Can. J. Math., Vol. XXVII, No. 3, 1975, pp. 555–560

SKEW-HADAMARD MATRICES OF THE GOETHALS-SEIDEL TYPE

EDWARD SPENCE

1. Introduction. We prove, using a theorem of M. Hall on cyclic projective planes, that if q is a prime power such that either $1 + q + q^2$ is a prime congruent to 3, 5 or 7 (mod 8) or $3 + 2q + 2q^2$ is a prime power, then there exists a skew-Hadamard matrix of the Goethals-Seidel type of order $4(1 + q + q^2)$. (A Hadamard matrix H is said to be of skew type if one of $H + I, H - I$ is skew symmetric.) If $1 + q + q^2$ is a prime congruent to 1 (mod 8), then a Hadamard matrix, not necessarily of skew type, of order $4(1 + q + q^2)$ is constructed. The smallest new Hadamard matrix obtained has order 292.

2. Cyclic projective planes. In this section we use cyclic projective planes to construct two ± 1 matrices R, S which will be utilized to obtain Hadamard matrices. The main result is

THEOREM 1. *If there exists a cyclic projective plane of order q^2 then there exist two ± 1 matrices R, S, both circulant and of order $1 + q + q^2$, such that*

$$RR^T + SS^T = 2q(q + 1)I + 2J$$

where I is the identity matrix of order $1 + q + q^2$ and J is the square matrix of order $1 + q + q^2$ all the entries of which are $+1$.

The following theorem was proved by M. Hall [**1**, Theorem 4.6].

THEOREM 2. *Let t be a multiplier of a cyclic planar difference set D of order n and let π denote the finite projective plane generated by D. Then if $(t - 1, 1 + n + n^2) = v$, there are v points of π and v translates of D fixed by t. If, further, $v > 3$, then $v = 1 + n_1 + n_1^2$ and the fixed points together with the fixed translates determine a cyclic subplane of order n_1.*

In the proof of this theorem it is shown that, if D is fixed by t and $1 + n + n^2 = vw$ $(v > 3)$ then there are precisely $n_1 + 1$ elements of D divisible by w. The cyclic subplane is generated by the difference set

$$D' = \{d/w \pmod v) : d \in D \text{ and } d \equiv 0 \pmod w\}.$$

We apply Theorem 2 to a cyclic planar difference set D with parameters $(1 + q^2 + q^4, 1 + q^2, 1)$. Since q is a multiplier of D we may assume D fixed

Received November 20, 1973 and in revised form, April 30, 1974.

https://doi.org/10.4153/CJM-1975-066-9 Published online by Cambridge University Press

by q (see [**1**] for the relevant theorems). Take $n = q^2$ and $t = q^3$ in Theorem 2 so that $v = 1 + q + q^2$, $w = 1 - q + q^2$ and $n_1 = q$. Also, there are precisely $q + 1$ elements of D divisible by $1 - q + q^2$, these elements yielding a cyclic projective plane of order q as described above.

Let

$$D_1 = \{d \in D : d \equiv 0 \pmod{1 - q + q^2}\},$$

so that $|D_1| = q + 1$ and the elements of D_1 are incongruent $(\text{mod } 1 + q + q^2)$. Now suppose that $d, d' \in D$ and that $d \equiv d' \pmod{1 + q + q^2}$, i.e., $d - d' \equiv h(1 + q + q^2) \pmod{1 + q^2 + q^4}$ for some integer h. Then

$$\begin{aligned} q^3d - q^3d' &\equiv h(q^3 + q^4 + q^5) \pmod{1 + q^2 + q^4} \\ &\equiv -h(1 + q + q^2) \pmod{1 + q^2 + q^4}. \end{aligned}$$

