J. Math. Soc. Japan
Vol. 36, No. 1, 1984

Studies on Hadamard matrices with "2-transitive" automorphism groups

By Noboru ITO*) and Hiroshi KIMURA

(Received March 10, 1981)
(Revised Dec. 7, 1982)

§ 1. Introduction.

An Hadamard matrix H of order n is a $\{-1, 1\}$-matrix of degree n such that $HH^t=H^tH=nI$, where t denotes the transposition. It is known that n equals one, two or a multiple of four. In this paper we assume that n is greater than eight. For the basic fact on Hadamard matrices see [1] or [7]. Let P be the set of $2n$ points $1, 2, \cdots, n, 1^*, 2^*, \cdots, n^*$. Then we define an n-subset α_i of P as follows: α_i contains j or j^* according as the (i, j)-entry of H equals $+1$ or -1 $(1\leqq i, j\leqq n)$. Let $\alpha_i^*=P-\alpha_i$. We call α_i and α_i^* blocks $(1\leqq i\leqq n)$. Let B be the set of $2n$ blocks $\alpha_1, \alpha_2, \cdots, \alpha_n, \alpha_1^*, \alpha_2^*, \cdots, \alpha_n^*$. Then $M(H)=(P, B)$ is called the matrix design of H. By definition each point belongs to exactly n blocks. By the orthogonality of columns of H each point pair not of the shape $\{a, a^*\}$ belongs to exactly $n/2$ blocks, and each point trio not containing a point pair of the shape $\{a, a^*\}$ belongs to exactly $n/4$ blocks. $\{a, a^*\}$ does not belong to any block. Similarly by the orthogonality of rows of H each block pair not of the shape $\{\alpha, \alpha^*\}$ intersects in exactly $n/2$ points, and each block trio not containing a block pair of the shape $\{\alpha, \alpha^*\}$ intersects in exactly $n/4$ points.

We assume that $a^{**}=a$. Then $\alpha^{**}=\alpha$. Let $\mathfrak{G}$ be the group of all permutations σ on P such that σ leaves B as a whole. Then we call $\mathfrak{G}$ the automorphism group of $M(H)$. Obviously $\mathfrak{G}$ is isomorphic to the automorphism group of H. Since $\zeta=\prod_{a=1}^{n}(a, a^*)=\prod_{i=1}^{n}(\alpha_i, \alpha_i^*)$ belongs to the center of $\mathfrak{G}$, $\mathfrak{G}$ is imprimitive on P. For the basic facts on permutation groups see [9] or [10]. Now let $\bar{P}$ and $\bar{B}$ be the set of point pairs $\bar{a}=\{a, a^*\}$ and block pairs $\bar{\alpha}=\{\alpha, \alpha^*\}$, where $a\in P$ and $\alpha\in B$, respectively. Then $\mathfrak{G}$ may be considered as permutation groups on $\bar{P}$ and on $\bar{B}$. We notice that ζ is trivial on $\bar{P}$ and on $\bar{B}$, and that there is no apparent incidence relation between $\bar{P}$ and $\bar{B}$. In this paper we assume that $\mathfrak{G}$ on $\bar{P}$ is doubly transitive and that $\mathfrak{G}$ on $\bar{P}$ contains a regular normal subgroup $\mathfrak{N}$ on $\bar{P}$. Then $\mathfrak{N}$ on $\bar{P}$ is an elementary Abelian 2-group of order n, and so n

*) This author is partially supported by NSF Grant MCS-7902750.

is a power of 2; $n=2^m$ $(m\geqq 4)$. For the case where $\mathfrak{G}$ on $\bar{P}$ is a doubly transitive permutation group not containing a regular normal subgroup see [**3**] and [**4**].

EXAMPLE 1. Let V be an $(m+1)$-dimensional vector space over $GF(2)$, M a maximal subspace of V and v a vector of V outside M. Then V contains 2^m maximal subspaces N not containing v (including M). Let $\mathfrak{N}$ be the set of all N's. Now we consider the following incidence matrix $H(m)$: Columns and rows of $H(m)$ are labeled by vectors of M and elements of $\mathfrak{N}$, respectively. The (N, w)-entry of $H(m)$ equals $+1$ or -1 according as $w\in N$ or $w\notin N$, where $N\in \mathfrak{N}$ and $w\in M$. We may assume that the first column and row correspond to O and M respectively. Then the first column and row are all 1 vectors respectively. Let N_i be any three distinct elements of $\mathfrak{N}$ $(i=1, 2, 3)$. Then, since N_i does not contain v, we have that $\dim(N_1\cap N_2\cap N_3)=m-2$. So it is easy to check that $H(m)$ is an Hadamard matrix of order $n=2^m$. Let $M(m)$ be the matrix design of $H(m)$. Then the set $P(m)$ of points of $M(m)$ equals $V=\{w, w+v; w\in M\}$ and the set $B(m)$ of blocks of $M(m)$ equals $\{N, N+v; N\in \mathfrak{N}\}$. Let $\mathfrak{G}(m)$ be the automorphism group of $M(m)$. For $x\in V$ define the mapping σ_x by $w\sigma_x=w+x$, $w\in V$. Then $N\sigma_x=N$ or $N+v$, and so σ_x belongs to $\mathfrak{G}(m)$. Let $\mathfrak{T}(m)$ be the subgroup of all σ_x's, $x\in V$. We notice that if we put $w^*=w+v$, $w\in M$, then it is easy to see that σ_v coincides with ζ, and that if we put $\bar{N}=\{N, N+v\}$ and $\overline{B(m)}=\{\bar{N}; N\in \mathfrak{N}\}$, then $\mathfrak{T}(m)$ is trivial on $\overline{B(m)}$. Now let $\sigma\in\mathfrak{G}(m)$ such that $O\sigma=O$. Since $O^*=v$, $v\sigma=v$. Now we show that σ is linear. In fact, first let $a, b\in M$ and consider $N\in B(m)$ such that $a, b\in N$. Then the intersection of such N's equals $\{0, a, b, a+b\}$ and that of $N\sigma$'s equals $\{0, a\sigma, b\sigma, a\sigma+b\sigma\}$. So we can conclude that $(a+b)\sigma=a\sigma+b\sigma$. Secondly if $a\in M$ and $b\notin M$, then we consider $\{a, b^*\}$ and get $(a+b^*)\sigma=a\sigma+b^*\sigma=a\sigma+b\sigma+v$. Since $(a+b^*)\sigma=(a+b+v)\sigma=((a+b)^*)\sigma=(a+b)\sigma+v$, we get $a\sigma+b\sigma=(a+b)\sigma$. The rest is similar. Now it is easy to see that $\mathfrak{T}(m)$ is a normal elementary Abelian 2-group of $\mathfrak{G}(m)$. Thus $\mathfrak{G}(m)$ is a subgroup of the split extension $\mathfrak{T}(m)GL(V)$ of $\mathfrak{T}(m)$ by $GL(V)$, the general linear group on V. It is not difficult to see that $\mathfrak{G}(m)$ is the centralizer of σ_v in $\mathfrak{T}(m)GL(V)$. Put $\bar{w}=\{w, w+v\}$ and $\overline{P(m)}=\{\bar{w}, w\in M\}$. Then $\mathfrak{G}(m)$ on $\overline{P(m)}$ is the split extension of $\mathfrak{T}(m)/\langle\sigma_v\rangle$ by $GL(V/\langle v\rangle)$. Thus $\mathfrak{G}(m)$ on $\overline{P(m)}$ is triply transitive and $\mathfrak{T}(m)/\langle\sigma_v\rangle$ is a regular normal subgroup.

