TOURNAMENTS AND HADAMARD MATRICES

TOURNAMENTS AND HADAMARD MATRICES

G. SZEKERES

To the memory of J. Karamata

1. A Hadamard matrix (H-matrix) is a square orthogonal matrix with all entries $+1$ or -1. Apart from the trivial cases $n = 1$ or 2, the order of an H-matrix must be divisible by 4, and it is a famous yet unsolved problem whether an H-matrix of order $n = 4m$ exists for all m.

The construction of certain H-matrices can be achieved via tournaments. A *tournament* $\mathscr{T}_n = \mathscr{T}(u_1, \dots, u_n)$ is a complete directed graph consisting of n nodes $u_1, \dots, u_n$ and one directed edge $\overrightarrow{u_i u_j}$ for each pair of nodes. We write $u_i \to u_j$ and say that u_i dominates u_j. $\mathrm{N}(\mathscr{T}_n)$ denotes the set of nodes of $\mathscr{T}_n$. For every subset $\{v_1, \dots, v_k\}$ of $\mathrm{N}(\mathscr{T}_n)$ we define

$$S(v_1, \dots, v_k) = \{ w \in N(\mathscr{T}_n); \quad w \to v_i, \quad i = 1, \dots, k \},$$

$$S'(v_1, \dots, v_k) = \{ w' \in N(\mathscr{T}_n); \quad v_i \to w', \quad i = 1, \dots, k \}.$$

The *dual* $\mathscr{T}_n' = \mathscr{T}(u_1', \dots, u_n')$ of $\mathscr{T}_n$ is defined by the dominance rule

$$u_i' \to u_j' \Leftrightarrow u_j \to u_i$$

An *automorphism* of $\mathscr{T}_n$ is a permutation π of its nodes which preserves orientation, $u_i \to u_j \Leftrightarrow u_{\pi(i)} \to u_{\pi(j)}$.

In an earlier paper [3] we have considered the following:

Property $T_{k,m}$: For every subset $\{v_1, \dots, v_k\} \subset \mathrm{N}(\mathscr{T}_n)$ of order k, $S(v_1, \dots, v_k)$ is at least of order m. A $T_{k,m}$ tournament $\mathscr{T}_n$ has order $n \geqslant 2^k(m+1) - 1$ ([3], Lemma 3). We shall call it *extreme* if its order is exactly $2^k(m+1) - 1$. It is easily seen that for every m there exists an extreme $T_{1,m}$ tournament (of order $2m+1$). We shall examine here the existence of extreme $T_{2,m}$ tournaments of order $4m+3$ for special values of m. Interest in these tournaments stems from the fact that they supply H-matrices of order $4m+4$. In fact the sets $S(u_i)$, $i = 1, \dots, 4m+3$ have the property that each $S(u_i)$ is of order $2m+1$ and $S(u_i) \cap S(u_j)$ for $i \neq i$ is of order m, and from sets with this property one can immediately construct an H-matrix of order $4m+4$ ([4], § 1). The converse is not necessarily true; there exist H-matrices and corresponding configurations of subsets with the above mentioned property which are not the sets $S(u_i)$ of any tournament. I owe to Dr. N. Smythe the remark that the existence of extreme $T_{2,m}$ tournaments is equivalent to the existence of "skew" H-matrices of order $4m+4$, that is H-matrices of the form $I+S$ where I is the identity matrix and S is skew symmetric. I also owe to Dr. Smythe the proof of Lemma 3. The hitherto known orders of skew H-matrices are given by E. C. Johnsen in [5], Theorem 2.6. The present Theorem 6 gives infinitely many new orders; the first one is 76.

2. *Lemma 1.*

Let $\mathscr{T}$ *be a* $T_{2,m}$ *tournament of order* $4m+3$. *Then*

(i) $\mathscr{T}$ *is regular, i.e.* $S(v)$, $S'(v)$ *are of order* $2m+1$ *for every* $v \in N(\mathscr{T})$.

(ii) $S(v_1, v_2)$ *is of order* m *for every pair of nodes* $v_1, v_2 \in N(\mathscr{T})$.

(iii) *The dual* $\mathscr{T}'$ *of* $\mathscr{T}$ *is also* $T_{2,m}$.

