4-\{4f+1; f+1; f+1\}$ sds.

Proof.

$$\Delta C_0+\Delta C_1+\Delta C_2+\Delta C_3 = (A+B+C+D)G\setminus\{0\} =$$

$$=(f-1)G\setminus\{0\}\,.$$

Lemma 11. *If* $q=1+4t^2=4f+1$ *(*f *even), then* C_0+C_2, C_1, C_3 *are* $3-\left\{4f+1; 2f, f; \frac{1}{2}(3f-2)\right.$ sds *and* $\{0\}+C_0+C_2$, $\{0\}+C_1$, $\{0\}+C_3$ *are* $\left.3-\ 4f+1; 2f+1, f+1, f+1; \frac{1}{2}(3f+2)\right\}$ sds.

Proof.

$$\Delta(C_0+C_2)+\Delta C_1+\Delta C_3 = (A+B+C+D+2C)(C_0+C_2)+$$

$$+(A+B+C+D+2E)(C_1+C_3)=$$

$$=\left(f-1+\frac{1}{4}(2f-1+s)\right)(C_0+C_2)+$$

$$+\left(f-1+\frac{1}{4}(2f+1-s)\right)(C_1+C_3)+$$

$$=\frac{1}{2}(3f-2)G\setminus\{0\}\,,\quad \text{with}\quad s=1\,.$$

Lemma 12. *If* $q = 25 + 4t^2 = 4f + 1$ *(f even), then* $C_0 + C_2$, $\{0\} + C_1$, $\{0\} + C_3$ *are* $3 - \{4f + 1; 2f, f + 1; 3f/2\}$ sds *(here* $s = 5$*).*

Lemma 13. *If* $q = 9 + 4t^2 = 4f + 1$ *(f even), then* $\{0\} + C_0 + C_2$, $\{0\} + C_1$, $\{0\} + C_3$ *are* $3 - \{4f + 1; 2f + 1, f, f; 3f/2\}$ sds *(here* $s = -3$*).*

Lemma 14. $q = s^2 = 4f + 1$ *(f even), then* $C_0 + C_1$, $C_2 + C_3$ *are* $2 - \{4f + 1; 2f; 2f - 1\}$ sds *and* $\{0\} + C_0 + C_1$, $\{0\} + C_2 + C_3$ *are* $2 - \{4f + 1; 2f + 1; 2f + 1\}$ sds.

Proof.

$$\begin{aligned}\Delta(C_0 + C_1) + \Delta(C_2 + C_3) = {} & \Delta C_0 + \Delta C_1 + \Delta C_2 + \Delta C_3 + \\ & + BC_0 + EC_1 + EC_2 + DC_3 + \\ & + EC_0 + DC_1 + BC_2 + EC_3 + \\ & + EC_0 + DC_1 + BC_2 + EC_3 + \\ & + BC_0 + EC_1 + EC_2 + DC_3 + \\ & = (2f - 1)G \setminus \{0\}, \quad \text{where} \quad t = 0.\end{aligned}$$

Lemma 15. *If* $q = 4f + 1$ *(f even), then* $C_0 + C_1$, $C_1 + C_2$, $C_2 + C_3$, $C_3 + C_0$ *are* $4 - \{4f + 1; 2f; 2(2f - 1)\}$ sds.

The case $e = 6$:

The cyclotomic matrix for $e = 6$ (f odd) is

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	E	C	I
2	H	J	G	F	I	B
3	A	G	H	A	G	H
4	G	F	I	B	H	J
5	H	I	E	C	I	G

$$2A + 2G + 2H = f - 1$$

$$B + F + G + H + I + J = f$$

$$C + E + G + H + 2I = f$$

$$A + B + C + D + E + F = f,$$

and in this case, the cyclotomic numbers are given by the relations

$$72A = 2q - 22 - 8x - 2a + 2c$$

$$72B = 2q + 2 - 3a - c - 9b + 9d$$

$$72C = 2q + 2 - 8x + a - c + 24y - 3b - 9d$$

$$72D = 2q + 2 + 24x + 6a + 2c$$

$$72E = 2q + 2 - 8x + a - c - 24y + 3b + 9d$$

$$72F = 2q + 2 - 3a - c + 9b - 9d$$

$$72G = 2q - 10 + 4x + a - c + 12y + 3b + 9d$$

$$72H = 2q - 10 + 4x + a - c - 12y - 3b - 9d$$

$$72I = 2q + 2 + 4x - 2a + 2c$$

$$72J = 2q + 2 - 12x + 6a + 2c$$

where $q = x^2 + 3y^2$, $4q = a^2 + 3b^2 = c^2 + 27d^2$.