Now W. M. Kantor characterized $H(m)$ as follows [**5**]; If $\mathfrak{G}$ on $\bar{P}$ is not faithful on $\bar{B}$, then H is equivalent to $H(m)$. So from now on we assume that $\mathfrak{G}$ on $\bar{P}$ is faithful on $\bar{B}$.

NOTATION. Let $\mathfrak{X}$ be a permutation group on Ω. Then for $W\subset\Omega$, $\mathfrak{X}_W$ denotes the stabilizer of W in $\mathfrak{X}$. Let Y be a finite set. Then $|Y|$ denotes the number of elements in Y. Let $\mathfrak{R}$ be a finite group and $\mathfrak{S}$ a subgroup of $\mathfrak{R}$. If χ is a character of $\mathfrak{R}$, then $\chi|\mathfrak{S}$ denotes the restriction of χ to $\mathfrak{S}$. If ϕ is a character of $\mathfrak{S}$, then $\phi^{\mathfrak{N}}$ denotes the character of $\mathfrak{N}$ induced by ϕ. $1_{\mathfrak{N}}$ denotes the trivial character of $\mathfrak{N}$. Let χ and ξ be characters of $\mathfrak{N}$. Then (χ, ξ) denotes the inner product $\sum_{x\in\mathfrak{N}}\chi(x)\xi(x)$.

§2. Some results on H.

LEMMA 1. *Let $\mathfrak{K}$ be the kernel of $\mathfrak{G}$ on $\bar{P}$. Then $\mathfrak{K}$ is an elementary Abelian 2-group containing ζ. If $\mathfrak{K}\neq\langle\zeta\rangle$, then H is equivalent to $H(m)$.*

PROOF. Since every non-identity element of $\mathfrak{K}$ has order two, $\mathfrak{K}$ is an elementary Abelian 2-group. Assume that $\mathfrak{K}\neq\langle\zeta\rangle$. Let $\sigma\in\mathfrak{K}-\langle\zeta\rangle$. Then σ has a fixed point and transfers some point a to a^*. Hence $\alpha\sigma\neq\alpha$, α^* for any $\alpha\in B$. Let α be a fixed block. Then $(\alpha\cap\alpha\sigma)\cup(\alpha^*\cap\alpha^*\sigma)$ is the set of fixed points of σ and $|\alpha\cap\alpha\sigma|=|\alpha^*\cap\alpha^*\sigma|=n/2$. So σ has n fixed points. Let $F(\sigma)=\{\bar{a}\in\bar{P};\ a\sigma=a\}$. Then $|F(\sigma)|=n/2$. Clearly σ is uniquely determined by $F(\sigma)$. So the number x of distinct $F(\sigma)$'s equals $|\mathfrak{K}|-2$. Let $\bar{a}$ and $\bar{b}$ be distinct elements of $\bar{P}$ and y the number of distinct $F(\sigma)$'s containing $\bar{a}$ and $\bar{b}$. Since $\mathfrak{G}$ on $\bar{P}$ is 2-transitive, we have that $x\binom{n/2}{2}=y\binom{n}{2}$. This implies that $x(n/2-1)=2(n-1)y$. Since σ is uniquely determined by $\alpha\sigma$, $x\leqq 2(n-1)$. So we have that $x=2(n-1)$. Then every block $\beta\neq\alpha, \alpha^*$ can be expressed as $\beta=\alpha\sigma$ for some $\sigma\in\mathfrak{K}-\langle\zeta\rangle$. Now we have that $\alpha\cap\beta\cap\gamma=\alpha\cap\beta\cap\gamma\sigma$ for any $\gamma\neq\alpha$, α^*, β, β^*. So by a theorem of C. Norman [**6**, Theorem 6] it is easy to see that H is equivalent to $H(m)$.

So from now on we assume that $\mathfrak{K}=\langle\zeta\rangle$.

Let $\mathfrak{X}$ be a subgroup of G. Then let $\bar{\mathfrak{X}}=\mathfrak{X}\langle\zeta\rangle/\langle\zeta\rangle$.

LEMMA 2. *N is elementary Abelian.*

PROOF. Deny. Let σ be an element of $\mathfrak{N}$ of order 4. Then since $\bar{\mathfrak{N}}$ is elementary Abelian, $\sigma^2=\zeta$. Since $\bar{\mathfrak{G}}$ is 2-transitive and $\bar{\mathfrak{N}}$ is a regular normal subgroup of $\bar{\mathfrak{G}}$, all the non-identity elements of $\bar{\mathfrak{N}}$ are conjugate with $\langle\zeta\rangle\sigma$. Hence ζ is the unique involution of $\mathfrak{N}$. So $\mathfrak{N}$ is a quaternion group and $n=4$. This is against our assumption that $n>8$.

