

## LARGE ORBITS IN COPRIME ACTIONS OF SOLVABLE GROUPS

SILVIO DOLFI

ABSTRACT. Let  $G$  be a solvable group of automorphisms of a finite group  $K$ . If  $|G|$  and  $|K|$  are coprime, then there exists an orbit of  $G$  on  $K$  of size at least  $\sqrt{|G|}$ . It is also proved that in a  $\pi$ -solvable group, the largest normal  $\pi$ -subgroup is the intersection of at most three Hall  $\pi$ -subgroups.

### 1. INTRODUCTION

All groups considered here are finite groups.

We prove the following:

**Theorem 1.1.** *Let  $G$  be a solvable group acting faithfully on a group  $K$ . If  $(|G|, |K|) = 1$ , then there exist  $x, y \in K$  such that*

$$C_G(x) \cap C_G(y) = 1.$$

As a consequence of Theorem 1.1, we have that in a faithful coprime action of a solvable group  $G$  there always exists an orbit of size at least  $\sqrt{|G|}$ . This answers a question raised by I. M. Isaacs in [9].

**Corollary 1.2.** *If  $G$  is a solvable group that acts faithfully on a group  $K$  with  $(|G|, |K|) = 1$ , then there exists  $x \in K$  such that*

$$|C_G(x)| \leq \sqrt{|G|}.$$

The main step in the proof of Theorem 1.1 is the study of large orbits of primitive solvable linear groups. This is accomplished in Theorem 3.4.

Theorem 1.1 can be rephrased in a somewhat different way:

**Theorem 1.3.** *Let  $\pi$  be a set of primes,  $G$  a  $\pi$ -solvable group and  $H$  a Hall  $\pi$ -subgroup of  $G$ . Then there exist  $x, y \in G$  such that*

$$H \cap H^x \cap H^y = O_\pi(G).$$

We remark that Theorem 1.3 was proved by D. S. Passman in [12] for sets  $\pi = \{p\}$  consisting of a single prime. We point out that in [18], V. I. Zenkov shows that if  $H$  is a nilpotent Hall  $\pi$ -subgroup of a  $\pi$ -solvable group  $G$ , then the intersection of any number of conjugates of  $H$  in  $G$  can be expressed as the intersection of (at most) three conjugates of  $H$ .

---

Received by the editors May 7, 2004 and, in revised form, September 7, 2005.

2000 *Mathematics Subject Classification.* Primary 20D45; Secondary 20D20.

*Key words and phrases.* Finite groups, coprime action, regular orbits.

This research was partially supported by MURST project ‘Teoria dei Gruppi e Applicazioni’.

©2007 American Mathematical Society  
 Reverts to public domain 28 years from publication

We also reprove a result by A. Seress ([13, Theorem 2.1]):

**Theorem 1.4.** *Let  $G$  be a solvable group and  $V$  a finite faithful  $G$ -module. If  $V$  is completely reducible, then there exist  $v_1, v_2, v_3 \in V$  such that*

$$C_G(v_1) \cap C_G(v_2) \cap C_G(v_3) = 1.$$

We point out that Theorem 1.4 can be improved for groups of odd order:

**Theorem 1.5** ([4, Theorem 3]). *Let  $G$  be a (solvable) group of odd order and  $V$  a finite faithful and completely reducible  $G$ -module. Then there exist  $v, w \in V$  such that*

$$C_G(v) \cap C_G(w) = 1.$$

As shown in [17], Theorem 1.5 holds for supersolvable groups  $G$ , but it fails for  $G$  solvable of even order.

## 2. PRELIMINARIES

By well established reduction methods, the proof of Theorem 1.1 boils down to showing that a solvable group  $G$ , acting faithfully and primitively on a finite module  $V$  with  $(|G|, |V|) = 1$ , has “enough” regular orbits on  $V \oplus V$ . That is given by Corollary 3.6, which follows from Theorem 3.4 where we consider a more general context, by dropping the coprimality assumption. We mention here that in the proof of Theorem 3.4 we are using the computer algebra system [GAP] in order to check some “small” primitive groups.

We recall that an irreducible  $G$ -module  $V$  is said to be primitive if there is no nontrivial decomposition of  $V$  into a direct sum of subspaces  $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$  such that  $G$  permutes the set  $\{V_1, V_2, \dots, V_m\}$ . A linear group  $G \leq \mathrm{GL}(d, p^k)$  is said to be primitive if the natural  $G$ -module is primitive.

It is clear that in looking for regular orbits of a primitive solvable linear group  $G$ , we can assume that  $G$  is a maximal primitive solvable linear group. Further, by reducing the scalars, there is no loss of generality in assuming that the ground field of the module is a prime field.

In the following lemma we collect a number of facts concerning the structure of maximal primitive solvable linear groups. We mainly adopt the notation in [14]. In particular, we denote by  $G_1 \wr G_2$  the central product of two groups  $G_1$  and  $G_2$  and by  $F_2(G)$  the second term of the Fitting series of  $G$  (i.e.  $F_2(G)/F(G) = F(G/F(G))$ ).

**Lemma 2.1.** *Let  $G$  be a primitive maximal soluble group of  $\mathrm{GL}(d, p)$ ,  $p$  a prime.*

*Then  $G$  has a unique maximal abelian normal subgroup  $A$ ,  $A$  is cyclic and  $|A| = p^a - 1$  for some integer  $a$ .*

*Let  $C = C_G(A)$  and let  $F = F(C)$  be the Fitting subgroup of  $C$ . Let  $e = e(G) = d/a$ . Then the following holds:*

- (1)  $G/C$  is a cyclic group and  $|G/C|$  divides  $a$ ;
- (2)  $C \leq \mathrm{GL}(e, p^a)$  (for a suitable embedding of  $\mathrm{GL}(e, p^a)$  in  $\mathrm{GL}(d, p)$ );
- (3)  $|F/A| = e^2$  and each prime divisor of  $e$  divides  $|A|$ ;
- (4)  $F/A$  is a completely reducible, faithful symplectic  $C/F$ -module (possibly over fields of different characteristic);
- (5) for each prime divisor  $q$  of  $e$ ,  $O_q(F) = O_q(A) \wr E_q$  with  $E_q$  an extraspecial group; if  $q$  is odd, then  $\exp(E_q) = q$ ; if  $|E_q| = q^{1+2n}$ , in  $\mathrm{GL}(q^n, p^a)$  there is a unique conjugacy class of subgroups  $\overline{E}_q$  isomorphic to  $E_q$ ;

- (6) if  $e = d = q_1^{n_1} q_2^{n_2}$ , with  $q_1, q_2$  distinct primes, then  $G$  is conjugate in  $\mathrm{GL}(d, p)$  to the Kronecker product  $G_1 \dot{\times} G_2$  where  $G_i$  is a maximal primitive solvable subgroup of  $\mathrm{GL}(q^{n_i}, p)$  with  $e(G_i) = q^{n_i}$  for  $i = 1, 2$ ;
- (7) if  $d$  is a prime and  $a = 1$ , then  $G \simeq (C_{p-1} \rtimes E).H$  where  $E$  is an extraspecial group of order  $d^3$  and exponent  $d$  if  $d$  is odd,  $E = Q_8$  if  $d = 2$ , and  $H$  is a maximal irreducible soluble subgroup of  $\mathrm{SL}(2, d)$ ; further,  $|H : F(H)| \leq 6$  and  $|H : F(H)| = 2$  if  $d = 2$ ;
- (8)  $G$  is isomorphic to the semilinear group  $\Gamma(p^d)$  if and only if  $e = 1$ .

