Hokkaido Mathematical Journal Vol. 9 (1980) p. 129–134

Note on Hadamard matrices of Pless type

To Goro Azumaya on his sixtieth birthday

Noboru ITO*

(Received May 14, 1979)

Let H be an Hadamard matrix of order n. Namely H is a ± 1 matrix of degree n such that $HH^{t}=nI$, where t denotes the transposition and I is the identity matrix of degree n. We assume that $n>1$. It is well known that $n=2$ or n is divisible by 4.

Let $P=\{1, \cdots, n, 1^{*}, \cdots, n^{*}\}$ be the set of $2n$ points, where we assume that $(i^{*})^{*}=i$ for $1\leqq i\leqq n$. Then with each row vector $\boldsymbol{a}$ of H we associate the block $\boldsymbol{a}$, and n-subset of P, as follows. $\boldsymbol{a}$ contains j or j^{*} according as the j-th entry of $\boldsymbol{a}$ is 1 or -1. The complement $\boldsymbol{a}^{*}=P-\boldsymbol{a}$ of $\boldsymbol{a}$ is also called a block. Let B be the set of $2n$ blocks. Then we call $M(H)=(P, B)$ the matrix design of H. $M(H)$ is a 1-design, namely each point belongs to exactly n blocks. Moreover it is almost a symmetric 2-design. Namely by the orthogonality of column vectors of H each 2-subset of P not of the form $\{i, i^{*}\}$ is contained in exactly $\frac{1}{2}n$ blocks, while $\{i, i^{*}\}$ is contained in no blocks.

Let $G(H)$ be the set of all permutations $\boldsymbol{s}$ on P such that (i) $\boldsymbol{s}(B)=B$ and that (ii) if $\boldsymbol{s}(a)=b$ then $\boldsymbol{s}(a^{*})=b^{*}$. Then $G(H)$ forms a subgroup of the symmetric group on P, namely the automorphism group of H. Let $\boldsymbol{z}=\prod_{i=1}^{n}(i, i^{*})$. Then $\boldsymbol{z}$ belongs to the center of $G(H)$ and it interchanges $\boldsymbol{a}$ with $\boldsymbol{a}^{*}$ for every $\boldsymbol{a}$. We call $\boldsymbol{z}$ the $*$-element of $G(H)$.

Now the purpose of this note is the following: (i) to show that an Hadamard matrix of order $2(q+1)$, where q is a prime power with $q\equiv 3 \pmod 4$, constructed by V. Pless in [6], $H_{3}(q)$ in her notation, which we call an Hadamard matrix of Pless type, is inequivalent to the Hadamard matrix of order $2(q+1)$ of Paley type, provided that $q>3$. It is well known that there exists exactly one equivalent class of Hadamard matrices of order 8; (ii) to determine the automorphism groups of two types of Hadamard matrices of degree $2(q+1)$ mentioned above.

§ 1. Kimberley and Longyear number.

Let H be an Hadamard matrix of order n and $M(H)=(P, B)$ the matrix design. Let $\{\boldsymbol{a}, \boldsymbol{b}\}$ be a 2-subset of B not of the form $\{\boldsymbol{c}, \boldsymbol{c}^*\}$. Then $\mathscr{K}(\boldsymbol{a}, \boldsymbol{b})$ and $K(\boldsymbol{a}, \boldsymbol{b})$ denote the set and half of the number of 2-subsets $\{\boldsymbol{c}, \boldsymbol{d}\}$ of B such that $\boldsymbol{a}\cap\boldsymbol{b}\cap\boldsymbol{c}=\boldsymbol{a}\cap\boldsymbol{b}\cap\boldsymbol{d}$ respectively. We notice that $\{\boldsymbol{a}, \boldsymbol{b}\}$ and $\{\boldsymbol{a}^*, \boldsymbol{b}^*\}$ belong to $\mathscr{K}(\boldsymbol{a}, \boldsymbol{b})$. We call $K(H)=\max_{\{\boldsymbol{a},\boldsymbol{b}\}} K(\boldsymbol{a}, \boldsymbol{b})$ and $L(H)=K(H^t)$ the Kimberley and Longyear numbers of H respectively. If $G(H)$ is transitive on B, then $K(H)=\max_{\boldsymbol{b}} K(\boldsymbol{a}, \boldsymbol{b})$ for any given $\boldsymbol{a}$. But we notice that this is not the case in general. Clearly $K(H)$ and $L(H)$ are invariant under the equivalence of Hadamard matrices.

