On some doubly transitive permutation groups of degree \( n \) and order \( 2^{(n-1)n} \)

By Hiroshi KIMURA

(Received Jan. 27, 1969)  
(Revised Nov. 22, 1969)

1. Introduction.

Doubly transitive permutation groups of degree \( n \) and order \( 2^{(n-1)n} \) were determined by N. Ito ([9]). Some doubly transitive permutation groups of degree \( n \) and order \( 4^{(n-1)n} \) were studied in [10].

The object of this paper is to prove the following result.

**Theorem.** Let \( Q \) be the set of symbols 1, 2, ..., \( n \). Let \( \mathcal{G} \) be a doubly transitive group on \( Q \) of order \( 2^{(n-1)n} \) (\( l > 1 \)) not containing a regular normal subgroup and let \( \mathcal{K} \) be the stabilizer of symbols 1 and 2. Assume that \( \mathcal{K} \) is cyclic. Then \( \mathcal{G} \) is isomorphic to one of the groups \( PGL(2, *) \), \( PSL(2, *) \), \( PSU(3, 3^2) \) and \( PSU(3, 5^2) \).

We use the standard notation. \( C_{\mathfrak{x}}(\mathfrak{T}) \) denotes the centralizer of a subset \( \mathfrak{T} \) in a group \( \mathfrak{x} \) and \( N_{\mathfrak{x}}(\mathfrak{T}) \) stands for the normalizer of \( \mathfrak{T} \) in \( \mathfrak{x} \). \( \langle S, T, \ldots \rangle \) denotes the subgroup of \( \mathfrak{x} \) generated by elements \( S, T, \ldots \) of \( \mathfrak{x} \).

2. On the degree of the permutation group \( \mathcal{G} \).

1. Let \( \mathcal{H} \) be the stabilizer of the symbol 1. \( \mathcal{H} \) is of order \( 2^l \) and it is generated by a permutation \( K \). Let us denote the unique involution \( K^{2^{l-1}} \) of \( \mathcal{H} \) by \( \tau \). Since \( \mathcal{G} \) is doubly transitive on \( Q \) it contains an involution \( I \) with the cyclic structure \( (1 2) \ldots \). Then we have the following decomposition of \( \mathcal{G} \);

\[
\mathcal{G} = \mathcal{H} + \mathcal{H}I\mathcal{H}.
\]

Since \( I \) is contained in \( N_{\mathfrak{g}}(\mathcal{H}) \), it induces an automorphism of \( \mathcal{H} \) and (i) \( K^I = K \) or \( K^I = K\tau \) or (iii) \( K^I = K^{-1} \). (For the case \( l = 2 \), (i) \( K^I = K \) or (iii) \( K^I = K^{-1} \)) If an element \( H^I \mathcal{H} \) of a coset \( \mathcal{H} \mathcal{H} \) of \( \mathcal{H} \) is an involution, then \( IHH^I = (HH^I)^{-1} \) is contained in \( \mathcal{H} \). Hence, in the case (i) the coset \( \mathcal{H}I\mathcal{H} \) contains just two involutions, namely \( H^{I} \mathcal{H} \) and \( H^{I}\tau \mathcal{H} \), in the case (ii) it contains just \( 2^{l-1} \) involutions, namely \( H^{I} \mathcal{H} \) for \( \mathcal{K} \in \langle K^2 \rangle \), and in the case

1) This work was supported by The Sakkokai Foundation.
(iii), it contains just $2^n$ involutions, namely $H^{-1}K' IH$ for $K' \in \mathfrak{S}$. Let $g(2)$ and $h(2)$ denote the numbers of involutions in $\mathfrak{S}$ and $\mathfrak{S}$, respectively. Then the following equality is obtained:

$$g(2) = h(2) + d(n-1),$$

where $d = 2, 2^2$ and $2^i$ for cases (i), (ii) and (iii), respectively.

2. For a set $\mathfrak{S}$ of permutations of $\mathfrak{G}$, the set of all symbols fixed by $\mathfrak{S}$ is denoted by $\mathfrak{S}(\mathfrak{S})$ and we denote the number of symbols in $\mathfrak{S}(\mathfrak{S})$ by $a(T)$. Let $K_{st_j}$ denote the permutation of $\mathfrak{S}$ such that $\alpha(x) = \alpha(K_{st_j}) > \alpha(K_{st_j'})$ and let $\mathfrak{S}_1$ be the subgroup of $\mathfrak{S}$ generated by $K_{st_j}$. Then the order of $\mathfrak{S}_1$ is equal to $2^n$. Let $\mathfrak{S}_i$ keep $i (i \geq 2)$ symbols of $\mathfrak{S}$, say $1, 2, \ldots, i$, unchanged. It is trivial that $N_\mathfrak{S}(\mathfrak{S}_i) = C_\mathfrak{S}(x)$. Put $\mathfrak{S} = \mathfrak{S}(\mathfrak{S}_i) = \{1, 2, \ldots, i\}$. We denote the factor group $N_\mathfrak{S}(\mathfrak{S}_i)/\mathfrak{S}_1$ by $\mathfrak{S}_i$. By a theorem of Witt ([15, Theorem 9.4]), $\mathfrak{S}_i$ can be considered as a doubly transitive permutation group on $\mathfrak{S}$. The stabilizer of symbols 1 and 2 in $\mathfrak{S}$ is the cyclic 2-group. Thus the orders of $N(\mathfrak{S}_1)$ and $N(1)$ are equal to $2^i(i-1)$ and $2^{i-1}$, respectively. Hence there exist $n(n-1)/i(i-1)$ involutions in $\mathfrak{S}$ each of which is conjugate to $T$.

At first, let us assume that $n$ is odd. Let $h_*(2)$ be the number of involutions in $\mathfrak{S}$ leaving only the symbol 1 fixed. Then from (2.1) and above argument the following equality is obtained:

$$h*(2)n + n(n-1)/i(i-1) = (n-1)/(i-1) + h*(2) + d(n-1).$$

Since $i$ is less than $n$, it follows from (2.2) that $h*(2) < d$ and hence $n = i(\beta i - \beta + 1)$, where $\beta = d - h*(2)$. Since $n$ is odd, $i$ must be odd.

Next let us assume that $n$ is even. Let $g*(2)$ be the number of involutions in $\mathfrak{S}$ leaving no symbol of $\mathfrak{S}$ fixed. Then corresponding to (2.2) the following equality is obtained from (2.1):

$$g*(2) + n(n-1)/i(i-1) = (n-1)/(i-1) + d(n-1).$$

It is easily proved that $g*(2)$ is a multiple of $n-1$ (see [8] or [9]). It follows from (2.3) that $g*(2) < d(n-1)$. Thus we have $n = i(\beta i - \beta + 1)$, where $\beta = d - g*(2)/(n-1)$. Since $n$ is even, $i$ must be even.

3. We prove the theorem by induction on the degree $n$. Let $SL(2, 8)$ denote the two-dimensional special linear group over the field $GF(8)$ of eight elements, and let $\sigma$ be the automorphism of $GF(8)$ of order three such that $\sigma(x) = x^2$ for every element $x$ of $GF(8)$. Then $\sigma$ can be considered in a usual way an automorphism of $SL(2, 8)$. Let $SL^*(2, 8)$ be the splitting extension of $SL(2, 8)$ by the group $\langle \sigma \rangle$. Then $SL^*(2, 8)$ has doubly transitive permutation representation on the set of Sylow 3-subgroups and its degree is equal to 28. The stabilizer of two symbols leaves four Sylow 3-subgroups fixed and every
involution is conjugate (see [8]).

**Theorem 1** (N. Ito, [8]). Let $\mathfrak{G}$ be a doubly transitive permutation group on $\Omega$ of order $2n(n-1)$ not containing a regular normal subgroup. Then $\mathfrak{G}$ is isomorphic to either $\text{PSL}(2, 5)$ or $\text{SL}^*(2, 8)$.

If $\mathfrak{G}$ contains a regular normal subgroup, then its degree is equal to a power of a prime number. Thus, by Theorem 1, if $l=1$, then $n$ is equal to 6, 28 or a power of a prime number.