*Proof.* For (1)–(4) we refer to [14, Thms. 2.5.13–15]. (5) comes from [14, Thm. 2.5.17] and [14, Thm. 2.4.7a)]. (6) is a particular case of [15, Thm. 20.17]. For (7) we refer to [14, pg. 62 and pg. 76]. Observe also that  $H = H_1 \cap \mathrm{SL}(2, d)$ , where  $H_1$  is a maximal irreducible soluble subgroup of  $\mathrm{GL}(2, d)$ . If  $H_1$  is imprimitive or semilinear, then  $|H_1 : F(H_1)| = 2$ . If  $H_1$  is primitive and  $e(H_1) = 2$ , then  $|H_1 : F(H_1)| \leq 6$ . (8) is [10, Corollary 2.3(a)].  $\square$

We remark that for  $G_i \leq \mathrm{GL}(n_i, p)$  with  $Z_i = Z(\mathrm{GL}(n_i, p)) \leq G_i$ , the Kronecker product  $G_1 \dot{\times} G_2$  is isomorphic to the central product  $G_1 \rtimes G_2$ , with  $Z_1, Z_2$  amalgamated.

We will maintain throughout the paper the meaning of the symbols  $a, e, A, C, F$  introduced in Lemma 2.1.

We state now a couple of well-known facts about symplectic modules. We say that an  $H$ -module  $U$  is *symplectic* if  $U$  carries a nonsingular symplectic form that is invariant by the action of  $H$ .

**Lemma 2.2.** *Let  $U$  be a finite symplectic  $S$ -module. If  $\mathrm{char}(U)$  does not divide  $|S|$ , then  $[S, U]$  and  $C_U(S)$  are nonsingular  $S$ -submodules of  $U$ .*

*Proof.* By the Zassenhaus decomposition,  $U = [U, S] \times C_U(S)$ . It is enough to show that  $C_U(S) = [U, S]^\perp$ , the orthogonal (with respect to the nonsingular  $S$ -invariant symplectic form  $\langle \cdot, \cdot \rangle$  on  $U$ ) of  $[U, S]$ . If  $w \in [U, S]^\perp$ , then for all  $u \in U, x \in S, 0 = \langle w, u^x - u \rangle = \langle w, u^x \rangle - \langle w, u \rangle = \langle w, u^x \rangle - \langle w^x, u^x \rangle = \langle w - w^x, u^x \rangle$ , so  $w - w^x = 0$  and  $w \in C_U(S)$ . Therefore  $[U, S]^\perp \leq C_U(S)$  and equality follows by considering dimensions.  $\square$

**Lemma 2.3.** *Let  $U$  be a symplectic  $H$ -module and assume that  $U = U_1 \oplus U_2$  with  $U_1, U_2$  totally isotropic  $H$ -submodules of  $U$ . Then  $C_H(U_1) = C_H(U_2)$ .*

*Proof.* One can choose  $x_1, x_2, \dots, x_k \in U_1$  and  $y_1, y_2, \dots, y_k \in U_2$  such that, for  $i = 1, \dots, k$ , the linear span  $P_i$  of  $x_i$  and  $y_i$  is a hyperbolic plane and  $U$  is the orthogonal sum of the  $P_i$ 's. Then observe that if  $h \in H$  centralizes all the elements  $x_i$ , then  $h$  centralizes also all the elements  $y_i$ .  $\square$

We need also some estimate on the order of centralizers in primitive linear actions. The following lemma is inspired by [16, Theorem 1.2(b)] and [13, Lemma 2.3]. We adopt the notation in Lemma 2.1.

**Lemma 2.4.** *Let  $G$  be a primitive maximal solvable subgroup of  $\mathrm{GL}(d, p)$ ,  $p$  a prime, and  $V$  the natural  $G$ -module. Let  $S$  be a subgroup of  $G$  of prime order  $s$ .*

*If  $S \leq C$ , then  $|C_V(S)| \leq p^{ae\alpha}$ , where:*

- (1) if  $S \leq A$ , then  $\alpha = 0$ ;
- (2) if  $S \leq F$ , then  $\alpha \leq 1/s$ ;

- (3) if  $[S, O_q(F)] \neq 1$  for some prime  $q \neq s$ , then  $|[S, O_q(F)]| = q^{2m+1}$  for some positive integer  $m$  and

$$\alpha \leq \frac{1}{s} \left( \frac{q^m + s - 1}{q^m} \right) \quad \text{if } s|q^m - 1,$$

$$\alpha \leq \frac{1}{s} \left( \frac{q^m + 1}{q^m} \right) \quad \text{if } s|q^m + 1;$$

- (4) if  $S \leq F_2(C)$ , then  $\alpha \leq 2/3$  and  $\alpha \leq 1/2$  if  $s \neq 2$ ;  
 (5)  $\alpha \leq 3/4$  in any case.

If  $S \not\leq C$ , then  $|C_V(S)| \leq p^{ea/2}$ .

*Proof.* The cyclic group  $A$  acts fixed point freely on  $V$ , so (1) is clear.

If  $S \not\leq C$ , then there exist  $x \in S$ ,  $a \in A$  such that  $[x, a]$  is a nontrivial element of  $A$ . Since  $C_V(x) \cap C_V(x^a) = C_V(x^{-1}) \cap C_V(x^a) \leq C_V([x, a]) = 0$  and  $|C_V(x)| = |C_V(x^a)|$ , we have  $|C_V(S)| \leq p^{ea/2}$ .

Therefore, we can assume  $S \leq C$ . By Lemma 2.1(2) a subgroup of  $C$  is a group of  $GF(p^a)$ -linear transformations of  $V$ .

Assume first that  $S \leq F$ ,  $S \not\leq A$ . Then  $s \neq p$  and  $S \leq E \leq G$ , with  $E$  an extraspecial  $s$ -group. We consider the restriction  $V_E$ . It is a direct sum of faithful irreducible  $E$ -modules, since  $Z(E) \leq A$  acts fixed point freely on  $V$ . As dimensions of centralizers do not change by extending the ground field and they add up in direct sums, we can assume that  $V$  is an irreducible, faithful  $E$ -module on an algebraically closed field  $\mathbb{F}$ . If  $\chi$  is the (Brauer) character corresponding to  $V$ , then, as  $\text{char}(\mathbb{F}) \neq s$ ,  $\dim_{\mathbb{F}}(C_V(S)) = [\chi_S, 1_S] = \frac{1}{s} \dim_{\mathbb{F}}(V)$  since  $\chi(x) = 0$  for every  $x \in E \setminus Z(E)$ , and (2) is proved.

Assume now that  $[S, F_q] \neq 1$ , where  $F_q = O_q(F)$ , for some prime  $q \neq s$ . Observe that  $S$  centralizes  $Z(F_q) \leq A$ . Hence  $U = F_q/Z(F_q)$  is a faithful nonsingular symplectic  $S$ -module and  $(|S|, |U|) = 1$ . Then by Lemma 2.2,  $Q = [F_q, S]$  is an extraspecial group and  $|Q| = q^{2m+1}$  for some positive integer  $m$ . Observe that  $S$  centralizes  $Z(Q)$  and by coprimality  $S$  acts fixed point freely on  $Q/Z(Q)$ . We may again assume that the ground field of  $V$  is algebraically closed. If  $W$  is a  $QS$ -submodule of  $V$ , then  $|C_V(S)| = |C_W(S)||C_{V/W}(S)|$ , and both  $W$  and  $V/W$  are faithful  $QS$ -modules (as nontrivial normal subgroups of  $QS$  containing  $Z(Q)$ , which acts fixed point freely). By induction on  $\dim(V)$ , we can hence assume that  $V$  is irreducible. Applying [7, Satz V.17.3] when  $\text{char}(V) \neq s$  and [8, Theorem 2.6] when  $\text{char}(V) = s$ , we get (3).

