J. Austral. Math. Soc. (Series A) 32 (1982), 399–404

DOUBLY REGULAR TOURNAMENTS OF SZEKERES TYPE

NOBORU ITO

(Received 9 September 1980; revised 2 February 1981)

Communicated by W. D. Wallis

Abstract

The purpose of this note is to determine the automorphism group of the doubly regular tournament of Szekeres type, and to use it to show that the corresponding skew Hadamard matrix H of order $2(q+1)$, where $q \equiv 5 (\text{mod}\, 8)$ and $q > 5$, is not equivalent to the skew Hadamard matrix $H(2q+1)$ of quadratic residue type when $2q+1$ is a prime power.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 05 B 20, 20 B 25.

1. Hadamard 2-design of Szekeres type and the associated tournament

Let q be a prime power such that $q \equiv 5 (\text{mod}\, 8)$ and $q > 5$, ρ a generator of $GF(q)^x$ and $Q = \langle \rho^4 \rangle$. Further let $Q_i = Q\rho^i$ $(0 \leq i \leq 3)$, $A = Q_0 \cup Q_1$, $B = Q_0 \cup Q_3$ and $C = Q_2 \cup Q_3$. Then an Hadamard 2-$(2q+1, q, \frac{1}{2}(q-1))$ design $D(q) = (P(q), B(q))$ of Szekeres type is constructed as follows (Szekeres (1969)). $P(q)$ is a union of $GF(q)$, its disjoint copy $GF(q)'$ and a further point t, where $a \leftrightarrow a'$ is an isomorphism between $GF(q)$ and $GF(q)'$. $B(q)$ consists of three kinds of blocks labelled as $\alpha(a)$, $\alpha(a)'$ $(a \in GF(q))$ and $\alpha(t)$, where

$$\alpha(a) = A + a \cup \{a'\} \cup B' + a',$$
$$\alpha(a') = B + a \cup \{t\} \cup C' + a'$$

and

$$\alpha(t) = GF(q).$$

This work was partially supported by NSF Grant MCS-7902750.

© Copyright Australian Mathematical Society 1982

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press

Now let $D = (P, B)$ be an Hadamard 2-design, where P and B denote the sets of points and blocks of D respectively. Then a bijection T from B to P is called a tournament of D if (i) $T(\alpha) \notin \alpha$ for every $\alpha \in B$ and (ii) $T(\alpha) \in \beta$ if and only if $T(\beta) \notin \alpha$ for any distinct $\alpha, \beta \in B$.

Now if we define T by $T(\alpha(a)) = a$, $T(\alpha(a')) = a'$ and $T(\alpha(t)) = t$, then T is a tournament of $D(q)$ (Szekeres (1969)). We call $(D(q), T)$ the tournament of Szekeres type.

An automorphism of D is called a T-automorphism if it commutes with T. The set of all T-automorphisms forms a subgroup, the automorphism group of the tournament, of the automorphism group of D. Obviously the automorphism group of a tournament has odd order, and hence by the Feit-Thompson theorem it is solvable.

Now let $G(T)$ denote the automorphism group of $(D(q), T)$. Then $G(T)$ contains the following permutations on $P(q)$:

(1) The permutation τ corresponding to an element τ of $GF(q)$; $\tau(a) = a + \tau$, $\tau(t) = t$, and $\tau(a') = a' + \tau'$.

(2) The permutation σ corresponding to an element σ of Q; $\sigma(a) = a\sigma$, $\sigma(t) = t$, and $\sigma(a') = a'\sigma'$, and

(3) The permutation θ corresponding to an automorphism θ of $GF(q)$ and $GF(q)'$; $\theta(a) = a^{\theta}$, $\theta(t) = t$, and $\theta(a') = a'^{\theta}$.

Clearly these permutations form a subgroup $G(T)^*$ of $G(T)$ of order $\frac{1}{4}q(q-1)r$, where $q = p^r$.