Now let $H=H_1\times H_2$ be a Kronecker product of two Hadamard matrices of orders n_1 and n_2 respectively. Then H is an Hadamard matrix of order $n=n_1n_2$. Let $M(H_i)=(P_i, B_i)$ and $M(H)=(P, B)$ be the matrix designs of H_i and H respectively $(i=1, 2)$. Then it is convenient to regard P as the set of all ordered pairs (a_1, a_2), where $a_i\in P_i$ $(i=1, 2)$, with the rule that $(a_1, a_2)^*=(a_1^*, a_2)=(a_1, a_2^*)$ and $(a_1^*, a_2^*)=(a_1, a_2)$. Then we denote the block of B corresponding to an ordered pair $(\boldsymbol{a}_1, \boldsymbol{a}_2)$ of blocks, where $\boldsymbol{a}_i\in B_i$ $(i=1, 2)$, by $(\boldsymbol{a}_1, \boldsymbol{a}_2)$ itself. Since $(\boldsymbol{a}_1, \boldsymbol{a}_2)=(\boldsymbol{a}_1^*, \boldsymbol{a}_2^*)$, $(\boldsymbol{a}_1, \boldsymbol{a}_2)$ contains $(a_1, a_2)^*$ if and only if exactly one of $\boldsymbol{a}_i$ contains a_i $(i=1, 2)$.

LEMMA 1. If $\{\boldsymbol{c}_i, \boldsymbol{d}_i\}$ belongs to $\mathscr{K}(\boldsymbol{a}_i, \boldsymbol{b}_i)$ $(i=1, 2)$, then $\{\boldsymbol{c}, \boldsymbol{d}\}$ belongs to $\mathscr{K}(\boldsymbol{a}, \boldsymbol{b})$, where $\boldsymbol{a}=(\boldsymbol{a}_1, \boldsymbol{a}_2)$, $\boldsymbol{b}=(\boldsymbol{b}_1, \boldsymbol{b}_2)$, $\boldsymbol{c}=(\boldsymbol{c}_1, \boldsymbol{c}_2)$ and $\boldsymbol{d}=(\boldsymbol{d}_1, \boldsymbol{d}_2)$.

Proof is straightforward.

Conversely let us assume that $\boldsymbol{a}\cap\boldsymbol{b}\cap\boldsymbol{c}=\boldsymbol{a}\cap\boldsymbol{b}\cap\boldsymbol{d}$, where $\boldsymbol{a}=(\boldsymbol{a}_1, \boldsymbol{a}_2)$, $\boldsymbol{b}=(\boldsymbol{b}_1, \boldsymbol{b}_2)$, $\boldsymbol{c}=(\boldsymbol{c}_1, \boldsymbol{c}_2)$ and $\boldsymbol{d}=(\boldsymbol{d}_1, \boldsymbol{d}_2)$. First we consider the case where $\boldsymbol{b}_i\neq\boldsymbol{a}_i$, $\boldsymbol{a}_i^*$ $(i=1, 2)$. Then we have that either $\boldsymbol{a}_i\cap\boldsymbol{b}_i\cap\boldsymbol{c}_i=\boldsymbol{a}_i\cap\boldsymbol{b}_i\cap\boldsymbol{d}_i$ or $\boldsymbol{a}_i\cap\boldsymbol{b}_i\cap\boldsymbol{c}_i=\boldsymbol{a}_i\cap\boldsymbol{b}_i\cap\boldsymbol{d}_i^*$ $(i=1, 2)$. There remain the cases where $\boldsymbol{a}_1=\boldsymbol{b}_1$ and $\boldsymbol{b}_2\neq\boldsymbol{a}_2^*$, or $\boldsymbol{a}_2=\boldsymbol{b}_2$ and $\boldsymbol{b}_1\neq\boldsymbol{a}_1$, $\boldsymbol{a}_1^*$. If $\boldsymbol{a}_1=\boldsymbol{b}_1$, then let $\boldsymbol{d}_1=\boldsymbol{c}_1$ for any $\boldsymbol{c}_1\in B_1$. Now if $\{\boldsymbol{c}_2, \boldsymbol{d}_2\}$ belongs to $\mathscr{K}(\boldsymbol{a}_2, \boldsymbol{b}_2)$, then $\{(\boldsymbol{c}_1, \boldsymbol{c}_2), (\boldsymbol{c}_1, \boldsymbol{d}_2)\}$ belongs to $\mathscr{K}(\boldsymbol{a}, \boldsymbol{b})$. The rest is similar. So we have the following lemma.