If  $S \leq F_2(C)$ , then  $[S, O_{s'}(F)] \neq 1$  or  $S \leq F$ ; thus (4) follows by (2) and (3).

Finally, if  $S \not\leq F$  there exist  $g \in G$ ,  $x \in S$  with  $1 \neq z = [x, g] \in F$ . By (2),  $\dim_{GF(p^a)} C_V(z) \leq e/2$  and since  $2 \dim_{GF(p^a)} C_V(x) = \dim_{GF(p^a)} C_V(x^{-1}) + \dim_{GF(p^a)} C_V(x^g) = e + \dim_{GF(p^a)} (C_V(x^{-1}) \cap C_V(x^g))$ , we have (5).  $\square$

The next two lemmas are probably known, but we have found no reference in the literature. Their proof uses arguments similar to those in [10, Thm. 3.5].

**Lemma 2.5.** *Let  $G$  a nontrivial solvable and completely reducible group of linear transformations of the finite vector space  $U$ . Then*

$$|G : F(G)| \leq \frac{|U|^\beta}{\lambda}$$

where  $\beta = \log_9(6\sqrt[3]{24})$  and  $\lambda = \sqrt[3]{24}$ .

*Remark 2.6.* The bound in Lemma 2.5 is attained when  $G = \mathrm{GL}(2, 3)$ , acting on its natural module. Observe also that  $2.884 \leq \lambda \leq 2.885$  and  $1.297 \leq \beta \leq 1.298$ .

*Proof.* We work by induction on  $|U|$ .

Let  $U = U_1 \oplus U_2$  for nontrivial  $G$ -modules  $U_1, U_2$  and let  $G_i = G/C_i$  with  $C_i = C_G(U_i)$ ,  $i = 1, 2$ . Then  $G$  is isomorphic to a subgroup of  $G_1 \times G_2$  and hence, by induction,

$$|G : \mathrm{F}(G)| \leq |G_1 \times G_2 : \mathrm{F}(G_1 \times G_2)| \leq \frac{|U_1|^\beta}{\lambda} \frac{|U_2|^\beta}{\lambda} = \frac{|U|^\beta}{\lambda^2} < \frac{|U|^\beta}{\lambda}.$$

We can hence suppose that  $U$  is an irreducible  $G$ -module. If  $U$  is imprimitive, there exists a normal subgroup  $N$  of  $G$  such that  $U_N$  is non-homogeneous; we choose  $N$  maximal with such properties. Let  $U_N = U_1 \oplus U_2 \oplus \cdots \oplus U_m$ , where the  $U_i$ 's are the homogeneous components of  $U_N$ . Then  $G/N$  is a faithful and primitive permutation group on the set  $\{U_1, U_2, \dots, U_m\}$  (see, for instance, [10, Proposition 0.2]). By induction, we have  $|N : \mathrm{F}(N)| \leq |U|^\beta / \lambda^m$ . As  $|G : \mathrm{F}(G)| \leq |G : \mathrm{F}(N)| = |G : N| |N : \mathrm{F}(N)|$ , it is enough to show that  $|G/N| \leq \lambda^{m-1}$ .

If  $M/N$  is a chief factor of  $G/N$ , then  $|M/N| = m$  and  $M/N$  is a faithful and irreducible  $G/M$ -module. By [10, Theorem 3.5 (a)]  $|G/N| \leq m^{\alpha+1}/\lambda$ , with  $3 < \alpha + 1 < 10/3$ . So we can assume  $m^{10/3} > \lambda^m$ , that implies  $2 \leq m \leq 5$ . If  $m$  is prime, then  $|G/N| \leq m(m-1) \leq \lambda^{m-1}$ . If  $m = 4$ , then  $|G/N| \leq |S_4| = \lambda^3$  and we are done in this case.

As the limitation of the index of the Fitting subgroups is inherited by subgroups, we can thus assume that  $G$  is a maximal solvable primitive subgroup of  $\mathrm{GL}(d, p)$ , where  $|U| = p^d$ ,  $p$  a prime.

We use the notation of Lemma 2.1. If  $e = 1$ , then by Lemma 2.1(8) we have  $|G : \mathrm{F}(G)| \leq d \leq p^{d\beta}/\lambda$  for all  $(p, d) \neq (2, 1)$ . But, if  $(p, d) = (2, 1)$ , then  $G$  is trivial. So we can assume  $e \geq 2$ . We remark also that if  $p = 2$ , then by Lemma 2.1(3) it must be  $a \geq 2$  and  $e$  odd.

By [10, Theorem 3.5 (a)],  $|C/F| \leq e^{2.9/4}$ , so  $|G : \mathrm{F}(G)| \leq |G : F| \leq a \cdot e^{9/2}$ . Recall that  $|U| = p^{ae}$ . As  $\beta > 5/4$ , we are done when  $\lambda a e^{9/2} \leq p^{ae5/4}$ . So we consider the function

$$f(p, e, a) = \frac{5ae}{4} \log p - \log a - \frac{9}{2} \log e - \frac{1}{3} \log 24$$

in  $D = \{(p, e, a) \mid p \text{ prime, } e, a \text{ positive integers, } e \geq 2\}$ .

Taking derivatives, one checks that  $f(p, e, a)$  is increasing with respect to  $p$  and  $a$  in  $D$ , and it is increasing in  $e$  whenever  $ea \geq 6$ .

Further,  $f$  is positive at  $(2, 6, 2)$ ,  $(2, 3, 3)$ ,  $(3, 8, 1)$ ,  $(7, 3, 1)$  and  $(3, 2, 2)$ . Therefore, recalling that the prime divisors of  $e$  must divide  $p^a - 1$ , we are left with the cases  $(p, e, a) = (2, 3, 2)$ ,  $(3, 4, 1)$  or  $p \geq 3$ ,  $e = 2$ ,  $a = 1$ .

Assume  $(p, e, a) = (2, 3, 2)$ . By Lemma 2.1(4),  $C/F$  is isomorphic to a subgroup of  $\mathrm{Sp}(2, 3)$ . Hence,  $\lambda |G : \mathrm{F}(G)| \leq \lambda 48 \leq 2^{6\beta}$ .

If  $(p, e, a) = (3, 4, 1)$ , then  $G/\mathrm{F}(G) = C/F$  is a solvable subgroup of the symplectic group  $\mathrm{Sp}(4, 2) \simeq S_6$ , so  $|G/\mathrm{F}(G)| \leq 72$ . As  $72\lambda \leq 3^{4\beta}$ , we are done in this case.

If  $e = 2$ , then by Lemma 2.1(7),  $|G/\mathrm{F}(G)| \leq 6$  and hence  $|G/\mathrm{F}(G)|\lambda \leq p^{2\beta}$  for all  $p \geq 3$  (with equality when  $p = 3$ ). The proof is complete.  $\square$

**Lemma 2.7.** *Let  $K$  be a nilpotent group and  $U$  be a nontrivial, finite, symplectic  $K$ -module. If  $U$  is faithful and completely reducible, then*

$$|K| \leq \frac{|U|^\gamma}{2}$$

where  $\gamma = \log_4(6)$ .