LEMMA 3. *$\bar{\mathfrak{N}}$ is regular on $\bar{B}$ and $\bar{\mathfrak{G}}$ is 2-transitive on $\bar{B}$.*

PROOF. Since $\bar{\mathfrak{N}}$ is faithful on $\bar{B}$, $\bar{\mathfrak{N}}$ moves some $\bar{\alpha}$ in $\bar{B}$. Then $|\bar{\mathfrak{N}}_{\bar{\alpha}}|=2^l<|\bar{\mathfrak{N}}|=2^m$. Now we show that $|\bar{\mathfrak{G}}_{\bar{a}}|\leqq 2^l y|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|$, where $\bar{a}$ and $\bar{b}$ are two distinct elements of $\bar{P}$ and y divides 2^l-1. Let $|\bar{\mathfrak{G}}_{\bar{a}}|=2^{a(2)}\prod_{p>2}p^{a(p)}$ and $|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|=2^{b(2)}\prod_{p>2}p^{b(p)}$ be the prime power decomposition of $|\bar{\mathfrak{G}}_{\bar{a}}|$ and $|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|$. If $a(p)\leqq b(p)$ for all odd p, then, since $|\bar{\mathfrak{G}}|=n(n-1)|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|=[\bar{\mathfrak{G}}:\bar{\mathfrak{G}}_{\bar{a}}]|\bar{\mathfrak{G}}_{\bar{a}}|$, $n-1$ divides $[\bar{\mathfrak{G}}:\bar{\mathfrak{G}}_{\bar{a}}]$. Since $[\bar{\mathfrak{G}}:\bar{\mathfrak{G}}_{\bar{a}}]\leqq n$, we have that $[\bar{\mathfrak{G}}:\bar{\mathfrak{G}}_{\bar{a}}]=n-1$. So $\bar{\mathfrak{G}}_{\bar{a}}$ contains a Sylow 2-subgroup of $\bar{\mathfrak{G}}$. Since $\bar{\mathfrak{N}}$ is normal in $\bar{\mathfrak{G}}$, $\bar{\mathfrak{N}}=\bar{\mathfrak{N}}_{\bar{\alpha}}$. This is a contradiction. So there exists an odd prime p such that $a(p)>b(p)$. Let p be such an odd prime and $\bar{\mathfrak{S}}$ a Sylow p-subgroup of $\bar{\mathfrak{G}}_{\bar{a}}$. Since p is odd, $\bar{\mathfrak{S}}$ fixes some element $\bar{a}$ of $\bar{P}$. Now $\bar{\mathfrak{S}}\mathfrak{N}_{\bar{a}}$ is a subgroup where $\mathfrak{N}_{\bar{a}}$ is normal. We consider $\bar{\mathfrak{S}}$-conjugacy class decomposition of $\mathfrak{N}_{\bar{a}}$. Notice that every $\bar{\mathfrak{S}}$-conjugacy class consists of a power of p (possibly 1) elements. Let Λ be an $\bar{\mathfrak{S}}$-conjugacy class $\neq\langle\zeta\rangle$ consisting of fewest elements. Let $\bar{g}$ be an element of Λ. Then $|\bar{\mathfrak{S}}|=|\Lambda||C_{\bar{\mathfrak{S}}}(\bar{g})|$. Let $\bar{a}\bar{g}=\bar{b}$. Then, since $\bar{g}\neq\langle\zeta\rangle$, $\bar{a}\neq\bar{b}$. Since $a(p)>b(p)$, $\bar{S}$ fixes no other point than $\bar{a}$. Since $C_{\bar{\mathfrak{S}}}(\bar{g})\subseteqq\bar{\mathfrak{G}}_{\bar{a},\bar{b}}$, $\bar{\mathfrak{S}}\neq C_{\bar{\mathfrak{S}}}(\bar{g})$. So $|\Lambda|>1$ and $|\Lambda|$ divides 2^l-1. Thus $|\bar{\mathfrak{S}}|$ divides $(2^l-1)|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|$. The same argument holds for $\bar{\mathfrak{S}}\mathfrak{N}$ and we have that $|\bar{\mathfrak{S}}|$ divides $(2^m-1)|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|$. This is true for every odd prime p such that $a(p)>b(p)$. Let $x=\prod_{p>2}p^{\min(a(p),b(p))}$. Then $|\bar{\mathfrak{G}}_{\bar{a}}|=2^{a(2)}xy$, and y divides 2^l-1 and 2^m-1. So y divides $2^{m-l}-1$. Let $\mathfrak{T}$ be a Sylow 2-subgroup of $\bar{\mathfrak{G}}_{\bar{a}}$. Then $\mathfrak{N}\mathfrak{T}=\mathfrak{N}(\mathfrak{N}\mathfrak{T}\cap\bar{\mathfrak{G}}_{\bar{a}})$. Since $\mathfrak{N}_{\bar{a}}\mathfrak{T}\cap\bar{\mathfrak{G}}_{\bar{a}}$ is a 2-group and $|\bar{P}|=2^m$, it fixes another element $\bar{b}$ $(\neq\bar{a})$ of $\bar{P}$. Thus $\mathfrak{N}\mathfrak{T}\cap\bar{\mathfrak{G}}_{\bar{a}}=\mathfrak{N}\mathfrak{T}\cap\bar{\mathfrak{G}}_{\bar{a},\bar{b}}$. Now $|\mathfrak{N}\mathfrak{T}\cap\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|=|\mathfrak{N}\mathfrak{T}/\mathfrak{N}|=|\mathfrak{T}/\mathfrak{N}_{\bar{a}}|=2^{a(2)-l}$. Thus we obtain that $|\bar{\mathfrak{G}}_{\bar{a}}|\leqq 2^l y|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|$. Now we have that

$$2^m\geqq\frac{|\bar{\mathfrak{G}}|}{|\bar{\mathfrak{G}}_{\bar{a}}|}=\frac{2^m(2^m-1)|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|}{2^l y|\bar{\mathfrak{G}}_{\bar{a},\bar{b}}|}\geqq\frac{2^m(2^m-1)}{2^l(2^{m-l}-1)}.$$

This implies that $l=0$. So $\mathfrak{N}$ is regular transitive on $\bar{B}$, and $\bar{\mathfrak{G}}=\mathfrak{N}\bar{\mathfrak{G}}_{\bar{a}}$.