These statements have been proved in [3] (Lemma 4).

Lemma 2.

Let $\mathscr{T}(u_1, \ldots, u_n)$ *be* $T_{2,m}$ *of order* $4m+3$. *Let* $u_i \to u_j$; *then the set* $\{u_k; u_i \to u_k \to u_j\}$ *is of order* m *and the set* $\{u_k; u_j \to u_k \to u_i\}$ *is of order* $m+1$.

Proof. The first set is identical with $S'(u_i) - S'(u_i, u_j) - \{u_j\}$, the second set is identical with $S(u_i) - S(u_i, u_j)$. The statement now follows from Lemma 1.

Theorem 1.

If there exists an extreme $T_{2,m}$ *tournament then there also exists an extreme* $T_{2,2m+1}$ *tournament (of order* $8m+7$).

This is basically the well known duplication theorem of H-matrices though not an obvious consequence of it.

Let $n = 4m+3$ and $u_1, \ldots, u_n$ the nodes of a $T_{2,m}$ tournament $\mathscr{T}_n$. Write $i \to j$ if $u_i \to u_j$. Let $u_1', \ldots, u_n'$ be the nodes of a dual $\mathscr{T}_n'$. We define $\mathscr{T} = \mathscr{T}_{2n+1}$ as containing the disjoint subtournaments $\mathscr{T}_n$, $\mathscr{T}_n'$ and another node v with the following additional dominance rules:

$$v \to u_i' \to u_i \to v \quad \text{for} \quad i = 1, \ldots, n. \tag{1}$$

Furthermore if $i \to j$ then

$$u_i' \to u_j, \quad u_i \to u_j'. \tag{2}$$

These rules define $\mathcal{T}$ completely; we show that $\mathcal{T}$ is $T_{2,2m+1}$. We merely enumerate $S(v_1, v_2)$ for all possible pairs of nodes of $\mathcal{T}$.

$$
\begin{aligned}
S(v, u_i) &= \{ u_k ; k \to i \}, \\
S(v, u_i') &= \{ u_k ; k \to i \} \text{ are of order } 2m+1 \text{ by Lemma 1 (i).} \\
S(u_i, u_j) &= \{ u_k ; k \to i, k \to j \} \text{ order } m \text{ by Lemma 1 (ii)} \\
&\quad \cup \{ u_k' ; k \to i, k \to j \} \text{ order } m \\
&\quad \cup \{ u_i' \} \text{ if } i \to j \\
&\qquad \{ u_j' \} \text{ if } j \to i \text{ order } 1. \\
S(u_i', u_j') &= \{ u_k' ; i \to k, j \to k \} \quad \text{order } m \text{ by Lemma 1 (iii)} \\
&\quad \cup \{ u_k ; k \to i, k \to j \} \text{ order } m \\
&\quad \cup \{ v \} \qquad \text{order } 1. \\
S(u_i, u_i') &= \{ u_k ; k \to i \} \qquad \text{order } 2m+1 \\
S(u_i, u_j') &= \{ u_k , k \to i, k \to j \} \quad \text{order } m \\
&\quad \cup \{ u_k' ; j \to k, k \to i \} \text{ order } m+1 \text{ if } i \to j \\
&\qquad\qquad \text{order } m \text{ if } j \to i, \text{ by Lemma 2} \\
&\quad \cup \{ u_i' \} \text{ if } j \to i \qquad \text{order } 1.
\end{aligned}
$$

The proof of Theorem 1 suggests that we should seek the existence of $T_{2,m}$ tournaments $\mathcal{T}_n$, $n = 4m+3$, with the following structure:

(E1) $\mathcal{T}_n$ contains two disjoint dual subtournaments $\mathcal{T}_{2m+1} = \mathcal{T}(u_\alpha; \alpha \in G)$, $\mathcal{T}'_{2m+1} = \mathcal{T}(u'_\alpha; \alpha \in G)$, indexed by an additive abelian group G of order $2m+1$, and another node v, such that

(E2) $\quad u_\alpha \to v \to u'_\alpha, \quad \text{all} \quad \alpha \in G,$

(E3) $\quad u_\alpha \to u_\beta \Rightarrow u_{\alpha+\gamma} \to u_{\beta+\gamma},$

$\quad\quad u_\alpha \to u'_\beta \Rightarrow u_{\alpha+\gamma} \to u'_{\beta+\gamma}, \quad \text{all} \quad \gamma \in G.$

Thus the regular representation of G acts as a group of automorphisms of $\mathcal{T}_{2m+1}$. We shall refer to conditions (E1)–(E3) as property (E).