*Remark 2.8.* The bound is sharp for  $K = \mathrm{F}(\mathrm{Sp}(2, 2))$ . Also,  $1.292 \leq \gamma \leq 1.293$ .

*Proof.* By induction on  $|U|$ .

Arguing as in step (1) of the proof of Theorem A in [3], we have an orthogonal decomposition  $U = W_1 \perp W_2 \perp \cdots \perp W_n$ , where each  $W_i$  is  $K$ -irreducible or the sum of an irreducible  $K$ -module and its dual. In both cases  $W_i$  is non-singular, for all  $i$ .

Working by induction on  $|U|$ , we can hence assume that  $U = W_1$ .

Let  $N$  be a normal subgroup of  $K$ . By step (2) of the proof of Theorem A in [3],  $U_N = U_1 \oplus U_2 \oplus \cdots \oplus U_h$  where each  $U_i$  is either homogeneous or the sum of the homogeneous components corresponding to an irreducible  $M$ -module and its dual.

If  $h > 1$  and  $M$  is the kernel of the transitive permutation action of  $K$  on  $\{U_1, U_2, \dots, U_h\}$ , by the induction hypothesis,

$$|M| \leq \prod_{i=1}^h \left| \frac{M}{C_M(U_i)} \right| \leq \prod_{i=1}^h \frac{|U_i|^\gamma}{2} \leq \frac{|U|^\gamma}{2^h}.$$

By [1, Theorem 3],  $|K/M| \leq 2^{h-1}$ ; hence  $|K| \leq |U|^\gamma/2$ .

Therefore, we can assume that, for all  $N \leq K$ ,  $U_N$  is either homogeneous or the sum of a homogeneous  $N$ -module and its dual. Since the kernel of a module is the same as the kernel of its dual, it follows that every abelian normal subgroup of  $K$  is cyclic. As  $K$  is nilpotent, it follows that there exists a cyclic normal subgroup  $B$  of  $K$  with  $|K : B| \leq 2$  (see for instance [7, III.7.6]). By [3, Lemma 1.1],  $|B|$  divides  $p^n \pm 1$ , where  $|U| = p^{2n}$ ,  $p$  a prime. Hence  $|K| \leq 2(p^n + 1)$  and, as  $4(p^n + 1) \leq p^{2n\gamma}$  for all  $p^n \geq 3$ , we are left with the case  $p^n = 2$ . Then  $K \leq \mathrm{Sp}(2, 2)$  and hence  $|K| \leq 3$ . As  $3 = 4^\gamma/2$ , the proof is finished.  $\square$

### 3. THE PRIMITIVE CASE

Given a group  $G$  and a prime  $q$ , we denote by  $n_q(G)$  the number of elements of order  $q$  of  $G$  and by  $n_{q'}(G)$  the number of elements of prime order  $\neq q$  of  $G$ .

We further denote by  $\nu(G)$  (resp.  $\nu_q(G)$ ; resp.  $\nu_{q'}(G)$ ) the number of subgroups of  $G$  of prime order (resp. of order  $q$ ; resp. of order a prime  $\neq q$ ) not contained in  $Z(G)$ .

The proof of the next lemma is straightforward and we omit it.

**Lemma 3.1.** *Let  $G$  be a group and  $q$  a prime.*

- (a) *If  $G = L \times M$ , then  $n_q(G) = (n_q(L) + 1)(n_q(M) + 1) - 1$ .*
- (b) *If  $Z = Z(G)$  is cyclic, then*

$$\nu_q(G) \leq \frac{(q, |Z|)}{q-1} n_q(G/Z).$$

**Lemma 3.2.** *Let  $H$  be a solvable and completely reducible subgroup of  $\mathrm{Sp}(4, 3)$ . Then there exists a 2-subgroup  $K$  of  $H$  such that  $|H : K| \leq 48$  and  $n_2(K) \leq 3$ .*

*Proof.* It is well known that a maximal subgroup of  $\mathrm{Sp}(4, 3)$  is conjugate to one of five groups  $M_1, M_2, \dots, M_5$ , where  $M_1 \simeq \mathrm{SL}(2, 3) \wr S_2$ ,  $|M_2| = |M_3| = 2^4 \cdot 3^4$ ,  $|O_3(M_2)| = |O_3(M_3)| = 3^3$ ,  $M_4 = 2.S_6$ ,  $M_5 = (D_8 \wr Q_8).A_5$ . We can hence assume that  $H$  is maximal among the solvable subgroups of  $M_i$  such that  $O_3(H) = 1$ , for some  $i$ . If  $i = 1$ , then  $H = M_1$  and we consider  $K = O_2(M_1) \simeq Q_8 \times Q_8$ . If  $i = 2$  or  $i = 3$ , then  $|H| \leq 48$ . If  $H \leq M_4$ , then  $Z = Z(M_4) \leq H$  and  $H/Z$  is isomorphic to a solvable subgroup  $L$  of  $S_6$  with  $O_3(L) = 1$ . It is easily checked that then  $L$  is isomorphic to a subgroup of either  $S_2 \wr S_3 \simeq S_4 \times C_2$  or a Frobenius group of order 20. Hence in this case  $|H| \leq 96$  and one takes  $K = Z$ . If, finally,  $H \leq M_5$ , then  $H \simeq (Q_8 \wr D_8).L$ , where  $L$  is isomorphic to  $S_3, A_4$  or a Frobenius group of order 10. We are done by taking as  $K$  a subgroup of  $H$  isomorphic to  $Q_8$ . (We observe also that this is the only case where  $K$  is not normal in  $H$ . If we take  $K = F(H) \simeq Q_8 \wr D_8$ , then  $n_2(K) = 11$  and  $|H : K| \leq 12$ .)  $\square$

By Lemma 2.1(4), symplectic groups are naturally involved in the structure of primitive linear groups. We collect in the following lemma some information about some small solvable symplectic groups (see also [13, 2.10, 2.11]).

**Lemma 3.3.** *Let  $R$  be a solvable group,  $U$  an elementary abelian normal  $q$ -subgroup of  $R$  ( $q$  a prime) and assume that  $R/U$  acts completely reducibly and faithfully, respecting a nonsingular symplectic form on  $U$ . Then there is a normal subgroup  $K$  of  $R$  with  $U \leq K$  and  $K/U$  nilpotent such that:*

- (a) *if  $|U| = 2^4$ , then  $|R : K| \leq 8$ ,  $\pi(K/U) \subseteq \{3, 5\}$  and  $n_3(K) \leq 80$ ,  $n_5(K) = 0$  or  $n_3(K) = 0$ ,  $n_5(K) \leq 64$ ;*
- (b) *if  $|U| = 2^6$ , then  $|R/K| \leq 48$ ,  $R/K$  has at most 23 subgroups of prime order,  $\pi(K/U) \subseteq \{3, 5, 7\}$  and one of the following holds:*
  - i)  $n_3(K) \leq 728$ ,  $n_5(K) = 0$ ,  $n_7(K) = 0$ ;
  - ii)  $n_3(K) \leq 8$ ,  $n_5(K) \leq 64$ ,  $n_7(K) = 0$ ;
  - iii)  $n_3(K) \leq 8$ ,  $n_5(K) = 0$ ,  $n_7(K) \leq 384$ ;
- (c) *if  $|U| = 2^8$  and  $U$  has no totally isotropic  $H$ -submodules, then  $|R/K| \leq 64$  or  $R/K$  is isomorphic to a subgroup of either  $S_2 \wr S_4$  or  $\mathrm{GL}(2, 3) \times C_2$ ; also  $\nu_{2'}(K) \leq 3280$ ;*
- (d) *if  $|U| = 3^6$ , then  $|R/K| \leq 1296$ ,  $\pi(K/U) = \{2\}$  and  $\nu_2(K) \leq 7 \cdot 3^8$ .*