Lemma 16. *If* $q = 6f + 1$ *(f odd),* C_0, C_1, C_2 *are* $3 - \{6f + 1; f; \frac{1}{2}(f-1)\}$ sds *and* $\{0\} + C_0$, $\{0\} + C_1$, $\{0\} + C_2$ *are* $3 - \{6f + 1; f + 1; \frac{1}{2}(f+1)\}$ sds.

Lemma 17. *If* $q = 6f + 1$ *(f odd),* $C_0 + C_i$, $C_1 + C_{i+1}$, $C_2 + C_{i+2}$, $i = 1, 2,$ *or* 3, *are* $3 - \{6f + 1; 2f; 2f - 1\}$ sds *and* $\{0\} + C_0 + C_i$, $\{0\} + C_1 + C_{i+1}$, $\{0\} + C_2 + C_{i+2}$, $i = 1, 2,$ *or* 3 *are* $3 - \{6f + 1; 2f + 1; 2f + 1\}$ sds.

The case $e = 8$:

The cyclotomic matrix for $e = 8$ (f odd) is

	0	1	2	3	4	5	6	7
0	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
1	*I*	*J*	*K*	*L*	*F*	*D*	*L*	*M*
2	*N*	*O*	*N*	*M*	*G*	*L*	*C*	*K*
3	*J*	*O*	*O*	*I*	*H*	*M*	*K*	*B*
4	*A*	*I*	*N*	*J*	*A*	*I*	*N*	*J*
5	*I*	*H*	*M*	*K*	*B*	*J*	*O*	*O*
6	*N*	*M*	*G*	*L*	*C*	*K*	*N*	*O*
7	*J*	*K*	*L*	*F*	*D*	*L*	*M*	*I*

$$2A + 2I + 2J + 2N = f - 1$$

$$B + H + I + J + K + M + 20 = f$$

$$C + G + K + L + M + 2N + 0 = f$$

$$D + F + I + J + K + 2L + M = f$$

$$A + B + C + D + E + F + G + H = f$$

and the cyclotomic numbers are given by the relations:

I. If 2 is a fourth power in G	II. If 2 is not a fourth power in G
$64A = q - 15 - 2x$	$64A = q - 15 - 10x - 8a$
$64B = q + 1 + 2x - 4a + 16y$	$64B = q + 1 + 2x - 4a - 16b$
$64C = q + 1 + 6x + 8a - 16y$	$64C = q + 1 - 2x + 16y$
$64D = q + 1 + 2x - 4a - 16y$	$64D = q + 1 + 2x - 4a - 16b$
$64E = q + 1 - 18x$	$64E = q + 1 + 6x + 24a$
$64F = q + 1 + 2x - 4a + 16y$	$64F = q + 1 + 2x - 4a + 16b$
$64G = q + 1 + 6x + 8a + 16y$	$64G = q + 1 + 2x - 16y$
$64H = q + 1 + 2x - 4a - 16y$	$64H = q + 1 + 2x - 4a + 16b$
$64I = q - 7 + 2x + 4a$	$64I = q - 7 + 2x + 4a + 16y$
$64J = q - 7 + 2x + 4a$	$64J = q - 7 + 2x + 4a - 16y$
$64K = q + 1 - 6x + 4a + 16b$	$64K = q + 1 + 2x - 4a$
$64L = q + 1 + 2x - 4a$	$64L = q + 1 - 6x + 4a$
$64M = q + 1 - 6x + 4a - 16b$	$64M = q + 1 + 2x - 4a$
$64N = q - 7 - 2x - 8a$	$64N = q - 7 + 6x$
$640 = q + 1 + 2x - 4a$	$640 = q + 1 - 6x + 4a$

where x, y, a and b are specified by:

I. $q = x^2 + 4y^2$, $x \equiv 1 \pmod 4$ is the unique proper representation of $q = p^\alpha$ if $p \equiv 1 \pmod 4$; otherwise,

$$q = (\pm p^{\alpha/2})^2 + 4.0^2; \quad \text{i.e.,} \quad x = \pm p^{\alpha/2}, \quad y = 0 .$$

II. $q = a^2 + 2b^2$, $a \equiv 1 \pmod 4$ is the unique proper representation of $q = p^\alpha$ if $p \equiv 1$ or $3 \pmod 8$; otherwise,

$$q = (\pm p^{\alpha/2})^2 + 2.0^2; \quad \text{i.e.,} \quad a = \pm p^{\alpha/2}, \quad b = 0 .$$

The signs of y and b are ambiguously determined.

Lemma 18. *If* $q = 8f + 1$ *(*f *odd),* C_0, C_1, C_2, C_3 *are* $4 - 4 - \left\{8f + 1; f; \frac{1}{2}(f-1)\right\}$ sds *and* $\{0\} + C_0$, $\{0\} + C_1$, $\{0\} + C_2$ $\{0\} + C_3$ *are* $4 - \left\{8f + 1; f + 1; \frac{1}{2}(f+1)\right\}$ sds.

Lemma 19. *If* $q = 8f + 1 = 1 + 2b^2$ *(*$f \equiv 1 \pmod 4$*) and* 2 *is a 4-th power, then* C_0, C_1 *are* $2 - \left\{8f + 1; f; \frac{1}{4}(f-1)\right\}$ sds *and* $\{0\} + C_0$, $\{0\} + C_1$ *are* $2 - \left\{8f + 1; f + 1; \frac{1}{4}(f+1)\right\}$ sds.

Proof.

$$\Delta C_0 + \Delta C_1 = (A + J)(C_0 + C_4) + (I + A)(C_1 + C_5) +$$
$$+ (N + I)(C_2 + C_6) + (J + N)(C_3 + C_7) =$$
$$= \frac{1}{4}(f-1)G \setminus \{0\}, \quad \text{when} \quad a = 1.$$

Lemma 20. *If* $q = 8f + 1 = 49 + 2b^2$ *(*$f \equiv -1 \pmod 4$*) and* 2 *is a 4-th power, then* $\{0\} + C_0$, $\{0\} + C_1$ *are* $2 - \left\{8f + 1; f + 1; \frac{1}{4}(f+1)\right\}$ sds.

Proof.

$$\Delta(\{0\} + C_0) + \Delta(\{0\} + C_1) = (A + J + 1)(C_0 + C_4) +$$
$$+ (A + I + 1)(C_1 + C_5) +$$
$$+ (N + I)(C_2 + C_6) +$$
$$+ (J + N)(C_3 + C_7) +$$
$$= \frac{1}{4}(f+1)G \setminus \{0\}, \quad \text{when} \quad a = -7.$$

Lemma 21. *If* $q = 8f + 1 = 81 + 4y^2 = 9 + 2b^2$ *(*f *odd) is a prime power and* 2 *is a fourth power in* G, C_0 *and* $\{0\} + C_0$ *are each repeated* 4 *times, are* $8 - \{8f + 1; 4{:}f, 4{:}(f+1); f\}$ sds.

Proof.

$$\Delta C_0 + \Delta(\{0\} + C_0) = (2A + 1)(C_0 + C_4) + 2I(C_1 + C_5) +$$
$$+ 2N(C_2 + C_6) + 2J(C_3 + C_7) =$$
$$= [(2q + 34 - 4x)(C_0 + C_4) +$$
$$+ (2q - 14 + 4x + 8a)(C_1 + C_3 + C_5 + C_7) +$$
$$+ (2q - 14 - 4x - 16a)(C_2 + C_6)]/64 =$$
$$= \frac{(2q-2)}{64} G \setminus \{0\} \quad \text{with} \quad a = -3,\ x = 9 .$$

Lemma 22. *If* $q = 8f + 1 = (-3)^2 + 2b^2$ *(i.e.,* $a = -3$*) then* C_0, $C_1, \{0\} + C_0$, $\{0\} + C_1$ *each repeated twice are* $8 - \{8f + 1; 4{:}f, 4{:}(f + 1); f\}$ sds *when* 2 *is a fourth power in* G.