Proposition 1. $G(T)^* = G(T)$.

Proof. For a subgroup X of $G(T)$, and $x, y, \ldots$ points of $P(q)$ $X_{x,y,\ldots}$ denotes the pointwise stabilizer of $x, y, \ldots$ in X. Now the set of all τ forms a normal subgroup N^* of $G(T)^* = G(T)^*_t$ of order q. If $q = p$, a prime, then N^* is minimal normal in $G(T)^*$. If $q = p^r$ with $r > 1$, then, since $q \equiv 5 (\bmod 8)$, r is odd. So by a theorem of Zsygmondy, Satz 4 of Rédei (1958), there exists a prime divisor l of $q - 1$ such that r is the order of p modulo l. We call such an l an essential prime divisor of $q - 1$. Since the order of $G(T)^*$ is divisible by l, N^* is minimal normal in $G(T)^*$. Since $G(T)$ is of odd order, $G(T)_t$ has $GF(q)$ as a point orbit on which $G(T)_t$ induces a faithful primitive permutation group. Let N be the minimal normal subgroup of $G(T)_t$. Since $N \cap N^*$ is normalized by $G(T)^*_{t,0}$, if $N \neq N^*$, then $N \cap N^* = 1$. Now N has order q and $C(N) = N$, where C denotes the centralizer in $G(T)$ (II.3.2, page 159 of Huppert (1967)). Since N^*N is a normal p-subgroup of $G(T)^*N$, $N \cap Z(N^*N)$, where Z denotes the center, is a non-trivial normal subgroup of $G(T)^*N$. As above N is minimal normal in $G(T)^*N$. So we have that $N = Z(N^*N)$, which is a contradiction. Thus we have that $N = N^*$.

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press

The set of all σ and θ forms the subgroup $G(T)^*_{t,0}$ of order $\frac{1}{4}(q-1)r$ of $G(T)_{t,0}$. The powers of σ form a normal subgroup S of $G(T)^*_{t,0}$ of order $\frac{1}{4}(q-1)$. Let M be a minimal normal subgroup of $G(T)_{t,0}$ of order m^s, where m is prime. Let us consider a subgroup $G(T)^*M = NMG(T)^*_0$. Since $C(N) = N$, by Sylow's theorem we have that $q \equiv 1(\operatorname{mod} m)$. If m is an essential prime divisor of $q-1$, then by P. Hall's theorem we may assume that M is contained in S. In particular, M is cyclic and irreducible as a subgroup of the general linear group $\mathrm{GL}(r, p)$. So by Hilfssatz 2 of Huppert (1957), we have that $G(T)^* = G(T)_t$.

Now let us assume that for every minimal normal subgroup M of order m^s of $G(T)_{t,0}$ m is not an essential prime divisor of $q-1$. Then let us consider a subgroup NML of $G(T)_t$ of order qm^sl, where L is a subgroup of S of order l, an essential prime divisor of $q-1$. If $C(L) \cap MN = 1$, then NML is a Frobenius group whose kernel is equal to NM. Then by a theorem of Thompson (V.8.7, page 499 of Huppert (1967)), NM is nilpotent, which contradicts the fact $C(N) = N$. Thus $M_1 = C(L) \cap MN \neq 1$. Clearly M_1 is an m-group and we may assume that $M_1 \subseteq M$. If $M_1 \neq M$, then by a theorem of Maschke (3.1.1, page 66 of Gorenstein (1968)), $M = M_1 \times M_2$, where M_2 is also normalized by L. Considering NM_2L instead of NML, we get $C(L) \cap M_2N \neq 1$, which is a contradiction. So $M = M_1$, and we see that every minimal normal subgroup of $G(T)_{t,0}$ is contained in $C(L)$, and hence every minimal normal subgroup of $G(T)_{t,0}$ is cyclic. Let F be the Fitting subgroup of $G(T)_{t,0}$. Then by Fitting's theorem F is not contained in $C(L)$. So there exists a Sylow m-subgroup $F(m)$ of F such that $F(m)$ is not contained in $C(L)$. If $F(m)$ is Abelian, then as above we see that $\Omega_1(F(m)) \subseteq C(L)$, where Ω_1 denotes the set of elements of order m, and hence $F(m) \subseteq C(L)$ (IV.5.5, page 435 of Huppert (1967)). So $F(m)$ is non-Abelian. By a theorem of Thompson (5.3.11, page 185 of Gorenstein (1968)), $F(m)$ contains a characteristic subgroup M^* such that M^* has class two and that $M^* \cap C(L) \subseteq Z(M^*)$, the center of M^*. Since $Z(M^*) \subseteq C(L)$, $Z(M^*)$ is cyclic. If $\Omega_1(M^*) \subseteq C(L)$, then $M^* \subseteq (L)$ (IV.5.5, page 435 of Huppert (1967)). So we may assume that $M^* = \Omega_1(M^*)$, namely M^* is extra-special.