*Proof.* By assumption  $H = R/U$  is a solvable completely reducible subgroup of the symplectic group  $\mathrm{Sp}(U)$ . Note that an irreducible  $H$ -submodule of  $U$  must be either nonsingular or totally isotropic. Observe also that we may shift to subgroups  $H_1 \leq \mathrm{GL}(U)$  containing  $H$ . Namely, if  $N_1$  is a normal nilpotent subgroup of  $H_1$  and  $K$  is the preimage in  $R$  of  $N_1 \cap H$ , then  $R/K$  is isomorphic to a subgroup of  $H_1/N_1$  and  $\pi(K/U) \subseteq \pi(N_1)$ . Also,  $K$  acts completely reducibly on  $U$ , so  $(|K|, |U|) = 1$  and  $K$  splits on  $U$ . It follows that  $n_q(K) \leq n_q(U \rtimes N_1)$ , for all primes  $q$ .

(a): If  $H$  is reducible or  $H$  is imprimitive, then  $H \leq H_1 = \mathrm{GL}(2, 2) \wr S_2$  (as a subgroup of  $\mathrm{GL}(4, 2)$ ). Considering  $N_1 = F(H_1)$ , we have  $|H_1 : N_1| = 8$  and  $n_{2'}(U \rtimes N_1) = n_3(A_4 \times A_4) = 80$ . If  $H$  is primitive, then  $H$  is a subgroup of the semilinear group  $\Gamma(2^4)$ . Since  $\mathrm{Sp}(4, 2) \simeq S_6$  has no element of order 15, the claim follows.

(b): Let  $|U| = 2^6$ . If  $U$ , as an  $H$ -module, is reducible and has an irreducible submodule of dimension 4, then  $H \leq L \times \mathrm{GL}(2, 2)$  where  $L$  is a maximal solvable irreducible subgroup of  $\mathrm{Sp}(4, 2)$  and by (a) we have i) or ii). If  $U$  has just one irreducible submodule of dimension 3, then  $H \leq L \times \mathrm{GL}(2, 2)$  where  $L$  is a maximal

solvable completely reducible subgroup of  $\mathrm{GL}(3, 2)$ . Thus,  $L \simeq \Gamma(2^3)$  and hence we have iii). If  $U = U_1 \oplus U_2$  with  $U_i$  irreducible submodules of dimension 3, then the  $U_i$  are both totally isotropic and by Lemma 2.3,  $C_H(U_1) = C_H(U_2)$ . Hence  $H \lesssim \Gamma(2^3) \leq \mathrm{GL}(3, 2)$  and iii) follows. If all irreducible submodules of  $H$  are at most 2-dimensional, then  $H \leq (\mathrm{GL}(2, 2))^3$ , hence i) follows.

Assume now that  $H$  is irreducible and imprimitive. If the blocks of  $H$  are 2-dimensional, then  $H \leq H_1 = \mathrm{GL}(2, 2) \wr S_3$ . With  $N_1 = O_3(H_1)$ , we have  $U \rtimes N_1 \simeq (A_4)^3$  and we have i). If the blocks are 3-dimensional, then they are totally isotropic (as the space generated by their radicals is  $H$ -invariant) and again they have the same centralizer in  $H$ . It follows that  $H \lesssim \Gamma(2^3).S_2$ , hence we have iii).

Suppose finally that  $H$  is primitive. Then, in the notation of Lemma 2.1,  $e(H) = 1$  or  $e(H) = 3$ . If  $e(H) = 1$ , then  $H \leq \Gamma(2^6)$  and, as  $\mathrm{Sp}(6, 2)$  has no element of order 21, we have i) or iii). If  $e(H) = 3$ , then  $H \leq H_1$  where  $H_1$  is the (unique up to conjugation) maximal primitive solvable subgroup of  $\mathrm{GL}(6, 2)$  with  $N_1 = \mathrm{F}(H_1)$  extraspecial of order  $3^3$ . One checks that  $H_1/N_1 \simeq \mathrm{GL}(2, 3)$ . As  $N_1 \leq \mathrm{SL}(3, 2^2)$ , the non-central elements in  $N_1$  have centralizers of order  $2^2$  in  $U$ . Hence  $U \rtimes N_1$  has  $2 \cdot 2^6 + 24 \cdot 2^4 = 512$  elements of order 3 and i) follows.

Observe that in any case  $R/K$  has at most 23 prime order subgroups, since either  $|R/K| \leq 16$  or  $R/K \lesssim \mathrm{GL}(2, 3)$  or  $S_2 \wr S_3$ .

(c): Assume that  $|U| = 2^8$  and that  $H$  fixes no totally isotropic subspace of  $U$ . Observe that  $U$  has no irreducible submodule of odd dimension. If  $U$  is reducible and one irreducible submodule of  $U$  has dimension 6, then  $H \leq L \times \mathrm{GL}(2, 2)$ , where  $L$  is an irreducible solvable subgroup of  $\mathrm{Sp}(6, 2)$ . By (b) (and the last paragraph in its proof), we get (c).

If the submodules of  $U$  are at most 4-dimensional, then  $H \leq \mathrm{Sp}(4, 2) \times \mathrm{Sp}(4, 2)$  and we are done by (a).

Assume now that  $U$  is irreducible and imprimitive. If the minimal blocks have dimension 2, then  $H \leq H_1 = \mathrm{GL}(2, 2) \wr S_4$ . Thus for  $N_1 = O_3(H_1)$  we have  $U \rtimes N_1 \simeq (A_4)^4$ , so  $\nu_2(U \rtimes N_1) = 3280$  and  $H_1/N_1 \simeq S_2 \wr S_4$ . If the minimal blocks are 4-dimensional, they are either both totally isotropic or both nonsingular. In the first case, the centralizer of one of them centralizes also the other and  $H \leq \Gamma(2^4).C_2$ . In the latter case,  $H \leq \Gamma(2^4) \wr S_2$  and, recalling that  $\mathrm{Sp}(4, 2)$  has no element of order 21, (c) follows.

Finally, if  $H$  is primitive, then  $H \leq H_1 \simeq \Gamma(2^8)$ . For  $N_1 = \mathrm{F}(H_1)$ ,  $|H_1 : N_1| = 8$  and  $\nu(U \rtimes N_1) \leq 2^8 3$ .