Since D is fixed by q, both q^3d and q^3d' belong to D, and since any integer modulo $1 + q^2 + q^4$ can be uniquely represented as a difference between elements of D, we have $q^3d \equiv d' \pmod{1 + q^2 + q^4}$. Conversely, it is obvious that if $q^3d \equiv d' \pmod{1 + q^2 + q^4}$, then $d \equiv d' \pmod{1 + q + q^2}$. Now d, d' are distinct elements of D unless $q^3d \equiv d \pmod{1 + q^2 + q^4}$ and this condition implies that $d \in D_1$. It follows that the $(1 + q^2) - (1 + q) = q(q - 1)$ elements of $D \backslash D_1$ can be partitioned into pairs (d_i, d_i') $d_i \not\equiv d_i' \pmod{1 + q^2 + q^4}$, $1 \leqq i \leqq \frac{1}{2}q(q - 1)$, such that $d_i \equiv d_i' \pmod{1 + q + q^2}$ and $d_i \not\equiv d_j \pmod{1 + q + q^2}$ if $i \neq j$. (Observe also that $d_i \not\equiv d \pmod{1 + q + q^2}$ for any $d \in D_1$.) Thus, if $\theta(x) = \sum_{d \in D} x^d$ is the Hall polynomial of D, so that

$$(1) \qquad \theta(x)\theta(x^{-1}) \equiv q^2 + T_m(x) \pmod{x^m - 1} \quad (m = 1 + q^2 + q^4 = vw)$$

where $T_r(x) = 1 + x + x^2 + \ldots + x^{r-1}$, we can write

$$(2) \qquad \theta(x) \equiv \sum_{i=1}^{\frac{1}{2}q(q-1)} (x^{d_i} + x^{d_i'}) + \sum_{d \in D_1} x^d \pmod{x^m - 1}.$$

Suppose

$$\psi(x) \equiv \sum_{d \in D_1} x^d \pmod{x^m - 1}$$

and

$$\varphi(x) \equiv \sum_{i=1}^{\frac{1}{2}q(q-1)} x^{d_i} \pmod{x^m - 1}.$$

Then Theorem 2 tells us that

$$(3) \qquad \psi(x)\psi(x^{-1}) \equiv q + T_v(x^w) \pmod{x^m - 1}.$$

Since $(w, v) = (1 - q + q^2, 1 + q + q^2) = 1$, reduction of (3) modulo $x^v - 1$ yields

$$(4) \qquad \psi(x)\psi(x^{-1}) \equiv q + T_v(x) \pmod{x^v - 1}.$$

https://doi.org/10.4153/CJM-1975-066-9 Published online by Cambridge University Press

Also, from (2), we have

(5) $\theta(x) \equiv 2\varphi(x) + \psi(x) \pmod{x^v - 1}$.

Reducing (1) mod $x^v - 1$ and using (5) gives

(6) $(2\varphi(x) + \psi(x))(2\varphi(x^{-1}) + \psi(x^{-1})) \equiv q^2 + wT_v(x) \pmod{x^v - 1}$.

Thus, from (4),

(7) $$(\varphi(x) + \psi(x))(\varphi(x^{-1}) + \psi(x^{-1})) + \varphi(x)\varphi(x^{-1}) \equiv \tfrac{1}{2}q(q+1) + \tfrac{1}{2}(q^2 - q + 2)T_v(x) \pmod{x^v - 1}.$$

Note that $\varphi(x) + \psi(x)$ and $\varphi(x)$, considered as polynomials mod $x^v - 1$ have coefficients 0 or 1 and

(8) $$\begin{cases} \varphi(x)T_v(x) \equiv \tfrac{1}{2}q(q-1)T_v(x) \pmod{x^v - 1}, \\ \psi(x)T_v(x) \equiv (q+1)T_v(x) \pmod{x^v - 1}. \end{cases}$$

Now consider D_1 as a set of integers modulo v and let

$$D_2 = \{d_i \pmod{v} : 1 \leqq i \leqq \tfrac{1}{2}q(q-1)\}.$$

We define ± 1 circulant matrices $R = [r_{ij}]$, $S = [s_{ij}]$ of order v as follows:

$$r_{ij} = \begin{cases} +1 \text{ if } j - i \equiv d \pmod{v} \text{ for some } d \in D_1 \cup D_2, \\ -1, \text{ otherwise,} \end{cases}$$

$$s_{ij} = \begin{cases} +1 \text{ if } j - i \equiv d \pmod{v} \text{ for some } d \in D_2, \\ -1, \text{ otherwise.} \end{cases}$$

Then, since (from (7) and (8))

$$[2(\phi(x) + \psi(x)) - T_v(x)][2(\phi(x^{-1}) + \psi(x^{-1})) - T_v(x)] + [2\phi(x) - T_v(x)][2\phi(x^{-1}) - T_v(x)] \equiv 2q(q+1) + 2T_v(x) \pmod{x^v - 1},$$

it follows that

$$RR^T + SS^T = 2q(q+1)I + 2J.$$

This proves Theorem 1.