Now the degree of any complex-valued faithful irreducible character of M^*L equals m^u, where m^{2u+1} is the order of M^* (5.5.5, page 208 of Gorenstein (1968)).

N provides a faithful r-dimensional representation R over $GF(p)$ of M^*L. Since $Z(M^*L)$ is the least normal subgroup of order m of M^*L, at least one absolutely irreducible component of R must be faithful for M^*L. Since p is relatively prime to the order of M^*L, M^*L has a faithful complex-valued irreducible character of degree at most r (For this see V, Section 5 of Huppert (1968).) Hence we obtain that $r \geqslant m^u$. On the other hand, by Sylow's theorem we have that $m^{2u} \equiv 1(\operatorname{mod} l)$. Since l and m are odd, we have that $m^u \geqslant l$, and hence $r \geqslant l$. Since l is an essential prime divisor of $q-1$ and $q = p^r$, we have that $l \equiv 1(\operatorname{mod} r)$. This is clearly a contradiction. So we have that $G(T)_t = G(T)^*$.

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press

If $G(T) = G(T)_t$, then we are done. So we assume that $G(T) \neq G(T)_t$. Since the point orbits of $G(T)_t$ are $GF(q)$, $GF(q)'$ and $\{t\}$, and since $G(T)$ has odd order, $G(T)$ is primitive on $P(q)$. So $2q + 1 = k^a$, where k is a prime such that $k \equiv 3 (\mathrm{mod}\, 4)$, and a is odd (II.3.2, page 159 of Huppert (1968)). If $a = 1$, then $2q + 1$ is a prime and $G(T)$ is primitive and solvable. So $G(T)_t$ is cyclic. But since $q > 5$, $\frac{1}{4}(q - 1) > 1$ and $G(T)^*$ is not cyclic. This is a contradiction. So $a > 1$. Now p is an essential prime divisor of $k^a - 1$, and hence $p \equiv 1 (\mathrm{mod}\, a)$. On the other hand, $2p^r = k^a - 1 = (k - 1)(k^{a-1} + \cdots + k + 1)$ implies that $k - 1 = 2p^s$ and $k^{a-1} + \cdots + k + 1 = p^t$. So if $k \neq 3$, then $k \equiv 1 (\mathrm{mod}\, p)$ and $a \equiv 0 (\mathrm{mod}\, p)$, which is a contradiction. So $k = 3$.

Since an element ($\neq 1$) of N fixes only the point t, $N \cap N^x = 1$ for $N \neq N^x$, where $x \in G(T)$. This implies that N is cyclic and $r = 1$ (V.8.7, page 499 of Huppert (1968)). Now by a theorem of Huppert (Hilfssatz 2 of Huppert (1957)), $G(T)$ is contained in the semi-linear group over $GF(3^a)$. In particular, the order of $G(T)$ divides $\frac{1}{2}3^a(3^a - 1)a$, and so $\frac{1}{12}(p - 1)$ divides a. Thus we have that $12a = \frac{1}{2}l(3^a - 3)$ or $a = \frac{1}{8}l(3^{a-1} - 1)$. This which implies that $a = 3$, $p = 13$. This case requires a combinatorial analysis, because the automorphism group of the Hadamard 2-(27, 13, 6) design of quadratic residue type has order $3^3.13.3$ (Theorem 6 of Kantor (1969)).