(d): Let  $|U| = 3^6$ . Assume first that  $H = R/U$  is reducible. Note that there is no irreducible  $H$ -submodule of  $U$  of dimension 5. If there is a 4-dimensional irreducible submodule, then  $H \leq \mathrm{Sp}(4, 3) \times \mathrm{GL}(2, 3)$  and, recalling the remark at the end of the proof of Lemma 3.2, there is a 2-group  $N \trianglelefteq H$  such that  $n_2(N) \leq 23$  and  $|H : N| \leq 48 \cdot 6 = 288$ . If there is a 3-dimensional irreducible  $H$ -submodule  $U_1$ , then  $U_1$  is totally isotropic. If  $U = U_1 \oplus U_2$  with  $U_2$  a totally isotropic  $H$ -module, then by Lemma 2.3,  $H \lesssim \mathrm{GL}(3, 3)$ . Otherwise,  $H \lesssim \mathrm{GL}(3, 3) \times \mathrm{Sp}(2, 3) \times \mathrm{GL}(1, 3)$ . Observe that if  $T$  is a completely reducible solvable subgroup of  $\mathrm{GL}(3, 3)$ , then  $T$  is either isomorphic to a subgroup of  $\mathrm{GL}(2, 3) \times \mathrm{GL}(1, 3)$  (if  $T$  is reducible), or  $\mathrm{GL}(1, 3) \wr S_3$  (if  $T$  is irreducible and imprimitive), or  $\Gamma(3^3)$  (if  $T$  is primitive). In all cases there is a 2-subgroup  $M \trianglelefteq T$  with  $n_2(M) \leq 7$  and  $|T : M| \leq 39$ . So it follows that if  $U$  has a 3-dimensional submodule, then there is a 2-group  $N \trianglelefteq H$



with  $n_2(N) \leq 31$  and  $|H : N| \leq 117$ . If the irreducible  $H$ -submodules of  $U$  are at most 2-dimensional, then  $H \leq (\text{GL}(2, 3))^3$  and hence there exists a 2-subgroup  $N \trianglelefteq H$  with  $|H : N| \leq 216$  and  $n_2(N) \leq 7$ .

Let us assume that  $H$  is irreducible and imprimitive. If  $H$  has blocks of dimension 1, then we can assume  $H \simeq \text{GL}(1, 3) \wr S_6$ . Since the solvable subgroups of  $S_6$  have order at most 72, taking as  $N$  the base group of  $H$  we have  $n_2(N) = 63$  and  $|H : N| \leq 72$ . If  $H$  has 2-dimensional minimal blocks, then we can assume  $H \simeq \text{GL}(2, 3) \wr S_3$ , and by taking  $N = O_2(H)$  we have  $n_2(N) = 7$  and  $|H : N| = 2^4 3^4 = 1296$ . Finally, if  $H$  has minimal blocks of dimension 3, then by Lemma 2.3,  $H \leq \text{GL}(3, 3).C_2$  and hence there is a 2-group  $N \trianglelefteq H$  with  $n_2(N) \leq 31$  and  $|H : N| \leq 234$ .

If  $H$  is primitive, then  $H \lesssim \Gamma(3^6)$  (if  $e(H) = 1$ ) or  $H \lesssim (C_{26} \rtimes Q_8).\text{Sp}(2, 2).C_3$  (if  $e(H) = 2$ ). In both cases there is a 2-subgroup  $N \trianglelefteq H$  with  $n_2(N) = 1$  and  $|H : N| \leq 546$ .

Therefore, in any case there is a  $K \trianglelefteq R$  with  $K/U$  a 2-group,  $|R : K| \leq 1296$  and  $\nu_2(K) \leq 63 \cdot 3^6$ .  $\square$

We now come to our main result about primitive solvable linear groups. We observe that the condition about multiplicities of regular orbits is needed for handling the imprimitive case. We also remark that in the proof of the following result, some small primitive groups have been checked by constructing them in the algebra computer system [GAP].

**Theorem 3.4.** *Let  $G$  be a solvable primitive subgroup of  $\text{GL}(d, p)$ ,  $p$  a prime,  $d$  a positive integer, and let  $V$  be the natural module for  $G$ . Then  $G$  has at least  $p$  regular orbits on  $V \oplus V$  or  $G$  is one of the following groups:*

- (1)  $\text{GL}(2, 2)$ ;
- (2)  $\text{SL}(2, 3)$  or  $\text{GL}(2, 3)$ ;
- (3)  $3^{1+2}.\text{SL}(2, 3)$  or  $3^{1+2}.\text{GL}(2, 3) \leq \text{GL}(6, 2)$ ;
- (4)  $(Q_8 \rtimes Q_8)H \leq \text{GL}(4, 3)$  where  $H$  is isomorphic to a subgroup of index 1, 2 or 4 of  $\text{O}^+(4, 2)$ .

*Proof.* We prove that if  $G$  is not one of the groups in (1)–(4), then  $G$  satisfies the following property:

(P) there is an element  $v \in V$  such that  $C_G(v)$  has at least  $p$  regular orbits on  $V$ .

Observe that we can assume that  $G$  is a maximal primitive solvable subgroup of  $\text{GL}(d, p)$ . We adopt the notation of Lemma 2.1.

Assume first that  $e = e(G) = 1$ .

Then  $G = \Gamma(p^d)$  and for any  $0 \neq v \in V$ ,  $|C_G(v)| = d$ . We can hence assume that  $C_G(v)$  is the Galois group of  $V = GF(p^d)$ . So the elements of  $V$  that do not belong to a regular orbit of  $C_G(v)$  are in the union of the subfields  $GF(p^{d/m})$ ,  $m$  varying among the prime divisors of  $d$ . Since the (distinct) prime divisors of  $d$  are at most  $\log_2(d)$ , it is enough to prove that  $f(p, d) = p^d - \log_2(d)p^{d/2} - dp$  is nonnegative. It is easily checked that  $f(3, d) \geq 0$  for all integers  $d \geq 1$  so, as  $f(p, d)$  is increasing in  $p$ ,  $f(p, d) \geq 0$  for all  $p \geq 3$ ,  $d \geq 1$ . Further,  $f(2, d) \geq 0$  for all  $d \geq 4$ . Thus we are left with the cases  $p^d = 2^i$ ,  $i = 1, 2, 3$ .  $\Gamma(2)$  and  $\Gamma(2^3)$  verify (P), while  $\Gamma(2^2) = \text{GL}(2, 2)$  is the exceptional case in (1).

Therefore, in the following we can assume  $e \geq 2$ .

To find a vector  $v$  as in (P), we are going to look for a regular orbit of the subgroup  $K = F_2(C)$ . If  $X$  is a subgroup of prime order of  $K$ , then  $|C_V(X)| = 1$  if  $X \leq A$  and  $|C_V(X)| \leq |V|^{2/3}$  in any case by 2.4(4). Further, if  $p^a - 1$  is a power of 2, then by Lemma 2.1(3) and (4),  $|K/F|$  is odd and by Lemma 2.4(4),  $|C_V(X)| \leq |V|^{1/2}$ . Let  $\mathcal{X}$  be the set of all subgroups of prime order of  $K$  which do not lie in  $A$ . Applying Lemma 2.7 to the symplectic  $K/F$ -module  $F/A$ , by Lemma 3.1(b) it follows that

$$|\mathcal{X}| \leq \sum_{q \in \pi(K)} \frac{q}{q-1} n_q(K/A) \leq 2|K/A| = 2|K/F||F/A| \leq |F/A|^{\gamma+1} = e^{2(\gamma+1)}$$

where  $\gamma = \log_4(6)$ . Hence  $K$  certainly has a regular orbit on  $V$  if  $|V| - |\mathcal{X}||V|^k > 0$ , where  $k = 1/2$  if  $p^a - 1$  is a power of 2 and  $k = 2/3$  otherwise. Taking logarithms, we consider the function

$$f_k(p, e, a) = (1 - k)ea - c \log_p(e)$$

where  $k = 1/2, 2/3$  and  $c = 2(\gamma + 1) \leq 4.585$ , in the domain  $p \geq 2, e \geq 2$  and  $a \geq 1$ . Note also that if  $p = 2$ , then  $a \neq 1$ .