LEMMA 2. If $\boldsymbol{b}_1=\boldsymbol{a}_1$ and $\boldsymbol{b}_2\neq\boldsymbol{a}_2$, $\boldsymbol{a}_2^*$ then $K(\boldsymbol{a}, \boldsymbol{b})=n_1K(\boldsymbol{a}_2, \boldsymbol{b}_2)$. If $\boldsymbol{b}_2=\boldsymbol{a}_2$ and $\boldsymbol{b}_1\neq\boldsymbol{a}_1$, $\boldsymbol{a}_1^*$ then $K(\boldsymbol{a}, \boldsymbol{b})=n_2K(\boldsymbol{a}_1, \boldsymbol{b}_1)$. If $\boldsymbol{b}_i\neq\boldsymbol{a}_i$, $\boldsymbol{a}_i^*$ $(i=1, 2)$ then $K(a, b)=2K(a_1, b_1)\,K(a_2, b_2)$. In particular, $K(H)\geqq\max\{n_1K(H_2), n_2K(H_1)\}$.

Now let G_i and G denote the automorphism groups of $M(H_i)$ and $M(H)$ respectively $(i=1, 2)$. Let 1_i, z_i, 1 and z denote the identity and $*$-elements of G_i and G respectively $(i=1, 2)$. Let $\boldsymbol{s}_i\in G_i$ $(i=1, 2)$. Then consider the mapping $\boldsymbol{s}_1\boldsymbol{s}_2(a_1, a_2)=(\boldsymbol{s}_1a_1, \boldsymbol{s}_2a_2)$ of P. Since $\boldsymbol{s}_1\boldsymbol{s}_2(\boldsymbol{a}_1, \boldsymbol{a}_2)=(\boldsymbol{s}_1\boldsymbol{a}_1, \boldsymbol{s}_2\boldsymbol{a}_2)$, it induces an element of G. Clearly z_11_2 and 1_1z_2 induce the same element of G. On the other hand, let $\boldsymbol{s}_1\boldsymbol{s}_2$ induce the identity element of

G. Then $(s_1 a_1, s_2 a_2)=(a_1, a_2)$ for every $(a_1, a_2)\in P$. So $s_1 a_1=a_1$ and $s_2 a_2=a_2$, or $s_2 a_1=a_1{}^*$ and $s_2 a_2=a_2{}^*$ for every (a_1, a_2). Thus we have the following lemma.

LEMMA 3. G contains a subgroup isomorphic to $G_1\times G_2/\langle z_1 z_2\rangle$. In particular, if G_i is transitive on P_i (or B_i) $(i=1, 2)$, then G is transitive on P (or B).

LEMMA 4. Let T be an Hadamard matrix of order 2. Then $G(T)$ is a dihedral group of order 8.

PROOF. Let $T=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. Then the permutations $(1, 1^*)$ and $(1, 2)$ $(1^*, 2^*)$ generate $G(T)$.

REMARK. It is easy to see that if $K(H)\,L(H)>1$ then $n\equiv 0 \pmod 8$.

§ 2. Hadamard matrices of Pless type.

Let $GF(q)$ be a field of q elements, where q is a prime power such that $q\equiv 3 \pmod 4$, and x the quadratic character of $GF(q)$ with $x(0)=0$.

$$\text{Let } S=\begin{pmatrix} 0 & 1\cdots 1\ 1 \\ -1 & \\ \vdots & \boldsymbol{x}(b-a) \\ -1 & \\ -1 & \end{pmatrix},$$ where $\boldsymbol{x}(b-a)$ is the (a, b)-entry of $S(a, b\in GF(q))$.

Here we give the label ∞ to the first column and row of S, but we omit to indicate an ordering of elements of $GF(q)$. Then $H_0=I+S$ is called an Hadamard matrix of order $q+1$ of quadratic residue type.

We begin with the following lemma.

LEMMA 5. Let H_0 be the Hadamard matrix of order $q+1$ of quadratic residue type. Then $K(H_0)=L(H_0)=1$ for $q>7$.