We notice that $GF(13)^{\times} = \langle 2 \rangle$, $Q_0 = \{1, 3, 9\}$, $Q_1 = \{2, 5, 6\}$, $Q_2 = \{4, 10, 12\}$, and $Q_3 = \{7, 8, 11\}$. Further we have that

$$\tau(1) = (0, 1, \ldots, 12)(0', 1', \ldots, 12')$$

and

$$\sigma = (1, 3, 9)(2, 6, 5)(4, 12, 10)(7, 8, 11)(1', 3', 9') \cdots (7', 8', 11').$$

Moreover these have similar presentations on blocks.

Let $\rho \neq 1$ be an element of the center of the Sylow 3-subgroup of $G(T)$ containing σ. Then we may assume that the cycle structure of ρ involves $(0, 0', t)$. So ρ leaves $\alpha(0) \cap \alpha(0') \cap \alpha(t)$ invariant. This implies that ρ leaves $\{1, 3, 9\}$, $\{2, 5, 6, 7, 8, 11, 7', 8', 11'\}$, $\{4, 10, 12, 1', 3', 4', 9', 10', 12'\}$ and $\{2', 5', 6'\}$ invariant. So ρ leaves $\alpha(1) \cap \alpha(3) \cap \alpha(9)$, and hence $\{4', 10', 12'\}$ invariant, too. Then $\langle \sigma, \rho \rangle$ contains a non-identity element fixing at least six points, which is a contradiction.

2. Hadamard matrix of order $2(q + 1)$ of quadratic residue type

Let $2q + 1$ be a prime power, $2q + 1 = k^a$ with k a prime. Then, since $q \equiv 5 (\mathrm{mod}\, 8)$, $k \equiv 3 (\mathrm{mod}\, 4)$ and a is odd. Let χ be the quadratic (residue) character of $GF(k^a)^{\#}$ with usual convention $\chi(0) = 0$. Let C be the matrix of

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press

order k^a whose (b, c)-entry equals $\chi(b - c)$. (We may choose any linear ordering of elements of $GF(k^a)$ to form the matrix C.) Put

$$S = \begin{pmatrix} 0 & 1\dots1 \\ -1 & \\ \vdots & C \\ -1 & \end{pmatrix}.$$

Then, since $k^a \equiv 3(\text{mod}\, 4)$, S is skew-symmetric. Now $H(2(q + 1)) = -I + S$, where I is the identity matrix of order $2(q + 1)$, is a skew Hadamard matrix of order $2(q + 1)$ of quadratic residue type.

PROPOSITION 2. *Let H be a skew Hadamard matrix corresponding to the Hadamard 2-design of Szekeres type in Section* 1. *Then H and $H(2(q + 1))$ are inequivalent, where $q > 5$.*

PROOF. Assume that H and $H(2(q + 1))$ are equivalent. Then $H(2(q + 1))$ must have an associated tournament isomorphic to the tournament of Szekeres type in Section 1.

To describe (3- and 2-) Hadamard designs associated with $H(2(q + 1))$ we adopt a row-block and column-point mode. Since $H(2(q + 1))$ is equivalent to its own transpose, Theorem 2.2 of Hall (1962), this does not lose any generality. Furthermore we label the first column and row by ∞. So the block $\alpha(\infty)$ corresponding to the first row consists of ∞^* and $GF(k^a)$, where * indicates the corresponding entry of $H(2(q + 1))$ is -1.