Now $\bar{\mathfrak{G}}$ is 2-transitive on $\bar{P}$ (or $\bar{B}$) if and only if $\bar{\mathfrak{G}}$ decomposes into exactly two double cosets of $\bar{\mathfrak{G}}_{\bar{a}}$ (or $\bar{\mathfrak{G}}_{\bar{\alpha}}$). Since $\mathfrak{N}$ is normal in $\bar{\mathfrak{G}}$, and $\bar{\mathfrak{G}}=\mathfrak{N}\bar{\mathfrak{G}}_{\bar{a}}=\mathfrak{N}\bar{\mathfrak{G}}_{\bar{\alpha}}$ and $\mathfrak{N}\cap\bar{\mathfrak{G}}_{\bar{a}}=\mathfrak{N}\cap\bar{\mathfrak{G}}_{\bar{\alpha}}=\langle\bar{1}\rangle$, the latter holds if and only if all the non-identity elements of $\mathfrak{N}$ are conjugate in $\bar{\mathfrak{G}}_{\bar{a}}$ (or $\bar{\mathfrak{G}}_{\bar{\alpha}}$). Since $\mathfrak{N}$ is elementary Abelian, all the non-identity elements of $\mathfrak{N}$ are conjugate in $\bar{\mathfrak{G}}_{\bar{a}}$ if and only if they are conjugate in $\bar{\mathfrak{G}}_{\bar{\alpha}}$. Since $\bar{\mathfrak{G}}$ is 2-transitive on $\bar{P}$, $\bar{\mathfrak{G}}$ is 2-transitive on $\bar{B}$.

LEMMA 4. *Let $\mathfrak{M}$ be a maximal subgroup of $\mathfrak{N}$ not containing ζ. Let Δ be an $\mathfrak{M}$-orbit on P. Then for every block α of B we have that* $|\Delta\cap\alpha|=\dfrac{n+\sqrt{n}}{2}$ *or* $\dfrac{n-\sqrt{n}}{2}$. *In particular, n is a perfect square.*

PROOF. Put $x=|\Delta\cap\alpha|$ and $y=|\Delta\cap\alpha^*|$. By Lemma 3, N is regular on B. So for every involution σ of M we have that $\alpha\sigma\neq\alpha^*$ and $|\alpha^*\cap\alpha\sigma|=n/2$. Since $|\Delta\cap\alpha^*\cap\alpha\sigma|=|\Delta^*\cap\alpha\cap\alpha^*\sigma|=|\Delta^*\cap\alpha^*\cap\alpha\sigma|$, we have that $|\Delta\cap\alpha^*\cap\alpha\sigma|=n/4$. Thus the cycle structure of every involution of $\mathfrak{M}$ has $n/4$ transpositions of the form (a, b^*), where $a\in\alpha\cap\Delta$ and $b^*\in\alpha^*\cap\Delta$. Since $\mathfrak{M}$ is regular on Δ, $\mathfrak{M}$ contains a unique element σ such that $a\sigma=b^*$ for $a\in\Delta\cap\alpha$ and $b^*\in\Delta\cap\alpha^*$. Therefore we have that $x+y=n$ and $xy=\dfrac{n(n-1)}{4}$. So the lemma follows.

PROPOSITION 1. *If n is not a square, then H is equivalent to $H(m)$.*

PROOF. This is a corollary to Lemma 4.

LEMMA 5. *Let $n=2^m$. Then there exists no prime factor of $(|\mathfrak{G}|, 2^{m-1}-1)$ which does not divide 2^i-1 for every i such that $1 \leqq i \leqq m-2$.*

PROOF. Deny. Let p be such a prime factor and $\mathfrak{S}$ a Sylow p-subgroup of $\mathfrak{G}$. Since $\mathfrak{S}$ acts on $\bar{\mathfrak{N}}$ by conjugation, $\mathfrak{S}$ may be considered as a subgroup of $GL(m, 2)$. By the assumption on p we have that $|C_{\bar{\mathfrak{N}}}(\mathfrak{S})|=2$. So we have that $|C_{\mathfrak{N}}(\mathfrak{S})|=4$. Thus p divides $n-4$. Since $n-4=2(2^{m-1}-1)-2$, this is a contradiction.

PROPOSITION 2. *If $\bar{\mathfrak{G}}$ is 3-transitive on $\bar{P}$, then H is equivalent to $H(m)$.*

PROOF. If $\bar{\mathfrak{G}}$ is 3-transitive on $\bar{P}$, then $n-2$ divides the order of $\bar{\mathfrak{G}}$. By a theorem of Zsigmondy [**11**] there exists a prime factor p of $\left(|\mathfrak{G}|, \dfrac{n-2}{2}\right)$ which does not divide 2^i-1 for every i such that $1 \leqq i \leqq m-2$. It is against Lemma 5.

§ 3. Further analysis.

Let $\bar{a}$ and $\bar{b}$ be two distinct elements of $\bar{P}$. Then we have the following diagram where $e=1$ or 2.

$$
\begin{tikzcd}
\mathfrak{G} \arrow[d, dash, "n"] & \\
\mathfrak{G}_{\bar{a}} \arrow[r, dash, "2"] \arrow[d, dash, "n-1"] & \mathfrak{G}_a \arrow[d, dash, "n-1"] \\
\mathfrak{G}_{\bar{a},\bar{b}} \arrow[r, dash] & \mathfrak{G}_{a,\bar{b}} \arrow[d, dash, "e"] \\
& \mathfrak{G}_{a,b}
\end{tikzcd}
$$

LEMMA 6. *The rank of $\mathfrak{G}$ on P equals three or four according as $e=2$ or 1.*

PROOF. If $e=2$, then the orbits of $\mathfrak{G}_a$ on P are $\{a\}$, $\{a^*\}$ and $P-\bar{a}$. If $e=1$, then $P-\bar{a}$ decomposes into two orbits of $\mathfrak{G}_a$ of length $n-1$.

