In another form these kinds of sets have been studied by Spence (see [2]).

First we give an existence theorem:

THEOREM 1. *A necessary condition for the existence of Szekeres type difference sets in a cyclic group of order* $2m$ *is that* $4m+1$ *be respresentable as the sum of two squares.*

Proof. Let $\theta_1(x)$ be the Hall polynomial for A and $\theta_2(x)$ the Hall polynomial for B. Then we have

$$\theta_1(x)\theta_1(x^{-1}) + \theta_2(x)\theta_2(x^{-1}) + \theta_1(x)$$
$$\equiv 2m + m(x + x^2 + \ldots + x^{2m-1}) \bmod (x^{2m} - 1)$$
$$\equiv m + mT_{2m}(x) \bmod (x^{2m} - 1)$$

where

$$T_{2m}(x) = 1 + x + x^2 + \ldots + x^{2m-1}.$$

Since $(-1)^{2m} = 1$ we may take $x = -1$. We get

$$[\theta_1(-1)]^2 + [\theta_2(-1)]^2 + \theta_1(-1) = m$$

or $$c^2 + c + d^2 = m$$

where we have put $c = \theta_1(-1)$, $d = \theta_2(-1)$.

It follows immediately that

$$(2c+1)^2 + (2d)^2 = 4m + 1,$$

which completes the proof of the theorem. □

Example. For $m = 7$, $2m = 14$, $4m+1 = 29$, $A = \{1,2,5,7,8,12,13\}$, $B = \{0,1,6,8,9,10,11\}$ we have

$$\theta_1(x) = x + x^2 + x^5 + x^7 + x^9 + x^{12} + x^{13}$$

$$\theta_2(x) = 1 + x + x^6 + x^8 + x^9 + x^{10} + x^{11}$$

so that

$$c = \theta_1(-1) = -3, \quad d = \theta_2(-1) = +1$$

$$(2c+1)^2 + (2d)^2 = (-5)^2 + 2^2 = 29.$$

For $m = 11$, $2m = 22$, $4m+1 = 45$ we have

$$45 = 3^2 + 6^2$$
$$= (2c+1)^2 + (2d)^2$$

so that

$$c = \theta_1(-1) = 1 \text{ or } -2$$

$$d = \theta_2(-1) = \pm 3 .$$

THEOREM 2. *If $q = 4m+1$ is a prime power and G is the cyclic group of order $2m$, then there exist Szekeres type difference sets A and B in G.*

Proof. Let x be a primitive root of $GF(q)$, $R = \{x^{2a}: a = 0,1,\ldots,2m-1\}$ the set of quadratic residues in $GF(q)$, $N = \{x^{2b+1}: b = 0,1,\ldots,2m-1\}$ the set of quadratic non-residues in $GF(q)$. Define A and B by the rules

$$a \in A \text{ iff } x^{2a} - 1 \in N,$$
$$b \in B \text{ iff } x^{2b+1} - 1 \in N.$$

Clearly $0 \notin A$. Furthermore, since

$$-1 = x^{2m} \in R$$

we have

$$x^{2a} - 1 \in N \to x^{-2a} - 1 = -x^{-2a}(x^{2a}-1) \in N,$$

so that $a \in A \to -a \in A$. Thus (i) and (ii) of the definition are satisfied.

Suppose that

$$d = a_2 - a_1 \neq 0, \quad a_1, a_2 \in A,$$

where

$$x^{2a_1} - 1 = x^{2(i-d)+1}$$

$$x^{2a_2} - 1 = x^{2j+1}$$

for suitable $i,j \in G$. Then

$$x^{2a_2} = x^{2(a_1+d)} = x^{2d} + x^{2i+1} .$$

Hence

$$x^{2d} - 1 = x^{2j+1} - x^{2i+1}$$

with

$$x^{2j+1} + 1 \in R .$$

Similarly, if

$$d = b_2 - b_1 \neq 0, \quad b_1, b_2 \in B$$

where

$$x^{2b_1+1} - 1 = x^{2(i-d)+1}$$

$$x^{2b_2+1} - 1 = x^{2j+1}$$

for some i,j in G, we get

$$x^{2b_2+1} = x^{2(b_1+d)+1} = x^{2d} + x^{2i+1} .$$

We now get

$$x^{2d} - 1 = x^{2j+1} - x^{2i+1}$$

with

$$x^{2j+1} + 1 \in N.$$

Conversely to every solution $i,j \in G$ of the equation

$$x^{2d} - 1 = x^{2j+1} - x^{2i+1}$$

we can determine $a \in A$ or $b \in B$ depending on whether $1+x^{2j+1} \in R$ or N

respectively. It is a well-known lemma that the number of solutions of

$$n = \beta - \beta', \quad \beta,\beta' \in N$$

is m if $n \in R$ and $m-1$ if $n \in N$. The assertion of the theorem now follows at once.