3. Complementary difference sets. Given an additive abelian group K of order $2k + 1$, two subsets U and V of K, each of order k, are called complementary difference sets in K (see [**5**; **6**]) if

(9) (i) $u \in U \Rightarrow -u \notin U$,
(ii) for each $g \in K$, $g \neq 0$, the total number of solutions of the equation $a_1 - a_2 = g$, where either $(a_1, a_2) \in U \times U$ or $(a_1, a_2) \in V \times V$, is $k - 1$.

These complementary difference sets are known to exist for various values of k.

https://doi.org/10.4153/CJM-1975-066-9 Published online by Cambridge University Press

For example, they exist in a cyclic group of order $2k + 1$ if $2k + 1$ is a prime $p \equiv 3, 5$ or $7 \pmod 8$ or $4k + 3$ is a prime power [**5**; **6**].

In what follows we consider the group K to be the cyclic group of integers modulo $2k + 1 = 1 + q + q^2 = v$. Corresponding to the subsets U, V of K we define incidence matrices $P = [p_{ij}]$, $Q = [q_{ij}]$ which are circulant of order v, by

$$p_{ij} = \begin{cases} +1 \text{ if } j - i \in U, \\ -1 \text{ if } j - i \notin U, \end{cases} \quad q_{ij} = \begin{cases} +1 \text{ if } j - i \in V, \\ -1 \text{ if } j - i \notin V, \end{cases}$$

so that $P + I$ is skew symmetric. Then (9) yields

$$\begin{aligned} PP^T + QQ^T &= 2(2k + 1)I - 2(J - I) \\ &= 2(q^2 + q + 2)I - 2J. \end{aligned}$$

Thus, if R and S are as in § 1, we have

$$PP^T + QQ^T + RR^T + SS^T = 4(1 + q + q^2)I.$$

The following matrix H, whose construction is due to Goethals and Seidel [**3**], is a skew-Hadamard matrix of order $4(1 + q + q^2)$:

$$(10) \quad H = \begin{bmatrix} P & QW & RW & SW \\ -QW & P & -S^TW & R^TW \\ -RW & S^TW & P & -Q^TW \\ -SW & -R^TW & Q^TW & P \end{bmatrix}$$

where $W = [w_{ij}]$ is the permutation matrix of order $1 + q + q^2$ defined by $w_{ij} = 1$ if $i + j \equiv 2 \pmod{1 + q + q^2}$, 0, otherwise. Hence we have

THEOREM 3. *If there exists a cyclic projective plane of order q^2 and two complementary difference sets in a cyclic group of order $1 + q + q^2$, then there exists a skew-Hadamard matrix of the Goethals-Seidel type of order $4(1 + q + q^2)$.*

From the results of Szekeres [**5**; **6**], the existence of these complementary difference sets is assured if either $1 + q + q^2$ is a prime congruent to 3, 5 or 7 (mod 8) or $2q^2 + 2q + 3$ is a prime power. Also, a cyclic projective plane of order q^2 exists if q is a prime power [**4**]. Hence we have skew-Hadamard matrices of the Goethals-Seidel type for $q = 2, 3, 4, 5, 13, 16, 17, 25, 27, 31, \ldots$ with corresponding orders 28, 52, 84, 124, 732, 1092, 1228, 2604, 3028, 3972, . . .

If condition (i) of (9) is removed, the resulting matrix H constructed in (10) is still a Hadamard matrix, but not necessarily of skew type. Now if $1 + q + q^2$ is an odd prime p, then taking U to consist of the quadratic residues (mod p) and V the quadratic non-residues (mod p), U and V satisfy condition (ii) of (9) with K the cyclic group of order $2k + 1 = p$. In particular, taking $q = 8$, so that $p = 73$, it is seen that there exists a Hadamard matrix of order $4 \cdot 73 = 292$. This is the smallest order of a new Hadamard matrix constructed by the above method.

4. Relative difference sets. An alternative method of obtaining the matrices R and S of § 1 is to use relative difference sets. We describe the method briefly.