We assume that the rank of $\mathfrak{G}$ on P equals three. So the permutation character $1_{\mathfrak{G}_a}^{\mathfrak{G}}$ decomposes into the sum of three characters:

$$1_{\mathfrak{G}_a}^{\mathfrak{G}}=1_{\mathfrak{G}}+\chi+\phi\,,$$

where χ is the irreducible character of $\mathfrak{G}$ of degree $n-1$ in the 2-transitive permutation representation of $\mathfrak{G}$ on $\bar{P}$ and the degree of ϕ equals n.

LEMMA 7. *$\mathfrak{G}_\alpha$ is transitive on α and on α^*, where $\alpha \in B$.*

PROOF. If $\mathfrak{G}_\alpha$ is not transitive on α, $\mathfrak{G}_\alpha$ has at least four orbits on P. So the permutation character $1_{\mathfrak{G}_a}^{\mathfrak{G}}$ has degree at least $1+3(n-1)$. Since $[\mathfrak{G}:\mathfrak{G}_\alpha]=2n$ by Lemma 3, this is a contradiction.

From Lemma 7 it follows that $\mathfrak{G}_{\bar{\alpha}}$ is transitive on $\bar{P}$. Thus we have the following diagram, where $\bar{a}$ and $\bar{b}$ are two distinct elements of $\bar{P}$ such that α contains a and b:

$$
\begin{tikzcd}[column sep=small]
 & & & \mathfrak{G} \arrow[dl, dash, "n"'] \arrow[dr, dash, "n"] & & & \\
 & & \mathfrak{G}_{\bar{\alpha}} \arrow[dl, dash, "2"'] \arrow[dr, dash, "n'"] & & \mathfrak{G}_{\bar{a}} \arrow[dl, dash, "n"'] \arrow[dr, dash, "n-1"] & & \\
 & \mathfrak{G}_\alpha \arrow[dr, dash, "n"] & & \mathfrak{G}_{\bar{\alpha},\bar{a}} \arrow[dl, dash, "2"'] \arrow[dr, dash, "n-1"] & & \mathfrak{G}_{\bar{a},\bar{b}} \arrow[dl, dash, "n"] & \\
 & & \mathfrak{G}_{\alpha,a}=\mathfrak{G}_{\bar{\alpha},a} \arrow[dr, dash, "n-1"] & & \mathfrak{G}_{\bar{\alpha},\bar{a},\bar{b}} \arrow[dl, dash, "2"] & & \\
 & & & \mathfrak{G}_{\alpha,a,b}=\mathfrak{G}_{\alpha,a,\bar{b}} & & &
\end{tikzcd}
$$

So $\mathfrak{G}_\alpha$ is 2-transitive on α. Since all 2-transitive permutation groups not containing a regular normal subgroup are known, by [3, Proposition 2] $\mathfrak{G}_\alpha$ contains a regular normal subgroup $\mathfrak{L}$. Then $\mathfrak{N}\mathfrak{L}$ is a normal 2-subgroup of $\mathfrak{G}$ such that $\mathfrak{N}\cap\mathfrak{L}=1$. Since $\bar{\mathfrak{N}}$ is a minimal normal subgroup of $\bar{\mathfrak{G}}$, $\bar{\mathfrak{N}}$ is contained in the center of $\overline{\mathfrak{N}\mathfrak{L}}$. Since $\bar{\mathfrak{N}}$ is transitive on $\bar{P}$, this implies that $\bar{\mathfrak{L}}=\langle\zeta\rangle$. This is a contradiction.

So the rank of $\mathfrak{G}$ on P equals four.

Since $\mathfrak{G}$ has rank 4 on P, the permutation character $1_{\mathfrak{G}_a}^{\mathfrak{G}}$ decomposes into the sum of four irreducible character of $\mathfrak{G}$:

$$1_{\mathfrak{G}_a}^{\mathfrak{G}}=1_{\mathfrak{G}}+\chi+\phi_1+\phi_2\,.$$

Let f_i be the degree of ϕ_i $(i=1, 2)$. Then $f_1+f_2=n$. Let F be the family of maximal subgroups of $\mathfrak{N}$ not containing ζ. Then $|F|=n$. Let $\mathfrak{M}$ be an element of F and let Γ and Γ^* be orbits of $\mathfrak{M}$ on P. Then exactly one of $\phi_1|\mathfrak{M}$ and $\phi_2|\mathfrak{M}$ contains $1_{\mathfrak{M}}$ with multiplicity 1. We say that $\mathfrak{M}$ is of type i if $\phi_i|\mathfrak{M}$ contains $1_{\mathfrak{M}}$ $(i=1, 2)$.

LEMMA 8. *$\mathfrak{N}$ consists of four $\mathfrak{G}_a$-conjugacy classes:* $\{1\}$, $\{\zeta\}$, $\mathfrak{C}_1$ *and* $\mathfrak{C}_2=\zeta\mathfrak{C}_1$, *where* $|\mathfrak{C}_1|=n-1$.