2. *Conference Matrices.*

THEOREM 3. *If A and B are two Szekeres type difference sets of size m in an additive abelian group of order $2m$ then there is a symmetric conference matrix of order $4m+2$.*

Proof. Let A be the set such that $a \in A \to -a \in A$. Let X be the type 1 incidence matrix of A, and Y be the type 2 incidence matrix of B (see [Geramita and Seberry p. 80] for definitions and related results). Then

$$XY^T = YX^T, \quad JX^T = JY^T = mJ$$

and

$$XX^T + YY^T + X = mI + mJ. \tag{1}$$

Choose

$$M = 2X + I - J, \quad N = 2Y - J.$$

Let e be the $1 \times 2m$ matrix of 1's and f the $1 \times 2m$ matrix of 0's. Then

$$eM^T = e, \quad eN^T = f, \quad MN^T = NM^T, \quad M^T = M, \quad N^T = N$$

and

$$MM^T + NN^T = (4m+1)I - 2J. \tag{2}$$

Thus the required symmetric conference matrix is

0	+	e	e
+	0	-e	e
e^T	$-e^T$	M	N
e^T	e^T	N	-M

(3)

Theorems 2 and 3 together do not produce new symmetric conference matrices because we know by a theorem of Paley (see [4, Theorem 3.13]) that if $q \equiv 1 \pmod 4$ is a prime power there is a symmetric conference matrix of order $q+1$.

In the case $m = 6$, $2m = 12$, $4m+1 = 25$ we may apply Theorems 2 and 3 to construct C_{26}. The elements of $GF(25)$ may be expressed in the form

$$ax + b, \quad a,b \in GF(5),$$

where x is a primitive root of $GF(25)$ satisfying the relation

$$x^2 = 4x + 3.$$

We find that

$$A = \{1,4,5,7,8,11\} \text{ and } B = \{4,6,8,9,10,11\}$$

are Szekeres type difference sets.

The conference matrix of order 26 can be now found by choosing M and N with first rows

$$0\ 1\ -\ -\ 1\ 1\ -\ 1\ 1\ -\ -\ 1 \text{ and } -\ -\ -\ -\ 1\ -\ 1\ -\ 1\ 1\ 1\ 1$$

respectively and substituting in (3). A complete computer search for a pair of Szekeres type difference sets for $m = 11$, $2m = 22$ which would have given C_{46} failed to find any solution.

3. Hadamard Matrices.

We can now show

THEOREM 4. *Let* $v = 4m+1$ *be a prime power. Suppose all orthogonal designs of type* $(a,b,\frac{1}{4}(n-a-b),\frac{1}{4}(n-a-b),\frac{1}{2}(n-a-b))$ *exist in every order* $n = 2^t$ *where* $t \geq [2\ell n_2(v-5)]-2$. *Then there is an Hadamard matrix of order* $2^{t-1}(v-1)$.

Proof. Let the variables of the orthogonal design be x_1,x_2,x_3,x_4,x_5 so that the design, D, may be written

$$D = x_1A_1 + x_2A_2 + x_3A_3 + x_4A_4 + x_5A_5$$

with

$$A_1A_1^T = aI, \quad A_2A_2^T = bI, \quad 2A_3A_3^T = 2A_4A_4^T = \frac{1}{2}(n-a-b)I, \quad \text{and}$$

$$A_iA_j^T + A_jA_i^T = 0, \quad i \neq j.$$

Let M and N be the matrices described above (see Theorem 3) and let

$$E = A_1 \times J + A_2 \times (J-2I) + A_3 \times (M+I) + A_4 \times (M-I) + A_5 \times N.$$

Then, noting M,N,J, and J-2I are all symmetric and pairwise commute,

$$\begin{aligned} EE^T &= aI \times 2mJ + bI \times [4I+(2m-4)J] + \frac{1}{4}(n-b-a)I \times [2MM^T+2I+2NN^T] \\ &= 4bI \times I + (2am+2bm-4b)I \times J + \frac{1}{2}(n-b-a)I \times [(4m+2)I - 2J] \\ &= [(2m+1)(n-b-a)+4b]I \times I + [a(2m+1)+b(2m-3)-n]I \times J \\ &= 2mn\, I_{2mn} \end{aligned}$$

for $m = a(2m+1) + b(2m-3)$, and so is a Hadamard matrix of order $2mn$.