A tournament $\mathcal{T}_{4m+3}$ with property (E) is completely described by two sets of elements of G, namely

$$A = \{ \alpha; \alpha \neq 0, u_\alpha \rightarrow u_0 \} ,$$

$$B = \{ \beta; u_\beta \rightarrow u_0' \} .$$

From (E3) it then follows that

(*E*3.1) $$u_{\gamma+\alpha} \rightarrow u_\gamma$$

(*E*3.2) $$u'_{\gamma-\alpha} \rightarrow u'_\gamma$$

(*E*3.3) $$u_{\gamma+\beta} \rightarrow u'_\gamma$$

(*E*3.4) $$u'_{\gamma-\beta'} \rightarrow u_\gamma$$

all

$$\gamma \in G , \quad \alpha \in A , \quad \beta \in B , \quad \beta' \in B' = G - B .$$

In order that (E3.1) be consistent, i.e. that $u_{\gamma+\alpha} \rightarrow u_\gamma$ and $u_\gamma \rightarrow u_{\gamma+\alpha}$ be mutually exclusive, it is necessary and sufficient that

(*E*4) $$\alpha \in A \Leftrightarrow - \alpha \notin A .$$

In particular A must contain exactly m elements.

We wish to set up conditions for $\mathcal{T}_{4m+3}$ to be $T_{2,m}$. We must examine $S(v_1, v_2)$ for all possible pairs of nodes of $\mathcal{T}_{4m+3}$.

$S(v, u_\gamma) = \{ u_{\gamma+\alpha}; \alpha \in A \}$ by (E1) and (E3.1) hence is of order m, as required.

$S(v, u'_\gamma) = \{ u_{\gamma+\beta}; \beta \in B \}$ by (E1) and (E3.3), thus B must also contain exactly m elements (hence $B' = G - B$ contains $m+1$ elements).

$$S(u_{\gamma_1}, u_{\gamma_2}) = \{ u_{\gamma_1+\alpha_1} = u_{\gamma_2+\alpha_2} ; \quad \alpha_1, \alpha_2 \in A \}$$
$$\cup \{ u'_{\gamma_1-\beta'_1} = u'_{\gamma_2-\beta'_2}; \quad \beta'_1, \beta'_2 \in B' \} .$$

Thus for $\mathcal{T}_{4m+3}$ to be $T_{2,m}$ it is necessary that for each $\delta = \gamma_1 - \gamma_2 \neq 0$, the total number of solutions of

(3.1) $$\delta = \alpha_2 - \alpha_1 , \quad \alpha_1, \alpha_2 \in A ,$$

(3.2) $$\delta = \beta'_1 - \beta'_2 , \quad \beta'_1, \beta'_2 \in B' ,$$

be m. We show that this condition is also sufficient.

Theorem 2.

In order that two subsets A $= \{ \alpha_1, ..., \alpha_m \}$, B $= \{ \beta_1, ..., \beta_m \}$ *of* G, *both of order* m, *define a* $T_{2,m}$ *tournament* $\mathcal{T}_{4m+3}$ *with property* (E), *it is necessary and sufficient that*

(i) $\alpha \in \mathrm{A} \Leftrightarrow -\alpha \notin \mathrm{A}$, *and*

(ii) *for each* $\delta \in \mathrm{G}$, $\delta \neq 0$ *the equations* (3.1) *and* (3.2) *should have altogether* m *distinct solutions.*