PROOF. $\mathfrak{G}_a$ has four orbits on P: $\{a\}$, $\{a^*\}$, Ω_1 and Ω_2, where $|\Omega_i|=n-1$ $(i=1, 2)$. $\mathfrak{G}_a$ has two orbits on $\bar{P}$. So we have that $\Omega_2=\Omega_1^*$. For any b in Ω_1 there exists a unique element $\rho(b)$ of $\mathfrak{N}$ such that $a\rho(b)=b$. Let b_1 and b_2 be two elements of Ω_1. Then there exists an element σ of $\mathfrak{G}_a$ such that $b_1\sigma=b_2$. Now we have that $a\rho(b_1)\sigma=a\rho(b_2)$. So there exists an element τ of $\mathfrak{G}_a$ such that $\rho(b_1)\sigma\rho(b_2)^{-1}=\zeta$. Then $\sigma^{-1}\rho(b_1)\sigma=\sigma^{-1}\tau\rho(b_2)$. Since $\mathfrak{N}\cap\mathfrak{G}_a=1$ and since $\mathfrak{N}$ is normal in $\mathfrak{G}$, we have that $\sigma=\zeta$. So $\rho(b_1)$ and $\rho(b_2)$ are conjugate in $\mathfrak{G}$. Since the argument may be reversed, we get the lemma.

LEMMA 9. *Let $\mathfrak{M}_1$ be an element of F of type* 1. *Put* $|\mathfrak{M}_1\cap\mathfrak{C}_i|=x_i$ $(i=1, 2)$. *Then we have the following:*

$$f_1+x_1\phi_1(c_1)+x_2\phi_1(c_2)=n\,, \tag{1}$$

$$f_2+x_1\phi_2(c_1)+x_2\phi_2(c_2)=0\,, \tag{2}$$

$$\phi_i(\zeta)=-f_i, \quad and \quad \phi_i(c_1)+\phi_i(c_2)=0\,, \tag{3}$$

where $c_i\in\mathfrak{M}_1\cap\mathfrak{C}_i$.

PROOF. Since $(\phi_1|\mathfrak{M}_1, 1_{\mathfrak{M}_1})=1$, $\sum_{u\in\mathfrak{M}_1}\phi_1(u)=\sum_{u\in\mathfrak{M}_1}1_{\mathfrak{M}_1}(u)=n$. This proves (1). Since $(\phi_2|\mathfrak{M}_1, 1_{\mathfrak{M}_1})=0$, we have (2). Put $\phi_i|\langle\zeta\rangle=d_{i1}1_{\langle\zeta\rangle}+d_{i2}\eta$, where d_{ij} are integers and η is the non-trivial linear character of $\langle\zeta\rangle$. Then $\phi_i(1)=d_{i1}+d_{i2}$ and $\phi_i(\zeta)=d_{i1}-d_{i2}$. Since $\phi_1(\zeta)+\phi_2(\zeta)=(1_{\mathfrak{G}_a}^{\mathfrak{G}}-1_{\mathfrak{G}_{\bar{a}}}^{\mathfrak{G}})\langle\zeta\rangle=-n=-\phi_1(1)-\phi_2(1)$, $d_{i1}=0$. Thus $\phi_i(\zeta)=-f_i$. Since $d_{i1}=0$, $\phi_i|\langle c_1, \zeta\rangle$ does not contain a trivial character of $\langle c_1, \zeta\rangle$. Thus $\phi_i(1)+\phi_i(c_1)+\phi_i(c_1\zeta)+\phi_i(\zeta)=0$. This proves (3).

LEMMA 10. *For $i=1, 2$ there exists an element $\mathfrak{M}_i$ of type i.*

PROOF. Assume that all elements of F are of type 1. We notice that each element of $\mathfrak{N}-\{1, \zeta\}$ appears exactly $n/2$ elements of F. So if we sum up the equation (1) for all elements of F, then we have that $f_1n=n^2$, which is a contradiction.

LEMMA 11. $[\mathfrak{G}: N(\mathfrak{M}_i)]=f_i$ $(i=1, 2)$. *In particular, F consists of two conjugacy classes.*

PROOF. Let Γ_i and Γ_i^* be orbits of $\mathfrak{M}_i$ on P $(i=1, 2)$. Then $[N(\mathfrak{M}_i): \mathfrak{G}_{\Gamma_i}]=2$ $(i=1, 2)$. Since $1_{\mathfrak{G}_{\Gamma_i}}^{N(\mathfrak{M}_i)}=1_{N(\mathfrak{M}_i)}+\varepsilon_i$, where ε_i is a non-trivial linear character of $N(\mathfrak{M}_i)$, ϕ_i appears in $\varepsilon_i^{\mathfrak{G}}$ $(i=1, 2)$. This shows that $[\mathfrak{G}: N(\mathfrak{M}_i)]\geqq f_i$ $(i=1, 2)$. Since $[\mathfrak{G}: N(\mathfrak{M}_1)]+[\mathfrak{G}: N(\mathfrak{M}_2)]=f_1+f_2=n$, we have the lemma.

Let $\mathfrak{M}_2$ be an element of F of type 2. Put $|\mathfrak{M}_2\cap\mathfrak{C}_i|=y_i$ $(i=1, 2)$. Then we have that

$$f_2+(y_1-y_2)\phi_2(c_1)=n \tag{4}$$

and

$$f_2+(x_1-x_2)\phi_2(c_1)=0\,. \tag{5}$$

By the equalities (2) and (5) we have that

$$(y_1-y_2-x_1+x_2)\phi_2(c_1)=n\,. \tag{6}$$

Now let $\hat{\mathfrak{C}}_i$ be the class sum of $\mathfrak{C}_i$ in the group ring $\boldsymbol{C}[\mathfrak{G}]$ over $\boldsymbol{C}$, the field of complex numbers. Put

$$\hat{\mathfrak{C}}_1^2=(n-1)1+z_1\hat{\mathfrak{C}}_1+z_2\hat{\mathfrak{C}}_2\,.$$

Then we have that

$$(n-1)\frac{\phi_i(c_1)^2}{f_i^2}=1+(z_1-z_2)\frac{\phi_i(c_1)}{f_i} \tag{7}$$

for $i=1, 2$. Since c_1 has no fixed points on $\bar{P}$ and on P, we have that $\phi_1(c_1)+\phi_2(c_1)=0$. So from (7) we have that

$$(n-1)\phi_1(c_1)^2=f_1f_2\,. \tag{8}$$

Since $f_1+f_2=n$, we may put $f_i=2^r g_i$ with odd g_i ($i=1, 2$). So by (6) and (8) we have that $g_1g_2=n-1$ and $|\phi_1(c_1)|=2^r$. Thus we may state the following lemma.

