

Title	On multiply transitive permutation groups
Author(s)	Yoshizawa, Mitsuo
Citation	Osaka Journal of Mathematics. 1979, 16(3), p. 775-795
Version Type	VoR
URL	<a href="https://doi.org/10.18910/6040">https://doi.org/10.18910/6040</a>
rights	
Note	

*Osaka University Knowledge Archive : OUKA*

<https://ir.library.osaka-u.ac.jp/>

Osaka University

## ON MULTIPLY TRANSITIVE PERMUTATION GROUPS

MITSUO YOSHIZAWA

(Received January 9, 1978)

### 1. Introduction

In this paper we shall give some improvements of the following four results:

RESULT 1 (E. Bannai [5] Theorem 1). Let  $p$  be an odd prime. Let  $G$  be a permutation group on a set  $\Omega = \{1, 2, \dots, n\}$  which satisfies the following condition: For any  $p^2$  elements  $\alpha_1, \dots, \alpha_{p^2}$  of  $\Omega$ , a Sylow  $p$ -subgroup  $P$  of the stabilizer in  $G$  of the  $p^2$  points  $\alpha_1, \dots, \alpha_{p^2}$  is nontrivial and fixes  $p^2 + r$  points of  $\Omega$ , and moreover  $P$  is semiregular on the set  $\Omega - I(P)$  of the remaining  $|\Omega| - p^2 - r$  points, where  $r$  is independent of the choice of  $\alpha_1, \dots, \alpha_{p^2}$  and  $0 \leq r \leq p - 1$ . Then  $n = p^2 + p + r$ , and one of the following three cases holds: (1) There exists an orbit  $\Omega_1$  of  $G$  such that  $|\Omega - \Omega_1| \leq r$  and  $G^{\Omega_1} \geq A^{\Omega_1}$ . Moreover,  $(G_{\Omega - \Omega_1})^{\Omega_1} \geq A^{\Omega_1}$ . (2)  $r = p - 1$ , and  $G$  has just two orbits  $\Omega$  and  $\Omega_2$  (with  $|\Omega_1| \geq |\Omega_2| \geq p$ ) such that  $G^{\Omega_1} \geq A^{\Omega_1}$ . Moreover  $(G_{\Omega_2})^{\Omega_1} \geq A^{\Omega_1}$  and  $G^{\Omega_2}$  is primitive and contains an element of a  $p$ -cycle (therefore  $G^{\Omega_2} \geq A^{\Omega_2}$  if  $|\Omega_2| \geq p + 3$ ). (3)  $r = p - 1$ , and  $G$  is imprimitive on  $\Omega$  with just two blocks  $\Omega_1$  and  $\Omega_2$ . Moreover,  $(G_{\Omega_1})^{\Omega_2} \geq A^{\Omega_2}$  and  $(G_{\Omega_2})^{\Omega_1} \geq A^{\Omega_1}$ .

RESULT 2 (E. Bannai [4] Theorem 1). Let  $p$  be an odd prime. Let  $G$  be a  $2p$ -transitive permutation group such that either (i) each element in  $G$  of order  $p$  fixes at most  $2p + (p - 1)$  points, or (ii) a Sylow  $p$ -subgroup of  $G_{1,2,\dots,2p}$  is cyclic. Then  $G$  is one of  $S_n$  ( $2p \leq n \leq 4p - 1$ ) and  $A_n$  ( $2p + 2 \leq n \leq 4p - 1$ ).

RESULT 3 (D. Livingstone and A. Wanger [10] Lemma 10). If  $G$  is a  $k$ -transitive group on a set  $\Omega$  of  $n$  points, with  $n > k \geq 4$ , then there exists a subset  $\Pi$  of  $k + 1$  points such that  $G_{(\Pi)}^{\Pi} \geq A^{\Pi}$ .

RESULT 4 (H. Wielandt [13] Satz B). If  $G$  is a nontrivial  $t$ -transitive group on  $\Omega$  of  $n$  points, and if  $t$  is sufficiently large, then  $\log(n - t) > \frac{1}{2}t$ .

In § 2 and § 3, we shall prove the following two theorems which improve Result 1 and Result 2.

**Theorem A.** *Let  $p$  be an odd prime. Let  $G$  be a permutation group on a*

set  $\Omega = \{1, 2, \dots, n\}$  which satisfies the following condition. For any  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  of  $\Omega$ , a Sylow  $p$ -subgroup  $P$  of the stabilizer in  $G$  of the  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  is nontrivial and fixes exactly  $2p+r$  points of  $\Omega$ , and moreover  $P$  is semiregular on the set  $\Omega - I(P)$  of the remaining  $n - 2p - r$  points, where  $r$  is independent of the choice of  $\alpha_1, \dots, \alpha_{2p}$  and  $0 \leq r \leq p - 2$ . Then  $n = 3p + r$ , and there exists an orbit  $\Gamma$  of  $G$  such that  $|\Gamma| \geq 3p$  and  $G^\Gamma \cong A^\Gamma$ .

**Theorem B.** Let  $p$  be an odd prime  $\geq 11$ . Let  $G$  be a permutation group on a set  $\Omega = \{1, 2, \dots, n\}$  which satisfies the following condition. For any  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  of  $\Omega$ , a Sylow  $p$ -subgroup  $P$  of the stabilizer in  $G$  of the  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  is nontrivial and fixes exactly  $3p - 1$  points of  $\Omega$ , and moreover  $P$  is semiregular on the set  $\Omega - I(P)$  of the remaining  $n - 3p + 1$  points. Then  $n = 4p - 1$ , and one of the following two cases holds: (1) There exists an orbit  $\Gamma$  of  $G$  such that  $|\Gamma| \geq 3p$  and  $G^\Gamma \cong A^\Gamma$ . (2)  $G$  has just two orbits  $\Gamma_1$  and  $\Gamma_2$  with  $|\Gamma_1| \geq p$ ,  $|\Gamma_2| \geq p$  and  $|\Gamma_1| + |\Gamma_2| = 4p - 1$ , and  $G^{\Gamma_i}$  is  $(|\Gamma_i| - p + 1)$ -transitive on  $\Gamma_i$  ( $i = 1, 2$ ). Moreover,  $G^{\Gamma_i} \cong A^{\Gamma_i}$  if  $|\Gamma_i| \geq p + 3$ .

REMARK. We note that T. Oyama proved:

RESULT 5 (T. Oyama [12] Theorem 1). Let  $G$  be a permutation group on  $\Omega = \{1, 2, \dots, n\}$ . Assume that a Sylow 2-subgroup  $P$  of the stabilizer of any four points in  $G$  satisfies the following condition:  $P$  is a nonidentity semiregular group and  $P$  fixes exactly  $r$  points. Then (I)  $r = 4$ , then  $|\Omega| = 6, 8$  or  $12$ , and  $G = S_6, A_8$  or  $M_{12}$  respectively. (II) If  $r = 5$ , then  $|\Omega| = 7, 9$  or  $13$ . In particular, if  $|\Omega| = 9$ , then  $G \leq A_9$ , and if  $|\Omega| = 13$ , then  $G = S_1 \times M_{12}$ . (III) If  $r = 7$  and  $N_G(P)^{I(P)} \leq A_7$ , then  $G = M_{23}$ .

Theorem A and Theorem B might look to be too technical. However they are useful in applications. In §4, we shall prove the following two consequences of them which improve Result 3 and Result 4 respectively.

**Theorem C.** Let  $p$  be an odd prime. Let  $G$  be a nontrivial  $2p$ -transitive group on  $\Omega = \{1, 2, \dots, n\}$ . Then there exists a subset  $\Gamma$  of  $\Omega$  such that  $|\Gamma| \geq 3p - 1$  and  $G_{(\Gamma)}^\Gamma \cong A^\Gamma$ .

**Theorem D.** Let  $G$  be a nontrivial  $t$ -transitive group on  $\Omega = \{1, 2, \dots, n\}$ . If  $t$  is sufficiently large, then  $\log(n - t) > \frac{3}{4}t$ .

We give the outline of §2. Let  $G$  be a group satisfying the assumption of Theorem A. Then,  $G$  has the only one orbit whose length is not less than  $p$ . So, we may assume that  $G$  is transitive on  $\Omega$ . Moreover, we find that if  $p \geq 5$ , then  $G$  is  $(p + 3)$ -transitive on  $\Omega$ , and that if  $p = 3$ , then  $G$  is 5-transitive on  $\Omega$ . Suppose that  $G \not\cong A^\Omega$ . Similarly to Bannai [4, §1], we get a contradiction by using the idea of Miyamoto and Nago which uses the formula of

Frobenius ingeniously (cf. [11, Lemma 1.1]).

Next we give the outline of § 3. Let  $G$  be a counter-example to Theorem B with the least degree. So, we may assume that  $G$  is transitive on  $\Omega$ . Moreover, we find that  $G$  is  $\left(p + \frac{p+1}{2} + 2\right)$ -transitive on  $\Omega$ . Again by the similar argument to that of [4, § 1], we get a contradiction.

NOTATION. Our notation will be more or less standard. Let  $\Omega$  be a set and  $\Delta$  be a subset of  $\Omega$ . If  $G$  is a permutation group on  $\Omega$ , then  $G_\Delta$  denotes the pointwise stabilizer of  $\Delta$  in  $G$ , and  $G_{(\Delta)}$  denotes the global stabilizer of  $\Delta$  in  $G$ . When  $\Delta = \{\alpha_1, \dots, \alpha_k\}$ , we also denote  $G_\Delta$  by  $G_{\alpha_1, \dots, \alpha_k}$ . The totality of points left fixed by a set  $X$  of permutations is denoted by  $I(X)$ , and if a subset  $\Gamma$  of  $\Omega$  is fixed as a whole by  $X$ , then the restriction of  $X$  on  $\Gamma$  is denoted by  $X^\Gamma$ . For a permutation  $x$ , let  $\alpha_i(x)$  denote the number of  $i$ -cycles of  $x$  and  $\alpha(x) = \alpha_1(x)$ .  $S^\Omega$  and  $A^\Omega$  denote the symmetric and alternating groups on  $\Omega$ . If  $|\Omega|$ , the cardinality of  $\Omega$ , is  $n$ , we denote them  $S_n$  and  $A_n$  instead of  $S^\Omega$  and  $A^\Omega$ .

Acknowledgement. The author would like to thank Professor E. Bannai for suggesting him the present research and giving him many advices.

**2. Proof of Theorem A**

Let  $G$  be a permutation group satisfying the assumption of Theorem A.

Step 1.  $G$  has an orbit  $\Gamma$  such that  $|\Gamma| \geq 3p$  and  $|\Omega - \Gamma| < p$ .

Proof. Since a Sylow  $p$ -subgroup of the stabilizer in  $G$  of  $2p$  points is nontrivial and fixes exactly  $2p+r$  points, we have  $|\Omega| \geq 3p+r$  and that  $G$  has an orbit  $\Gamma$  whose length is at least  $p$ . Set  $|\Gamma| \equiv k \pmod p$  with  $0 \leq k \leq p-1$ .

Suppose that  $|\Gamma| = p+k$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$  from  $\Gamma$  and  $2p-k-1$  points  $\alpha_{k+2}, \dots, \alpha_{2p}$  from  $\Omega - \Gamma$ . A Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{2p}}$  fixes at least  $3p-1$  points, which contradicts the assumption of Theorem A. Hence we have  $|\Gamma| \geq 2p+k$ .

Suppose that  $|\Omega - \Gamma| \geq p$ . We take  $p+k+1$  points  $\alpha_1, \dots, \alpha_{p+k+1}$  from  $\Gamma$  and  $p-k-1$  points  $\alpha_{p+k+2}, \dots, \alpha_{2p}$  from  $\Omega - \Gamma$ . A Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{2p}}$  fixes at least  $3p-1$  points, which contradicts the assumption of Theorem A. Hence we have  $|\Omega - \Gamma| < p$ . So, we have  $|\Gamma| \geq 3p$ . (q.e.d.)

By Step 1, from now on we may assume that  $G$  is transitive on  $\Omega$ .

Step 2. Let  $1 \leq t \leq p+2$ . If  $G$  is  $t$ -transitive on  $\Omega$ , then  $G$  is  $t$ -primitive on  $\Omega$ .

Proof. Suppose, by way of contradiction, that  $G$  is  $t$ -transitive on  $\Omega$ , and that  $G_{1, \dots, t-1}$  is imprimitive on  $\Omega - \{1, \dots, t-1\}$ . Let  $\Gamma_1, \dots, \Gamma_s$  be a system

of imprimitivity of  $G_{1,\dots,t-1}$ . Let  $|\Gamma_1| \equiv k \pmod p$ , where  $0 \leq k \leq p-1$ . We divide the consideration into the following two cases: (I)  $2p-(t-1) > k$ . (II)  $2p-(t-1) \leq k$ .