PROOF. By a theorem of M. Hall Jr. [2] H_0^t is equivalent to H_0. So it suffices to show that $K(H_0)=1$. Since $G(H_0)$ is doubly transitive on the set $\{\{\boldsymbol{a}(\infty), \boldsymbol{a}(\infty)^*\}, \{\boldsymbol{a}(a), \boldsymbol{a}(a)^*\}, a\in GF(q)\}$, it suffices to show that $K(\boldsymbol{a}(\infty), \boldsymbol{a}(0))=1$. Now assume that $K(\boldsymbol{a}(\infty), \boldsymbol{a}(0))>1$. Then there exist $a, b\in GF(q)$ with $a\neq b$ such that $Q\cap Q+a=Q\cap Q+b$, where $Q=(GF(q)^{\times})^2$. This implies that $Q\cap Q-a=Q\cap Q+b-a$ and that $Q\cap Q+ac=Q\cap Q+bc$, $c\in Q$. So we have that $K(a(\infty), a(0))=\frac{1}{2}(q+1)$. Then by a theorem of C. Norman [5] H_0 is equivalent to the character table of an elementary Abelian 2-group. By theorems of W. Kantor [4] this is a contradiction for $q>7$.

REMARK. Ronald Evans (UCSD, La Jolla, CA) has obtained a more informative proof for Lemma 5.

Now let $H_1=T\times H_0$. H_1 is called an Hadamard matrix of Paley type. Then it follows from Lemma 2 that $K(H_1)= L(H_1)=q+1$.

On the other hand, in [6] V. Pless has constructed a series of Hadamard matrices of order $2(q+1)$ of the following type

$$H_2=\begin{pmatrix} I+S & I+S \\ I-S & -I+S \end{pmatrix},$$

which we call Hadamard matrices of order $2(q+1)$ of Pless type. Moreover, V. Pless has shown that $G(H_2)$ is transitive on both P and B, where $M(H_2)=(P, B)$. Multiplying the second, third, $\cdots$, $(q+1)$-st rows of H_2 by -1 we normalize H_2, and from now on H_2 indicates the normalized matrix.

Putting subscripts 1 and 2 to $\{\infty\}\cup GF(q)$, we indicate the left and right halves, and top and bottom halves of H_2. Moreover, we put

$$P=\left\{\infty_1, GF(q)_1, \infty_2, GF(q)_2, \infty_1{}^*, GF(q)_1{}^*, \infty_2{}^*, GF(q)_2{}^*\right\}$$

and $Q_i=(GF(q)_i{}^{\times})^2$ $(i=1, 2)$. Let $\boldsymbol{a}(\infty_i)$ and $\boldsymbol{a}(a_i)$ denote the blocks corresponding to the rows ∞_i and a_i respectively $(i=1, 2;\ a\in GF(q))$. Then we have that

$$\boldsymbol{a}(\infty_1)=\left\{\infty_1,\ GF(q)_1,\ \infty_2,\ GF(q)_2\right\}$$
$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_1)=\{\infty_1,\ -Q_1+a_1,\ \infty_2,\ -Q_2+a_2\}$$
$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)=\left\{\infty_1,\ GF(q)_2\right\}$$

and

$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_2)=\{\infty_1,\ a_1,\ -Q_1+a_1,\ Q_2+a_2\}\ ,$$

where $a\in GF(q)$. Now let us consider $K(\boldsymbol{a}(\infty_1), \boldsymbol{a}(\infty_2))$. We have that $\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)\cap\boldsymbol{a}(a_1)=\{\infty_1,\ -Q_2+a_2\}$ and $\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)\cap\boldsymbol{a}(a_2)=\{\infty_1,\ Q_2+a_2\}$. Thus $K(\boldsymbol{a}(\infty_1), \boldsymbol{a}(\infty_2))=1$, unless $q=3$. The rest is similar. So we have the followin proposition.

Poroposition 1. $K(H_2)=1$. *In particular, H_1 and H_2 are inequvalent for $q>3$.*

Porposition 2. $L(H_2)=q+1$.