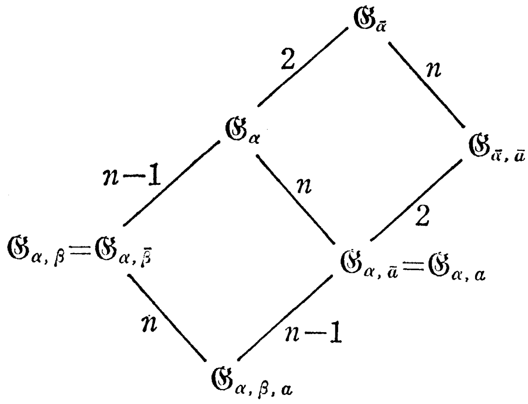
LEMMA 12. *We may put $f_i=2^r g_i$ with odd g_i. Moreover we have that $g_1g_2=n-1$ and $|\phi_1(c_1)|=2^r$.*

LEMMA 13. *It holds that $\{f_1, f_2\}=\{n-1, 1\}$ or $\left\{\frac{n+\sqrt{n}}{2}, \frac{n-\sqrt{n}}{2}\right\}$.*

PROOF. Since $g_1+g_2=2^{m-r}$ and $g_1g_2=2^m-1$, we have that $x^2-2^{m-r}x+2^m-1=0$ for $x=g_1$ and g_2, which implies that $(x-2^{m-r-1})^2=2^{2(m-r-1)}-2^m+1$. Put $t=|x-2^{m-r-1}|$. Then we have that $(t-1)(t+1)=2^m(2^{m-2r-2}-1)$. If $t=1$, then $m=2r+2$, $(x-2^{r+1})^2=1$ and $\{g_1, g_2\}=\{2^{r+1}+1, 2^{r+1}-1\}$. Since $2^r=\frac{\sqrt{n}}{2}$, we have that $\{f_1, f_2\}=\left\{\frac{n+\sqrt{n}}{2}, \frac{n-\sqrt{n}}{2}\right\}$. So we assume that $t>1$. If $t\equiv 1 \pmod 4$, then $t-1=2^{m-1}s$ with s an odd integer. Then we have that $s(2^{m-2}s+1)=2^{m-2r-2}-1$. Obviously this is a contradiction. So $t\equiv 3 \pmod 4$ and $t+1=2^{m-1}s$ with s an odd integer. Then we have that $s(2^{m-2}s-1)=2^{m-2r-2}-1$, which implies that $s=1$ and $r=0$. So $f_i=g_i$ ($i=1, 2$), $f_1+f_2=2^m$ and $f_1f_2=2^m-1$. Thus we have that $\{f_1, f_2\}=\{n-1, 1\}$.

LEMMA 14. *For α in B $\mathfrak{G}_\alpha$ has four orbits on P.*

PROOF. First we show that $\mathfrak{G}_{\bar{\alpha}}$ is not transitive on $\bar{P}$. Assume that $\mathfrak{G}_{\bar{\alpha}}$ is transitive on $\bar{P}$. Then for $a\in\alpha\cap\beta$ ($\alpha\neq\beta$) we have the following diagram:



This contradicts $|\alpha\cap\beta|=n/2$. Since $[\mathfrak{G}:\mathfrak{G}_{\bar{\alpha}}]=n$, we have that $1_{\mathfrak{G}_{\bar{\alpha}}}^{\mathfrak{G}}=1+\chi$. So $\mathfrak{G}_{\bar{\alpha}}$ has two orbits on P. Therefore $\mathfrak{G}_{\alpha}$ has four orbits on P. Since $[\mathfrak{G}:\mathfrak{G}_{\alpha}]=2n$, we have that $1_{\mathfrak{G}_{\alpha}}^{\mathfrak{G}}=1+\chi+\phi_1+\phi_2$.

We may add a little more information. If $\{f_1, f_2\}=\{n-1, 1\}$, then we may assume that $f_1=n-1$ and $f_2=1$. There exists exactly one maximal subgroup $\mathfrak{M}_n$ of type 2. $\mathfrak{M}_n$ is normal in $\mathfrak{G}$. We may assume that $\mathfrak{M}_n=1+\mathfrak{C}_2$ in $\boldsymbol{C}[\mathfrak{G}]$. So we have that $\mathfrak{C}_2^2=(n-1)1+(n-2)\mathfrak{C}_2$. Furthermore, $\phi_2(c_2)=1$ for $c_2\in\mathfrak{C}_2$. If $\{f_1, f_2\}=\left\{\frac{n+\sqrt{n}}{2}, \frac{n-\sqrt{n}}{2}\right\}$, then we may assume that $f_1=\frac{n+\sqrt{n}}{2}$ and $f_2=\frac{n-\sqrt{n}}{2}$. Moreover we may assume that $\phi_1(c_1)=2^r$. Then from (7) we get $\mathfrak{C}_1^2=(n-1)1+\frac{n-4}{2}\mathfrak{C}_1+\frac{n}{2}\mathfrak{C}_2$.

§ 4. Another presentation of $H(m)$.

EXAMPLE 2. Let V be a $(2r+1)$-dimensional vector space over $GF(2)$, where r is a positive integer, and $\{e_i, 0\leqq i\leqq 2r\}$ the standard basis for V.

Let $D(x)=x_0^2+x_1x_{1+r}+\cdots+x_rx_{2r}$ be a quadratic form on V, where $x=\sum_{i=0}^{2r}x_ie_i$. Let $R=R(r)$ and $N=N(r)$ be the sets of zeros and non-zeros of $D(x)$ in V respectively.