3. The case $n$ is odd.

1. Since $n = i(\alpha-i+1)$ is odd, $i$ must be odd. The group $\mathfrak{G}_i = N_\mathfrak{a}(\mathfrak{s}_i)/\mathfrak{s}_i$ is a doubly transitive permutation group on $\mathfrak{s}_i$ and the stabilizer of symbols 1 and 2 is the subgroup $\mathfrak{s}_i$ of order $2^{i-1}$. By the inductive hypothesis, $\mathfrak{G}_i$ contains a regular normal subgroup and, in particular, $i$ is equal to a power of an odd prime number, say $p^m$. Let $\mathfrak{B}_1$ be a Sylow $p$-subgroup of $N_\mathfrak{a}(\mathfrak{s}_i)$ of order $i = p^m$. Since $\mathfrak{s}_1/\mathfrak{s}_i$ is a regular normal subgroup of $\mathfrak{G}_i$, $\mathfrak{B}_1$ is elementary abelian and normal in $N_\mathfrak{a}(\mathfrak{s}_i)$. Let $\mathfrak{B}$ denote the subgroup $\mathfrak{B}_1 \cap N_\mathfrak{a}(\mathfrak{s}_i)$. Then the order of $\mathfrak{B}$ is equal to $2^i(p^m-1)$.

2. Case $n = i^2 = p^m$. It can be proved in the same way as in [9, Case A] that there exists no group satisfying the conditions of the theorem in this case.

3. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta > 1$ and $\beta, \beta - 1 \equiv 0 \pmod{p}$. In this case it can be proved in the same way as in [10, §2.5] that there is no group satisfying the conditions of the theorem in this case.

4. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta > 1$ and $\beta \equiv 0 \pmod{p}$. Since $\beta \geq 3, d$ must be greater than 2 and hence $\langle K, I \rangle$ is dihedral or semi-dihedral.

Consider the cyclic structure of $K$ and it can be seen that $n - i = \beta p^m(p^m-1)$ is divisible by $2^i$. Set $p = 2^q + 1$, where $q(> 0)$ is odd. Since $2^i \geq \beta \geq p$, $\beta$ is not divisible by $2^{i-k}$ and therefore $p^m-1$ must be divisible by $2^{i-k}$. Hence $m$ is even.

At first assume that the order of $N_\mathfrak{a}(\mathfrak{S})$ is divisible by $2^{i+2}$. Since $N_\mathfrak{a}(\mathfrak{S})/\mathfrak{S}$ is a complete Frobenius group on $\mathfrak{S}(\mathfrak{S})$, any Sylow subgroup of a complement $\mathfrak{S} \cap N_\mathfrak{a}(\mathfrak{S})/\mathfrak{S}$ is cyclic or quaternion (ordinary or generalized). Hence there exists a subgroup $\mathfrak{S}$ of $N_\mathfrak{a}(\mathfrak{S})$ such that $\mathfrak{S} \supseteq \langle I, K \rangle$ and $\mathfrak{S}/\mathfrak{S}$ is a cyclic group of order 4. $\mathfrak{S}$ contains $S$ such that $S^2 = I(\mathfrak{S})$, $S$ induces an automorphism of $\mathfrak{S}$ of order 4 and $S^2$ and $I$ induce the same automorphism. But it is easily seen that, for any automorphism $\zeta$ of $\mathfrak{S}$ of order 4, $K^{\zeta} = \tau K$. This is a contradiction since $\langle K, I \rangle$ is dihedral or semi-dihedral.

Next assume that the order of $N_\mathfrak{a}(\mathfrak{S})$ is not divisible by $2^{i+2}$. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $N_\mathfrak{a}(\mathfrak{s}_i)$ containing $\langle I, K \rangle$. Since $m$ is even, the order
of $\mathfrak{S}$ is greater than $2^{l+2}$. By the assumption of the order of $N_6(\mathfrak{R})$, $\mathfrak{S} \cap N_6(\mathfrak{R}) = \langle K, I \rangle$ is a Sylow 2-subgroup of $N_6(\mathfrak{R})$. Therefore $N_6(\langle K, I \rangle)$ is greater than $N_6(\mathfrak{R})$. Let $S$ (≠ 1) be a permutation of $N_6(\langle K, I \rangle)$, $\langle K, I \rangle$. Since $K^S$ is contained in $\langle K, I \rangle$, we have $K^S = K'I$, where $K'$ is a permutation of $\mathfrak{R}$. Hence, if $\langle K, I \rangle$ is dihedral, then $(K^S)^2 = 1$ and the order of $K$ equals 2 and, if $\langle K, I \rangle$ is semi-dihedral, then $(K^S)^4 = 1$ and the order of $K$ equals 4. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

5. Case $n = p^m(\beta p^m - \beta + 1)$ with $\beta - 1 = 0 \pmod{p}$.

At first we shall prove that the order of $C_6(\mathfrak{R})$ is equal to $2^{j'} p^{m+m' y}$, where $j' \geq j$, $m' > 0$ and $y$ is a factor of $\beta p^m - (\beta - 1)$ and not divisible by $p$. Assume that the order of $C_6(\mathfrak{R})$ is equal to $2^{j'} p^{m'}$. Let $\mathfrak{R}'$ be a Sylow 2-subgroup of $C_6(\mathfrak{R})$. Every element (≠ 1) of $\mathfrak{R}$ leaves no symbol of $\mathfrak{Q}$ fixed. Then $\mathfrak{R}'$ must leave at least two symbols of $\mathfrak{Q}$ fixed. Therefore $\mathfrak{R}'$ is conjugate to a subgroup of $\mathfrak{R}$ containing $\mathfrak{R}_1$. Since $C_6(\mathfrak{R})$ is a direct product of $\mathfrak{R}'$ and $\mathfrak{R}$, $\mathfrak{R}'$ is normal in $N_6(\mathfrak{R})$. Since the order of $N_6(\mathfrak{R}_1)$ is a factor of the order of $N_6(\mathfrak{R})$, the order of $N_6(\mathfrak{R}_1)$ is greater than or equal to the order of $N_6(\mathfrak{R})$. This contradicts the order of $N_6(\mathfrak{R})$. Hence the order of $C_6(\mathfrak{R})$ is equal to $2^{j'} p^{m+y}$, where $y$ is odd and $y > 1$. Let $q$ (≠ 2, $p$) be a prime factor of the order of $C_6(\mathfrak{R})$ and let $Q$ be a permutation of $C_6(\mathfrak{R})$ of order $q$. If $q$ is a factor of $n-1$, then $Q$ leaves just one symbol of $\mathfrak{Q}$ fixed and hence $Q$ cannot be contained in $C_6(\mathfrak{R})$. Thus $q$ is a factor of $n$ and so is $y$. Next assume that $y$ is not divisible by $p$. Let $\mathfrak{R}'$ be a normal $p$-complement in $C_6(\mathfrak{R})$. Since $\mathfrak{R}'$ is cyclic, $\mathfrak{R}'$ has a normal 2-complement $\mathfrak{R}''$. Since $\mathfrak{R}''$ is a normal Hall subgroup of $\mathfrak{R}'$, $\mathfrak{R}''$ is normal even in $N_6(\mathfrak{R})$. Let $Y' \neq 1$ be a permutation of $\mathfrak{R}''$. Then $Y'$ does not leave any symbol of $\mathfrak{Q}$ fixed. If $\mathfrak{R} \cap C_6(Y')$ contains an involution $\tau'$, then $\tau'$ is conjugate to $\tau$ under $\mathfrak{S}$ and, since $C_6(\tau')$ contains $Y'$, the order of $C_6(\tau')$ is divisible by the order of $Y'$. But since $C_6(\tau')$ is conjugate to $C_6(\tau) = N_6(\mathfrak{R}_1)$ and the order of $N_6(\mathfrak{R}_1)$ and $y$ are relatively prime, the order of $\mathfrak{R} \cap C_6(Y')$ is odd. Let $q$ be a prime factor of the order of $\mathfrak{R} \cap C_6(Y')$ and let $Q$ be a permutation of $\mathfrak{R} \cap C_6(Y')$ of order $q$. Then $Q$ leaves at least one symbol of $\mathfrak{Q}$ fixed and hence it leaves at least two symbols of $\mathfrak{Q}$ fixed, which is a contradiction. Thus $\mathfrak{R} \cap C_6(Y') = 1$. Hence we have the following relation:

$$y-1 = |\mathfrak{R}'| - 1 \geq |\mathfrak{R}|,$$

i.e., $y \geq 2^{j'} (p^{m+y} - 1) = 2^{j'} p^{m+y} - (2^{j'} - 1)$. On the other hand $y$ is a factor of $\beta p^{m+y} - (\beta - 1)p^{-1}$. This is a contradiction. Hence $y$ is divisible by $p$. 