Suppose that Case (I) holds. First assume that  $|\Gamma_1| \geq 2p$ . We take  $k+1$  points  $\alpha_i, \dots, \alpha_{t+k}$  from  $\Gamma_1$  and  $2p-t-k$  points  $\alpha_{t+k+1}, \dots, \alpha_{2p}$  from  $\Gamma_2$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,t-1,\alpha_t,\dots,\alpha_{2p}}$  fixes at least  $3p-1$  points, which is a contradiction. Next assume that  $p \leq |\Gamma_1| < 2p$ . We take  $k+1$  points  $\alpha_i, \dots, \alpha_{t+k}$  from  $\Gamma_1$ . Moreover, we are able to take  $2p-t-k$  points  $\alpha_{t+k+1}, \dots, \alpha_{2p}$  from  $\Omega - (\Gamma_1 \cup \{1, \dots, t-1\})$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,t-1,\alpha_t,\dots,\alpha_{2p}}$  fixes at least  $3p-1$  points, which is a contradiction. Hence we may assume that  $|\Gamma_1| < p$ . Let  $\gamma_i$  be a point of  $\Gamma_i$  ( $i=1, \dots, s$ ). Assume  $s \leq 2p-t+1$ . Then a Sylow  $p$ -subgroup of  $G_{1,\dots,t-1,\gamma_1,\dots,\gamma_s}$  is trivial, a contradiction. Hence  $s > 2p-t+1$ . Since a Sylow  $p$ -subgroup of  $G_{1,\dots,t-1,\gamma_1,\dots,\gamma_{2p+t-1}}$  fixes at most  $3p-2$  points, we have  $(k-1) \leq (2p-t+1) \leq p-2$ . But, since  $t \leq p+2$  and  $k \geq 2$ , we have a contradiction.

Suppose that Case (II) holds. In this case, we have  $t=p+2$  and  $k=p-1$ . We take a point  $\alpha$  from  $\Gamma_1$  and  $p-2$  points  $\beta_1, \dots, \beta_{p-2}$  from  $\Gamma_2$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,p+1,\alpha,\beta_1,\dots,\beta_{p-2}}$  fixes at least  $3p-1$  points, which is a contradiction. (q.e.d)

Step 3.  $G$  is  $(p+3)$ -transitive on  $\Omega$  when  $p \geq 5$ , and  $G$  is 5-transitive on  $\Omega$  when  $p=3$ .

Proof. In order to prove Step 3, we show that if  $G$  is  $t$ -transitive on  $\Omega$  then  $G$  is  $(t+1)$ -transitive on  $\Omega$ , where  $1 \leq t \leq p+2$  when  $p \geq 5$  and  $1 \leq t \leq 4$  when  $p=3$ . Suppose, by way of contradiction, that  $G$  is  $t$ -transitive on  $\Omega$ , but  $G$  is not  $(t+1)$ -transitive on  $\Omega$ . By Step 2,  $G$  is  $t$ -primitive on  $\Omega$ . Let  $\Delta_1, \dots, \Delta_s$  be the orbits of  $G_{1,\dots,t}$  on  $\Omega - \{1, \dots, t\}$ , where  $s \geq 2$ . By Theorem 18.4 in [14],  $|\Delta_i| \geq p$  for every  $\Delta_i$  ( $i=1, \dots, s$ ). Let  $|\Delta_i| \equiv u_i \pmod p$ , where  $0 \leq u_i \leq p-1$  ( $i=1, \dots, s$ ). By the assumption of  $t$ , we have that  $p-2 \leq 2p-t \leq 2p-1$  when  $p \geq 5$ , and  $2 \leq 2p-t \leq 5$  when  $p=3$ . We divide the consideration into the following two cases: (I)  $2p-t \geq p$ . (II)  $2p-t < p$ .

Suppose that Case (I) holds. First assume that  $2p-t-u_1-1 \leq p$ . We take  $u_1+1$  points  $\alpha_1, \dots, \alpha_{u_1+1}$  from  $\Delta_1$  and  $2p-t-u_1-1$  points  $\beta_1, \dots, \beta_{2p-t-u_1-1}$  from  $\Delta_2$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,t,\alpha_1,\dots,\alpha_{u_1+1},\beta_1,\dots,\beta_{2p-t-u_1-1}}$  fixes at least  $3p-1$  points, which is a contradiction. Next assume that  $2p-t-u_1-1 > p$  and  $|\Delta_1| \geq 2p$ . we take  $u_1+p+1$  points  $\alpha_1, \dots, \alpha_{u_1+p+1}$  from  $\Delta_1$  and  $p-t-u_1-1$  points  $\beta_1, \dots, \beta_{p-t-u_1-1}$  from  $\Delta_2$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,t,\alpha_1,\dots,\alpha_{u_1+p+1},\beta_1,\dots,\beta_{p-t-u_1-1}}$  fixes at least  $3p-1$  points, which is a contradiction. Hence we may assume that  $2p-t-u_1-1 > p$  and  $|\Delta_1| < 2p$ . We take  $u_1+1$  points  $\alpha_1, \dots, \alpha_{u_1+1}$  from  $\Delta_1$ . Moreover we are able to take  $2p-t-u_1-1$  points  $\beta_1, \dots, \beta_{2p-t-u_1-1}$  from  $\Omega - (\{1, \dots, t\} \cup \Delta_1)$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,\alpha_1,\dots,\alpha_{u_1+1},\beta_1,\dots,\beta_{2p-t-u_1-1}}$  fixes

at least  $3p-1$  points, which is a contradiction.

Suppose that Case (II) holds. In this case, we have that  $2p-t=p-2$  or  $p-1$  when  $p \geq 5$ , and  $2p-t=2$  when  $p=3$ . Assume that there is an orbit  $\Delta_i$  of  $G_{1,\dots,t}$  with  $u_i < 2p-t$ . We take  $u_i+1$  points  $\alpha_1, \dots, \alpha_{u_i+1}$  from  $\Delta_i$  and  $2p-t-u_i-1$  points  $\beta_1, \dots, \beta_{2p-t-u_i-1}$  from  $\Omega - (\{1, \dots, t\} \cup \Delta_i)$ . A Sylow  $p$ -subgroup of  $G_{1,\dots,t,\alpha_1,\dots,\alpha_{u_i+1},\beta_1,\dots,\beta_{2p-t-u_i-1}}$  fixes at least  $3p-1$  points, which is a contradiction. Hence  $u_i \geq 2p-t$  for every  $\Delta_i$  ( $i=1, \dots, s$ ). Assume that  $s \geq 3$  or  $p=3$ . We take a point  $\alpha_1$  from  $\Delta_1$  and a point  $\alpha_2$  from  $\Delta_2$ . If  $p=3$ , then a Sylow  $p$ -subgroup of  $G_{1,2,3,4,\alpha_1,\alpha_2}$  fixes at least 8 points, which is a contradiction. If  $p \geq 5$ , we take  $2p-t-2$  points  $\beta_1, \dots, \beta_{2p-t-2}$  from  $\Delta_3$ . Then a Sylow  $p$ -subgroup of  $G_{1,\dots,t,\alpha_1,\alpha_2,\beta_1,\dots,\beta_{2p-t-2}}$  fixes at least  $3p-1$  points, which is a contradiction. Thus we have  $p \geq 5$  and  $s=2$ . So,  $\Omega = \{1, \dots, t\} \cup \Delta_1 \cup \Delta_2$ . Hence  $2p+r = t + \mu_1 + \mu_2$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G_{1,\dots,t}$ . Then,  $N_G(Q)^{I(Q)}$  is  $t$ -transitive and has an element of order  $p$ . Since  $3p-2 \geq |I(Q)| = t + u_1 + u_2 \geq t + 2(2p-t) = 2p + (2p-t)$ , we have  $|I(Q)| = 3p-2$ , and  $N_G(Q)^{I(Q)} \geq A^{I(Q)}$  by [14, Theorem 13.10]. So,  $N_G(Q)^{I(Q)}$  has an element of order  $p$ . Hence  $Q$  is not a Sylow  $p$ -subgroup of  $G_{1,\dots,t}$ , a contradiction. (q.e.d)

Step 4.  $G \geq A^{\Omega}$ , or  $\alpha_p(x) \geq 4$  for any element  $x$  of order  $p$  of  $G$ .

Proof. Let us assume that  $\min\{\alpha_p(X) \mid x \text{ is an element of order } p \text{ of } G\} = m \leq 3$ . Hence  $|\Omega| \geq 2p + mp$ . Since  $G$  is 5-transitive, we have  $G \geq A^{\Omega}$  by [14, Theorem 13.10]. (q.e.d.)

From now on we assume that  $G \not\geq A^{\Omega}$ , and prove that this case does not occur.

Step 5. Let  $a$  be an element of order  $p$  of  $G$  with  $\alpha(a) = 2p+r$ . Then there exists an orbit  $\Delta$  of  $C_G(a)^{I(a)}$  such that  $C_G(a)^{\Delta} \geq A^{\Delta}$  and  $|\Delta| \geq 2p$ .

Proof. We may assume that

$$a = (1)(2) \cdots (2p+r)(2p+r+1, \dots, 3p+r) \cdots .$$

Set  $T = C_G(a)_{2p+r+1, \dots, 3p+r}^{I(a)}$ . For any  $p$  points  $\alpha_1, \dots, \alpha_p$  of  $I(a)$ ,  $a$  normalizes  $G_{\alpha_1, \dots, \alpha_p, 2p+r+1, \dots, 3p+r}$ . Hence  $a$  centralizes an element of order  $p$  of  $G_{\alpha_1, \dots, \alpha_p, 2p+r+1, \dots, 3p+r}$ . So,  $T_{\alpha_1, \dots, \alpha_p}$  has an element of order  $p$  for any  $p$  elements  $\alpha_1, \dots, \alpha_p$  of  $I(a)$ . Thus  $T$  has an orbit  $\Gamma$  with  $|\Gamma| \geq p$ . Let  $|\Gamma| = p+k$ . Suppose that  $0 \leq k \leq p-1$ . We take  $k+1$  points  $\delta_1, \dots, \delta_{k+1}$  from  $\Gamma$  and  $p-k-1$  points  $\delta_{k+2}, \dots, \delta_p$  from  $I(a) - \Gamma$ . Then  $T_{\delta_1, \dots, \delta_p}$  has no element of order  $p$ , which is a contradiction. Therefore  $T$  has an orbit  $\Gamma$  whose length is at least  $2p$ . Since it is easily seen that  $T^{\Gamma}$  is primitive, we have  $T^{\Gamma} \geq A^{\Gamma}$  by [14, Theorem 13.9]. Let  $\Delta$  be an orbit of maximal length of  $C_G(a)^{I(a)}$ , then  $C_G(a)^{\Delta} \geq A^{\Delta}$  and  $|\Delta| \geq 2p$ . (q.e.d.)

Step 6. For any  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  of  $\Omega$ , the order of a Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{2p}}$  is  $p$ .

Proof. Suppose, by way of contradiction, that for some  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$ , the order of a Sylow  $p$ -subgroup  $P$  of  $G_{\alpha_1, \dots, \alpha_{2p}}$  is more than  $p$ . We may assume that  $\{\alpha_1, \dots, \alpha_{2p}\} = \{1, \dots, 2p\}$  and  $I(P) = \{1, \dots, 2p, \dots, 2p+r\}$ . For any  $2p$  points  $\gamma_1, \dots, \gamma_{2p}$  of  $I(P)$ , the order of a Sylow  $p$ -subgroup of  $G_{\gamma_1, \dots, \gamma_{2p}}$  is  $|P|$ . Let  $a$  be an element of order  $p$  of  $Z(P)$ . We may assume that

$$a = (1)(2) \cdots (2p+r)(2p+r+1, \dots, 3p+r) \cdots.$$

Since  $a$  normalizes  $G_{1, \dots, p, 2p+r+1, \dots, 3p+r}$ ,  $G_{1, \dots, p, 2p+r+1, \dots, 3p+r}$  has an element  $b$  of order  $p$  commuting with  $a$ . We may assume that

$$b = (1) \cdots (p)(p+1, \dots, 2p)(2p+1) \cdots (2p+r)(2p+r+1) \cdots (3p+r) \cdots.$$

Then we may assume that  $P^b = P$ . Since  $C_p(b)$  is semiregular on  $I(b) - (\{1, \dots, p\} \cup \{2p+1, \dots, 2p+r\}) = \{2p+r+1, \dots, 3p+r\}$ , we have  $|C_p(b)| = p$ , and  $b$  does not centralize  $P$ . On the other hand, since  $\langle P, b \rangle = P \cdot \langle b \rangle$ , we have  $\langle a \rangle \times \langle b \rangle \cong C_{\langle P, b \rangle}(b) \cong Z(\langle P, b \rangle)$ . Hence  $|Z(\langle P, b \rangle)| = |\langle a \rangle| = p$ , since  $[P, b] \neq 1$ .

Now, since  $I(a) = I(P)$ , we have  $C_G(a) \subseteq G_{I(P)} = N_G(G_{I(P)})$ . By the Frattini-Sylow argument,  $N_G(G_{I(P)}) = N_G(P) \cdot G_{I(P)}$ . So,  $C_G(a) \subseteq N_G(P)G_{I(P)}$ . Hence  $C_G(a)^{I(a)} = C_G(a)^{I(P)} \subseteq N_G(P)^{I(P)}$ . Thus by Step 5,  $N_G(P)^{I(P)}$  has an orbit  $\Delta$  of maximal length such that  $N_G(P)^\Delta \geq A^\Delta$  and  $|\Delta| \geq 2p$ . We may assume that  $\Delta = \{1, 2, \dots, |\Delta|\}$ . Set  $\Gamma = \{2, 3, \dots, 2p\}$ , then  $N_G(P)^\Gamma \geq A^\Gamma$ . Since  $|I(P) - \Gamma| \leq p-1$ ,  $|N_G(P)^\Gamma|_p$  (= the order of a Sylow  $p$ -subgroup of  $N_G(P)^\Gamma$ ) =  $|P|$ . Moreover since  $|N_G(P)^\Gamma|_p = p$ , we have  $N_G(P)^\Gamma|_p = p \cdot |P|$ . Thus  $\langle P, b \rangle$  is a Sylow  $p$ -subgroup of  $N_G(P)^\Gamma$ .