By a theorem of Sylvester (see [1, p. 302] every number $n_0 > 2m(2m-4) = 4m(m-2)$ can be written as a positive linear combination of $2m+1$ and $2m-3$, i.e. $n_0 = a_0(2m+1) + b_0(2m-3)$.

In particular if $n = 2^t$ is the first power of two such that $2^t > 4m(m-2)$ then there exist a,b such that

$$m = 2^t = a(2m+1) + b(2m-3) .$$

Thus if $t \geq [2\ell n_2(v-5)]-2$, $t+2 \geq \ell n_2(v-5)^2$, $2^{t+2} \geq (v-5)^2 = 2^4(m-1)^2 > 2^4m(m-2)$ and $2^t \geq 4m(m-2)$ giving the result.

Remark. Unfortunately, while this construction differs from previous constructions giving a marginally lower bound for t it gives no new Hadamard matrices of order $< 40,000$.

Suppose there is a skew-Hadamard matrix of order m then there is an orthogonal design of type $(1,m-1)$ in order m and hence an orthogonal design of type $(1,1,2,m-1,m-1,2(m-1))$ in order $4m$. Replacing the variables by $J,J-2I,M+I,M-I,N$ of the appropriate orders will give an Hadamard matrix and hence we have

THEOREM 5. *Suppose m is the order of a skew-Hadamard matrix then if*

(a) $2m+5$ is a prime power;

(b) $2m+1$ is a prime power;

there is an Hadamard matrix of order

(a) $4m(m+2)$; (b) $4m^2$.

Proof. Replace the variables by $J,J-2I,J-2I,M+I,M-I,N$ and $J-2I,J,J,M+I,M-I,N$ respectively.

Remark. The case (b) does not give new Hadamard matrices, just a new construction as an Hadamard matrix of order $4m^2$ can be obtained by taking the Kronecker product with the Hadamard matrix of size 4. Case (a) is new but gives no new Hadamard matrices of order $< 40,000$.

If $t \equiv 1 \pmod 4$ is a prime power or if there is a conference matrix of order $t+1$ then there is an orthogonal design of type $(2,2t)$ in order $2(t+1)$ and an orthogonal design of type $(2,2,4,4t,4t,8t)$ or $(4,4,4t,4t,8t)$ in order $8(t+1)$.

Hence replacing the variables by $J, J-2I, M+I, M-I, N$ respectively we have

THEOREM 6. *Suppose $t+1$ is the order of a symmetric conference matrix and*

(a) $4t+1$; or (b) $4t+9$; or (c) $4t+5$ are prime powers

then (a) $16t(t+1)$; (b) $16(t+1)(t+2)$; (c) $16(t+1)^2$ respectively are the orders of an Hadamard matrix.

Remark. Case (c) does not give new classes of Hadamard matrices, just a new construction. The other two constructions are new but give no new Hadamard matrices of order $< 40{,}000$.

References

[1] A.V. Geramita and Jennifer Seberry, *Orthogonal designs: quadratic forms and Hadamard matrices*, Marcel Dekker, New York-Basel, 1979.

[2] E. Spence, *Hadamard matrices from relative difference sets*, J. Combinatorial Theory, Ser. A, 19 (1975), 287-300.

[3] G. Szekeres, *Tournaments and Hadamard matrices*, Enseignment Math., 15 (1969), 269-278.

[4] Jennifer Seberry Wallis, *Hadamard matrices*, Part IV of Room squares, sum free sets, Hadamard matrices, by W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Vol. 292, Lecture Notes in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

Department of Applied Mathematics
University of Sydney
Sydney, 2006 N.S.W.
Australia

Department of Mathematics
University of Southern California
Los Angeles, CA 90089
U.S.A.