Proof.

$$\Delta C_0 + \Delta C_1 + \Delta(\{0\} + C_0) + \Delta(\{0\} + C_1) =$$
$$= [(4q + 20 + 8a)(C_0 + C_1 + C_4 + C_5) +$$
$$+ (4q - 28 - 8a)(C_2 + C_3 + C_6 + C_7)]/64 =$$
$$= \frac{4q-4}{64} G \setminus \{0\} \quad \text{with} \quad a = -3 .$$

Lemma 24. *Suppose* $q = 8f + 1$ *(*f *odd) is a prime power, then if in the unique proper representation of* q

(i) $y = 0$, $C_0 + C_1$, $C_3 + C_6$, $C_2 + C_3$, $C_0 + C_5$ *are* $4 - \{8f + 1; 2f; 2f - 1\}$ sds; *and if*

(ii) $b = 0$, $C_0 + C_1$, $C_3 + C_6$, $C_1 + C_2$, $C_4 + C_7$ *are* $4 - \{8f + 1; 2f; 2f - 1\}$ sds.

Proof. (i) If 2 is not a fourth power

$$\Delta(C_0 + C_1) + \Delta(C_3 + C_6) = (A + J + B + I)(C_0 + C_4) +$$
$$+ (I + A + J + H)(C_1 + C_5) +$$

$$+ (N + I + O + M)(C_2 + C_6) +$$

$$+ (J + N + O + K)(C_3 + C_7) +$$

$$+ (I + N + K + L)(C_0 + C_4) +$$

$$+ (N + J + L + M)(C_1 + C_5) +$$

$$+ (J + A + F + I)(C_2 + C_6) +$$

$$+ (A + I + D + J)(C_3 + C_7) =$$

$$= \frac{1}{8}[(q - 5 + 2y - 2b)(C_0 + C_4) +$$

$$+ (q - 5 - 2y + 2b)(C_1 + C_5) +$$

$$+ (q - 5 + 2y + 2b)(C_2 + C_6) +$$

$$+ (q - 5 - 2y - 2b)(C_3 + C_7)] .$$

So

$$\Delta(C_0 + C_1) + \Delta(C_3 + C_6) + \Delta(C_2 + C_3) + \Delta(C_0 + C_5) =$$

$$= \frac{1}{8}[(2q - 10 + 4y)(C_0 + C_4 + C_2 + C_6) +$$

$$+ (2q - 10 - 4y)(C_1 + C_3 + C_5 + C_7)] =$$

$$= (2f - 1)G \setminus \{0\} \quad \text{when} \quad y = 0 .$$

Also

$$\Delta(C_0 + C_1) + \Delta(C_3 + C_6) + \Delta(C_1 + C_2) + \Delta(C_4 + C_7) =$$

$$= \frac{1}{8}[(2q - 10 - 4b)(C_0 + C_4) +$$

$$+ (2q - 10)(C_1 + C_5) +$$

$$+ (2q - 10 + 4b)(C_2 + C_6) +$$

$$+ (2q - 10)(C_3 + C_7)] =$$

$$= (2f - 1)G \setminus \{0\} \quad \text{when} \quad b = 0 .$$

(ii) If 2 is a fourth power

$$\Delta(C_0 + C_1) + \Delta(C_3 + C_6) = \frac{1}{8}[(q - 5 + 2y + 2b)(C_0 + C_4) +$$
$$+ (q - 5 - 2y - 2b)(C_1 + C_5) +$$
$$+ (q - 5 + 2y - 2b)(C_2 + C_6) +$$
$$+ (q - 5 - 2y + 2b)(C_3 + C_7)]$$

and proceeding as before we have the result.

5. AN APPLICATION OF SUPPLEMENTARY DIFFERENCE SETS TO THE CONSTRUCTION OF BALANCED INCOMPLETE BLOCK DESIGNS

The following theorem is a generalization of a result shown us by S. Lin.