Suppose that  $C_G(P)^\Gamma = 1$ . Since  $N_G(P)^\Gamma / C_G(P)^\Gamma \leq \text{Aut}(P)$ ,  $A_{2p-1}$  is involved in  $\text{Aut}(P)$ . But, we can easily see that  $A_{2p-1}$  is not involved in  $\text{Aut}(P)$  (cf. [2, § 2, (3)]), which is a contradiction. Therefore we have  $C_G(P)^\Gamma \geq A^\Gamma$ . Since the center of a Sylow  $p$ -subgroup of  $N_G(P)^\Gamma$  is of order  $p$ , this is a contradiction. (q.e.d.)

Step 7.  $|\Omega| - (2p+r) \not\equiv p \pmod{p^2}$ .

(The proof of this step is the same as that of [4, § 2], but we repeat it for the completeness.)

Proof. We may assume that there exist two elements  $a$  and  $b$  of order  $p$  which commute to each other such that

$$a = (1) \cdots (2p)(2p+1) \cdots (2p+r)(2p+r+1, \dots, 3p+r)(3p+r+1, \dots, 4p+r) \cdots,$$

and

$$b = (1, \dots, p)(p+1, \dots, 2p)(2p+1) \cdots (2p+r)(2p+r+1) \cdots \\ \cdots (3p+r)(3p+r+1) \cdots (4p+r) \cdots.$$

Since  $\langle a, b \rangle$  normalizes  $G_{p+1, \dots, 2p, 2p+r+1, \dots, 3p+r}$ ,  $G_G(\langle a, b \rangle)_{p+1, \dots, 2p, 2p+r+1, \dots, 3p+r}$  has an element  $c$  of order  $p$ . The element  $c$  must be of the form

$$c = (1, \dots, p)^\alpha (p+1) \cdots (2p) \cdots (2p+r) \cdots (3p+r)(3p+r+1, \dots, 4p+r)^\beta \cdots,$$

where  $1 \leq \alpha, \beta \leq p-1$ . Suppose, by way of contradiction, that  $|\Omega| - (2p+r) \equiv p \pmod{p^2}$ .  $\langle a, c \rangle$  has at least  $p+2$  orbits of length  $p$ . Hence there is an integer  $\gamma$  ( $1 \leq \gamma \leq p-1$ ) such that  $|I(ac^\gamma)| \geq 3p$ , which is a contradiction. (q.e.d)

From now on, let  $a$  be an element of order  $p$  of  $G$  such that

$$a = (1) \cdots (2p)(2p+1) \cdots (2p+r)(2p+r+1, \dots, 3p+r)(3p+r+1, \dots, 4p+r) \cdots.$$

By Step 5,  $C_G(a)^{I(a)}$  has an orbit  $\Delta$  such that  $C_G(a)^\Delta \geq A^\Delta$  and  $|\Delta| \geq 2p$ . Hereafter we may assume that  $\Delta = \{1, 2, \dots, |\Delta|\}$ .

Step 8. Set  $C_G(a)_0 = C_G(a)$ . If  $p \geq 5$ , then there is an integer  $i$  ( $0 \leq i \leq 2$ ) such that  $C_G(a)_{0, \dots, i}$  and  $C_G(a)_{0, \dots, i, i+1}$  have exactly  $m$  orbits on  $\Omega - I(a)$ , where  $m$  is at most three, and moreover  $m$  is at most two when  $|\Omega| - (2p+r) \equiv 0 \pmod{p^2}$ . If  $p=3$ , then there is an integer  $i$  ( $0 \leq i \leq 1$ ) such that  $C_G(a)_i$  and  $C_G(a)_{i, i+1}$  have exactly  $m$  orbits on  $\Omega - I(a)$ , where  $m$  is at most two, and moreover  $m$  is one when  $|\Omega| - (2p+r) \equiv 0 \pmod{p^2}$ .

Proof. Suppose that  $p \geq 5$ . In order to prove Step 8 for  $p \geq 5$ , it is sufficient to show that  $C_G(a)_{1,2,3}$  has at most three orbits on  $\Omega - I(a)$ , and that  $C_G(a)_{1,2,3}$  has at most two orbits on  $\Omega - I(a)$  when  $|\Omega| - (2p+r) \equiv 0 \pmod{p^2}$ .

Set  $H = G_{1,2,3}$ . Then  $H$  is  $p$ -transitive on  $\Omega - \{1, 2, 3\}$  by Step 3. By the remark following Lemma 1.1 in [11], we get the following expression:

$$\frac{|H|}{p} = \sum_{x \in H} \alpha_p(x) \geq \sum_k \frac{|H|}{|C_H(u_k)|} \frac{1}{p} \sum_y' \alpha^*(y),$$

where  $u_k$  ranges all representatives of conjugacy classes (in  $H$ ) of elements of order  $p$ , and  $y$  ranges all  $p'$ -elements in  $C_H(u_k)$  and  $\alpha^*(y) = \alpha(y^{\Omega - I(u_k)})$ . Hence,

$$\frac{|H|}{p} \geq \frac{|H|}{|C_H(a)|} \frac{1}{p} \sum_y' \alpha^*(y).$$

Assume that  $|\Omega| - (2p+r) \equiv 0 \pmod{p^2}$ . Since  $a$  normalizes  $G_{1, \dots, p, 2p+r+1, \dots, 3p+r}$ ,  $G_{1, \dots, p, 2p+r+1, \dots, 3p+r}$  has an element  $b$  of order  $p$  with  $ab=ba$ . If  $|I(X)| = 2p+r$  for any nontrivial element  $x$  of  $\langle a, b \rangle$ , then  $\langle a, b \rangle$  has just  $p-1$  orbits of length  $p$  on  $\Omega - \{1, \dots, 3p+r\}$ . So  $|\Omega| - (2p+r) \equiv 0 \pmod{p^2}$ , a contradiction. Hence  $H$  ( $\supseteq \langle a, b \rangle$ ) contains an element of order  $p$  which fixes less than  $2p+r$  points, and so, the equality in the above expression does not hold. Now, assume that  $x \in C_H(a)$  and  $p \nmid |x|$ . Set  $|x| = p \cdot s$ . Since  $|I(x^s)| \leq 2p+r$ , we have  $\alpha^*(x^s) \leq p \cdot \alpha_p((x^s)^{I(a)})$ . So,  $\alpha^*(x) \leq p \cdot \alpha_p(x^{I(a)}) + 2p \cdot \alpha_{2p}(x^{I(a)})$ . Hence, we have that



$\sum_y \alpha^*(y) \geq \sum_{y \in \Omega_{H(a)}} (y) - p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_p(y^{I(a)}) - 2p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_{2p}(y^{I(a)})$ . Since  $C_H(a)^{\Delta-(1,2,3)} \geq A^{\Delta-(1,2,3)}$  and  $|\Delta| \geq 2p$ , we get  $p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_p(y^{I(a)}) = p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_p(y^{\Delta-(1,2,3)}) = |C_H(a)|$  by the formula of Frobenius. Similarly, if  $2p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_{2p}(y^{I(a)}) \neq 0$ , then  $2p \cdot \sum_{y \in \Omega_{H(a)}} \alpha_{2p}(y^{I(a)}) = |C_H(a)|$ . On the other hand,  $\sum_{y \in \Omega_{H(a)}} \alpha^*(y) = f \cdot |C_H(a)|$ , where  $f$  is the number of orbits of  $C_H(a)$  on  $\Omega - I(a)$ . Hence we get

$$\frac{|H|}{p} \geq \frac{|H|}{p} (f-2), \text{ and hence } f \leq 3.$$

In the above expression, if  $|\Omega| - (2p+r) \not\equiv 0 \pmod{p^2}$ , the equality does not hold.

Suppose that  $p=3$ . Then  $r=0$  or  $1$ . If  $r=0$ , then  $G$  is 6-transitive on  $\Omega$  by [10, Lemma 6]. So, we have  $G \geq A^{\Omega}$  by [4, Theorem 1]. But this contradicts our assumption. Hence  $r=1$ . Since  $\langle a \rangle \in \text{Syl}_3(G_{1,2,3,4,5})$ , we have  $N_G(\langle a \rangle)^{I(a)} \geq A_7$  by Step 3. Hence  $C_G(a)^{I(a)} \geq A_7$ . Set  $H = G_{1,2}$ . Then  $H$  is 3-transitive on  $\Omega - \{1, 2\}$ , and  $C_H(a)^{I(a)-(1,2)} \geq A_5$ . By the similar argument as in the case  $p \geq 5$ , we have that  $C_H(a)$  has at most two orbits on  $\Omega - I(a)$ , and that  $C_H(a)$  is transitive on  $\Omega - I(a)$  when  $|\Omega| - 7 \not\equiv 0 \pmod{9}$ . Therefore, the consequences of Step 8 hold. (q.e.d.)

Step 9.  $C_G(a)_{1,2,\dots,|\Delta|}$  has at most  $2m$  orbits on  $\Omega - I(a)$ . Moreover  $C_G(a)_{1,\dots,p,(p+1,p+2),p+3,\dots,|\Delta|} (= C_{G_{(p+1,p+2)}}(a)_{1,\dots,p,p+3,\dots,|\Delta|})$  has exactly  $m$  orbits on  $\Omega - I(a)$ .

Proof. By Step 8,  $C_G(a)_{0,\dots,i}$  has exactly  $m$  orbits on  $\Omega - I(a)$ . Let  $\Gamma_1, \dots, \Gamma_m$  be the orbits. We take an arbitrarily fixed orbit  $\Gamma_j$ . Let  $\Sigma_1, \dots, \Sigma_k$  be the orbits of  $C_G(a)_{1,\dots,|\Delta|}$  on  $\Gamma_j$ . Since  $C_G(a)_{0,\dots,i} \triangleright C_G(a)_{1,\dots,|\Delta|}$  and  $\Gamma_j$  is an orbit of  $C_G(a)_{0,\dots,i}$ ,  $C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)}$  acts on the set  $\{\Sigma_1, \dots, \Sigma_k\}$  transitively. Let  $Y = C_{G_{0,\dots,i}}(a)_{(\Sigma_1)}$ . Then  $|C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)} : Y^{\Delta-(1,\dots,i)}| = k$ . Similarly, we have  $|C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)} : Y_{i+1}^{\Delta-(1,\dots,i)}| = k$ . Hence,  $|C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)} : C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)}| = |Y^{\Delta-(1,\dots,i)} : Y_{i+1}^{\Delta-(1,\dots,i)}| = |\Delta| - i$ . Therefore  $Y$  is transitive on  $\Delta - \{1, \dots, i\}$ . Let  $(\beta_1, \dots, \beta_p)$  be a  $p$ -cycle of  $a$  such that  $\{\beta_1, \dots, \beta_p\} \subseteq \Sigma_1$ . For any  $p-i$  elements  $\alpha_1, \dots, \alpha_{p-i}$  of  $\Delta - \{1, \dots, i\}$ ,  $G_{0,\dots,i,\alpha_1,\dots,\alpha_{p-i},\beta_1,\dots,\beta_p}$  has an element  $b$  of order  $p$  commuting with  $a$ . Then  $b \in Y$  and  $b^{\Delta}$  is a  $p$ -cycle, and so,  $Y_{\alpha_1,\dots,\alpha_{p-i}}^{\Delta-(1,\dots,i)}$  has the  $p$ -cycle. Since  $\alpha_1, \dots, \alpha_{p-i-1}, \alpha_{p-i}$  are any  $p-i$  elements of  $\Delta - \{1, \dots, i\}$ , we have  $Y^{\Delta-(1,\dots,i)} \geq A^{\Delta-(1,\dots,i)}$  (cf. [14, Theorem 8.4, Theorem 13.9]). Therefore  $k \leq 2$ . If  $k=2$ , then  $Y^{\Delta-(1,\dots,i)} = A^{\Delta-(1,\dots,i)}$  and  $C_G(a)_{0,\dots,i}^{\Delta-(1,\dots,i)} = S^{\Delta-(1,\dots,i)}$ . Therefore  $\Gamma_j$  is an orbit of  $C_G(a)_{1,\dots,p,(p+1,p+2),p+3,\dots,|\Delta|}$  on  $\Omega - I(a)$ , even if  $k=2$ . (q.e.d.)

Step 10.  $|\Omega| - (2p+r) \equiv 2p \pmod{p^2}$  and  $p \geq 5$ .