We have already seen that the conditions are necessary. To prove sufficiency we have to show that the sets $S(u'_{\gamma 1}, u'_{\gamma 2})$, $S(u_{\gamma 1}, u'_{\gamma 2})$ contain m elements. Now

$$\begin{aligned} S(u'_{\gamma_1}, u'_{\gamma_2}) &= \{ u_{\gamma_1+\beta_1} = u_{\gamma_2+\beta_2}; \quad \beta_1, \beta_2 \in B \} \\ &\cup \{ u'_{\gamma_1-\alpha_1} = u'_{\gamma_2-\alpha_2}; \quad \alpha_1, \alpha_2 \in A \} \\ &\cup \{ v \}, \\ S(u_{\gamma_1}, u'_{\gamma_2}) &= \{ u_{\gamma_1+\alpha} = u_{\gamma_2+\beta}; \quad \alpha \in A, \beta \in B \} \\ &\cup \{ u'_{\gamma_1-\beta'} = u'_{\gamma_2-\alpha}; \quad \alpha \in A, \beta' \in B' \}. \end{aligned}$$

But for $\delta = \gamma_1 - \gamma_2 \in G$ the total number of solutions of $\delta = \beta - \alpha$, $\delta = \beta' - \alpha$, $\alpha \in A$, $\beta \in B$, $\beta' \in B'$ is equal to the number of elements in A since $\delta + \alpha$ is either β or β'. Hence $S(u_{\gamma_1}, u'_{\gamma_2})$ contains m elements. On the other hand for $\delta = \gamma_1 - \gamma_2 \neq 0$ the total number of solutions of $\delta = \beta_2 - \beta_1$, $\delta = \alpha_1 - \alpha_2$ is $m-1$, by (3.1) and (3.2) and by the following Lemma (with $k = m$, $n = 2m+1$):

Lemma 3.

Let $\mathrm{B} = \{ \beta_1, \ldots, \beta_k \}$, $\mathrm{B}' = \{ \beta'_1, \ldots, \beta'_{n-k} \}$ *be a partition of an abelian group* G *of order* n *into two disjoint subsets. For fixed* $\gamma \in \mathrm{G}$ *denote by* $\mathrm{N}(\gamma)$, $\mathrm{N}'(\gamma)$ *the number of solutions of the equations*

$$\gamma = \beta_i - \beta_j, \qquad \gamma = \beta'_{i'} - \beta'_{j'},$$

respectively. Then

$$N'(\gamma) - N(\gamma) = n - 2k.$$

Proof. Form the sums $\gamma + \beta_j$, $j = 1, \ldots, k$. If r of these sums are in the set B then $k - r$ are in the set B'; consequently the number of sums $\gamma + \beta'_{j'}$ in B' is $(n-k) - (k-r) = n - 2k + r$. But then $\mathrm{N}(\gamma) = r$, $\mathrm{N}'(\gamma) = n - 2k + r$.

Two subsets A and B of an additive abelian group G of order $2m+1$ will be called *complementary difference sets* in G if

(D0) A contains m elements,

(D1) $\alpha \in A \Rightarrow -\alpha \notin A$, and

(D2) for each $\delta \in G$, $\delta \neq 0$ the equations

$$\delta = \alpha_1 - \alpha_2\,, \qquad \delta = \beta_1 - \beta_2$$

have altogether $m-1$ distinct solution vectors

$$(\alpha_1, \alpha_2) \in A \times A\,, \qquad (\beta_1, \beta_2) \in B \times B\,.$$

From conditions (D0) and (D1) it follows that $0 \notin A$. From condition (D2) it follows that also B must contain m elements. Furthermore by Lemma 3, (D2) is equivalent to the condition that (3.1) and (3.2) have altogether m distinct solution vectors $(\alpha_1, \alpha_2) \in A \times A$, $(\beta_1', \beta_2') \in B' \times B'$ where $B' = G - B$. Our main purpose is to demonstrate the existence of complementary difference sets when (i) $4m+3$ is a prime power, (ii) $2m+1$ is a prime power $\not\equiv 1 \pmod 8$. In the case when $2m+1$ is a prime power $\equiv 1$ (mod 8), a general existence theorem does not seem to hold; a machine search by David Blatt at Sydney University has shown that in the lowest non-trivial case $m = 8$ there do not exist any complementary difference sets in the cyclic group of order 17.

3. We now pass to the construction of complementary difference sets in the cases indicated.

Theorem 3.