One checks, for both values of  $k$ , that  $f_k$  is increasing in  $p$  and  $a$ , and it is increasing in  $e$  when  $ea \geq 13$ . Therefore, evaluating  $f_k$  at suitable points, it follows that:

$a = 1$ ):  $f_{2/3}(p, e, 1) > 0$  for  $e \geq 22, p \geq 7$ ,  $f_{1/2}(5, e, 1) > 0$  for  $e \geq 16$ ,  $f_{1/2}(3, e, 1) > 0$  for  $e \geq 28$ ;

$a = 2$ ):  $f_{2/3}(p, e, 2) > 0$  for  $e \geq 10, p \geq 5$ ,  $f_{2/3}(2, e, 2) > 0$  for  $e \geq 36$ ,  $f_{1/2}(3, e, 2) > 0$  for  $e \geq 10$ ;

$a = 3$ ):  $f_{2/3}(p, e, 3) > 0$  for  $e \geq 4, p \geq 5$ ,  $f_{2/3}(3, e, 3) > 0$  for  $e \geq 10$ ,  $f_{2/3}(2, e, 3) > 0$  for  $e \geq 20$ ;

$a = 4$ ):  $f_{2/3}(p, e, 4) > 0$  for  $e \geq 2, p \geq 5$ ,  $f_{2/3}(3, e, 4) > 0$  for  $e \geq 6$ ,  $f_{2/3}(2, e, 4) > 0$  for  $e \geq 13$ ;

and that  $f_{2/3}(p, e, a) > 0$  for all  $p \geq 3, e \geq 2, a \geq 5$ , while  $f_{2/3}(2, e, 5) > 0$  for  $e \geq 9$ ,  $f_{2/3}(2, e, 6) > 0$  for  $e \geq 6$ ,  $f_{2/3}(2, e, 7) > 0$  for  $e \geq 4$  and  $f_{2/3}(2, e, a) > 0$  for all  $e \geq 3$  when  $a \geq 8$ . Observe that if  $e = 20$ , then  $p \geq 11$  and  $f_{2/3}(11, 20, 1) > 0$ . If  $e = 21$ , then  $p \geq 43$  and  $f_{2/3}(43, 21, 1) > 0$ .

Therefore, recalling that each prime divisor of  $e$  divides  $p^a - 1$ , there exist an element  $v \in V$  such that  $C_G(v) \cap K = 1$ , or we are in one of the following cases:

TABLE 1

- (1)  $a = 1$ :  $e \leq 19$  for  $p \geq 7$ ,  $e = 2^i$  ( $1 \leq i \leq 4$ ) for  $p = 3, 5$ ;
- (2)  $a = 2$ :  $e \leq 9$  for  $p \geq 3$ ,  $e = 3^i$  ( $1 \leq i \leq 3$ ) for  $p = 2$ ;
- (3)  $a = 3$ :  $e \leq 3$  for  $p \geq 5$ ,  $e = 2^i$  ( $1 \leq i \leq 3$ ) for  $p = 3$ ,  $e = 7$  for  $p = 2$ ;
- (4)  $a = 4$ :  $e \leq 5$  for  $p = 3$ ,  $e = 3, 5, 9$  for  $p = 2$ ;
- (5)  $a = 6$ ,  $e = 3, p = 2$ .

Therefore, except for the cases in Table 1,  $|C_G(v)| \leq |G/K| \leq a|C/K| \leq a|F/A|^\beta/\lambda = ae^{2\beta}/\lambda$  where  $\beta$  and  $\lambda$  are as in Lemma 2.5. As  $|C_V(S)| \leq |V|^{3/4}$  for every prime order subgroup  $S$  of  $D = C_G(v)$ , to prove (P) it is enough to show that  $|V| - |D||V|^{3/4} \geq p|D|$  or equivalently that  $p^{ea} \geq \frac{a}{\lambda}e^{2\beta} \left( p^{\frac{3}{4}ea} + p \right)$ . We observe

that  $p^{\frac{3}{4}ea + \frac{1}{6}} \geq p^{\frac{3}{4}ea} + p$  for  $ea \geq 6$ , so taking logarithms it is enough to study the positivity of the function

$$h(p, e, a) = \frac{1}{4}ea - 2\beta \log_p(e) - \log_p(a) + \log_p(\lambda) - \frac{1}{6}$$

for  $p \geq 2$ ,  $e \geq 2$ ,  $a \geq 1$ .

One checks that  $h(p, e, a)$  is increasing in  $p$ ,  $e$  and  $a$  when  $ea \geq 10$  and that  $h(p, e, a) > 0$  with the exceptions mentioned in Table 1 and also  $(p, e, a) = (3, 28, 1)$  and  $(p, e, a) = (3, 10, 2)$ . But if  $(p, a) = (3, 1)$  or  $(3, 2)$ , then  $e$  is a power of 2.

Therefore, we are just left with the cases in Table 1 to check.

$e$  prime:

Assume first  $e \geq 5$ . By Lemma 2.1(4),  $C/F$  is an irreducible subgroup of  $\text{Sp}(2, e) = \text{SL}(2, e)$ . Hence  $|C/F|$  divides  $e^2 - 1$ , and there exists a nilpotent normal subgroup  $K/F$  of  $C/F$  such that  $|C : K|$  divides 6 and  $K/F$  has at most one subgroup of order  $q$  for each prime  $q$  (see for instance [15, pp. 165–166] or [10, Theorem 2.11]). We therefore have  $\nu_e(K) = e(e+1)$  and by Lemma 3.1b),  $\nu_2(K) \leq 2e^2$  and  $\nu_q(K) \leq e^2 q \leq e^2 \frac{e+1}{2}$  for each prime divisor  $q \neq 2$  of  $|K/F|$ . Since the odd prime divisors of  $|K/F|$  are at most  $\frac{e-1}{2} + \frac{e+1}{2} = e$ ,  $K$  has at most  $e^3 \left(\frac{e+1}{2}\right) + e(e+1)$  subgroups  $S$  of odd prime order. Observe also that, by Lemma 2.4(4),  $|C_V(S)| \leq |V|^{1/2}$ . Further, by Lemma 2.4(3),  $|C_V(x)| \leq |V|^{3/5}$  for each involution  $x \in K$ . Observe that  $e \geq 5$  divides  $p^a - 1$ , so  $p^a = 8$  or  $p^a \geq 11$ . We show that  $K$  has a regular orbit on  $V$ , by considering the function

$$f(x, e) = x^e - 2e^2 x^{\frac{3}{5}e} - \left(e^3 \left(\frac{e+1}{2}\right) + e(e+1)\right) x^{\frac{1}{2}e}.$$

One checks that  $f(x, e)$  is increasing in  $x$  for  $x = p^a \geq 11$  and that  $f(11, e) > 0$  for  $e \geq 7$ .

For  $e = 5$  or  $e = 7$ , observe that the only odd prime divisor of  $e^2 - 1$  is 3. Thus  $\nu_2(K) = \nu_3(K) + \nu_e(K) \leq 3 \cdot e^2 + e(e+1)$  and again  $K$  has a regular orbit on  $V$ .

Thus for  $e \geq 5$  there is a  $v \in V$  such that  $|C_G(v)| \leq |G : K| \leq 6a$ . Since  $p^{ea} - 6 \cdot a \left(p^{\frac{3}{4}ea} + p\right) > 0$  for  $p^a \geq 11$ ,  $e \geq 5$  and  $p^a = 8$ ,  $e = 7$  we are done for  $e$  prime,  $e \neq 2, 3$ .

Assume  $e = 2$ . Note that hence  $p \geq 3$  and then by Lemma 2.1(2) and Lemma 2.4 each nontrivial element in  $G$  centralizes at most  $p^a$  elements of  $V$ .