Proof. Since  $a$  is an element of order  $p$  of the form

$$a = (1) \cdots (p)(p+1) \cdots (2p)(2p+1) \cdots (2p+r)(2p+r+1, \dots, 3p+r) \\ (3p+r+1, \dots, 4p+r) \cdots,$$

we may assume that  $C_G(a)_{p+1, \dots, 2p, 2p+r+1, \dots, 3p+r}$  has an element  $b$  of order  $p$ . By Step 7, we may assume that

$$b = (1, \dots, p)(p+1) \cdots (2p)(2p+1) \cdots (2p+r)(2p+r+1) \cdots \\ (3p+r)(3p+r+1, \dots, 4p+r) \cdots.$$

Let  $K = G_{1, \dots, p(p+1, p+2) p+3, \dots, | \Delta |}$  and  $L = \langle b \rangle \cdot K$ . Then  $|C_L(a) : C_K(a)| = p$ . By Step 9,  $C_K(a)$  and  $C_L(a)$  have exactly  $m$  orbits on  $\Omega - I(a)$ . Since  $m | C_K(a) | = \sum_{y \in \sigma_{K(a)}} \alpha^*(y)$  and  $m | C_L(a) | = \sum_{y \in \sigma_{L(a)}} \alpha^*(y)$ , we have

$$m \frac{p-1}{p} | C_L(a) | = \sum_{y \in \sigma_{L(a)} - \sigma_{K(a)}} \alpha^*(y).$$

Next we show that the elements of order  $p$  of  $\langle a, b \rangle$  are not conjugate to each other in  $C_L(a)$ . Suppose  $a^i b^j$  and  $a^{i'} b^{j'}$  are conjugate to each other, where  $0 \leq i, j, i', j' \leq p-1$ . If  $j \neq j'$ , then  $(a^i b^j)^{(1, \dots, p)} \neq (a^{i'} b^{j'})^{(1, \dots, p)}$ , which is a contradiction. Hence  $j = j'$ . Assume  $i \neq i'$ . There exists an element  $x$  in  $C_L(a)$  such that  $(a^i b^j)^x = a^{i'} b^j$ . Then  $(b^j)^x = a^{i'-i} b^j$ . Since  $(b^j)^{x^p} = a^{(i'-i)p} b^j = b^j$ , we have  $p \mid |x|$ . Hence there exists a  $p$ -element  $x_0$  in  $C_L(a) \cap N_L(\langle a, b \rangle)$  such that  $x_0 \notin C_L(\langle a, b \rangle)$ . Since  $\langle a, b \rangle \in \text{Syl}_p(C_L(a))$ , this is a contradiction. Thus  $i = i'$  and  $j = j'$ .

Let  $s$  be the number of orbits of length  $p$  of  $\langle a, b \rangle$  on  $\Omega - I(a)$ . For each fixed  $j$  ( $1 \leq j \leq p-1$ ), there are  $s$  elements  $i_1, \dots, i_s$  of  $\{0, 1, \dots, p-1\}$  such that  $|I(a^{i_k} b^j)| = |I(a)|$  ( $k=1, \dots, s$ ). Let  $i$  be an arbitrarily fixed element of  $\{i_1, \dots, i_s\}$ , and let  $\{\gamma_1, \dots, \gamma_s\} = I(a^i b^j) \cap (\Omega - I(a))$ . Since  $\langle a, b \rangle$  is a Sylow  $P$ -subgroup of  $C_L(\langle a, b \rangle)$ ,  $C_L(\langle a, b \rangle)$  has the normal subgroup  $Y$  such that  $C_L(\langle a, b \rangle) = \langle a, b \rangle \times Y$ , where  $(|Y|, p) = 1$ , and  $Y \subseteq C_K(a)$ . Since  $Y$  acts on  $I(\langle a, b \rangle) = \{p+1, \dots, 2p, 2p+1, \dots, 2p+r\}$ ,  $Y$  acts on  $\{\gamma_1, \dots, \gamma_s\}$ . Since  $a^{(\gamma_1 \dots \gamma_s)}$  is a  $p$ -cycle and  $[Y, a] = 1$ , we have  $Y^{(\gamma_1 \dots \gamma_s)} = 1$ . Hence any element of  $a^i b^j \cdot Y$  fixes at least  $p$  points of  $\Omega - I(a)$ . Moreover, it is clear that  $a^i b^j \cdot Y \cap C_K(a) = \phi$ . Therefore

$$\sum_{y \in \sigma_{L(\langle a, b \rangle)} - \sigma_{K(a)}} \alpha^*(y) \geq s(p-1)p | C_L(\langle a, b \rangle) : \langle a, b \rangle |.$$

Let  $d$  be any element of  $C_L(a)$  such that  $d$  is conjugate to  $b$  in  $C_L(a)$  and  $d \neq b$ . Then  $\langle a, b \rangle \cap \langle a, d \rangle = \langle a \rangle$ . Hence  $C_L(\langle a, b \rangle) \cap C_L(\langle a, d \rangle) \subseteq C_K(a)$ .

Therefore, we have

$$\sum_{y \in \sigma_{L(a)} - \sigma_{K(a)}} \alpha^*(y) \geq s(p-1)p | C_L(a) : C_{C_L(a)}(b) | | C_L(\langle a, b \rangle) : \langle a, b \rangle | \\ = \frac{s(p-1)}{p} | C_L(a) |.$$

Hence,  $\frac{m(p-1)}{p} |C_L(a)| \geq \frac{s(p-1)}{p} |C_L(a)|$ . Then  $m \geq s$ . On the other hand, if  $|\Omega| - (2p+r) \equiv hp \pmod{p^2}$ , where  $2 \leq h \leq p$ , then we have  $s=h$ . Therefore, we have that  $|\Omega| - (2p+r) \equiv 2p \pmod{p^2}$  and  $p \geq 5$ , by Step 8. (q.e.d.)

Step 11. *We complete the proof.*

Proof. By Step 10,  $\{2p+r+1, \dots, 3p+r\}$  and  $\{3p+r+1, \dots, 4p+r\}$  are the orbits of length  $p$  of  $\langle a, b \rangle$  on  $\Omega - I(a)$ , and  $m=2$  and  $p \geq 5$ . By Step 4 we have  $\alpha_p(a) \geq 4$ , hence  $|\Omega - I(a)| \geq p^2 + 2p$ . Let  $\Gamma_1, \dots, \Gamma_l$  be the orbits of  $C_G(a)_{1,2,\dots,|\Delta|}$  on  $\Omega - I(a)$ , where  $2 \leq l \leq 4$  by Step 9. Since  $|b| = p$ ,  $b$  acts on the set  $\{\Gamma_1, \dots, \Gamma_l\}$  trivially. If  $l=2$ , then  $\Gamma_1$  and  $\Gamma_2$  are the orbits of  $C_G(a)_{1,\dots,p(p+1,p+2)p+3,\dots,|\Delta|}$  on  $\Omega - I(a)$  by Step 9, and one of the following three cases holds: (i)  $|\Gamma_1| \equiv 2p \pmod{p^2}$ ,  $|\Gamma_2| \equiv 0 \pmod{p^2}$ . (ii)  $|\Gamma_1| \equiv 0 \pmod{p^2}$ ,  $|\Gamma_2| \equiv 2p \pmod{p^2}$ . (iii)  $|\Gamma_1| \equiv |\Gamma_2| \equiv p \pmod{p^2}$ . If  $l=3$ , then we may assume that  $\Gamma_1 \cup \Gamma_2$  and  $\Gamma_3$  are the orbits of  $C_G(a)_{1,\dots,p(p+1,p+2)p+3,\dots,|\Delta|}$  on  $\Omega - I(a)$ , and one of the following two cases holds: (i)  $|\Gamma_1| = |\Gamma_2| \equiv 0 \pmod{p^2}$ ,  $|\Gamma_3| \equiv 2p \pmod{p^2}$ . (ii)  $|\Gamma_1| = |\Gamma_2| \equiv p \pmod{p^2}$ ,  $|\Gamma_3| \equiv 0 \pmod{p^2}$ . If  $l=4$ , then we may assume that  $\Gamma_1 \cup \Gamma_2$  and  $\Gamma_3 \cup \Gamma_4$  are the orbits of  $C_G(a)_{1,\dots,p(p+1,p+2)p+3,\dots,|\Delta|}$  on  $\Omega - I(a)$ , and one of the following two cases holds: (i)  $|\Gamma_1| = |\Gamma_2| \equiv 0 \pmod{p^2}$ ,  $|\Gamma_3| = |\Gamma_4| \equiv p \pmod{p^2}$ . (ii)  $|\Gamma_1| = |\Gamma_2| \equiv p \pmod{p^2}$ ,  $|\Gamma_3| = |\Gamma_4| \equiv 0 \pmod{p^2}$ . We have the following for any value of  $l$ : There is a  $\Gamma_j$  ( $1 \leq j \leq 4$ ) such that  $|\Gamma_j| \equiv 0$  or  $p \pmod{p^2}$  and  $|\Gamma_j| \geq p^2$ . Let  $(\beta_1, \dots, \beta_p)$  and  $(\gamma_1, \dots, \gamma_p)$  be two  $p$ -cycles of  $a$  such that  $\{\beta_1, \dots, \beta_p, \gamma_1, \dots, \gamma_p\} \subseteq \Gamma_j$ .  $C_G(a)_{\beta_1,\dots,\beta_p,\gamma_1,\dots,\gamma_p}$  has an element  $c$  of order  $p$ . Hereafter we examine the relation between  $a$  and  $c$ . We may assume that

$$c = (1, \dots, p)(p+1, \dots, 2p)(2p+1) \cdots (2p+r)(\beta_1) \cdots (\beta_p)(\gamma_1) \cdots (\gamma_p) \cdots.$$

Since  $|\Gamma_j| \equiv 2p \pmod{p^2}$ ,  $\langle a, c \rangle$  has at least  $p+2$  orbits of length  $p$  on  $\Omega - I(a)$ . Let  $K = G_{1,2,\dots,|\Delta|}$ , and  $L = \langle c \rangle \cdot K$ . By the same argument as in the proof of Step 10, we have that  $l \cdot \frac{p-1}{p} |C_L(a)| = \sum_{y \in \sigma_{L(a)} - \sigma_K(a)} \alpha^*(y)$ , and that the elements of  $\langle a, c \rangle - \{1\}$  are not conjugate to each other in  $C_L(a)$ . For each fixed  $j$  ( $1 \leq j \leq p-1$ ), there are at least  $\frac{p+3}{2}$  elements  $i_1, \dots, i_{(p+3)/2}$  of  $\{0, 1, \dots, p-1\}$  such that  $|I(a^{i_k c^j})| \geq p+r$  ( $k=1, \dots, \frac{p+3}{2}$ ). Let  $i$  be an arbitrarily fixed element of  $\{i_1, \dots, i_{(p+3)/2}\}$ . Since  $\langle a, c \rangle$  is a Sylow  $p$ -subgroup of  $C_L(\langle a, c \rangle)$  there exists the normal subgroup  $M$  of  $C_L(\langle a, c \rangle)$  such that  $C_L(\langle a, c \rangle) = \langle a, c \rangle \times M$ . First assume that  $a^i c^j$  fixes exactly  $p$  points  $\delta_1, \dots, \delta_p$  in  $\Omega - I(a)$ . Then, by the same argument as in the proof of Step 10, any element of  $a^i c^j \cdot M$  fixes  $\{\delta_1, \dots, \delta_p\}$  pointwise. Next assume that  $a^i c^j$  fixes exactly  $2p$  points  $\eta_1, \dots, \eta_{2p}$  in  $\Omega - I(a)$

and  $a$  fixes  $\{\beta_1, \dots, \beta_p\}$  and  $\{\gamma_1, \dots, \gamma_p\}$  with  $\{\beta_1, \dots, \beta_p\} \cup \{\gamma_1, \dots, \gamma_p\} = \{\eta_1, \dots, \eta_{2p}\}$ . If  $M$  fixes  $\{\beta_1, \dots, \beta_p\}$  and  $\{\gamma_1, \dots, \gamma_p\}$ , then any element of  $a^i c^j \cdot M$  fixes  $\{\eta_1, \dots, \eta_{2p}\}$  pointwise. And if  $M$  transposes  $\{\beta_1, \dots, \beta_p\}$  and  $\{\gamma_1, \dots, \gamma_p\}$  then there exists the subgroup  $M_0$  of index two of  $M$  such that any element of  $a^i c^j \cdot M_0$  fixes  $\{\eta_1, \dots, \eta_{2p}\}$  pointwise. Therefore, by the same argument as in the proof of Step 10, we have that

$$\begin{aligned} \sum_{y \in C_L(a) - C_K(a)} \alpha^*(y) &\geq \frac{p+3}{2} \cdot (p-1) \cdot p |C_L(a) : C_{C_L(a)}(c) || C_L(\langle a, c \rangle) : \langle a, c \rangle| \\ &= \frac{(p+3)(p-1)}{2p} \cdot |C_L(a)|. \end{aligned}$$

Hence  $l \geq \frac{p+3}{2}$ . So, we have  $p=5$  and  $l=4$ .

We may assume that  $|\Gamma_1| = |\Gamma_2| \equiv 0 \pmod{5^2}$ . Let  $(\delta_1, \dots, \delta_5)$  and  $(\eta_1, \dots, \eta_5)$  be two 5-cycles of  $a$  such that  $\{\delta_1, \dots, \delta_5\} \subseteq \Gamma_1$  and  $\{\eta_1, \dots, \eta_5\} \subseteq \Gamma_2$ .  $C_G(a)_{\delta_1, \dots, \delta_5, \eta_1, \dots, \eta_5}$  has an element  $d$  of order 5. Since  $d$  acts on the set  $\{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4\}$  trivially,  $\langle a, d \rangle$  has at least  $2 \cdot 5 + 2$  orbits of length 5 on  $\Omega - I(a)$ . Hence, there exists an element  $x$  of order 5 of  $\langle a, d \rangle$  such that  $|I(x)| \geq 3 \cdot 5 + r$ , which is a contradiction. (q.e.d.)