266 H. KIMURA
Let us assume $p^m < 2^l$. Let $\mathfrak{A}$ be a normal 2-complement of $C_0\mathfrak{B}$. Then $\mathfrak{A}$ is normal in $N_0(\mathfrak{B})$. Let $\mathfrak{V}$ be a Sylow $p$-subgroup of $\mathfrak{A}$. By the Frattini argument $N_0(\mathfrak{V}) = N_0(\mathfrak{B} \cap N_0(\mathfrak{B}))$. Since the order of $\mathfrak{A}$ is odd, we may assume that $\mathfrak{A}$ is a subgroup of $N_0(\mathfrak{B}) \cap N_0(\mathfrak{B})$. Thus there exists a homomorphism $\pi$ of $\mathfrak{A}$ into $\text{Aut} \mathfrak{V}/\mathfrak{B}$. If $\pi$ is contained in $\ker \pi$, then $\pi$ acts trivially on $\mathfrak{V}/\mathfrak{B}$ and $\mathfrak{B}$. Therefore $\pi$ acts also trivially on $\mathfrak{V}$ and $C_0\pi$ contains $\mathfrak{V}$ ([4, Theorem 5.3.2]). Hence we have $\ker \pi = 1$ and $\text{Aut} \mathfrak{V}/\mathfrak{B}$ contains a cyclic subgroup of order $2^l$. But the order $p^m$ of $\mathfrak{V}/\mathfrak{B}$ is less than $2^l$. This is a contradiction. If $m' \leq m$, then $p^m < 2^l$. Thus we may assume $p^m > 2^l$. Then $m' > m$.

Assume $y > 1$. Since $\mathfrak{A}$ is solvable, there exists a subgroup $\mathfrak{Y}$ of $\mathfrak{A}$ of order $y$. Now $\mathfrak{Y}$ is a factor of $\beta(1-p)^m$. By the Frattini argument it can be assumed that $\mathfrak{A}$ is a subgroup of $N_0(\mathfrak{Y})$. Thus there exists a homomorphism $\pi'$ of $\mathfrak{A}$ into $\text{Aut} \mathfrak{Y}$. Since the orders of $C_0(\mathfrak{A})$ and $\mathfrak{Y}$ are relatively prime, any elements $(\pm 1)$ of $\mathfrak{Y}$ are not fixed by $\pi'(\tau)$. Therefore we have $y > 2^l$. This is impossible and hence $y = 1$. $\mathfrak{Y}$ is normal in $N_0(\mathfrak{B})$. Let $P'$ $(\pm 1)$ be an element of $\mathfrak{Y}$. It can be seen that $\mathfrak{Y} \cap C_0(\mathfrak{Y})$ is a subgroup of $\mathfrak{A}$. Hence we have the following relation:

$$p^{m + m'} - 1 = x(p^m - 1), \quad x > 1.$$  

From this it is easily seen that $m'$ is divisible by $m$.

If $\beta p^m - \beta + 1$ is divisible by $p^m$ $(\delta > 1)$ exactly, then $\beta - 1$ must be equal to $p^{mz} + p^{(\beta - 1)m} + \cdots + p^n (z > 1)$. If $\beta - 1$ is equal to $p^{mz} + p^{(\beta - 1)m} + \cdots + p^n (z > 1)$, then $2^l > p^m$ $(\geq p^m)$. Therefore we may assume $\beta = p^{mz} + \cdots + p^n + 1 = (p^m - 1)/(p^m - 1)$ and $m' = \delta m$. $\mathfrak{Y}$ is a Sylow $p$-subgroup of $\mathfrak{A}$.

Next we shall prove that $m = 1$ and $K$ has only $2^l$-cycles in its cyclic decomposition, i.e., $N_0(\mathfrak{A}) = C_0(\pi)$ and $\mathfrak{R} \cap \mathfrak{R}^\sigma = 1$ or $\mathfrak{R}$ for every element $G$ of $\mathfrak{A}$. From (2.2) it can be seen that the number of involutions with the cyclic structures $(1, 2) \cdots$ which are conjugate to $\tau$ is equal to $\beta$. If $\langle K, I \rangle$ is dihedral, then every involution in $i\mathfrak{R}$ is conjugate to $I$ or $iK$ and if $\langle K, I \rangle$ is semi-dihedral, then every involution in $i\mathfrak{R}$ is conjugate to $I$. Since all involutions with the cyclic structures $(1, 2) \cdots$ are contained in $i\mathfrak{R}$, $\beta$ is equal to $d/2$ or $d$. Thus $p^m + 1$ is a power of two and hence $m = 1$. Therefore $\mathfrak{A}$ is a complete Frobenius group, $\mathfrak{A}(\tau) = \mathfrak{A}(K), N_0(\mathfrak{A}) = C_0(\pi)$ and $C_0(\mathfrak{A})$ contains $\mathfrak{B}$. Therefore the number of elements which leave only the symbol 1 fixed is equal to $2(n - 1) - 1 = (2^l - 1)(\beta i + 1)$ and the number of elements which leave $i$ symbols of $\Omega$ fixed is equal to $(2^l - 1)(\beta i - \beta + 1)(\beta i + 1)$. Let $G$ be an element of $\mathfrak{A}$ of order $2^l p^l (l' \geq 1)$. Then $\alpha(G) = 0$ and $\alpha(G') = i$. Therefore the number of cyclic subgroups of $\mathfrak{A}$ of order $2^l p$ is equal to $(\beta i - \beta + 1)(\beta i + 1)$ and those
groups are independent. Thus the number of elements of order $2^i p' (l' \geq 1)$ which leave no symbol of $Q$ fixed is equal to $(2^i-1)(i-1)(\beta i - \beta +1)(\beta i +1)$. Therefore we have

$$|\mathcal{G}| - (n(2^i(n-1)-1-(2^i-1)(\beta i +1))+(2^i-1)(\beta i - \beta +1)(\beta i +1)$$

$$+(2^i-1)(n-1)(\beta i - \beta +1)+1) = n-1.$$  

Hence $\mathcal{G}$ is a regular normal subgroup of $\mathcal{G}$.

Thus there exists no group satisfying the conditions of the theorem in this case.

4. The case $n$ is even and $N_a(R_1)/R_1$ contains a regular normal subgroup.

1. Since $n = i(\beta i - \beta +1)$ is even, $i$ must be even. $G_1 = N_a(R_1)/R_1$ is a doubly transitive permutation group on $Z(R_1)$ containing a regular normal subgroup. In particular, $i$ is equal to a power of 2, say $2^m$.

Let $\mathcal{G}$ be the normal 2-subgroup of $N_a(R_1)$ containing $R_1$ such that $\mathcal{G}/R_1$ is a regular normal subgroup of $G_1 = N_a(R_1)/R_1$. Since the order of $\mathcal{G} \cap N_a(R_1)$ is equal to $2^i(2^m-1)$, $\mathcal{G}$ is a Sylow 2-subgroup of $G_1 \cap N_a(R_1)$. Let $\Psi$ be a normal 2-complement of $G_1 \cap N_a(R_1)$. The group $\Psi \mathcal{G}/R_1$ is a complete Frobenius group on $Z(1)$ with kernel $\mathcal{G}/R_1$, and complement $\Psi_1/R_1 (\cong \Psi)$. Since $C_{R_1}(\mathcal{G}) \cap \Psi \mathcal{G}$ is normal in $\Psi \mathcal{G}$, $C_{R_1}(\mathcal{G}) \cap \Psi \mathcal{G}$ contains $\mathcal{G}$ or is contained in $\mathcal{G}$ ([13, 12.6.8]). If $\mathcal{G}$ is greater than $C_{R_1}(\mathcal{G}) \cap \Psi \mathcal{G}$, since the index of $\mathcal{G}$ in $\Psi \mathcal{G}$ must be equal to a power of two, we have $m = 1$. Hence $\mathcal{G}$ is a Zassenhaus group. Thus we have that $\mathcal{G}$ is isomorphic to either $PGL(2, 2^i+1)$ or $PSL(2, 2^{i+1}+1)$, where $2^i+1$ and $2^{i+1}+1$ are powers of prime numbers for $PGL(2, 2^i+1)$ and $PSL(2, 2^{i+1}+1)$, respectively ([11], [8], [14] and [18]). Thus it will be assumed that $\mathcal{G}$ is contained in $C_{R_1}(\mathcal{G}) \cap \Psi \mathcal{G}$ and $m$ is greater than one.

Since the index of $\Psi \mathcal{G} \cap C_{R_1}(\mathcal{G})$ in $\Psi \mathcal{G}$ is odd and the order of $\text{Aut} R_1$ is equal to $2^{i-1}$, $\Psi \mathcal{G} \cap C_{R_1}(\mathcal{G})$ is equal to $\Psi \mathcal{G}$. Hence $C_{R_1}(\mathcal{G})$ is equal to $N_a(R_1)$ since $N_a(R_1) = \Psi \mathcal{G}$.