Proof. Let us consider $H_2{}^t$. Then using the same notation as above we have that

$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_1)=\{\infty_1,\ Q_1+a_1,\ a_2\ Q_2+a_2\}$$
$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)=\left\{\infty_1,\ GF(q)_1\right\}$$

and

$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_2)=\{\infty_1\ Q_1+a_1,\ \infty_2,\ -Q_2+a_2\}\ .$$

So we have that $\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)\cap\boldsymbol{a}(a_1)=\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(\infty_2)\cap\boldsymbol{a}(a_2)=\{\infty_1, Q_1+a_1\}$ for every $a\in GF(q)$ and hence $K(\boldsymbol{a}(\infty_1), \boldsymbol{a}(\infty_2))=q+1$.

REMARK. (i) If $q=7$, then H_1 and H_2 are equivalent to H_1 and H_4 of [1] respectively. (ii) If $q=11$, then H_1 and H_2 are equivalent to H_1 and H_{10} of [3] respectively.

§ 3. Automorphism groups.

For $q=7$ and 11 $G(H_1)$ and $G(H_2)$ are determined in [1, 3]. So from now on we assume that $q>11$.

PROPOSITION 3. *$G(H_1)$ is isomorphic with $G(T)\times G(H_0)/\langle z_T z_0\rangle$, where z_T and z_0 are *-elements of $G(T)$ and $G(H_0)$ respectively.*

PROOF. Let $M(T)=(P_T, B_T)$, $M(H_0)=(P_0, B_0)$ and $M(H_1)=(P, B)$ be the matrix designs of T, H_0 and H_1 respectively. Let $\boldsymbol{a}=(\boldsymbol{a}_1, \boldsymbol{a}_2)$, $\boldsymbol{b}=(\boldsymbol{b}_1, \boldsymbol{b}_2)$ and $\boldsymbol{c}=(\boldsymbol{a}_1, \boldsymbol{c}_2)$ be three blocks of B such that $\boldsymbol{b}_1\neq\boldsymbol{a}_1$, $\boldsymbol{a}_1{}^*$ and $\boldsymbol{c}_2\neq\boldsymbol{a}_2$, $\boldsymbol{a}_2{}^*$. Then by Lemmas 2 and 5 we have that $K(\boldsymbol{a}, \boldsymbol{b})=q+1$, $K(\boldsymbol{a}, \boldsymbol{c})=2$ and $K(\boldsymbol{b}, \boldsymbol{c})=1$. Let $G(H_0)_{\{\boldsymbol{a}_2, \boldsymbol{a}_2{}^*\}}$ and $G(H_1)_{\boldsymbol{a}}$ be the stabilizers of $\{\boldsymbol{a}_2, \boldsymbol{a}_2{}^*\}$ and $\boldsymbol{a}$ in $G(H_0)$ and $G(H_1)$ respectively. Then there is no element of $G(H_1)_{\boldsymbol{a}}$ which transfers $\boldsymbol{b}$ to $\boldsymbol{c}$. So $G(H_1)_{\boldsymbol{a}}$ is isomorphic with $G(H_0)_{\{\boldsymbol{a}_2, \boldsymbol{a}_2{}^*\}}$. Since $[G(H_1):G(H_1)_{\boldsymbol{a}}]=4(q+1)$ and by a theorem of W. Kantor [4] $|G(H_0)|=(q+1)\,q(q-1)\,m$, where $q=p^m$ with p a prime, we have proved Proposition 3.

PROPOSITION 4. *$G(H_2)$ is isomorphic to the semi-direct product of a two-dimensional semi-linear group over $GF(q)$ and a cyclic group of order* 2.

PROOF. First we remark that the automorphisms of H_2 (or the code $C(q)$ in [6]) corresponding to the automorphisms of $GF(q)$ are not explicitly mentioned in [6].

Now $G(H_2)$ and $G(H_2{}^t)$ are clearly isomorphic. So we consider $G(H_2{}^t)$ instead of $G(H_2)$. Then the automorphism of $H_2{}^t$ corresponding to Z_2 in [6] is the generator of the cyclic group of order 2 mentioned in Proposition 4, and takes the following form; $Z_2=(\infty_2, \infty_2{}^*)\prod_{a\in GF(q)}(a_2, a_2)^*$. Z_2 interchanges $\boldsymbol{a}(\infty_1)$ with $\boldsymbol{a}(\infty_2)$, and $\boldsymbol{a}(a_1)$ with $\boldsymbol{a}(a_2)$ $(a\in GF(q))$.