### 3. Proof of Theorem B

In the proof of Theorem B, we shall use the following Lemma.

**Lemma.** *There is no group satisfying the following condition: Let  $G$  be a 3-transitive group on  $\Omega$ . Let  $\alpha$  and  $\beta$  be two points of  $\Omega$ .  $G_{\alpha, \beta}$  is an imprimitive group on  $\Omega - \{\alpha, \beta\}$  with two blocks  $\Delta_1, \Delta_2$  of length  $\frac{|\Omega|}{2} - 1$ , and moreover, for any point  $\gamma$  of  $\Delta_1$  and any point  $\delta$  of  $\Delta_2$ ,  $G_{\alpha, \beta, \gamma, \delta}^{\Delta_1, \gamma}$  and  $G_{\alpha, \beta, \gamma, \delta}^{\Delta_2, \delta}$  are 2-transitive groups.*

(I think that this lemma is essentially known already in [7, § 1, Proof of Theorem 1])

Proof of Lemma (cf. [7, § 1, Proof of Theorem 1]). Let  $G$  be a group satisfying the above condition.

Set  $|\Omega| = n$  and  $|\Delta_i| = v + 1$  ( $i = 1, 2$ ). Then  $G_{\alpha, \beta, \gamma}$  has just two orbits  $\Sigma_1$  and  $\Sigma_2$  on  $\Omega - \{\alpha, \beta, \gamma\}$  such that  $|\Sigma_1| = v + 1$  and  $|\Sigma_2| = v$ .

For any subset  $\Delta$  of  $\Omega$  with  $|\Delta| = 4$ ,  $G_\Delta$  has two orbits  $\Pi_1$  and  $\Pi_2$  on  $\Omega - \Delta$  such that  $|\Pi_1| = |\Pi_2|$  or  $||\Pi_1| - |\Pi_2|| = 2$ . In either case,  $G_\Delta$  is a subgroup of  $G_{\alpha_1, \alpha_2, \alpha_3}$  which satisfies the assumption of the Witt's Lemma [14, Theorem 9.4], where  $\alpha_1, \alpha_2, \alpha_3$  are three elements of  $\Delta$ . Hence  $G_{(\Delta)}^\Delta$  is a 3-transitive group. Thus,  $G_{(\Delta)}^\Delta = S_4$ . Therefore,  $G$  acts on  $\Omega^{(2)}$ , the set of unordered pairs of elements of  $\Omega$ , as a transitive permutation group of rank 4, where the orbitals,  $\Gamma_0, \Gamma_1, \Gamma_2$  and  $\Gamma_3$  of this permutation group are defined as follows: for  $\{\alpha, \beta\} \in$

$$\Omega^{(2)}, \Gamma_0(\{\alpha, \beta\}) = \{\alpha, \beta\}$$

$$\Gamma_1(\{\alpha, \beta\}) = \{(\gamma, \delta) \in \Omega^{(2)} \mid \{\alpha, \beta\} \cap \{\gamma, \delta\} = 1\}$$

$$\Gamma_2(\{\alpha, \beta\}) = \{(\gamma, \delta) \in \Omega^{(2)} \mid \{\alpha, \beta\} \cap \{\gamma, \delta\} = \phi.$$

$\delta$  is in the orbit of length  $v$  of  $G_{\alpha\beta\gamma}$  on  $\Omega - \{\alpha, \beta, \gamma\}$

$$\Gamma_3(\{\alpha, \beta\}) = \{(\gamma, \delta) \in \Omega^{(2)} \mid \{\alpha, \beta\} \cap \{\gamma, \delta\} = \phi.$$

$\delta$  is in the orbit of length  $v+1$  of  $G_{\alpha\beta\gamma}$  on  $\Omega - \{\alpha, \beta, \gamma\}$ .

The degrees corresponding to  $\Gamma_i$  ( $i=0, 1, 2, 3$ ) are respectively

$$1, 2(n-2) = 4(v+1), \quad \frac{(n-2)v}{2} = v(v+1), \quad \frac{(n-2)(v+1)}{2} = (v+1)^2.$$

Moreover, these orbitals  $\Gamma_i$  ( $i=0, 1, 2, 3$ ) are all self-paired.

Let us define the intersection matrices  $M_i$  ( $i=0, 1, 2, 3$ ) for the permutation group  $G$  on  $\Omega^{(2)}$  as follows:

$$M_i = (\mu_{jk}^{(i)}) \text{ with } 0 \leq j \leq 3, 0 \leq k \leq 3, \text{ where}$$

$$\mu_{jk}^{(i)} = |\Gamma_j(x) \cap \Gamma_k(y)| \text{ with } y \in \Gamma_k(x)$$

(where  $x, y \in \Omega^{(2)}$ ).

Now we can obtain the intersection matrix  $M_2$  (cf. [9, §4]). This is,

$$M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & v & 2v-2 & 2v \\ v(v+1) & \frac{v(v-1)}{2} & -v+2 & v(v-1) \\ 0 & \frac{v(v+1)}{2} & v^2-1 & 0 \end{pmatrix}$$

By direct calculations, we obtain the eigenvalues  $\theta_0, \theta_1, \theta_2$  and  $\theta_3$  of  $M_2$ .

$$\theta_0 = v(v+1), \quad \theta_1 = -v, \quad \theta_2 = \frac{-v^2+2+\sqrt{v^4+4v+4}}{2} \text{ and}$$

$$\theta_3 = \frac{-v^2+2-\sqrt{v^4+4v+4}}{2}.$$

Since  $(v^2)^2 < v^4+4v+4 < (v^2+2)^2$ , it is clear that  $\theta_2$  and  $\theta_3$  are irrational numbers.

Let us denote by  $\pi^{(2)}$  the permutation character of  $G$  on  $\Omega^{(2)}$ . Then  $\pi^{(2)}$  is multiplicity free and  $\pi^{(2)} = 1 + X_1 + X_2 + X_3$ , where  $X_1 = X^{(n-1,1)}|G$  and  $X_2$  and  $X_3$  are irreducible characters appearing in  $X^{(n-2,2)}|G$  corresponding to  $\theta_2$  and  $\theta_3$  respectively. Since  $\theta_2$  and  $\theta_3$  are irrational,  $X_2$  and  $X_3$  are not rational characters (cf. [6, Lemma 1]), so  $X_2$  and  $X_3$  are algebraic conjugate

and especially of the same degree. Therefore  $X_2(1)=X_3(1)=n(n-3)/4$  and  $X_1(1)=n-1$ . By a theorem of Frame [14, Theorem 30.1 (A)], we obtain that the number

$$q = \left\{ \frac{n(n-1)}{2} \right\}^2 \frac{2(n-2) \cdot v(n-2)/2 \cdot (n-2)(v+1)/2}{(n-1) \cdot n(n-3)/4 \cdot n(n-3)/4}$$

must be an integer. But, since  $n=2v+4$ , we have a contradiction. (q.e.d.)

Proof of Theorem B. Let  $G$  be a counter-example to the theorem with the least possible degree.

Step 1. *The number of orbits of  $G$  on  $\Omega$  is at most two.*

Proof. By Theorem A and the assumption for  $G$ ,  $G$  has no orbit on  $\Omega$  whose length is less than  $p$ .

Suppose, by way of contradiction, that  $G$  has three orbits  $\Delta_1, \Delta_2$  and  $\Delta_3$  with  $|\Delta_i| \geq p$  ( $i=1, 2, 3$ ). Set  $|\Delta_i| \equiv k_i \pmod p$ , where  $0 \leq k_i \leq p-1$  ( $i=1, 2, 3$ ). Assume that  $2p-(k_1+k_2+2) \geq p$ . We take  $k_1+p-1$  points  $\alpha_1, \dots, \alpha_{k_1+p-1}$  from  $\Delta_1$ ,  $k_2+1$  points  $\beta_1, \dots, \beta_{k_2+1}$  from  $\Delta_2$  and  $p-k_1-k_2$  points  $\gamma_1, \dots, \gamma_{p-k_1-k_2}$  from  $\Delta_3$ . A Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{k_1+p-1}, \beta_1, \dots, \beta_{k_2+1}, \gamma_1, \dots, \gamma_{p-k_1-k_2}}$  fixes at least  $3p$  points, which contradicts the assumption of Theorem B. Hence  $2p-(k_1+k_2+2) < p$ . We take  $k_1+1$  points  $\alpha_1, \dots, \alpha_{k_1+1}$  from  $\Delta_1$ ,  $k_2+1$  points  $\beta_1, \dots, \beta_{k_2+1}$  from  $\Delta_2$  and  $2p-k_1-k_2-2$  points  $\gamma_1, \dots, \gamma_{2p-k_1-k_2-2}$  from  $\Delta_3$ . A Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{k_1+1}, \beta_1, \dots, \beta_{k_2+1}, \gamma_1, \dots, \gamma_{2p-k_1-k_2-2}}$  fixes at least  $3p$  points, which is a contradiction. (q.e.d.)

Step 2. *We may assume that  $G$  is transitive on  $\Omega$ . ( $|\Omega| \equiv p-1 \pmod p$ .)*

Proof. Suppose that  $G$  is not transitive on  $\Omega$ . By Step 1,  $G$  has two orbits  $\Delta_1$  and  $\Delta_2$  such that  $\Delta_1 \cup \Delta_2 = \Omega$  and  $|\Delta_i| \geq p$  ( $i=1, 2$ ). Set  $|\Delta_i| = s_i p + k_i$ , where  $0 \leq k_i \leq p-1$  ( $i=1, 2$ ). In this case  $k_1+k_2=p-1$ . By the assumption of Theorem B,  $s_1 \geq 2$  or  $s_2 \geq 2$ . We may assume that  $s_1 \geq 2$  and  $s_1 \geq s_2$ . We divide the consideration into the following three cases: (I)  $s_1 \geq 3$ . (II)  $s_1 = s_2 = 2$ . (III)  $s_1 = 2, s_2 = 1$ .

Suppose that Case (I) holds. By Theorem A and the assumption for  $G$ ,  $G^{\Delta_1} \geq A^{\Delta_1}$ , and so,  $s_1 = 3$ . For  $k_2+1$  points  $\alpha_1, \dots, \alpha_{k_2+1}$  of  $\Delta_2$ ,  $G_{\alpha_1, \dots, \alpha_{k_2+1}}^{\Delta_1}$  is  $(p+k_1)$ -transitive by [10, Lemma 6]. Since  $G_{\alpha_1, \dots, \alpha_{k_2+1}}^{\Delta_1}$  has an element  $x$  of order  $p$  with  $\alpha_p(x) = 2$ , we have  $G_{\alpha_1, \dots, \alpha_{k_2+1}}^{\Delta_1} \geq A^{\Delta_1}$  by [14, Theorem 13.10]. This is a contradiction.

Suppose that Case (II) holds. We may assume that  $k_1 \geq k_2$ . For  $p+k_2+1$  points  $\alpha_1, \dots, \alpha_{p+k_2+1}$  of  $\Delta_2$ ,  $G_{\alpha_1, \dots, \alpha_{p+k_2+1}}^{\Delta_1}$  has an element of order  $p$ , and moreover  $G_{\alpha_1, \dots, \alpha_{p+k_2+1}}^{\Delta_1}$  is  $k_1$ -transitive by [10, Lemma 6]. Since  $k_1 \geq 5$ ,  $G_{\alpha_1, \dots, \alpha_{p+k_2+1}}^{\Delta_1} \geq A^{\Delta_1}$  by [14, Theorem 13.10]. This is a contradiction.

Suppose that Case (III) holds. By [10, Lemma 6] and [14, Theorem 13.10],  $G$  is a group satisfying the consequence (2) of Theorem B. This is a contradiction. (q.e.d.)

Step 3.  $G$  is primitive on  $\Omega$ . For any element  $x$  of order  $p$  of  $G$ ,  $\alpha_p(x) \geq 8$  holds.

Proof. Suppose, by way of contradiction, that  $G$  is imprimitive on  $\Omega$ . Let  $\Delta_1, \dots, \Delta_s$  be a system of imprimitivity of  $G$ . Set  $|\Delta_i| \equiv k \pmod p$ , where  $0 \leq k \leq p-1$ . First assume that  $|\Delta_i| \leq p$ . Then  $s > 2p$  and we are able to take  $2p$  points  $\delta_1, \dots, \delta_{2p}$  from  $\Omega$  such that  $\delta_i \in \Delta_i$  ( $i=1, \dots, 2p$ ). A Sylow  $p$ -subgroup of  $G_{\delta_1, \dots, \delta_{2p}}$  fixes at least  $4p$  points, which is a contradiction. Next assume that either  $p < |\Delta_i| < 2p$ , or  $|\Delta_i| \geq 2p$  and  $s \geq 3$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$  from  $\Delta_1$  and  $k+1$  points  $\beta_1, \dots, \beta_{k+1}$  from  $\Delta_2$ . We are able to take  $2p-2k-2$  points  $\gamma_1, \dots, \gamma_{2p-2k-2}$  from  $\Omega - (\Delta_1 \cup \Delta_2)$ . A Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{k+1}, \beta_1, \dots, \beta_{k+1}, \gamma_1, \dots, \gamma_{2p-2k-2}}$  fixes at least  $3p$  points, which is a contradiction. Therefore, we have that  $|\Delta_i| \geq 2p$  and  $s=2$ . Then  $\Omega = \Delta_1 \cup \Delta_2$  and  $k = \frac{p-1}{2}$ .