PROPOSITION 4.1. Let $\mathcal{G}$ be as in Theorem and let $R_1$ and $\mathcal{G}_1$ as above. Assume that $\mathcal{G}_1$ contains a regular normal subgroup and $N_a(R_1)$ is equal to $C_{R_1}(\mathcal{G})$. Let $\mathcal{G}$ be as above. Then $\mathcal{G}$ contains an involution ($\neq \tau$).

PROOF. If $R_1$ is equal to $R$, then $\mathcal{G}$ is a normal Sylow 2-subgroup of $N_a(R)$ and hence it contains $I$. Therefore it can be assumed that $R_1$ is less than $R$ and $I \notin \mathcal{G}$. Assume that $\tau$ is the unique involution in $\mathcal{G}$. Since $\mathcal{G}/R_1$ is an elementary abelian group of order $2^m$ and $m \geq 2$, $\mathcal{G}$ is a quaternion group (ordinary or generalized) and hence $m = 2$ (and $i = 4$). Thus we have $\alpha(K) = \cdots = \alpha(K^{2^{i-1}}) = 2 < \alpha(K^{2^i}) = 4$. Since $\Psi \mathcal{G}$ is a Sylow 2-subgroup of
Doubly transitive groups 269

N_{\alpha}(\mathfrak{R})$, it may be assumed that $I$ is contained in the coset $K^{st-j-1}\mathfrak{S}$ and hence we have $IK^{st-j-1}=S$, where $S$ is an element $(\neq K_0)$ of $\mathfrak{S}$. Thus $(K^{st-j-1})_1 = S^2K^{st-j-1}$. Since $N_{\alpha}(\mathfrak{R})=C_{\alpha}(\mathfrak{R})$, we have $K^{st-j}=S^4K^{st}$ and $S^4=K^{st+j+1}$. At first assume that $S^4=1$. Then $j=1$ and $(K^{st+j})_1=K^{st-2}=K^{st-2}$. This implies $d=2$. Hence $n_1=16$ or 28. Since $n-i$ and $i-\alpha(K)$ are divisible by 21 and 21-1, respectively, the order of $\mathfrak{S}$ is equal to four. It can easily be seen that there exists no group satisfying the conditions of Proposition in these cases. Next assume that $S^4\neq 1$ (i.e., $j \neq 1$). Then $(K^{st+j})_1=K^{st-j-1}$ or $K^{st-j-1}$. This implies $n=16$ or 28. Since $n-i$ is divisible by 21 and $j>1$, we have $n=28$, $l=3$ and $j=2$. By [15] $\mathfrak{S}$ must be isomorphic to $PSU(3, 3^2)$. But a Sylow 2-subgroup of $PSU(3, 3^2)$ is isomorphic to $Z_4 \times Z_2$ and it does not contain a quaternion group of order 16. This is a contradiction. Thus the proof is completed.

COROLLARY 4.2. Let $\mathfrak{S}$, $\mathfrak{S}$ be as in Proposition 4.1. If $d$ is equal to two, then $\mathfrak{S}$ contains an involution $\tau'$ such that it is conjugate to $\tau$.

PROOF. By Proposition, $\mathfrak{S}$ contains an involution $\eta(\pm \tau)$ with the cyclic structure $(1 \ a) \ldots$, where $a$ is a symbol of $3(\mathfrak{R})$. Then $\eta \tau$ has also the cyclic structure $(1 \ a) \ldots$. Hence since $\mathfrak{S}$ is doubly transitive, there exist two involutions with the cyclic structure $(1, b)$, where $b$ is any symbol of $Q$, such that those are conjugate to $\eta$ or $\eta \tau$. If $\tau$ is neither conjugate to $\eta$ nor $\eta \tau$, then $g^*(2)$ is greater than $(n-1)$. This contradicts the inequality $g^*(2) < d(n-1)$.

By the above proposition, since $N_{\alpha}(\mathfrak{R})/\mathfrak{R}$ is doubly transitive, we may assume that $I$ is contained in $\mathfrak{S}$. Since $\mathfrak{S}/\mathfrak{R}$ is complete Frobenius group, all elements $(\neq 1)$ of $\mathfrak{S}/\mathfrak{R}$ are conjugate under $\mathfrak{S}/\mathfrak{R}$. Thus every permutation $(\neq \mathfrak{R})$ of $\mathfrak{S}$ can be represented in the form $V^{-1}KV'$, where $V$ and $K$ are permutations of $\mathfrak{S}$ and $\mathfrak{R}$, respectively.

2. Case $\mathfrak{R}=\mathfrak{R}$. In this case $\mathfrak{S}$ is a normal Sylow 2-subgroup of $N_{\alpha}(\mathfrak{R})$. Let $S$ be an element of order 2 of $\mathfrak{S}$. Since $S^2$ is contained in $\mathfrak{S}$, $S^{st-1}$ is equal to $\tau$. Assume that $I$ is conjugate to $\tau$. Since $C_{\alpha}(\mathfrak{R})$ and $C_{\alpha}(I)$ are conjugate and $K$ is contained in $C_{\alpha}(I)$, $K^{st-1}$ must be equal to $I$. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

3. Case $\mathfrak{R} \supseteq \mathfrak{R} \supseteq \langle \tau \rangle$. Since $\mathfrak{R}$ is greater than $\langle \tau \rangle$, a group $\langle K, I \rangle$ is neither dihedral nor semi-dihedral and therefore $d$ is equal to two. By Corollary 4.2 it may be assumed that $I$ is conjugate to $\tau$.

LEMMA 4.3. If $\mathfrak{R}$ is greater than $\langle \tau \rangle$ and less than $\mathfrak{S}$, then the order of $\mathfrak{R}$ is equal to four and $I$ is not contained in $C_{\alpha}(\mathfrak{R})$.

PROOF. At first assume that the order of $\mathfrak{R}$ is greater than four. Let $\mathfrak{S}'$ be a Sylow 2-subgroup of $N_{\alpha}(\mathfrak{R})$. Let $S$ be an element of $\mathfrak{S}'$ of order
The index of $\mathfrak{S}$ in $\mathfrak{S}'$ is equal to $2^{l-j}$. Therefore $S^{2^{l-j}}$ is contained in $\mathfrak{S}$ and, since $\mathfrak{S}/\mathfrak{S}$ is elementary abelian, $S^{2^{l-j+1}}$ is contained in $\mathfrak{S}$. Since $j$ is greater than 2, $S^{2^{l-j+1}}$ is not identity element. Thus we have that $S^{2^{l-2}}$ is equal to $\tau$. Since $IKI$ is equal to $K$ or $K\tau$, $I$ is contained in $C_{\mathfrak{S}}(K^2)$ and hence $K^2$ is contained in $C_{\mathfrak{S}}(I)$. Since $N_\mathfrak{S}(\mathfrak{S}_i) = C_{\mathfrak{S}}(\tau)$ is conjugate to $C_{\mathfrak{S}}(I)$, we have that $(K^2)^{2^{l-2}} = \tau$ must be equal to $I$. This is a contradiction.

Next assume that $I$ is contained in $C_\mathfrak{S}\mathfrak{R}$. Let $\mathfrak{S}'$ be as above. Let $S$ be an element of $\mathfrak{S}'$ of order $2^{l}$. Then $S^{2^{l-j}}$ is contained in $\mathfrak{S}$, $S^{2^{l-j+1}}$ is contained in $K_1$ and finally $S^{2^{l-1}}$ is equal to $\tau$. Since $K$ is contained in $C_\mathfrak{S}(I)$ and $C_\mathfrak{S}(I)$ is conjugate to $C_\mathfrak{S}(\tau)$, $K^{2^{l-1}}$ must be equal to $I$. This is a contradiction. Thus the proof is completed.

Lemma 4.4. Let $\mathfrak{S}_i$ be as in Lemma 4.3. Then the order of $\mathfrak{S}$ is equal to 8.

Proof. Assume that the order of $\mathfrak{S}$ is greater than 8. Then $\langle K^{2^{l-3}}, I \rangle$ is abelian since $d = 2$ and $l > 3$. Let $\eta$ be an involution of $\mathfrak{S}_i(\langle K^{2^{l-3}} \rangle)$. Then $\langle K^{2^{l-3}}, \eta \rangle$ must be abelian, for if it is not abelian, then $\langle K^{2^{l-3}}, I \rangle$ is dihedral and hence $d = 2$.