If q $=$ 4m$+$3 *is a prime power and* G *the cyclic group of order* 2m$+$1 *then there exist complementary difference sets in* G.

Corollary. *If* q $=$ 4m$+$3 *is a prime power then there exists a* $\mathrm{T}_{2,m}$ *tournament of type (E) and order* q.

Proof. Let ρ be a primitive root of $GF(q)$, $Q = \{\rho^{2\beta}; \beta = 1, \ldots, 2m+1\}$ the set of quadratic residues in $GF(q)$. Define A and B by the rules

$$\alpha \in A \quad \text{iff} \quad \rho^{2\alpha} - 1 \in Q\,, \tag{4.1}$$

$$\beta \in B \quad \text{iff} \quad \rho^{2\beta} - 1 \in Q\,. \tag{4.2}$$

Since

$$-1 = \rho^{2m+1} \notin Q\,,$$

$$\rho^{2\alpha} - 1 \in Q \Leftrightarrow \rho^{-2\alpha} - 1 = -\rho^{-2\alpha}(\rho^{2\alpha} - 1) \notin Q$$

so that $\alpha \in A \Rightarrow -\alpha \notin A$, and conditions (D0) and (D1) are satisfied. Also

$$\beta' \in B' \quad \text{if} \quad -(\rho^{2\beta'} + 1) \in Q\,. \tag{4.3}$$

Suppose now that

$$\delta = \alpha_2 - \alpha_1 \neq 0\,, \qquad \alpha_1, \alpha_2 \in A \tag{5.1}$$

where

$$\rho^{2\alpha_1} = 1 + \rho^{2(\lambda_1 - \delta)}\,, \tag{5.2}$$

$$\rho^{2\alpha_2} = 1 + \rho^{2\lambda_2} \tag{5.3}$$

by (4.1) for suitable $\lambda_1, \lambda_2 \in G$. Then

$$\rho^{2\alpha_2} = \rho^{2(\alpha_1 + \delta)} = \rho^{2\delta} + \rho^{2\lambda_1}$$

by (5.1) and (5.2), hence by (5.3)

$$\rho^{2\delta} - 1 = \rho^{2\lambda_2} - \rho^{2\lambda_1} \tag{5.4}$$

where $\rho^{2\lambda_2} + 1 \in Q$ by (5.3).

Similarly if

$$\delta = \beta_2' - \beta_1' \neq 0\,, \qquad \beta_1', \beta_2' \in B' \tag{5.1$'$}$$

where

$$-\rho^{2\beta_1'} = 1 + \rho^{2(\lambda_1 - \delta)} \tag{5.2$'$}$$

$$-\rho^{2\beta_2'} = 1 + \rho^{2\lambda_2} \tag{5.3$'$}$$

for some $\lambda_1, \lambda_2 \in G$, we get

$$-\rho^{2\beta_2'} = -\rho^{2(\delta + \beta_1')} = \rho^{2\delta} + \rho^{2\lambda_1}$$

hence again

$$\rho^{2\delta} - 1 = \rho^{2\lambda_2} - \rho^{2\lambda_1}$$

with $-(\rho^{2\lambda_2} + 1) \in Q$ by (5.3′).

Conversely to every solution $\lambda_1, \lambda_2 \in G$ of equation (5.4) we can determine uniquely $\alpha_2 \in A$ or $\beta_2' \in B$ from (5.3) or (5.3′) depending on whether $1 + \rho^{2\lambda_2} = \rho^{2\delta} + \rho^{2\lambda_1}$ is in Q or not, hence α_1 or β_1' from (5.1), (5.1′) so that also (5.2) or (5.2′) be satisfied, implying $\alpha_1 \in A$, $\beta_1' \in B'$. Thus the total number of solutions of (5.1) and (5.1′) is equal to the number of solutions of (5.4) which is m by the following Lemma (with $\gamma = \rho^{2\delta} - 1$):

Lemma 4.

Given $\gamma \in GF(q)$, $\gamma \neq 0$, $q = 4\mathrm{m}+3$, *the equation*

$$\gamma = \sigma_2 - \sigma_1 \tag{6}$$

has exactly m *distinct solution vectors* $(\sigma_1, \sigma_2) \in Q \times Q$.