By Theorem A,  $|\Delta_i| = 3p + \frac{p-1}{2}$  or  $2p + \frac{p-1}{2}$ . By the similar argument to that of Case (II) of Step 2, we have a contradiction. Thus  $G$  is primitive on  $\Omega$ . By [14, Theorem 13.10], for any element  $x$  of order  $p$  of  $G$ , we have  $\alpha_p(x) \geq 8$ . (q.e.d.)

Step 4. Let  $2 \leq t \leq p + \frac{p-1}{2} + 2$ . If  $G$  is  $t$ -transitive on  $\Omega$ , then  $G$  is  $t$ -primitive on  $\Omega$ .

Proof. Suppose, by way of contradiction, that  $G$  is  $t$ -transitive on  $\Omega$  and  $G_{1, \dots, t-1}$  is imprimitive on  $\Omega - \{1, \dots, t-1\}$ . Let  $\Delta_1, \dots, \Delta_s$  be a system of imprimitivity of  $G_{1, \dots, t-1}$  on  $\Omega - \{1, \dots, t-1\}$ . Set  $|\Delta_i| \equiv k \pmod p$  and  $|\Delta_i| = lp + k$ , where  $0 \leq k \leq p-1$ . In this case,  $(t-1) + sk \equiv p-1 \pmod p$ . We divide the consideration into the following two cases: (I)  $2p-t+1 \geq p$ . (II)  $2p-t+1 < p$ .

Suppose that Case (I) holds. First assume that  $l=0$ . Then  $s > 2p-t+1$  and we are able to take  $2p-t+1$  points  $\delta_1, \dots, \delta_{2p-t+1}$  of  $\Omega$  such that  $\delta_i \in \Delta_i$  ( $i=1, \dots, 2p-t+1$ ). A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \delta_1, \dots, \delta_{2p-t+1}}$  fixes at least  $3p$  points, which is a contradiction. Secondly assume that  $l=1$ . By Step 3, we get  $s \geq 8$ . Assume that  $k \geq \frac{p-1}{2}$ . We take a point  $\alpha$  from  $\Delta_1$ , a point  $\beta$  from  $\Delta_2$ , a point  $\gamma$  from  $\Delta_3$  and  $2p-t-2$  points  $\delta_1, \dots, \delta_{2p-t-2}$  from  $\Delta_4 \cup \Delta_5$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha, \beta, \gamma, \delta_1, \dots, \delta_{2p-t-2}}$  fixes at least  $3p$  points, which is a contradiction. Hence we have  $k \leq \frac{p-3}{2}$  when  $l=1$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$

from  $\Delta_1, k+1$  points  $\beta_1, \dots, \beta_{k+1}$  from  $\Delta_2$  and  $2p-t-2k-1$  points  $\gamma_1, \dots, \gamma_{2p-t-2k-1}$  from  $\Delta_3 \cup \Delta_4$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \dots, \alpha_{k+1}, \beta_1, \dots, \beta_{k+1}, \gamma_1, \dots, \gamma_{2p-t-2k-1}}$  fixes at least  $3p$  points, which is a contradiction. Thirdly assume that  $l \geq 2$  and  $2p-t-k \neq k, k+p$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$  from  $\Delta_1$  and  $2p-t-k$  points  $\beta_1, \dots, \beta_{2p-t-k}$  from  $\Delta_2$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \dots, \alpha_{k+1}, \beta_1, \dots, \beta_{2p-t-k}}$  fixes at least  $3p$  points, which is a contradiction. Fourthly assume that  $l \geq 2$  and  $2p-t-k = k+p$ . Assume that  $s \geq 3$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$  from  $\Delta_1, k+1$  points  $\beta_1, \dots, \beta_{k+1}$  from  $\Delta_2$  and  $p-1$  points  $\gamma_1, \dots, \gamma_{p-1}$  from  $\Delta_3$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \dots, \alpha_{k+1}, \beta_1, \dots, \beta_{k+1}, \gamma_1, \dots, \gamma_{p-1}}$  fixes at least  $3p$  points, which is a contradiction. Hence we have  $\Omega = \{1, \dots, t-1\} \cup \Delta_1 \cup \Delta_2$  when  $l \geq 2$  and  $2p-t-k = k+p$ . Since  $k = \frac{p-t}{2}$  and  $t \geq 2$ , we get  $t \geq 3$ . Let  $\gamma$  be any point of  $\Delta_1$ , and  $\delta$  be any point of  $\Delta_2$ . By [10, Lemma 6], it is easily seen that  $G_{1, \dots, t-1, \gamma, \delta}^{\Delta_1, \dots, \{ \gamma \}}$  and  $G_{1, \dots, t-1, \gamma, \delta}^{\Delta_2, \dots, \{ \delta \}}$  are  $(k-1+p)$ -transitive. By Lemma, we have a contradiction. Fifthly assume that  $l \geq 2$  and  $2p-t-k = k$ . In this case,  $k = \frac{2p-t}{2} \geq \frac{p-1}{2}$ . Assume that  $s \geq 3$ . We take  $k+1$  points  $\alpha_1, \dots, \alpha_{k+1}$  from  $\Delta_1, k-1$  points  $\beta_1, \dots, \beta_{k-1}$  from  $\Delta_2$  and a point  $\gamma$  from  $\Delta_3$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \dots, \alpha_{k+1}, \beta_1, \dots, \beta_{k-1}, \gamma}$  fixes at least  $3p$  points, which is a contradiction. Hence, we have  $\Omega = \{1, \dots, t-1\} \cup \Delta_1 \cup \Delta_2$  when  $l \geq 2$  and  $2p-t-k = k$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G_{1, \dots, t}$ . Then  $N_G(Q)^{I(Q)}$  is a  $t$ -transitive group and  $|I(Q)| \geq t-1+2k=2p-1$ . Let  $x$  be an element of order  $p$  of  $Q$  with  $|I(x)| = 3p-1$ , and  $(\gamma_1, \dots, \gamma_p)$  be a  $p$ -cycle of  $x$ . Let  $\{\delta_1, \dots, \delta_p\}$  be a subset of  $\Omega$  such that if  $|I(Q)| = 2p-1$ , then  $\{\delta_1, \dots, \delta_p\} = I(x) - I(Q)$ , and if  $|I(Q)| = 3p-1$ , then  $x^{(\delta_1, \dots, \delta_p)}$  is a  $p$ -cycle of  $x$  different from  $(\gamma_1, \dots, \gamma_p)$ .  $C_G(x)_{\gamma_1, \dots, \gamma_p, \delta_1, \dots, \delta_p}$  has an element  $y$  of order  $p$ . Since  $y$  fixes  $I(Q)$ , we may assume that  $y \in N_G(Q)$ . Then  $y^{I(Q)}$  is an element of order  $p$  of  $N_G(Q)^{I(Q)}$  which is 2-transitive on  $I(Q)$  and we have  $N_G(Q)^{I(Q)} \geq A^{I(Q)}$ . Since  $G_{1, \dots, t-1}$  is imprimitive on  $\Omega - \{1, \dots, t-1\}$ , this is a contradiction.

Suppose that Case (II) holds. In this case,  $p+2 \leq t \leq p + \frac{p-1}{2} + 2$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G_{1, \dots, t}$ . Then  $N_G(Q)^{I(Q)}$  is  $t$ -transitive on  $I(Q)$ . Since  $|\Omega| \equiv p-1 \pmod{p}$ , we have  $|I(Q)| \equiv p-1 \pmod{p}$ , and so,  $|I(Q)| = 2p-1$  or  $3p-1$ . Since  $t \geq p+2$ ,  $N_G(Q)^{I(Q)}$  has an element of order  $p$ , and so, we get  $N_G(Q)^{I(Q)} \geq A^{I(Q)}$ . We may assume that  $\{\Delta_1, \dots, \Delta_u\}$  is the subset of  $\{\Delta_1, \dots, \Delta_s\}$  such that  $I(Q) \cap \Delta_i \neq \emptyset$  for  $1 \leq i \leq u$  and  $I(Q) \cap \Delta_i = \emptyset$  for  $u < i \leq s$ . Since  $G_{1, \dots, t-1}$  is imprimitive on  $\Omega - \{1, \dots, t-1\}$ , we have that  $k \leq 1$  or  $u=1$ . Assume that  $k \geq 2$ . Then  $u=1$ , and so,  $(t-1)+k \equiv p-1 \pmod{p}$ . Hence  $t-1+k = 2p-1$ . Then  $p - \frac{p-1}{2} - 2 \leq k \leq p-2$ . On the other hand,  $(t-1)+sk \equiv p-1 \pmod{p}$ . Then  $(t+k)+(s-1)k \equiv 0 \pmod{p}$ , and so,  $p|s-1$ . Hence



$s \geq p+1$ . Let  $\alpha_i$  be a point of  $\Delta_i$  ( $i=1, \dots, s$ ). A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \dots, \alpha_{k+1}}$  fixes at least  $2p+(k+1)(k-1)$  points. But,  $(k+1)(k-1) \geq \left(p - \frac{p-1}{2} - 1\right) \left(p - \frac{p-1}{2} - 3\right) \geq p$ , which is a contradiction. Therefore  $k=0$  or

1. We take two points  $\alpha_1, \alpha_2$  from  $\Delta_1$  and  $2p-t-1$  points  $\beta_1, \dots, \beta_{2p-t-1}$  from  $\Delta_2$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \alpha_2, \beta_1, \dots, \beta_{2p-t-1}}$  fixes at least  $3p$  points, which is a contradiction. (q.e.d.)

Step 5.  $G$  is  $\left(p + \frac{p+1}{2} + 2\right)$ -transitive on  $\Omega$ .

Proof. By Step 3 and Step 4, in order to prove Step 5 we show that if  $G$  is  $t$ -primitive on  $\Omega$  then  $G$  is  $(t+1)$ -transitive on  $\Omega$ , where  $1 \leq t \leq p + \frac{p-1}{2} + 2$ .

Suppose, by way of contradiction, that  $G$  is  $t$ -primitive on  $\Omega$ , but  $G$  is not  $(t+1)$ -transitive on  $\Omega$ . Let  $\Delta_1, \dots, \Delta_s$  be the orbits of  $G_{1, \dots, t}$  on  $\Omega - \{1, \dots, t\}$ , where  $s \geq 2$ . We may assume that  $|\Delta_1| \geq |\Delta_2| \geq \dots \geq |\Delta_s| \geq p$  (cf. [14, Theorem 18.4]). Set  $|\Delta_i| \equiv k_i \pmod{p}$  ( $i=1, \dots, s$ ), then  $t+k_1+\dots+k_s \equiv p-1 \pmod{p}$ . We divide the consideration into the following two cases: (I)  $2p-t \geq p+1$ . (II)  $2p-t \leq p$ .

Suppose that Case (I) holds. First assume that  $|\Delta_1|=p$  or  $p+1$ . We take two points  $\alpha_1, \alpha_2$  from  $\Delta_1$  and two points  $\beta_1, \beta_2$  from  $\Delta_2$ . We are able to take  $2p-t-4$  points  $\gamma_1, \dots, \gamma_{2p-t-4}$  from  $\Delta_3 \cup \dots \cup \Delta_s$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \dots, \gamma_{2p-t-4}}$  fixes at least  $3p$  points, which is a contradiction. Therefore  $|\Delta_1| \geq p+2$ . Secondly assume that  $2p-t-k_1 \geq p$  and  $|\Delta_1| \geq 2p+k_1$ . We take  $p-t-k_1$  points  $\beta_1, \dots, \beta_{p-t-k_1}$  from  $\Delta_2 \cup \dots \cup \Delta_s$ . By [10, Lemma 6],  $G_{1, \dots, t, \beta_1, \dots, \beta_{p-t-k_1}}^{\Delta_1}$  is  $(p+k_1)$ -transitive, which contradicts Theorem 17.7 in [14]. If  $k_1=0$  or 1 then our assumptions are satisfied. Therefore  $k_1 \geq 2$ . Thirdly assume that either  $2p-t-k_1 \geq p$  and  $|\Delta_1|=p+k_1$ , or  $2p-t-k_1 < p$ . We are able to take  $2p-t-k_1$  points  $\beta_1, \dots, \beta_{2p-t-k_1}$  from  $\Delta_2 \cup \dots \cup \Delta_s$ . By [10, Lemma 6],  $G_{1, \dots, t, \beta_1, \dots, \beta_{2p-t-k_1}}^{\Delta_1}$  is  $k_1$ -transitive, which contradicts Theorem 17.7 in [14].