Theorem 23. *Suppose* $B_1, B_2, \ldots, B_n$ *are* $n - \{v; k; \lambda\}$ *supplementary difference sets from an abelian group* G *of order* v. *Let* $A_1, A_2, \ldots, A_k$ *be obtained from* B_1 *by successively removing one element.*

Write $\textcircled{A}_i$ *for the incidence matrix of* A_i *and* $\textcircled{B}_j$ *for the incidence matrix of* B_j. *Then*

	each repeated α *times*	β *times*	*each repeated* γ *times*
$C =$	$\textcircled{A}_1\ \textcircled{A}_2 \cdots \textcircled{A}_k$	$\textcircled{B}_1$	$\textcircled{B}_2 \cdots \textcircled{B}_n$
	11 11	00	 0

is the incidence matrix of a BIBD $(v + 1, \alpha v(v + 1), \alpha v k, k, \alpha k(k - 1))$

$$r = \alpha v k = (\beta + (n - 1)\gamma)k + k(k - 1)\alpha$$

$$\alpha = k(k - 1)\alpha = \lambda\gamma$$

$$\gamma = \alpha(k - 2) + \beta .$$

Proof. Each matrix $\textcircled{A}_i$ has $k-1$ elements per row and column, so C has k elements per column and

$$r = \alpha k\nu = \alpha k(k-1) + (\beta + (n-1)\gamma)k$$

elements per row.

Let $\Delta\beta_1$ be differences between elements of B_1, then

$$\sum_{i=1}^{k} \Delta A_i = (k-2)\Delta B_1 .$$

Now since the sets $B_1, \ldots, B_n$ are supplementary difference sets,

$$\lambda(\nu - 1) = nk(k-1)$$

and

$$\sum_{j=1}^{n} \Delta B_j = \Delta B_1 + \sum_{j=2}^{n} \Delta B_j = \lambda G/\{0\} .$$

So we want

$$\alpha \sum_{i=1}^{k} \Delta A_i + \beta\Delta B_1 + \gamma \sum_{j=2}^{n} \Delta B_j = \mu G/\{0\} ,$$

that is

$$(\alpha(k-2) + \beta)\Delta B_1 + \gamma(\lambda G/\{0\} - \Delta B_1) = \mu G/\{0\}$$

and

$$\mu = \lambda\gamma, \quad \alpha(k-2) + \beta = \gamma$$

(unless B_1 is a difference set).

Also we need the inner product of the last row of C with the other rows to be μ, so

$$\mu = \alpha k(k-1) .$$

Now we wish to simplify

(7) $$\mu = \alpha k(k-1) = \lambda\gamma$$

(8) $r = \alpha\nu k = (\beta + (n-1)\gamma)k + k(k-1)\alpha$

(9) $\lambda(\nu - 1) = nk(k-1)$

(10) $\mu\nu = r(k-1)$

(11) $\alpha(k-2) + \beta = \gamma$

If $\alpha = 1$, then (11) and (8) give

$$n\gamma = \nu - 1$$

$$\beta = \gamma - k + 2\,,$$

and a BIBD $(\nu + 1, b, \nu k, k, k(k-1))$ = BIBD $(\nu + 1, \nu(\nu+1), \nu k, k, k(k-1))$.

Corollary. *If p is an odd prime power, there exist* $2 - \{p; \frac{p-1}{2}; \frac{p-3}{2}\}$ *and* $2 - \{p; \frac{p+1}{2}; \frac{p+1}{2}\}$ sds *so there exist*

$$\text{BIBD}\left(p+1, p(p+1), p\left(\frac{p-1}{2}\right), \left(\frac{p-1}{2}\right), \left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)\right)$$

and

$$\text{BIBD}\left(p+1, p(p+1), p\left(\frac{p+1}{2}\right), \left(\frac{p+1}{2}\right), \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\right)$$