At first we shall prove that a coset $K^{2^{l-3}}\mathfrak{S}$ does not contain an element of order 4. By Lemma 4.3 the order of $\mathfrak{S}_i$ is equal to 4. Let $K^{2^{l-3}}S$ be an element of order 4 in $K^{2^{l-3}}\mathfrak{S}$, where $S$ is an element of $\mathfrak{S}$. Then $S$ is not contained in $C_\mathfrak{S}(K^{2^{l-3}})$. Set $S = I^V K_1$, where $K_1$ and $V$ are elements of $\mathfrak{S}_i$ and $\mathfrak{S}$, respectively. Then $K^{2^{l-3}}I^V$ must be of order 4. Thus it may be assumed that $S$ is equal to $I^V$ not contained in $C_\mathfrak{S}(K^{2^{l-3}})$, where $V$ is an element of $\mathfrak{S}$. $(K^{2^{l-3}}S)^\eta$ is an element of $\mathfrak{S}$ and therefore is equal to $\tau$, $I^W$ or $I^W\tau$, where $W$ is an element of $\mathfrak{S}$. If $(K^{2^{l-3}}S)^\eta = \tau$, then $(K^{2^{l-3}}S)^\eta = (K^{2^{l-3}})\tau$ and hence $S \in N_\mathfrak{S}(\langle K^{2^{l-3}} \rangle)$. Thus $\langle K^{2^{l-3}}, S \rangle$ must be abelian. This is a contradiction. If $(K^{2^{l-3}}S)^2 = I^W$ or $I^W\tau$, then $(K^{2^{l-3}}S)^2 = K^{-2^{l-3}}I^W$ or $K^{-2^{l-3}}I^W\tau$, respectively. Hence
\[ K^{2^{l-2}} = (K^{2^{l-3}}S)^2 = (K^{-2^{l-3}}I^W)^2 \]
and
\[ (K^{-2^{l-3}}I^W = K^{2^{l-2}}K^{2^{l-3}}. \]

Thus $I^W$ is contained in $N_\mathfrak{S}(\langle K^{2^{l-3}} \rangle)$ and therefore $\langle I^W, K^{2^{l-3}} \rangle$ must be abelian. Hence $K^{2^{l-3}}K^{2^{l-3}} = K^{-2^{l-3}}$. Thus the order of $\mathfrak{S}$ must be equal to $l-1$. This is a contradiction.

Next let $S$ be an element of order $2^{l-1}$ in $\mathfrak{S}\mathfrak{S}$, and let $\mathfrak{S}$ be the image of $S$ by the natural homomorphism of $\mathfrak{S}\mathfrak{S}$ onto $\mathfrak{S}\mathfrak{S}/\mathfrak{S}$. If the order of $\mathfrak{S}$ is equal to $2^{l-2}$, then $S^{2^{l-3}}$ is contained in a coset $K^{2^{l-3}}S$. This contradicts the first part in the proof. Hence we have that the order of $\mathfrak{S}$ is less than $2^{l-2}$ and hence $S^{2^{l-3}}$ is contained in $S$. Therefore $S^{2^{l-3}}$ is equal to $\tau$. Since $C_{\mathfrak{S}}(I)$ is conjugate to $N_\mathfrak{S}(\mathfrak{S}_i)$ and $K^2$ is contained in $C_{\mathfrak{S}}(I)$, $K^{2^{l-1}} = I$. This is a contradiction. Thus the proof is completed.
By two lemmas the orders of \( \mathfrak{R} \) and \( \mathfrak{R}_1 \) are equal to 8 and 4, respectively. Clearly \( N_\mathfrak{R}(\mathfrak{R})/\mathfrak{R} \) is a complete Frobenius group on \( \mathfrak{Z}(\mathfrak{R}) \). Apply the argument in § 2 to \( N_\mathfrak{R}(\mathfrak{R}_1)/\mathfrak{R}_1 \), and we obtain that \( \alpha(\mathfrak{R}) \) must be a power of two and \( i = \alpha(\mathfrak{R})^2 \). Thus a Frobenius kernel of \( N_\mathfrak{R}(\mathfrak{R})/\mathfrak{R} \) is a Sylow 2-subgroup of \( N_\mathfrak{R}(\mathfrak{R})/\mathfrak{R} \). Since, by Lemma 4.3, I is not contained in \( C_\alpha(K) \), a Sylow 2-subgroup of \( N_\mathfrak{R}(K) \) is greater than \( C_\alpha(\mathfrak{R}) \) ([13, 12.6.8]). Since the order of \( N_\mathfrak{R}(\mathfrak{R})/C_\alpha(\mathfrak{R}) \) is a power of two, \( \alpha(K)-1 \) must be equal to one and hence \( \alpha(K) = 2 \). Thus we have \( i = 4 \) and \( n = 16 \) or 28. Since \( n-i \) must be divisible by the order of \( \mathfrak{R} \), we have \( n = 28 \). \( \mathfrak{R} \) satisfies the conditions of the theorem in [15] and hence \( \mathfrak{R} \) is isomorphic to \( PSU(3, 3^2) \).

4. Case \( \mathfrak{R}_1 = \langle \tau \rangle \). We shall prove that \( d = 2 \) or the order of \( \mathfrak{R} \) is equal to four, \( \langle K, I \rangle \) is dihedral and \( i = 4 \). In this case every permutation \( (\mathfrak{R}_1) \) of \( \mathfrak{R} \) can be represented uniquely in the form \( I^r \tau \) or \( I^r \tau \tau \), where \( V \) is any permutation of \( \mathfrak{R} \). Thus every permutation \( (\mathfrak{R}_1) \) of \( \mathfrak{R} \) is of order 2 and hence \( \mathfrak{R} \) is elementary abelian. Set \( \mathfrak{R}_2 = \langle K^{2^{l_i-j_i}} \rangle \), where \( \alpha(\tau) = \alpha(K^{2^{l_i-j_i}}) = \cdots = \alpha(K^{2^{l_i-j_i}}) \). Set \( i' = \alpha(\mathfrak{R}_2) \). Then we may assume \( \mathfrak{Z}(\mathfrak{R}_2) = \{1, 2, \ldots, i'\} \).

Hence \( i' \) is equal to a power of two, say \( 2^{m'} \). By the inductive hypothesis \( N_\mathfrak{R}(\mathfrak{R}_2)/\mathfrak{R}_2 \) contains a regular normal subgroup. Let \( \mathfrak{S}_2 \) be a normal 2-subgroup of \( N_\mathfrak{R}(\mathfrak{R}_2) \) containing \( \mathfrak{R}_2 \) such that \( \mathfrak{S}_2/\mathfrak{R}_2 \) is a regular normal subgroup of \( N_\mathfrak{R}(\mathfrak{R}_2)/\mathfrak{R}_2 \) and let \( \mathfrak{B}_2 \) be a 2-complement of \( \mathfrak{S}_2 \cap N_\mathfrak{R}(\mathfrak{R}_2) \). Then \( \mathfrak{B}_2 \mathfrak{R}_2/\mathfrak{R}_2 \) is a complete Frobenius group on \( \mathfrak{Z}(\mathfrak{R}_2) \). Thus \( C_\alpha(\mathfrak{R}_2) \cap \mathfrak{B}_2 \mathfrak{S}_2 \) contains \( \mathfrak{S}_2 \) or is less than \( \mathfrak{S}_2 \).

If \( C_\alpha(\mathfrak{R}_2) \cap \mathfrak{B}_2 \mathfrak{S}_2 \) is less than \( \mathfrak{S}_2 \), then \( I \) is not contained in \( C_\alpha(\mathfrak{R}_2) \) and, since the order of \( \mathfrak{S}_2 \mathfrak{R}_2/C_\alpha(\mathfrak{R}_2) \cap \mathfrak{B}_2 \mathfrak{S}_2 \) is a power of two, \( m' \) must be equal to one. Thus \( \mathfrak{S}_2/\mathfrak{R}_2 \mathfrak{R}_2/\mathfrak{R}_2 \). On the one hand, it is trivial that \( i-2 \) must be divisible by \( 2^{l_i} \). On the other hand, \( i \) is of a form \( 2^{l_i} \beta^i - \beta^j + 1 \) where \( \beta^j \) is less than or equal to \( 2^{l_i} \) and hence \( \beta^j \) is odd. Therefore we have \( l = 2 \), \( \beta^j = 1 \) and \( i = 4 \).

If \( C_\alpha(\mathfrak{R}_2) \cap \mathfrak{B}_2 \mathfrak{S}_2 \) contains \( \mathfrak{S}_2 \), then \( K^j = K \) or \( K^j \) and hence \( d = 2 \).

5. Case \( |\mathfrak{R}| = 4, \mathfrak{R}_1 = \langle \tau \rangle \) and \( K = K^j \). Let \( \mathfrak{R}_2 \) and \( \mathfrak{S}_2 \) be as in § 4.4. Since \( \mathfrak{R}_2 = \mathfrak{R}_1, \mathfrak{S}_2/\mathfrak{R}_1 \) is a regular normal subgroup of \( N_\mathfrak{R}(\mathfrak{S}_2)/\mathfrak{R}_1 \) and \( N_\mathfrak{R}(\mathfrak{R})/\mathfrak{R}_1 \mathfrak{R}_1 \).