Suppose that Case (II) holds. In this case,  $p \leq t \leq p + \frac{p-1}{2} + 2$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G_{1, \dots, t}$ , then  $N_G(Q)^{I(Q)}$  is  $t$ -transitive, and  $|I(Q)|=2p-1$  or  $3p-1$ . Since  $t \geq p$ , we have  $N_G(Q)^{I(Q)} \geq A^{I(Q)}$ . Hence, there is a unique orbit  $\Delta_j$  such that  $k_j \neq 0$ . Since  $t+k_j \equiv p-1 \pmod{p}$ , we have that  $k_j=2p-1-t \geq 3$ . By [10, Lemma 6],  $G_{1, \dots, t}^{\Delta_j}$  is  $k_j$ -transitive, and so, we have  $j \neq 1$  by [14, Theorem 17.7]. Assume that  $s \geq 3$ . We take a point  $\alpha$  from  $\Delta_1$ ,  $2p-t-2$  points  $\beta_1, \dots, \beta_{2p-t-2}$  from  $\Delta_j$  and a point  $\gamma$  from  $\Delta_i$  where  $1 < i \leq s$  and  $i \neq j$ . A Sylow  $p$ -subgroup of  $G_{1, \dots, t-1, \alpha, \beta_1, \dots, \beta_{2p-t-2}, \gamma}$  fixes at least  $3p$  points, which is a contradiction. Therefore  $s=j=2$ . If  $p \geq 13$ , then  $k_j=2p-1-t \geq 4$ . This is a contradiction by [1]. Hence, we have  $p=11$ . Moreover, we have

$k_j=2p-1-t=3$  by [1]. By [8, Theorem 5], we have that either (i)  $|\Delta_1|+|\Delta_2|+1=\frac{1}{2}(|\Delta_2|^2+|\Delta_2|+2)$ , or (ii)  $|\Delta_1|+|\Delta_2|+1=(\lambda+1)^2(\lambda+4)^2$ ,  $|\Delta_2|=(\lambda+1)(\lambda^2+5\lambda+5)$ , for some positive interger  $\lambda$ . Case (i) does not hold, since  $3+1 \not\equiv \frac{1}{2}(3^2+3+2) \pmod{11}$ . Moreover Case (ii) does not hold, since for every  $\lambda$  ( $\lambda=0, 1, \dots, 10$ ), we have  $3+1 \not\equiv (\lambda+1)^2(\lambda+4)^2 \pmod{11}$  or  $3 \not\equiv (\lambda+1) \cdot (\lambda^2+5\lambda+5) \pmod{11}$ . (q.e.d.)

Step 6. Let  $a$  be an element of order  $p$  of the form

$$a = (1) \dots (p) \dots (2p) \dots (3p-1)(3p, \dots, 4p-1) \dots .$$

Then one of the following holds for  $C=C_G(a)_{3p, \dots, 4p-1}^{I(a)}$ .

- (i)  $C$  has an orbit  $\Delta$  such that  $C^\Delta \geq A^\Delta$  and  $|\Delta| \geq 2p$ .
- (ii) There exist two orbits  $\Delta_1$  and  $\Delta_2$  of  $C$  such that  $|\Delta_i| \geq p$  and  $C^{\Delta_i}$  is  $(|\Delta_i|-p+1)$ -transitive ( $i=1, 2$ ), and  $\Delta_1 \cup \Delta_2 = I(a)$ . Moreover, if  $|\Delta_i| \geq p+3$ , then  $C^{\Delta_i} \geq A^{\Delta_i}$ .
- (iii)  $C$  is an imprimitive group with two blocks  $\Gamma_1$  and  $\Gamma_2$  of length  $p+\frac{p-1}{2}$  such that  $C^{\Gamma_i} \geq A^{\Gamma_i}$  ( $i=1, 2$ ).

Proof. For any  $p$  points  $\alpha_1, \dots, \alpha_p$  of  $I(a)$ ,  $C_{\alpha_1, \dots, \alpha_p}$  has an element of order  $p$ . Since  $C$  has an element of order  $p$ , it has an orbit whose length is at least  $p$ . Assume that  $C$  has two orbits  $\Delta_1$  and  $\Delta_2$  with  $|\Delta_i| \geq p$  ( $i=1, 2$ ). Set  $|\Delta_i|=p+k_i$  ( $i=1, 2$ ). If  $\Delta_1 \cup \Delta_2 \neq I(a)$ , then  $k_1+k_2+2 \leq p$ . We take  $k_1+1$  points  $\alpha_1, \dots, \alpha_{k_1+1}$  from  $\Delta_1$  and  $k_2+1$  points  $\beta_1, \dots, \beta_{k_2+1}$  from  $\Delta_2$ , so  $C_{\alpha_1, \dots, \alpha_{k_1+1}, \beta_1, \dots, \beta_{k_2+1}}$  has no element of order  $p$ , a contradiction. Hence  $\Delta_1 \cup \Delta_2 = I(a)$ . By [10, Lemma 6], we have that  $C$  is a group satisfying (ii). Assume that  $C$  has a unique orbit  $\Delta$  with  $|\Delta| \geq p$ . Then we have  $|\Delta| \geq 2p$ . If  $C^\Delta$  is primitive, by [14, Theorem 13.9] we have that  $C^\Delta$  is a group satisfying (i). Assume that  $C^\Delta$  is imprimitive. Let  $\Gamma_1, \dots, \Gamma_s$  be a system of imprimitivity of  $C^\Delta$ . If  $|\Gamma_1| < p$ , then  $|\Gamma_1|=2$ . We take  $p$  points  $\alpha_1, \dots, \alpha_p$  with  $\alpha_i \in \Gamma_i$  ( $i=1, \dots, p$ ), so  $C_{\alpha_1, \dots, \alpha_p}$  has no element of order  $p$ , a contradiction. Hence  $|\Gamma_1| \geq p$ , and so we have  $s=2$  and  $|\Gamma_1|=|\Gamma_2|=p+\frac{p-1}{2}$ . By [10, Lemma 6], we have that  $C$  is a group satisfying (iii). (q.e.d.)

Step 7. For any  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$  of  $\Omega$ , the order of a Sylow  $p$ -subgroup of  $G_{\alpha_1, \dots, \alpha_{2p}}$  is  $p$ .

Proof. Suppose, by way of contradiction, that for some  $2p$  points  $\alpha_1, \dots, \alpha_{2p}$ , the order of a Sylow  $p$ -subgroup  $P$  of  $G_{\alpha_1, \dots, \alpha_{2p}}$  is more than  $p$ . We may assume that  $\{\alpha_1, \dots, \alpha_{2p}\} = \{1, \dots, 2p\}$  and  $I(P) = \{1, \dots, 2p, \dots, 3p-1\}$ . Let  $a$  be an element of order  $p$  of  $Z(P)$ . We may assume that

$$a = (1) \cdots (3p-1)(3p, \dots, 4p-1) \cdots .$$

Since  $C_{G_1}(a)^{I(a)^{-1}}$  is a permutation group of degree  $3p-2$ , one of the following two cases holds:

(I)  $C_{G_1}(a)^{I(a)^{-1}}$  has an orbit  $\Delta$  such that  $C_{G_1}(a)^\Delta \geq A^\Delta$  and  $|\Delta| \geq 2p-1$ .

(II)  $C_{G_1}(a)^{I(a)^{-1}}$  has two orbits  $\Delta_1, \Delta_2$  such that  $|\Delta_i| \geq p$  and  $C_{G_1}(a)^{\Delta_i}$  is  $(|\Delta_i|-p+1)$ -transitive ( $i=1, 2$ ), and  $\Delta_1 \cup \Delta_2 = I(a) - \{1\}$ . Moreover, if  $|\Delta_i| \geq p+3$ , then  $C_{G_1}(a)^{\Delta_i} \geq A^{\Delta_i}$ .

Suppose that Case (I) holds. We may assume that  $\Delta = \{2, 3, \dots, |\Delta|, |\Delta|+1\}$ . Let  $\Gamma = \{2, 3, \dots, 2p\}$ , then  $\Gamma \subseteq \Delta$ . Since  $C_{G_1}(a)^\Delta \geq A^\Delta$ , we have  $G_{1(\Gamma)}^\Gamma \geq A^\Gamma$ . On the other hand, by the Frattini-Sylow argument,  $G_{1(\Gamma)} = N_{G_1(\Gamma)}(G_{1\Gamma}) = N_{G_1(\Gamma)}(P) \cdot G_{1\Gamma}$ . Hence,  $N_{G_1}(P)_{(\Gamma)}^\Gamma = G_{1(\Gamma)}^\Gamma \geq A^\Gamma$ , so we have  $|N_{G_1}(P)_{(\Gamma)}|_p$  (=the order of a Sylow  $p$ -subgroup of  $N_{G_1}(P)_{(\Gamma)}$ ) =  $|P| \cdot p$ .  $C_G(a)_{1, 2p+1, \dots, 3p-1, 3p, \dots, 4p-1}$  has an element  $b$  of order  $p$ . Since  $|\Gamma| < 2p$ ,  $b^\Gamma$  is a  $p$ -cycle. Since  $b$  normalizes  $G_{1, \dots, 3p-1}$ , we may assume that  $P^b = P$ . Then  $\langle b, P \rangle \in \text{Syl}_p(N_{G_1}(P)_{(\Gamma)})$ . Since  $C_p(b)$  is semiregular on  $(\Omega - I(P)) \cap I(b) = \{3p, \dots, 4p-1\}$ , we have  $|C_p(b)| = p$ . Hence, since  $[P, b] \neq 1$  we have  $|Z(\langle P, b \rangle)| = p$ . Assume that  $C_{G_1}(P)_{(\Gamma)}^\Gamma = 1$ . Since  $N_{G_1}(P)_{(\Gamma)} / C_{G_1}(P)_{(\Gamma)} \leq \text{Aut}(P)$ ,  $A_{2p-1}$  is involved in  $\text{Aut}(P)$ . But, we can easily see that  $A_{2p-1}$  is not involved in  $\text{Aut}(P)$  (cf. [2, §2. (3)]), which is a contradiction. Hence  $C_{G_1}(P)_{(\Gamma)}^\Gamma \geq A^\Gamma$ . Since the center of a Sylow  $p$ -subgroup of  $N_{G_1}(P)_{(\Gamma)}$  is of order  $p$ , this is a contradiction.

Suppose that Case (II) holds. Then, one of the following two cases holds:

(i)  $N_{G_1}(P)^{I(P)^{-1}} \geq A^{I(P)^{-1}}$ .

(ii)  $\Delta_1$  and  $\Delta_2$  are the orbits of  $N_{G_1}(P)^{I(P)^{-1}}$ .  $N_{G_1}(P)^{\Delta_i}$  is  $(|\Delta_i|-p+1)$ -transitive ( $i=1, 2$ ), and if  $|\Delta_i| \geq p+3$ , then  $N_{G_1}(P)^{\Delta_i} \geq A^{\Delta_i}$ .

If Case (i) holds, then we have a contradiction by the similar argument to that of Case (I). Hence we assume that Case (ii) holds. We may assume that  $|\Delta_1| > |\Delta_2|$  and  $\Delta_1 = \{2, 3, \dots, |\Delta_1|, |\Delta_1|+1\}$ . Let  $\Gamma = \{2, 3, \dots, 2p\}$ . Since  $|\Gamma \cap \Delta_2| \leq \frac{p-1}{2}$ , we have  $(C_{G_1}(a)_{\Gamma \cap \Delta_2})^{\Delta_1} \geq A^{\Delta_1}$  by [10, Lemma 6]. Then

$N_{G_1}(P)_{(\Gamma)}^{\Delta_1} \geq A^{\Delta_1}$ , and so,  $|N_{G_1}(P)_{(\Gamma)}|_p = |P| \cdot p$ .  $C_G(a)_{1, 2p+1, \dots, 3p-1, 3p, \dots, 4p-1}$  has an element  $b$  of order  $p$ . Then  $b^{\Delta_1}$  is a  $p$ -cycle, and we may assume that  $P^b = P$ . So  $\langle b, P \rangle \in \text{Syl}_p(N_{G_1}(P)_{(\Gamma)})$ . By the same argument as in Case (I), we have  $|Z(\langle b, P \rangle)| = p$ . Assume that  $C_{G_1}(P)_{(\Gamma)}^{\Delta_1} = 1$ . Then  $C_{G_1}(a)_{\Delta_1} \geq C_{G_1}(a)_{(\Gamma)}$ . Since  $N_{G_1}(P)_{(\Gamma)} / C_{G_1}(P)_{(\Gamma)} \leq \text{Aut}(P)$  and  $N_{G_1}(P)_{(\Gamma)} / N_{G_1}(P)_{\Delta_1} \cong N_{G_1}(P)_{(\Gamma)}^{\Delta_1} \geq A^{\Delta_1}$ , we have that  $A_{(3p-1)/2}$  is involved in  $\text{Aut}(P)$ . But, we can easily see that  $A_{(3p-1)/2}$  is not involved in  $\text{Aut}(P)$  (cf. [2, §2. (3)]), which is a contradiction. Hence  $C_{G_1}(P)_{(\Gamma)}^{\Delta_1} \geq A^{\Delta_1}$ . Since the center of a Sylow  $p$ -subgroup of  $N_{G_1}(P)_{(\Gamma)}$  is of order  $p$ , this is a contradiction. (q.e.d.)

By the same argument as in Step 7 in the proof of Theorem A, we have

Step 8.  $|\Omega| - (3p-1) \equiv p \pmod{p^2}$ .