This is a well known result on perfect difference sets, e.g. Ryser [2], p. 133 in the case of q prime. We give here a brief proof, to prepare the ground for Theorem 5 where a similar but more involved argument will be used.

Denote by $\mathrm{N}(\gamma)$ the number of solutions $(\sigma_1, \sigma_2) \in Q \times Q$ of (6) and consider the equations

$$1 = \sigma_2 - \sigma_1 \tag{6.1}$$

$$-1 = \sigma_2' - \sigma_1', \tag{6.2}$$

$\sigma_1, \sigma_2, \sigma_1', \sigma_2' \in Q$. Each solution of (6.1) yields, by multiplication with $\gamma_o \in Q$, a solution of (6) with $\gamma = \gamma_o$, and conversely each solution of (6) with $\gamma = \gamma_o \in Q$ yields, by multiplication with γ_0^{-1}, a solution of (6.1). Hence $\mathrm{N}(\gamma_o) = \mathrm{N}(1)$ for each $\gamma_o \in Q$, and similarly $\mathrm{N}(-\gamma_o) = \mathrm{N}(-1)$. On the other hand $1 = \sigma_2 - \sigma_1 \Leftrightarrow -1 = \sigma_2' - \sigma_1'$ with $\sigma_2' = \sigma_1' = \sigma_2$ hence also $\mathrm{N}(1) = \mathrm{N}(-1)$ and we conclude (since each $\gamma \neq 0$ is either γ_o or $-\gamma_o$) that $\mathrm{N}(\gamma)$ is the same number μ for each $\gamma \neq 0$. Therefore $\mu(\mathrm{q}-1) = 2\mu(2m+1)$ is equal to the number of expressions $\sigma_1 - \sigma_2 \neq 0$, $\sigma_1, \sigma_2 \in Q$ i.e. to $2m(2m+1)$, giving $\mu = m$.

Theorem 4.

Let $\mathrm{q} = 4\mathrm{m}+3$ *be a prime power* p^k *and* G *the elementary abelian* p*-group of order* p^k *and exponent* p. *Then there exist complementary difference sets in* G.

Corollary. *If* $\mathrm{q} = 4\mathrm{m}+3$ *is a prime power then there exists a* $T_{2,2m+1}$ *tournament of type (E) and order* $2\mathrm{q}+1$.

The proof follows immediately from Paley's construction of H-matrices of order q and the doubling described in Theorem 1. The group G of Theorem 4 is isomorphic to the additive group of $GF(q)$ and we can use the elements of $GF(q)$ to represent G. As before we denote by Q the set of quadratic residues of $GF(q)$ and set $A = B = Q$; then (D1) is trivially satisfied and also (D2) (with m being replaced by $2m+1$) since by Lemma 4 both equations $\delta = \alpha_1 - \alpha_2$ ($\alpha_1\ \alpha_2 \in A = Q$) and $\delta = \beta_1 - \beta_2$ ($\beta_1, \beta_2 \in B = Q$) have m solutions.

Theorem 5.

Let $\mathrm{q} = 2\mathrm{m}+1$ *be a prime power* $\mathrm{p}^k \equiv 5 \pmod 8$ *(hence* $\mathrm{m} \equiv 2 \pmod 4$*)* *and* G *the elementary abelian* p*-group of order* p^k *and exponent* p. *Then there exist complementary difference sets in* G.

Corollary. If $\mathrm{q} = 2\mathrm{m}+1$ *is a prime power* $\equiv 5 \pmod 8$ *then there exists a* $\mathrm{T}_{2,m}$ *tournament of order* $4\mathrm{m}+3 = 2\mathrm{q}+1$ *and type (E).*

An immediate consequence is

Theorem 6.

For q *prime power* $\equiv 5 \pmod 8$ *there exists a skew Hadamard matrix of order* $2(\mathrm{q}+1)$.

Although Hadamard matrices of order $2(q+1)$ are known to exist even when $q \equiv 1 \pmod 8$ (Paley [1], Lemma 4) the result in Theorem 6 seems to be new. Paley's matrices are not skew and it is very unlikely that their rows and columns can be rearranged so as to yield skew H-matrices and $\mathrm{T}_{2,m}$ tournaments. The configurations obtained from the present construction are definitely not isomorphic to those of Paley, except when $q = 5$.