Since $D(x)=0$ if and only if $D(x+e_0)=1$, we have that $R+e_0=N$. Since $V=R\cup N$ and $R\cap N=\emptyset$, we have that $|R(r)|=|N(r)|=2^{2r}$. Now $x\in R$ belongs to $R+e_1$ if and only if $x_{r+1}=0$. Moreover $|\{x\in R\,;\ x_1=x_{r+1}=0\}|=|\{x\in R\,;\ x_1=0,\ x_{r+1}=1\}|=|\{x\in R\,;\ x_1=1,\ x_{r+1}=0\}|=|R(r-1)|$ and $|\{x\in R\,;\ x_1=1,\ x_{r+1}=1\}|=|N(r-1)|$. Hence we have that $|R\cap R+e_1|=2|R(r-1)|=2^{2r-1}$. Let $\mathfrak{G}(D)$ be the orthogonal group corresponding to $D(x)$. Then $\mathfrak{G}(D)$ is transitive on $R-\{0\}$ [2]. So we have that $|R+a\cap R+b|=2^{2r-1}$ for $a, b\in V$ such that $R+b\neq R+a$, $R+a+e_0$. Now let B be the family of all translates $R+a$, $a\in V$, of R. Then we have a matrix design $M(D)=(V, B)$ of an Hadamard matrix $H(D)$.

Now let $R\neq R+a$, $R+b$, $R+a+e_0$, $R+b+e_0$ and $R+a\neq R+b$, $R+b+e_0$. If $x\in R\cap R+a\cap R+b$, then $D(x+a+b)=a_1b_{r+1}+b_1a_{r+1}+\cdots+a_rb_{2r}+b_ra_{2r}$. Therefore either $R\cap R+a\cap R+b\subseteqq R+a+b$ or $R\cap R+a\cap R+b\subseteqq R+a+b+e_0$. So by a theorem of Norman [6] $H(D)$ is equivalent to $H(2r)$.

Let $R_i=R_i(r)$ be the set of elements x of R such that $x_0=i\,(i=0, 1)$. Then we have that $|R_0(1)|-|R_1(1)|=2$ and that $|R_0(r)|=3|R_0(r-1)|+|R_1(r-1)|$ and $|R_1(r)|=3|R_1(r-1)|+|R_0(r-1)|$. So we have that $|R_0(r)|-|R_1(r)|=2(|R_0(r-1)|-|R_1(r-1)|)=2^r$, which implies that $|R_0(r)|=2^{2r-1}+2^{r-1}$ and $|R_1(r)|=2^{2r-1}-2^{r-1}$.

Now let $\mathfrak{M}_1=\langle e_i,\ 1\leqq i\leqq 2r\rangle$ and $\mathfrak{M}_2=\mathfrak{M}_2(r)=\langle e_1+e_0,\ e_{r+1}+e_0,\ e_i,\ e_{r+i},\ 2\leqq i\leqq r\rangle$. Then we have that $\mathfrak{M}_1\cap R=R_0$. On the other hand, we have that $\mathfrak{M}_2(1)\cap R=\{0\}$ and $|\mathfrak{M}_2\cap R|=3|\mathfrak{M}_2(r-1)\cap R(r-1)|+|\mathfrak{M}_2(r-1)\cap N|=3(2^{2r-3}-2^{r-2})+(2^{2r-3}+2^{r-2})=2^{2r-1}-2^{r-1}$.

Let $[\mathfrak{G}(D): N_{\mathfrak{G}(D)}(\mathfrak{M}_i)]=w_i$ and consider the orbit of $\mathfrak{M}_i\cap R$ of $\mathfrak{G}(D)$ for $i=1, 2$. Since $\mathfrak{G}(D)$ has three orbits on $V-\{0\}$, and since the family of maximal subgroups of V containing e_0 forms a union of orbits of $\mathfrak{G}(D)$, we have that $w_1+w_2=2^{2r}$ by [8, (2.2)]. Moreover we have that $w_1(2^{2r-1}+2^{r-1}-1)\equiv 0 \pmod{2^{2r}-1}$ and $w_2(2^{2r-1}-2^{r-1}-1)\equiv 0 \pmod{2^{2r}-1}$, which implies that $w_1\equiv 0 \pmod{2^r+1}$ and $w_2\equiv 0 \pmod{2^r-1}$. Put $w_1=(2^r+1)y_1$ and $w_2=(2^r-1)y_2$.

Let $y_i=2^s z_i$ with odd z_i $(i=1, 2)$. Then we have that $(2^r+1)y_1+(2^r-1)y_2=2^{2r-s}$, which implies that $y_1-y_2\equiv 0 \pmod{2^r}$. The last congruence implies that $y_1=y_2=1$ and $s=r-1$. So we have that $w_1=2^{2r-1}+2^{r-1}$ and $w_2=2^{2r-1}-2^{r-1}$.

Finally we notice that $\mathfrak{G}(D)_0=\mathfrak{G}(D)_R$, i.e., a point stabilizer coincides with a block stabilizer.

References

[1] M. Hall, Jr., Combinatorial theory, Blaisdell, Waltham, Mass., 1967.

[2] J. Dieudonné, La géométrie des groupes classiques, Springer, Berlin, 1955.

[3] N. Ito, Hadamard matrices with "doubly transitive" automorphism groups, Arch. Math., **35** (1980), 100-111.

[4] N. Ito and Jeffrey S. Leon, An Hadamard matrix of order 36, J. Combinatorial Theory Ser. A, **34** (1983), 244-247.

[5] W. M. Kantor, Automorphisms of Hadamard matrices, J. Combinatorial Theory, **6** (1969), 279-281.

[6] M. E. Kimberley, On the construction of certain Hadamard designs, Math. Z., **119** (1971), 41-59.

[7] Z. Kiyasu, Hadamard matrix and its applications, Denshi-Tsushin Gakkai, Tokyo, 1980 (Japanese).

[8] H. Lüneburg, Transitive Erweiterungen endlicher Permutationsgruppen, Lecture Notes in Math., **84**, Springer-Verlag, Berlin, 1969.

[9] T. Oyama, Finite permutation groups, Shokabo, Tokyo, 1981 (Japanese).

[10] H. Wielandt, Finite permutation groups, Academic Press, New York, 1964.

[11] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys., **3** (1892), 265-284.

Noboru Ito
Department of Applied Mathematics
Konan University
Kobe 658, Japan

Hiroshi Kimura
Department of Mathematics
Ehime University
Matsuyama 790, Japan