From now on, let  $a$  be an element of order  $p$  of the form

$$a = (1) \cdots (2p)(2p+1) \cdots (3p-1)(3p, \dots, 4p-1)(4p, \dots, 5p-1) \cdots$$

We divide the consideration into the following two cases:

- ( $\alpha$ )  $C_G(a)^{I(a)}$  has an orbit  $\Delta$  such that  $|\Delta| \geq 2p$  and  $C_G(a)^\Delta \geq A^\Delta$ ;
- ( $\beta$ ) otherwise.

When Case ( $\alpha$ ) holds, we may assume that  $\Delta = \{1, \dots, |\Delta|\}$ . When Case ( $\beta$ ) holds, we may assume that  $\Delta_1 = \{1, \dots, w\}$  and  $\Delta_2 = \{w+1, \dots, 3p-1\}$  are the orbits or the blocks of  $C_G(a)^{I(a)}$ , and that  $|\Delta_1| \geq |\Delta_2| \geq p$ .

By the same argument as in Step 8, Step 9, Step 10 and Step 11 in the proof of Theorem A, we have

Step 9. *Case ( $\alpha$ ) does not hold.*

Hereafter we assume that Case ( $\beta$ ) holds.

Step 10. *Set  $C_G(a)_{w+1, w+2, \dots, 2p, 0} = C_G(a)_{w+1, w+2, \dots, 2p}$ . There is an integer  $i$  ( $0 \leq i \leq 1$ ) such that  $C_G(a)_{w+1, w+2, \dots, 2p, i}$  and  $C_G(a)_{w+1, w+2, \dots, 2p, i+1}$  have exactly  $m$  orbits on  $\Omega - I(a)$ , where  $m$  is at most two, and moreover  $m=1$  when  $|\Omega| - (3p-1) \not\equiv 0 \pmod{p^2}$ .*

Proof. In order to prove Step 10, it is sufficient to show that  $C_G(a)_{w+1, \dots, 2p, 1, 2}$  has at most two orbits on  $\Omega - I(a)$ , and is transitive on  $\Omega - I(a)$  when  $|\Omega| - (3p-1) \equiv 0 \pmod{p^2}$ .

Set  $H = G_{w+1, \dots, 2p, 1, 2}$ . Then  $H$  is  $p$ -transitive on  $\Omega - \{w+1, \dots, 2p, 1, 2\}$  by Step 5. By the remark following Lemma 1.1 in [11], we get the following expression:

$$\frac{|H|}{p} \geq \frac{|H|}{|C_H(a)|} \frac{1}{p} \sum_y \alpha^*(y),$$

where  $y$  ranges all  $p'$ -elements in  $C_H(a)$  and  $\alpha^*(y) = \alpha(y^{\Omega - I(a)})$ . Here the equality does not hold when  $|\Omega| - (3p-1) \equiv 0 \pmod{p^2}$  (cf. Step 8 in the proof of Theorem A). Now,  $\sum_y \alpha^*(y) \geq \sum_{y \in \sigma_H(a)} \alpha^*(y) - p \cdot \sum_{y \in \sigma_H(a)} \alpha_p(y^{I(a)})$ . Since

$|\Delta_1 - \{1, 2\}| \geq p + \frac{p-1}{2} - 2 \geq p+3$ , we have  $C_H(a)^{\Delta_1 - \{1, 2\}} \geq A^{\Delta_1 - \{1, 2\}}$  by Step 6.

Hence,  $p \cdot \sum_{y \in \sigma_H(a)} \alpha_p(y^{I(a)}) = p \cdot \sum_{y \in \sigma_H(a)} \alpha_p(y^{\Delta_1 - \{1, 2\}}) = |C_H(a)|$  by the formula of Frobenius. On the other hand,  $\sum_{y \in \sigma_H(a)} \alpha^*(y) = f \cdot |C_H(a)|$ , where  $f$  is the number of orbits of  $C_H(a)$  on  $\Omega - I(a)$ . Hence we get

$$\frac{|H|}{p} \geq \frac{|H|}{p} (f-1), \quad \text{and hence } f \leq 2.$$

In the above expression, if  $|\Omega| - (3p-1) \equiv 0 \pmod{p^2}$ , the equality does not hold. (q.e.d.)

Step 11.  $C_G(a)_{1,2,\dots,2p}$  has at most  $2m$  orbits on  $\Omega - I(a)$ . Moreover,  $C_G(a)_{1,\dots,p,(p+1,p+2)p+3,\dots,2p}$  ( $= C_{G((p+1,p+2))}(a)_{1,\dots,p,p+3,\dots,2p}$ ) has exactly  $m$  orbits on  $\Omega - I(a)$ .

Proof. By Step 10,  $C_G(a)_{w+1,\dots,2p,i}$  has exactly  $m$  orbits on  $\Omega - I(a)$ . Let  $\Gamma_1, \dots, \Gamma_m$  be the orbits. We take an arbitrarily fixed orbit  $\Gamma_j$  of  $C_G(a)_{w+1,\dots,2p,i}$  on  $\Omega - I(a)$ . Let  $\Sigma_1, \dots, \Sigma_k$  be the orbits of  $C_G(a)_{1,2,\dots,2p}$  on  $\Gamma_j$ . Since  $C_G(a)_{w+1,\dots,2p,i} \triangleright C_G(a)_{1,2,\dots,2p}$  and  $\Gamma_j$  is an orbit of  $C_G(a)_{w+1,\dots,2p,i}$ ,  $C_G(a)_{w+1,\dots,2p,i}^{\Delta_1^{-1}(i)}$  acts on the set  $\{\Sigma_1, \dots, \Sigma_k\}$  transitively. Let  $Y = C_{G(\Sigma_1)}(a)_{w+1,\dots,2p,i}$  then  $|C_G(a)_{w+1,\dots,2p,i}^{\Delta_1^{-1}(i)}: Y^{\Delta_1^{-1}(i)}| = k$ . Similarly we have that  $|C_G(a)_{w+1,\dots,2p,i,i+1}^{\Delta_1^{-1}(i)}: Y_{i+1}^{\Delta_1^{-1}(i)}| = k$ . Hence,  $|C_G(a)_{w+1,\dots,2p,i}^{\Delta_1^{-1}(i)}: C_G(a)_{w+1,\dots,2p,i,i+1}^{\Delta_1^{-1}(i)}| = |Y^{\Delta_1^{-1}(i)}: Y_{i+1}^{\Delta_1^{-1}(i)}| = |\Delta_1| - i$ . Therefore  $Y$  is transitive on  $\Delta_1 - \{i\}$ . Let  $(\beta_1, \dots, \beta_p)$  be a  $p$ -cycle of  $a$  such that  $\{\beta_1, \dots, \beta_p\} \subseteq \Sigma_1$ . For any  $w-p-i$  elements  $\alpha_1, \dots, \alpha_{w-p-i}$  of  $\Delta_1 - \{i\}$ ,  $C_G(a)_{i,\alpha_1,\dots,\alpha_{w-p-i},w+1,\dots,2p,\beta_1,\dots,\beta_p}$  has an element  $b$  of order  $p$ . Then  $b \in Y$  and  $b^{\Delta_1}$  is a  $p$ -cycle, and so,  $Y_{\alpha_1,\dots,\alpha_{w-p-i}}^{\Delta_1^{-1}(i)}$  has the  $p$ -cycle. Since  $\alpha_1, \dots, \alpha_{w-p-i-1}, \alpha_{w-p-i}$  are any  $w-p-i$  points of  $\Delta_1 - \{i\}$ , we have  $Y^{\Delta_1^{-1}(i)} \geq A^{\Delta_1^{-1}(i)}$  (cf. [14, Theorem 13.9]). Therefore  $k \leq 2$ . If  $k=2$ , then  $Y^{\Delta_1^{-1}(i)} = A^{\Delta_1^{-1}(i)}$  and  $C_G(a)_{w+1,\dots,2p,i}^{\Delta_1^{-1}(i)} = S^{\Delta_1^{-1}(i)}$ . Therefore  $\Gamma_j$  is an orbit of  $C_G(a)_{1,\dots,p,(p+1,p+2)p+3,\dots,2p}$  on  $\Omega - I(a)$ , even if  $k=2$ . (q.e.d.)

Step 12. We complete the proof.

Proof. Since  $a$  is an element of order  $p$  of the form

$$a = (1) \cdots (p)(p+1) \cdots (3p-1)(3p, \dots, 4p-1)(4p, \dots, 5p-1) \cdots,$$

$C_G(a)_{p+1,\dots,2p,3p,\dots,4p-1}$  has an element  $b$  of order  $p$ . By Step 8, we may assume that

$$b = (1, \dots, p)(p+1) \cdots (3p-1)(3p) \cdots (4p-1)(4p, \dots, 5p-1) \cdots.$$

Let  $K = G_{1,\dots,p,(p+1,p+2)p+3,\dots,2p}$  and  $L = \langle b \rangle \cdot K$ . By the same argument as Step 10 in the proof of Theorem A, we have a contradiction. (q.e.d.)

#### 4. Proofs of Theorem C and Theorem D

Proof of Theorem C. Let  $G$  be a nontrivial  $2p$ -transitive group on  $\Omega = \{1, \dots, n\}$ . Let  $P$  be a Sylow  $p$ -subgroup of  $G_{1,\dots,2p}$ , then  $P \neq 1$  and  $P$  is not semiregular on  $\Omega - I(P)$  by [3] and [4]. Moreover,  $N_G(P)^{I(P)}$  is  $S_m$  ( $2p \leq m \leq 3p-1$ ) or  $A_m$  ( $2p+2 \leq m \leq 3p-1$ ). Hence, if  $n \equiv |I(P)| \equiv p-1 \pmod{p}$ , then Theorem C holds. Suppose that  $n \not\equiv p-1 \pmod{p}$ . Let  $Q$  be a subgroup of  $P$  such that the order of  $Q$  is maximal among all subgroups of  $P$  fixing more than  $|I(P)|$  points. Set  $N = N_G(Q)^{I(Q)}$ , then  $N$  has an orbit  $\Gamma$  such that  $N^\Gamma \geq A^\Gamma$  and  $|\Gamma| \geq 3p$ , by Theorem A. (q.e.d.)

Proof of Theorem D. Let  $G$  be a nontrivial  $t$ -transitive group on  $\Omega =$

$\{1, \dots, n\}$ . Suppose that  $t$  is sufficiently large. By Satz B in [13],  $\log(n-t) > \frac{t}{2}$ .

By the proof of [13, Satz B], we can see that  $\log(n-t) > \left(\frac{1}{2} + \varepsilon_0\right)t$  for some  $\varepsilon_0 > 0$ . Moreover, we can see that, in the proof of [13, Satz B], it was only used that for any  $k$ -transitive group  $H$  on  $\Sigma$ , there exists a subset  $\Pi$  of  $\Sigma$  such that  $|\Pi| = k$  and  $H_{(\Pi)}^{\Pi} \geq A^{\Pi}$ .

Let  $p_1=2, p_2=3, \dots$ , and  $p_i$  be the  $i$ -th prime number. Then  $\lim_{i \rightarrow \infty} \frac{p_{i+1}}{p_i} \rightarrow 1$ . (This result is well known in the theory of numbers.)

Since  $t$  is sufficiently large, by the above remark and Theorem C, there exists a positive number  $\varepsilon$  which is sufficiently close to 0, and exists a subset  $\Delta$  of  $\Omega$  such that  $|\Delta| \geq \left(\frac{3}{2} - \varepsilon\right)t$  and  $G_{(\Delta)}^{\Delta} \geq A^{\Delta}$ . Therefore we have

$$\log(n-t) > \frac{3}{4}t. \quad (\text{q.e.d.})$$

GAKUSHUIN UNIVERSITY

#### References

- [1] E. Bannai: *On rank 3 groups with a multiply transitive constituent*, J. Math. Soc. Japan **24** (1972), 252–254.
- [2] E. Bannai: *On multiply transitive permutation groups I*, Osaka J. Math. **11** (1974), 401–411.
- [3] E. Bannai: *On multiply transitive permutation groups II*, Osaka J. Math. **11** (1974), 413–416.
- [4] E. Bannai: *On multiply transitive permutation groups IV*, Osaka J. Math. **13** (1976), 123–129.
- [5] E. Bannai: *A note on multiply transitive permutation groups II*, J. Algebra **36** (1975), 294–301.
- [6] E. Bannai: *Normal subgroups of 6-transitive permutation groups*, J. Algebra **42** (1976), 46–59.
- [7] E. Bannai: *On some triply transitive permutation groups*, Geometriae Dedicata **6** (1977), 1–11.
- [8] P.J. Cameron: *Biplanes*, Math. Z. **131** (1973), 85–101.
- [9] D.G. Higman: *Intersection matrices for finite permutation groups*, J. Algebra **6** (1967), 22–42.
- [10] D. Livingstone and A. Wagner: *Transitivity of finite permutation groups on unordered set*, Math. Z. **90** (1965), 393–403.
- [11] I. Miyamoto: *Multiply transitive permutation groups and odd primes*, Osaka J. Math. **11** (1974), 9–13.
- [12] T. Oyama: *On multiply transitive groups X*, Osaka J. Math. **8** (1971), 99–130.
- [13] H. Wielandt: *Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad*, Schr. Math. Sem. Inst. angew. Math. Univ. Berlin **2** (1934), 151–174.
- [14] H. Wielandt: *Finite permutation groups*, Academic Press, New York and London, 1964.