Since \( \langle K, I \rangle \) is dihedral, involutions with the cyclic structure \( (12) \cdots \) are \( I, IK, IK^2, \) and \( IK^3 \), and \( I \) and \( IK \) are conjugate to \( IK^2 \) and \( IK^3 \), respectively. Therefore \( g^*(2) = 0 \) or \( 2(n-1) \).

If \( g^*(2) = 0 \), then \( n = 4(4-4-3) = 4 \cdot 13 \). Let \( \mathfrak{S}_{13} \) be a Sylow 13-subgroup of \( \mathfrak{R} \). Since every involution leaves four symbols of \( \Omega \) fixed, the order of \( C_\alpha(\mathfrak{S}_{13}) \) is equal to 13. Thus the index of \( N_\mathfrak{R}(\mathfrak{S}_{13}) \) in \( \mathfrak{R} \) is a multiple of 17.4. This contradicts the Sylow's theorem.

If \( g^*(2) = 2(n-1) \), then \( n = 4(2n-1) = 4 \cdot 7 \). Let \( \eta \) be an involution leaving
no symbol of $\Omega$ fixed. Then, since $g^*(2) = 2(n-1)$, $G_{\Omega^1}$ must be equal to $2n$. Let $\mathfrak{P}_1$ be a Sylow 7-subgroup of $\mathfrak{S}$ contained in $C_{\Omega^1}$. Using Sylow's theorem $\mathfrak{P}_1$ is normal in $C_{\Omega^1}$. Hence the order of $N_{\mathfrak{S}}(\mathfrak{P}_1)$ is a multiple of $8 \cdot 7$. This contradicts the Sylow's theorem.

Thus there exists no group satisfying the conditions of the theorem in this case.

6. Case $\mathfrak{S}_1 = \langle \tau \rangle$, $d = 2$ and $n = i^2$. In this case a normal subgroup $\mathfrak{S}$ of $N_{\mathfrak{S}}(\mathfrak{S}_1)$ is an elementary abelian 2-group. We shall prove several lemmas.

**Lemma 4.5.** $\mathfrak{S}$ contains every involution of $N_{\mathfrak{S}}(\mathfrak{S}_1)$.

**Proof.** Let $a$ be an involution of $N_{\mathfrak{S}}(\mathfrak{S}_1)$. If $a$ does not contain an involution, then the proof is complete. Let $a$ be an involution in a coset $S^2 = S^2$. Therefore, since $S$ is an involution, $d$ must be greater than two. This is a contradiction.

**Lemma 4.6.** Let $G$ be an element of $\mathfrak{S}$. Then $\mathfrak{S} \cap \mathfrak{S} = 1$ or $\mathfrak{S}$.

**Proof.** Let $\tau'$ be an involution of $\mathfrak{S} \cap \mathfrak{S}$. If $\tau'$ is conjugate to $\tau$, then, since $C_{\mathfrak{S}}(\tau')$ contains $\mathfrak{S}$ and $\mathfrak{S}$ coincides with $\mathfrak{S}$ by Lemma 4.5. Thus an involution of $\mathfrak{S}$ which is conjugate to $\tau$ in $\mathfrak{S}$ is conjugate to $\tau$ in $N_{\mathfrak{S}}(\mathfrak{S})$. By Corollary 4.2, $I$ or $I\tau$ is conjugate to $\tau$ in $G$. On the other hand, $I$ or $I\tau$ is not conjugate to $\tau$ in $\mathfrak{S}$, since $g^*(2) = n-1$. Hence the number of involutions of $\mathfrak{S}$ each of which is conjugate to $\tau$ is equal to $i$ and the number of involutions of $\mathfrak{S}$ each of which leaves no symbol of $\Omega$ fixed is equal to $i - 1$. Hence the order of $N_{\mathfrak{S}}(\mathfrak{S})$ is equal to $2^i(i-1)$ and the following relation is obtained:

$$n - 1 = g^*(2) \leq (i-1)[\mathfrak{S} : N_{\mathfrak{S}}(\mathfrak{S})] = n - 1.$$ 

Thus $\mathfrak{S} \cap \mathfrak{S} = 1$ or $\mathfrak{S}$.

**Lemma 4.7.** Let $\eta$ and $\zeta$ be different involutions. If $\alpha(\eta) = \alpha(\zeta) = 0$, then $\alpha(\eta \zeta) = 0$.

**Proof.** Let $a$ be a symbol of $\mathfrak{S}(\eta \zeta)$. Let $\langle a, b \rangle \cdots$ and $\langle b, c' \rangle \cdots$ be the cyclic structure of $\eta$ and $\zeta$, respectively. Then $a = c'$. Since $g^*(2) = n-1$, there exists just one involution leaving no symbol of $\Omega$ fixed with the cyclic structure $\langle a, b \rangle \cdots$ and hence $\eta = \zeta$.

**Corollary 4.8.** A set $\mathfrak{S}_1$ consisting of all involutions of $\mathfrak{S}$ each of which is not conjugate to $\tau$ and identity element is a characteristic subgroup of $\mathfrak{S}$. In particular $N_{\mathfrak{S}}(\mathfrak{S}_1) = N_{\mathfrak{S}}(\mathfrak{S})$.

By Corollary 4.8, there exists just $i + 1$ subgroups $\mathfrak{S}_1, \mathfrak{S}_2, \ldots, \mathfrak{S}_{i+1}$ which are conjugate in $\mathfrak{S}$ and $\mathfrak{S}_1 \cap \mathfrak{S}_i = 1$ for $s \neq t$.

**Lemma 4.9.** Let $\tau'$ be an involution of $N_{\mathfrak{S}}(\mathfrak{S})$. If $\tau'$ is conjugate to $\tau$, then $\tau'$ is contained in $\mathfrak{S}$.

**Proof.** Set $\tau^a = \tau'$. Since the order of $\mathfrak{S}$ is even, it is trivial that there
exists an element ζ of $\mathfrak{G}$ with $ζτ' = ζ$. $\mathfrak{G}^a$ is normal in $C_θ(τ')$ and it contains $ζ$ and $τ'$ by Lemma 4.5. Thus $\mathfrak{G}_f \cap \mathfrak{G}^a$ contains $ζ$ and hence $\mathfrak{G} = \mathfrak{G}^a$ by Lemma 4.6. Finally $τ'$ is an element of $\mathfrak{G}$.

**Lemma 4.10.** Let $η$ be an involution which is not contained in $\mathfrak{G}$. If $α(η) = 0$, then $α(τη) = 0$ and the order of $τη$ is equal to $2^r$ with $r > 1$.

**Proof.** Assume $α(τη) ≠ 0$. Let $a$ be a symbol of $3(τη)$. It is trivial that $a$ is not a symbol of $3(τ)$. Thus let $(a, b) \cdots$ and $(b, c') \cdots$ be the cyclic structures of $τ$ and $η$, respectively. Then $a = c'$ and $τητ = (a, b) \cdots$. Since $g^*(2) = n-1$, there exists just one involution with the cyclic structure $(a, b) \cdots$ such that it leaves no symbol of $Ω$ fixed. Thus we have $τητ = η$. Therefore $η$ must be contained in $\mathfrak{S}$ and hence $α(τη) = 0$. Next assume that the order of $τη$ is not equal to $2^r$. Let $p$ be an odd prime factor of the order of $τη$ and let $pq$ be the order of $τη$. Then the order of $(τη)^p$ is equal to $p$ and hence $α((τη)^p) = 1$. Therefore $α(τη) = 1$. Thus the order of $τη$ is equal to a power of two.

**Lemma 4.11.** Let $η$ be an involution which is not conjugate to $τ$. Then $η$ is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.

**Proof.** Let us assume that $η$ is not contained in $\mathfrak{G}$. By Lemma 4.10, the order of $τη$ is equal to $2^r$ with $r > 1$. Thus $τ(τη)^{2^r} = τ$. Set $γ_{τη}(s) = τ(τη)^{2^s} = τ^{2^s}$. Then $γ_{τη}(r-1)$ is contained in $C_θ(τ)$ and hence by Lemma 4.5, it is contained in $\mathfrak{S}$. Since $γ_{τη}(r-1) = τ^{r-2}$, $γ_{τη}(r-2)$ is contained in $N_{\mathfrak{G}}(\mathfrak{S})$ by Lemma 4.6. By Lemma 4.9 it is contained in $\mathfrak{S}$. Continuing in the similar way, it can be shown that $γ_{τη}(1) = τ^1$ is contained in $\mathfrak{S}$. By Lemma 4.6, $η$ is contained in $N_{\mathfrak{G}}(\mathfrak{S})$.