Now in the notation of Proposition 2, we have that

$$\begin{aligned}&\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_1)\cap\boldsymbol{a}(b_1)\\&\qquad=\left\{\infty_1, (Q_1+a_1)\cap(Q_1+b_1), \{a_2, Q_2+a_2\}\cap\{b_2, Q_2+b_2\}\right\},\\&\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_1)\cap\boldsymbol{a}(c_2)\\&\qquad=\left\{\infty_1, (Q_1+a_1)\cap(Q_1+c_1), \{Q_2, Q_2+a_2\}\cap\{\infty_2, -Q_2+c_2\}\right\},\end{aligned}$$

and that

$$\boldsymbol{a}(\infty_1)\cap\boldsymbol{a}(a_2)\cap\boldsymbol{a}(c_2)$$
$$=\left\{\infty_1, (Q_1+a_1)\cap(Q_1+c_1),\ \infty_2, (-Q_2+a_2)\cap(-Q_2+c_2)\right\}.$$

So it follows that $K(\boldsymbol{a}(\infty_1), \boldsymbol{a}(a_1))=K(\boldsymbol{a}(\infty_1), \boldsymbol{a}(a_2))=2$.

Let $X=G(H_2^t)_{\boldsymbol{a}(\infty_1)}$ be the stabilizer of $\boldsymbol{a}(\infty_1)$ in $G(H_2^t)$. Then X leaves $\{\boldsymbol{a}(\infty_2), \boldsymbol{a}(\infty_2)^*\}$ invariant, and so it leaves $\{\infty_1, GF(q)_1\}$ and $\{\infty_2, GF(q)_2\}$ invariant or interchanges them. X is an automorphism group of an Hadamard 3-design of H_2^t at $\boldsymbol{a}(\infty_1)$. So if X does not leave $\{\infty_1, \infty_2\}$ invariant, then it follows that an Hadamard 3-design of H_0 at $\infty_i\cup GF(q)_i$ ($i=1$ or 2) has a doubly transitive automorphism group, which is against a theorem of W. Kantor [4], since $I-S$ is equivalent to H_0 by a theorem of M. Hall, Jr. [2]. So X leaves $\{\infty_1, \infty_2\}$ invariant.

Let Y be a subgroup of X of index at most 2 leaving $\{\infty_1\}$ and $GF(q)_1$ invariant. Then Y can be represented as an automorphism group of the matrix design corresponding to $I-S$. The kernel of this representation leaves ∞_1 and $GF(q)_1$ pointwise. Hence it is trivial by the construction of $C(q)$ [6].

Finally we show that $Y=X$. Otherwise, we have an involution $\boldsymbol{r}$ which interchanges ∞_1 with ∞_2 and $GF(q)_1$ with $GF(q)_2$. $\boldsymbol{r}$ leaves $\{\boldsymbol{a}(a_2), a\in GF(q)\}$ invariant. Since q is odd, $\boldsymbol{r}$ fixes at least one of them, say $\boldsymbol{a}(b_2)$. Then r interchanges b_1 with b_2, Q_1+b_1 with $-Q_2+b_2$ and $-Q_1+b_1$ with Q_2+b_2. Now if $\boldsymbol{r}$ fixes another $\boldsymbol{a}(c_2)$, then r interchanges c_1 with c_2. Since c_1 and c_2 are both squares or non-squares, this contradicts the above. If $\boldsymbol{r}$ interchanges $\boldsymbol{a}(c_2)$ with $\boldsymbol{a}(c_2')$, we get the similar contradiction.

By theorems of V. Pless [6] this proves Proposition 4.

Bibliography

[1] M. HALL Jr.: Hadamard matrix of order 16. J.P.L. Research Summary No. 36-10, 1 (1961), 21-26.

[2] M. HALL Jr.: Note on Mathieu group M_{12}. Arch. Math. 13 (1962), 334-340.

[3] N. ITO, J. LEON and J. LONGYEAR: Classification of 3-(24, 12, 5) designs, to appear.

[4] W. KANTOR: Automorphism groups of Hadamard matrices, JCT 6 (1969) 279-281.

[5] M. E. KIMBERLEY: On the construction of certain Hadamard designs. MZ 119 (1971) 41-59.

[6] V. PLESS: Symmetry codes over $GF(3)$ and new five-designs, JCTA 12 (1972), 119-142.

* This work is partially supported by NSF Grant. MCS 7810017

Department of Mathematics
University of Illinois at Chicago Circle