A set $B = \{b_1, b_2, \ldots, b_k\}$ of k elements in an additive abelian group G of order mn is said to be a difference set relative to the subgroup H of order n if the elements of B are distinct coset representatives of H in G and for each $g \in G \backslash H$ there exist exactly λ pairs (b_i, b_j) with $b_i, b_j \in B$ such that $b_i - b_j = g$. Such a relative difference set is denoted by $B(m, n, k, \lambda)$. For more details of relative difference sets see [**2**].

We shall be interested in relative difference sets B with parameters $(1 + q + q^2, 2, q^2, \frac{1}{2}q(q - 1))$ in the cyclic group of integers modulo $2(1 + q + q^2)$ relative to a subgroup of order 2. These relative difference sets exist for q an odd prime power by [**2**, Corollary 5.1.1]. If $\alpha(x) = \sum_{b \in B} x^b$, it follows directly from the above definition that

$$(11) \quad \alpha(x)\alpha(x^{-1}) \equiv q^2 + \tfrac{1}{2}q(q - 1)\{T_{2v}(x) - T_2(x^v)\} \pmod{x^{2v} - 1},$$

with $v = 1 + q + q^2$ as before. Let a_1 be the number of odd integers in B and a_2 the number of even integers in B. Then, putting $x = -1$ in (11), we immediately deduce that either $a_1 = \frac{1}{2}q(q + 1)$ and $a_2 = \frac{1}{2}q(q - 1)$, or $a_1 = \frac{1}{2}q(q - 1)$ and $a_2 = \frac{1}{2}q(q + 1)$. Since a translate of B is also a relative difference set with the same parameters, we may assume that $a_1 = \frac{1}{2}q(q + 1)$ and $a_2 = \frac{1}{2}q(q - 1)$. Write $B_1 = \{b \in B : b \text{ is odd}\}$ and $B_2 = \{b \in B : b \text{ is even}\}$. It is a simple matter to prove that, if

$$\alpha_1(x) = \sum_{b \in B_1} x^{(b+v)/2} \quad \text{and} \quad \alpha_2(x) = \sum_{b \in B_2} x^{b/2},$$

then

$$\alpha_1(x)\alpha_1(x^{-1}) + \alpha_2(x)\alpha_2(x^{-1}) \equiv \tfrac{1}{2}q(q + 1) + \tfrac{1}{2}q(q - 1)T_v(x) \pmod{x^v - 1}.$$

The matrices R and S can now be constructed in the same way as in § 1.

As mentioned earlier, the results of Elliott and Butson ensure the existence of a cyclic relative difference set with parameters $(1 + q + q^2, 2, q^2, \frac{1}{2}q(q - 1))$ when q is an odd prime power. Such a relative difference set also exists for q a power of 2 as can be seen from the results of § 1. For if, in the notation of § 1,

$$\beta(x) \equiv T_v(x^2) - \varphi(x^2) - \psi(x^2) + x^v\varphi(x^2) \pmod{x^{2v} - 1},$$

it is easily verified that β has coefficients 0 or 1 and

$$\beta(x)\beta(x^{-1}) \equiv q^2 + \tfrac{1}{2}q(q - 1)\{T_{2v}(x) - T_2(x^v)\} \pmod{x^{2v} - 1},$$

so that β is the incidence polynomial of a cyclic relative difference set with parameters $(1 + q + q^2, 2, q^2, \frac{1}{2}q(q - 1))$, where q can be taken to be any prime power.

References

1. L. D. Baumert, *Cyclid difference sets*, Springer-Verlag Lecture Notes in Mathematics, No. *182*, 1971.

2. J. E. H. Elliott and A. T. Butson, *Relative difference sets*, Illinois J. Math. *10* (1966), 517–531.

3. J. M. Goethals and J. J. Seidel, *A skew-Hadamard matrix of order* 36, J. Austral. Math. Soc. *11* (1970), 343–344.

4. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377–385.

5. G. Szekeres, *Cyclotomy and complementary difference sets*, Acta Arith. *18* (1971), 349–353.

6. ——— *Tournaments and Hadamard matrices*, Enseignment Math. *15* (1969), 269–278.

The University of Glasgow,
Glasgow G12 8QW, Scotland.