By Lemma 4.11, $N_{\mathfrak{G}}(\mathfrak{S}) = N_{\mathfrak{G}}(\mathfrak{S}_i)$ contains $\mathfrak{S}_t (2 ≤ t ≤ i+1)$. Similarly $N_{\mathfrak{G}}(\mathfrak{S}_i)$ contains $\mathfrak{S}_t$. Therefore $\mathfrak{S}_t \mathfrak{S}_i$ is the direct product $\mathfrak{S}_t × \mathfrak{S}_i$. In the similar way it can be proved that every element of $\mathfrak{S}_t$ is commutative with any element of $\mathfrak{S}_t'$ ($1 ≤ t, t' ≤ i+1$). Thus $\mathfrak{K} = \mathfrak{S}_1 \cup \cdots \cup \mathfrak{S}_{i+1}$ is a group. Hence $\mathfrak{K}$ is a regular normal subgroup of $\mathfrak{S}$.

Thus there exists no group satisfying the conditions of the theorem in this case.

7. Case $\mathfrak{K}_1 = \langle τ \rangle$, $d = 2$ and $n = i(2i-1)$. In this case $g^*(2) = 0$. Hence every involution is conjugate to $τ$. The order of $\mathfrak{S}$ is equal to $2^m(2m+1-1)$ ($2^{m+1}+1)(2m-1)$.

Set $\mathfrak{S}' = \mathfrak{S}/\mathfrak{S}$. Since $\mathfrak{S}'/\mathfrak{S}$ is a cyclic Sylow 2-subgroup of $N_{\mathfrak{G}}(\mathfrak{S})/\mathfrak{S}$, $N_{\mathfrak{G}}(\mathfrak{S})/\mathfrak{S}$ is solvable and hence $N_{\mathfrak{G}}(\mathfrak{S})$ is solvable. We shall prove that the order of $N_{\mathfrak{G}}(\mathfrak{S})$ is equal to $2^{m+1}2^{m-1}$. Remark that Lemma 4.5 is also true for this case. Let $τ' = τ^v$ be an element of $\mathfrak{S}$, where $G$ is an element of $\mathfrak{G}$. The same argument as in the proof of Lemma 4.6 shows that $G$ is contained in $N_{\mathfrak{G}}(\mathfrak{S})$. Thus every element ($≠ 1$) of $\mathfrak{S}$ is conjugate to $τ$ under $N_{\mathfrak{G}}(\mathfrak{S})$. 

*Doubly transitive groups*
Hence the index of $C_0(\tau)$ in $N_4(\Omega)$ is equal to $2^{m+1}-1$.

Let $\mathfrak{B}$ be a normal 2-complement of $\mathfrak{H} \cap N_4(\Omega)$. Since $N_4(\Omega)$ is solvable, there exists a Hall subgroup $\mathfrak{A}$ of order $(2^m-1)(2^{m+1}-1)$ of $N_4(\Omega)$ containing $\mathfrak{B}$. Since $\mathfrak{H}/\mathfrak{A}$ is a complete Frobenius group of degree $2^n$, all Sylow subgroups of $\mathfrak{H}$ are cyclic. Let $r$ be the least prime factor of the order of $\mathfrak{B}$. Let $\mathfrak{H}$ be a Sylow $r$-subgroup of $\mathfrak{B}$. Then $\mathfrak{A}$ is cyclic and leaves only the symbol 1 fixed. Hence $N_4(\mathfrak{B})$ is contained in $\mathfrak{H}$. Let $\mathfrak{R}$ be a Sylow 2-subgroup of $C_0(\Omega)$. Since $\mathfrak{H}$ is a Sylow 2-subgroup of $\mathfrak{H}$ and $C_0(\Omega)$ is a subgroup of $\mathfrak{H}$, $\mathfrak{R}$ is conjugate to a subgroup of $\mathfrak{H}$. Thus it may be assumed that $\mathfrak{R}$ is a subgroup of $\mathfrak{H}$. Using Sylow's theorem, we obtain that $N_4(\mathfrak{B}) = C_0(\Omega)(N_4(\mathfrak{B}) \cap N_4(\Omega)) = C_0(\Omega)(N_4(\mathfrak{B}) \cap N_4(\mathfrak{B}))$ since $N_4(\mathfrak{B})$ is a subgroup of $\mathfrak{H}$. Let $CVR'$ be an element of $N_4(\Omega)$ of odd order $u$, where $C$, $V$, and $K'$ are elements of $C_0(\Omega)$, $\mathfrak{B}$ and $\mathfrak{R}$, respectively. Then $(CVR')^u = C(VK')^u$, where $C'$ is an element of $C_0(\Omega)$, and $(VK')^u = C^{-1}$. Set $s = |(VK')^u| / |K'|$, where $|CVR'|$ and $|K'|$ are orders of $(VK')^u$ and $K'$, respectively. Then $s$ is an odd integer and $(VK')^u$ is contained in a Sylow 2-subgroup of $C_0(\Omega)$ and hence so is $VK'$. In particular $CVR'$ is an element of $C_0(\Omega)$. Hence we obtain that $N_4(\mathfrak{B}) \cap \mathfrak{H} = C_0(\Omega)(N_4(\mathfrak{B}) \cap \mathfrak{B}) \cap \mathfrak{H} = C_0(\Omega)(N_4(\mathfrak{B}) \cap \mathfrak{B}) \cap \mathfrak{H} = C_0(\Omega) \cap \mathfrak{H}$. By the splitting theorem of Burnside $\mathfrak{H}$ has the normal $r$-complement. Continuing in the similar way, it can be shown that $\mathfrak{H}$ has the normal subgroup $\mathfrak{B}$ of order $2^{m+1}-1$, which is a complement of $\mathfrak{B}$. Every permutation $\tau \not= 1$ of $\mathfrak{B}$ leaves no symbol of $\Omega$ fixed and hence it is not commutative with any permutation $\not= 1$ of $\mathfrak{B}$. Let $B$ be a permutation of $\mathfrak{B}$ of a prime order, say $q$. Then all the permutations are conjugate to either $B$ or $B^{-1}$ under $\mathfrak{B}$. This implies that $\mathfrak{B}$ is an elementary abelian $q$-group of order $q^r$. Then it follows that $2^{m+1}-1 = q^s$. Hence $s = 1$ and $\mathfrak{B}$ is cyclic of order $q$. $\mathfrak{B}$ is also cyclic.

Let the order of $N_4(\mathfrak{B})$ be equal to $\frac{1}{2}x(q-1)q$. If the order of $C_0(\mathfrak{B})$ is even, then there exists an involution $\tau'$ in $C_0(\mathfrak{B})$ which is conjugate to $\tau$ and such that $C_0(\tau')$ contains $\mathfrak{B}$. But the orders of $C_0(\tau)$ and $\mathfrak{B}$ are relatively prime. Hence, since $C_0(\tau')$ is conjugate to $C_0(\tau)$, the order of $C_0(\mathfrak{B})$ is odd. Therefore, since the order of the automorphism group of $\mathfrak{B}$ is equal to $q-1 = 2^{m+1}-2$, the order of $N_4(\mathfrak{B})$ is not divisible by four.

Using Sylow's theorem we obtain the following congruence:

$$2^{l-1}(q+1)(q+2)/x \equiv 1 \pmod{q}.$$ 

This implies that $2^{l-1}(q+1)(q+2) = x(qy+1)$, where $y$ is positive since $x$ is less than $2^{l-1}(q+1)(q+2)$. Then we have that $x = yq + 2l$, where $2^{l-1}z \geq 0$. It can be proved that $z$ must be equal to 0 or $2^{l-1}$. If $z = 0$, then the order of $N_4(\mathfrak{B})$ is equal to $2^l q^l(q-1)$ and hence, since $l > 1$, it is divisible by four. If $z = 2^{l-1}$,
then the order of $N_{a}(B)$ is equal to $2^{n-1}(q+2) \frac{1}{2} q(q-1)$. Let $Y$ be a permutation $(\neq 1)$ of odd prime order dividing $(q+2) \frac{1}{2} (q-1)$ which is contained in $N_{a}(B)$. Since $Y$ leaves just one symbol of $\Omega$ fixed, $Y$ is not contained in $C_{a}(B)$. Hence we obtain the following;

$$q-1 \geq \frac{|N_{a}(B)/C_{a}(B)|}{\frac{1}{2} (q+2)(q-1)}.$$  

But this is impossible.

Thus there exists no group satisfying the conditions of the theorem in this case.

5. The case $n$ is even and $N_{a}(R_{a})/R_{a}$ does not contain a regular normal subgroup.

1. Since $N_{a}(R)/R$ is a complete Frobenius group and hence it contains a regular normal subgroup, $R_{a}$ is a proper subgroup of $R$.