Proof of Theorem 5. We again identify G with the additive group of $GF(q)$. Let ρ be a primitive root of $GF(q)$ and G_o the multiplicative group of $GF(q)$, of order $q-1$ and generated by ρ. Denote by $H_o = gp\,\{\rho^4\}$ the subgroup of index 4 of G_o, H_i, $i = 1, 2, 3$ the coset mod H_o in G_o containing ρ^i, and set $K = H_o \cup H_1$, $K^* = H_o \cup H_3$.

We take $A = K$, $B = K^*$. Both contain m elements since H_o contains $\frac{1}{4}(q-1) = \frac{1}{2}m$ elements. Also condition (D1) is satisfied since $-1 = \rho^{\frac{1}{2}(q-1)} = \rho^m \in H_2$ by assumption hence $\alpha \in K \Rightarrow -\alpha \in H_2 \cup H_3$.

To verify condition (D2) consider for fixed $\delta_o \in H_o$ the following equations in $\alpha_1, \alpha_2 \in K$, $\beta_1, \beta_2 \in K^*$:

$$\delta_0 = \alpha_1 - \alpha_2 \tag{7.0}$$

$$\rho\delta_0 = \beta_1 - \beta_2 \tag{7.1}$$

$$\rho^2\delta_0 = \alpha_1 - \alpha_2 \tag{7.2}$$

$$\rho^3\delta_0 = \beta_1 - \beta_2 . \tag{7.3}$$

Clearly the number of solutions of each of these equations is independent of the choice of $\delta_o \in H_o$ since

$$\alpha \in K, \quad \beta \in K^* \Rightarrow \rho^{4i} \alpha \in K, \quad \rho^{4i} \beta \in K^*$$

for every i. Furthermore the numbers of solutions of (7.0) and (7.3) are equal to each other because $\alpha \in K \Rightarrow \beta = \alpha \rho^3 \in K^*$ and $\beta \in K^* \Rightarrow \rho^{-3}$ $\beta = \alpha \in K$. Similarly the numbers of solutions of (7.1) ans (7.2) are equal because

$$\beta \in K^* \Rightarrow \rho\beta^* \in K .$$

Finally (7.0) and (7.2) have the same number of solutions because

$$\alpha \in K \Rightarrow -\rho^2 \alpha \in K .$$

By the same argument it can be shown that the number of solutions of each of the equations

(8.0) $$\delta_0 = \beta_1 - \beta_2$$

(8.1) $$\rho\delta_0 = \alpha_1 - \alpha_2$$

(8.2) $$\rho^2 \delta_0 = \beta_1 - \beta_2$$

(8.3) $$\rho^3 \delta_0 = \alpha_1 - \alpha_2$$

is the same. Hence for each $\delta \neq 0$ the total number of solutions of

$$\delta = \alpha_1 - \alpha_2 , \quad \delta = \beta_1 - \beta_2$$

is the same number μ. Therefore $\mu(q-1) = 2\mu m$ is equal to the total number of expressions $\alpha_1 - \alpha_2$, $\beta_1 - \beta_2$, i.e. to $2m(m-1)$, giving $\mu = m$—1 as required.

REFERENCES

[1] PALEY, R. E. A. C., On orthogonal matrices. *J. Math. Phys.*, *12* (1933), pp. 311-320.

[2] RYSER, H. J., Combinatorial Mathematics. *Carus Mathematical Monographs*, No. 14.

[3] SZEKERES, E. and G., On a problem of Schütte and Erdös. *Math. Gazette*, *49* (1965), pp. 290-293.

[4] TODD, J. A., A combinatorial problem. *J. Math. Phys.*, *12* (1933), pp. 321-333.

[5] JOHNSEN, E. J., Integral Solutions to the incidence Equation for finite projective plane cases of orders $n \equiv 2$ (mod. 4). *Pacific J. Math.*, *17* (1966), pp. 97-120.

(Reçu le 15 avril 1968)

G. Szekeres
University of New South Wales,
Kensington, N.S.W., Australia.