Corollary. *If there exists a* (ν, k, λ) *and a* $(\nu, \nu - k, \nu - 2 + \lambda)$ *difference set, then there exist*

$$\text{BIBD}\,(\nu+1, \nu(\nu+1), \nu k, k, k(k-1))$$

and

$$\text{BIBD}\,(\nu+1, \nu(\nu+1), \nu(\nu-k), \nu-k, (\nu-k)(\nu-k-1))$$

Corollary. *If* $p = ef + 1$ *is a prime power, there exist*

$$e - \{ef+1; f; f-1\} \quad \textit{and} \quad e - \{ef+1; f+1; f+1\}$$

supplementary difference sets and so there exist

$$\text{BIBD}\,(ef+2, (ef+2)(ef+1), (ef+1)f, f, f(f-1))$$

and

$$\text{BIBD}\,(ef+2, (ef+1)(ef+2), (ef+1)(f+1), f+1, f(f+1))\,.$$

Comment. It was pointed out to us by Mr. Dean Hoffman that in the above corollaries the BIBD's obtained from complementary sds are not themselves complementary.

Clearly the method of this section also has application to $n-\{v; k_1, k_2, \ldots, k_n; \lambda\}$ sds.

6. AN APPLICATION OF SDS IN CONSTRUCTING SKEW-HADAMARD MATRICES

Lemma 24. *Let* $p = 4f+1 = s^2 + 4t^2 \equiv 5 \pmod 8$ *be a prime power. Suppose there exists a skew-Hadamard matrix* $S+I$ *of order* $|t|+1$. *Then there exists a skew-Hadamard matrix of order* $(|t|+1)(p+1)$.

Proof. From lemma 6

$$C_0 + C_1 \quad \text{and} \quad |t| \quad \text{copies of} \quad C_0 + C_2$$

are $(|t|+1) - \{4f+1; 2f; \frac{1}{2}(|t|+1)(2f-1)\}$ supplementary difference sets with the property that

$$x \in C_0 + C_1 \Rightarrow -x \notin C_0 + C_1\,,$$

and

$$y \in C_0 + C_2 \Rightarrow -y \in C_0 + C_2\,.$$

Then the type 1 $(1,-1)$ incidence matrix A and the type 2 $(1,-1)$ incidence matrix B of $C_0 + C_1$ and $C_0 + C_2$ satisfy.

$$AJ = BJ = -J,\ (A+I)^T = -(A+I),\ B^T = B\,,$$

$$AA^T + |t|BB^T = (|t|+1)(p+1)I - (|t|+1)J\,.$$

Now $SS^T = |t|I$, $S^T = -S$ and we consider

$$H = \left[\begin{array}{c|c} S + I & (S + I) \times e \\ \hline (S - I) \times e^T & I \times -A + S \times B \end{array}\right],$$

where e is the $1 \times p$ matrix of ones. It is easily verified that H is a skew-Hadamard matrix of order $(|t| + 1)(p + 1)$.

REFERENCES

[1] D.C. Hunt – J. Wallis, Cyclotomy, Hadamard arrays and supplementary difference sets, *Proceedings Second Manitoba Conference on Numerical Mathematics,* (1972), 351-381.

[2] T. Storer, *Cyclotomy and Difference Sets,* Markham Publishing Company, Chicago, 1967.

[3] G. Szekeres, Cyclotomy and complementary difference sets, *Acta Arithmetica,* 18 (1971), 349-353.

[4] J. Wallis, Amicable Hadamard matrices, *J. Combinatorial Th. Ser. A*, 11 (1971), 296-298.

[5] J. Wallis, A note on Amicable Hadamard matrices, *Utilitas Math.*, 3 (1973), 119-125.

[6] J. Wallis, On supplementary difference sets, *Aeq. Math.*, 8 (1973), 242-257.

[7] J. Wallis, A note on supplementary difference sets, *Aeq. Math.* 10 (1974), 46-49.

[8] J.S. Wallis, Some matrices of Williamson type, *Utilitas Math.* 4 (1973), 147-154.

[9] J.S. Wallis, Construction of Williamson type matrices, (to appear).

[10] J. Wallis – A.L. Whiteman, Some classes of Hadamard matrices with constant diagonal, *Bull. Austral. Math. Soc.*, 7 (1972), 233-249.