2. Case $R_{a} = \langle \tau \rangle$ and $2 \leq 8$. By inductive hypothesis, if $2' = 4$, then $G_{a} = N_{a}(R_{a})/R_{a}$ is isomorphic to either $PSL(2, 5)$ or $SL*(2, 8)$ and, if $2' = 8$, then $G_{a}$ is isomorphic either $PGL(2, 5)$ or $PSL(2, 9)$.

At first assume that $d = 2$. If $2' = 8$, then $i = 6$ or 10. Hence $n - i = \beta(i - 1)$ $(\beta = 1$ or 2) is not divisible by 8. But $n - i$ must be divisible by the order of $R$. This is a contradiction. If $G_{a}$ is isomorphic to $PSL(2, 5)$, then $i = 6$ and, since $n - i$ must be divisible by 4, $n$ is equal to $6(2i - 1) = 6 \cdot 11$. Let $\Psi_{11}$ be a Sylow 11-subgroup of $G$. It is trivial that, since $g * (2) = 0$ and the order of $N_{a}(R_{a})$ is equal to $6 \cdot 5 \cdot 4$, the order of $C_{a}(\Psi_{11})$ is odd. Since the order of $C_{a}(\Psi_{11})$ and $n - 1$ are relatively prime, the order of $C_{a}(\Psi_{11})$ is equal to 11 or 33. The index of $C_{a}(\Psi_{11})$ in $N_{a}(R_{a})$ is a factor of 10. Thus this contradicts the Sylow's theorem.

If $G_{a}$ is isomorphic to $SL*(2, 8)$, then $i = 28$. Since every involution of $G_{a}$ leaves just four symbols of $B$, we obtain that $\alpha(I) = 0$. Therefore, since every involution of $G$ is conjugate to a permutation with the cyclic structure $(12) \cdots$, we have that $g * (2) = 0$ and hence $n = i(2i - 1)$. Thus the order of $G$ is equal to $4 \cdot 3^{i} \cdot 19$. Since $G$ is cyclic, $G$ has a normal 2-complement $C$ of order $3^{i} \cdot 19$. Let $\Psi_{19}$ be Sylow 19-subgroup of $G$. By Sylow's theorem $\Psi_{19}$ is normal in $G$. Since the order of the automorphism group of $\Psi_{19}$ is equal to 18, $\tau$ must be contained in $C_{a}(\Psi_{19})$. This is a contradiction.

Next we shall consider the case $d \neq 2$. If $2' = 4$, then $\langle K, I \rangle$ is dihedral. If $G_{a}$ is isomorphic to $PSL(2, 5)$, then $i = 6$ and, since $n - i = i\beta(i - 1)$ must be divisible by 4, $\beta = 2$ or 4. Therefore $\langle K, I \rangle$ is a Sylow 2-subgroup of $G$. By [4, Theorem 7.7.3] $C_{a}(\tau)$ has a normal 2-complement and hence $C_{a}(\tau)$ is solvable.
Thus \( \Theta_1 = C_\alpha(\tau)/\langle \tau \rangle \) must be solvable and this is a contradiction. If \( \Theta_1 \) is isomorphic to \( SL^*(2, 8) \), then, since for every involution \( \gamma \) of \( SL^*(2, 8) \), \( \alpha(\gamma) = 4 \), \( \alpha(\Theta) = 4 \). Hence the order of \( N_\Theta(\Theta)/\Theta \) is equal to 4·3. Since \( I \) is not contained in \( C_\alpha(\Theta) \) and \( N_\Theta(\Theta)/\Theta \) is a complete Frobenius group, \( C_\alpha(\Theta) \) is contained in a Sylow 2-subgroup. Thus the order of \( N_\Theta(\Theta)/C_\alpha(\Theta) \) is divisible by 3. This is a contradiction.

If \( 2z = 8 \), then \( i = 6 \) or 10. Since \( n - i = 3(i-1) \) must be divisible by 8, \( 3 \) is equal to 4 or 8. If \( \langle K, I \rangle \) is dihedral, then \( \langle K, I \rangle \) is a Sylow 2-subgroup of \( \Theta \). Thus \( C_\alpha(\tau) \) is solvable and also \( C_\alpha(\tau)/\langle \tau \rangle \) is solvable. Hence \( \langle K, I \rangle \) must be semi-dihedral and \( d = 4 \). Since \( g^*(2) = 0 \) and \( \Theta_1 \) is Zassenhaus group, all involutions are conjugate and a permutation leaving at least three symbols of \( \Omega \) fixed is an involution. Thus \( \Theta \) satisfies the conditions in [12]. Hence by [6] and [12], \( \Theta \) is isomorphic to either \( PSU(3, 5^p) \) or one of the groups of Ree type (see [16]). Since a Sylow 2-subgroup of a group of Ree type is elementary abelian of order 8, \( G \) is isomorphic to \( PSU(3, 5^p) \).

3. Case \( \mathfrak{R}_1 = \langle \tau \rangle \) and \( 2^d > 8 \). \( \Theta_1 \) is isomorphic to one of the groups \( PSU(3, 3^p) \), \( PSU(3, 5^p) \), \( PGL(2, *) \) and \( PSL(2, *) \). Then \( i \) is not divisible by 8. Since \( n - i = 3(i-1) \) is divisible by \( 2^d \), \( \beta \) is divisible by 4. Thus we have that \( d > 2 \) and hence \( \langle K, I \rangle \) is dihedral or semi-dihedral and in particular \( \langle K, I \rangle/\langle \tau \rangle \) is dihedral. Therefore \( \Theta_1 \) is isomorphic to either \( PGL(2, *) \) or \( PSL(2, *) \) and \( i \) is divisible by 2 exactly. Thus we have that \( \beta = 2^{i-1} \) or \( 2^i \). Thus \( \langle K, I \rangle \) is a Sylow 2-subgroup of \( \Theta \). If \( \langle K, I \rangle \) is dihedral, then \( C_\alpha(\tau) \) is solvable and \( \Theta_1 \) is semi-dihedral. Then \( \beta = 2^{i-1} \) and \( g^*(2) = 0 \). Again by [6] and [12], \( G \) must be isomorphic to either \( PSU(3, 5^p) \) or one of the groups of Ree type. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

4. Case \( \mathfrak{R}_1 > \langle \tau \rangle \). Since \( \mathfrak{R}_1 \) is a proper subgroup of \( \mathfrak{R} \), the order of \( \mathfrak{R} \) is greater than 4. At first assume that \( d = 2 \). By inductive hypothesis \( i \) is not divisible by 8. Since \( n - i = 3(i-1) \) is divisible by \( 2^i \), \( \beta = 2 \), \( 2^i = 8 \) and \( i \) is divisible by 4. Thus we obtain that \( \Theta_1 \) is isomorphic to \( SL^*(2, 8) \) and \( n = 2^i \cdot 7 \cdot 5 \cdot 11 \). If we consider a Sylow 19-subgroup of \( \Theta \), likewise in 5.2, we can obtain a contradiction.

Next we assume that \( d > 2 \). Then \( \langle K, I \rangle/\mathfrak{R}_1 \) is dihedral. Hence \( \Theta_1 \) is isomorphic to either \( PGL(2, *) \) or \( PSL(2, *) \). Since \( n - i \) is divisible by \( 2^i \), we have that \( \beta = 2^i \) or \( 2^{i-1} \). Therefore \( \langle K, I \rangle \) is a Sylow 2-subgroup of \( \Theta \). If \( \langle K, I \rangle \) is dihedral, then \( C_\alpha(\tau) \) is solvable and hence \( C_\alpha(\tau)/\mathfrak{R}_1 \) must be solvable. Thus \( \langle K, I \rangle \) is semi-dihedral. Set \( \Theta_0 = C_\alpha(\tau)/\langle \tau \rangle = N_\Theta(\mathfrak{R}_1)/\langle \tau \rangle \). Then, since \( \langle K, I \rangle/\mathfrak{R}_1 \) is a Sylow 2-subgroup of \( \Theta_0 \) and a dihedral group. Let \( \eta = K^{i-2}\langle \tau \rangle \) be the involution in the center of \( \langle K, I \rangle/\langle \tau \rangle \). It can be easily
Doubly transitive groups

proved that \( \eta \) is contained in the center of \( G_\eta \). Thus, by [4, Theorem 7.7.3], \( G_\eta \) has a normal 2-complement and hence \( G_\eta \) is solvable. Hence \( G_\eta \) must be solvable. This is a contradiction.

Thus there exists no group satisfying the conditions of the theorem in this case.

Thus Theorem is proved.

Hokkaido University

References