Now the automorphism group G of $H(2(q + 1))$ is determined by M. Hall, Jr. and W. Kantor, Theorem 2.1 of Hall (1962) and Theorem 6 of Kantor (1969). G is transitive on rows of $H(2(q + 1))$. So all the Hadamard 3-designs associated with $H(2(q + 1))$ are isomorphic, and we have only to consider the Hadamard 3-design $H(2(q + 1))(\alpha(\infty))$ at $\alpha(\infty)$. $G_{\alpha(\infty)}$ has two point orbtis, $\{\infty\}$ and $GF(k^a)$. The contraction of $H(2(q + 1))(\alpha(\infty))$ at ∞ is the usual Hadamard 2-design D of quadratic residue type. Namely let R be the set of quadratic residues (squares) of $GF(k^a)^\#$. Then blocks of D have the form $R + x$, $x \in GF(k^a)$. Furthermore, $T(R + x) = x$ is a tournament of D, and the automorphism group of (D, T) coincides with that of D and has order $(2q + 1)qa$. Here we notice that T might not be the unique tournament of D. On the other hand, the contraction of $H(2(q + 1))(\alpha(\infty))$ at 0 has automorphism group of order qa.

First let us assume that D has a tournament which is isomorphic to the tournament of Szekeres type in Section 1. Then $\frac{1}{4}(q - 1)r$ divides $(2q + 1)a$. Then $k^a - 3$ divides $8ak^a$. So we may put $(8a + b)(k^a - 3) = 8ak^a$ for some positive integer b. This implies that $b(k^a - 3) = 24a$. If $a = 1$, then $k = 2q + 1$ is a prime. By assumption $q \equiv 3(\text{mod}\, 8)$ and $q > 5$. Since $k < 27$, we have that

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press

$q = 11$ and $k = 23$. This contradicts $b(k-3) = 24$. Thus $a > 1$. Since a is odd, $a \geqslant 3$. If $k \geqslant 5$, then $k^a - 3 \geqslant 5^a - 3 > 24a$. So $k = 3$. If $a \geqslant 5$, then $3^a - 3 > 24a$. So $a = 3$ and $q = 13$.

Next we assume that the contraction of $H(2(q+1))(\alpha(\infty))$ at 0 has a tournament of Szekeres type in Section 1. Then $\frac{1}{4}(q-1)r$ divides a. Since $q > 5$, $a > 1$. Since a is odd, $a \geqslant 3$. If $k \geqslant 5$, then $\frac{1}{4}(q-1) = \frac{1}{8}(k^a - 3) \geqslant \frac{1}{8}(5^a - 3) > a$. So $k = 3$. If $a \geqslant 5$, then $\frac{1}{8}(3^a - 3) > a$. So $a = 3$ and $q = 13$.

Thus, possibly except for $q = 13$, $H(2(q+1))$ has no associated tournament isomorphic to the tournament of Szekeres type in Section 1. But a tedious hand checking shows that the above mentioned natural tournament is the only tournament attached to $H(28)$.

References

D. Gorenstein (1968), *Finite groups* (Harper and Row).

M. Hall, Jr. (1962), 'Note on the Mathieu group M_{12}', *Arch. Math. (Basel)* **13**, 334–340.

B. Huppert (1957), 'Zweifach transitive, ausflösbare Permutationsgruppen', *Math. Z.* **68**, 126–150.

B. Huppert (1967), *Endliche Gruppen I* (Springer-Verlag).

W. M. Kantor (1969), 'Automorphism groups of Hadamard matrices', *J. Combinatorial Theory* **6**, 279–281.

L. Rėdei (1958), 'Über die algebraischzahlentheortische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy', *Acta Sci. Math. Szeged.* **19**, 98–126.

G. Szekeres (1969), 'Tournaments and Hadamard matrices', *Enseignment Math.* **15**, 269–278.

Department of Mathematics
University of Illinois at Chicago Circle
Box 4348
Chicago, Illinois 60680
U.S.A.

https://doi.org/10.1017/S1446788700024952 Published online by Cambridge University Press