Let  $L$  be the normalizer in  $C$  of a Sylow 3-subgroup of  $C$ . Then  $|C : L| = 4$  and in  $L$  there are at most 9 subgroups of prime order not contained in  $A$  (namely at most 6 involutions and at most 3 subgroups of order 3). Therefore,  $L$  has a regular orbit on  $V$  for all  $p^a \geq 9$ ; that is, there exists a  $v \in V$  such that  $|C_G(v)| \leq |G : L| = 4a$ . Since  $p^{2a} - 1 - (4a - 1)(p^a - 1) - 4ap > 0$  for  $p^a \geq 9$ , we are left with the cases  $p^a = 3, 5, 7$  to check.

If  $p^a = 3$ , then  $G$  is a subgroup of  $\text{GL}(2, 3)$  that contains the normal quaternion subgroup of  $\text{GL}(2, 3)$ . Thus  $G$  is either contained in a Sylow 2-subgroup of  $\text{GL}(2, 3)$  and hence it satisfies (P), or  $G$  contains  $\text{SL}(2, 3)$  and we have the exceptional cases in (2).

Assume now  $a = 1$ ,  $p = 5, 7$  and let  $H = G \cap \text{SL}(2, p)$ . Observe that  $H$  acts fixed point freely on  $V$ , since an element  $x \in \text{SL}(2, p)$  has 1 as an eigenvalue only if  $p$  divides  $|x|$ . Therefore,  $C_G(v) \cap H = 1$  for any  $1 \neq v \in V$  and hence  $C_G(v)$  is isomorphic to a subgroup of the cyclic group  $G/H$ . Observe that  $|G : H| = 4$

if  $p = 5$ . If  $p = 7$ , then  $|G : H| = 3$  since  $G$  is the normalizer in  $\mathrm{GL}(2, 7)$  of a subgroup  $E \simeq Q_8$  and  $E$  is normal in a Sylow 2-subgroup of  $\mathrm{SL}(2, 7)$ . Thus  $C_G(v)$  has just one subgroup of prime order and hence it has at least  $(p^2 - p)/(p - 1) = p$  regular orbits on  $V$ .

Assume finally  $e = 3$ . First let  $a = 1$ , so that  $G = C \leq \mathrm{GL}(3, p)$  and  $p \geq 7$ . Define  $H = (K \cap \mathrm{SL}(3, p))B$ , where  $K = \mathrm{F}_2(C)$  and  $B$  is the 2-complement of  $A$ . Note that  $H$  is metanilpotent. Further,  $G/H$  is a cyclic  $\{2, 3\}$ -group, since  $G/K$  is cyclic of order 3 and  $K = (K \cap \mathrm{SL}(3, p))A$  (since  $F \leq (K \cap \mathrm{SL}(3, p))A$ , so 3 does not divide  $|K : (K \cap \mathrm{SL}(3, p))A|$  and  $|(K \cap \mathrm{SL}(3, p))A : K \cap \mathrm{SL}(3, p)| = |A : A \cap \mathrm{SL}(3, p)| = \frac{p-1}{3}$ ), and hence  $K/H$  is a cyclic 2-group. The Sylow 2-subgroups of  $H$  are quaternion groups, so  $\nu_2(H) = 9$ , and if  $x \in H$  is an involution,  $\dim(C_V(x)) \leq 1$  as 1 cannot be a double eigenvalue of  $x$ . Also,  $\nu_3(H) = 12$ . As  $p^3 - 1 - (9 + 12)(p - 1) > 0$ , there is a  $v \in V$  such that  $D = C_G(v)$  is a cyclic  $\{2, 3\}$ -group and  $|D| \leq 3(p - 1)$ .  $D$  has at most two subgroups of prime order and  $p^3 - 2p^2 - 3(p - 1)p > 0$  for all  $p \geq 7$ , so  $D$  has at least  $p$  regular orbits on  $V$ .

Assume now  $a \geq 2$ . As  $C/F \leq \mathrm{Sp}(2, 3)$ ,  $K = \mathrm{F}_2(C)$  has at most 9 involutions if  $p = 2$  and at most 18 involutions otherwise. Also,  $\nu_3(K) = 12$ . One checks that  $y^3 - 18y^2 - 12y > 0$  for all  $y = p^a$  with  $p$  odd (recall that  $p \neq 3$ ) and that  $y^3 - 9y^2 - 12y > 0$  if  $y = 2^a$  with  $a \geq 4$ . So for  $a \geq 2$ ,  $p$  odd or  $a \geq 4$ , there exists a  $v \in V$  such that  $|C_G(v)| \leq |G/K| \leq 3a$ . Hence (P) holds for  $a \geq 2$ ,  $p$  odd or  $a \geq 4$ , since in this case  $p^{3a} - 3a(p^{2a} + p) > 0$ . By Lemma 2.1(3), we are hence left with the case  $p = a = 2$ , which gives the exceptional group  $G_0 \simeq 3^{1+2}.\mathrm{GL}(2, 3)$ . It is not difficult to check that the only proper primitive subgroup of  $G_0$  that does not satisfy (P) is  $3^{1+2}.\mathrm{SL}(2, 3)$ .

$e = 4$ :

The central products  $D_8 \wr D_8$ ,  $D_8 \wr Q_8$  and  $D_8 \wr D_8 \wr C_4$  have respectively 18, 10 and 30 noncentral involutions. By Lemma 3.3(a), there is a normal subgroup  $K$  of  $C$  such that  $K/F$  is a nilpotent 3- or 5-group, and by Lemma 3.1b),  $\nu_2(K) \leq 40$  if 3 and 5 do not divide  $p^a - 1$ ,  $\nu_2(K) \leq 80$  if  $3 \nmid p^a - 1$  and  $\nu_2(K) \leq 120$  otherwise. We have that  $x^4 - 1 - \nu(K)(x^2 - 1) > 0$  for  $x = p^a \geq 9$  if  $3, 5 \nmid p^a - 1$ , for  $x \geq 11$  if  $3 \nmid p^a - 1$  and for  $x \geq 12$  otherwise. Hence, if  $p^a \neq 3, 5, 7$  there is a  $v \in V$  such that  $|C_G(v)| \leq |G/K| \leq 8a$ . Using Lemma 2.4 and recalling that here  $p$  is odd, (P) follows by checking that  $p^{4a} - 7(p^{3a} - 1) - 8(a - 1)(p^{2a} - 1) - 8ap$  is positive for  $p^a \geq 9$ .

The cases  $p^a = 5$  and  $p^a = 7$  are done using [GAP]: one checks that the normalizer in  $\mathrm{GL}(4, p)$  of an extraspecial subgroup of order  $p^3$  (there are two conjugacy classes of such groups when  $p = 7$  and just one if  $p = 5$ ) verifies (P).

Assume finally  $p = 3$  and  $a = 1$ . In  $\mathrm{GL}(4, 3)$  there are two conjugacy classes of maximal primitive solvable subgroups with  $e = 4$ :  $G_0 \simeq (D_8 \wr Q_8).H$  with  $H$  a Frobenius group of order 20 and  $G_1 \simeq (Q_8 \wr Q_8).O^+(4, 2)$  (see for instance [14, §8.1]). Using [GAP] one checks that (P) holds for  $G_0$  but not for  $G_1$ . By [14, Thm. 8.3.1] there is an epimorphism  $\varphi : W \rightarrow G_1$  where  $W = \mathrm{GL}(2, 3) \wr S_2$  and  $\mathrm{Ker}(\varphi) = Z(W)$  has order 2. The primitive subgroups  $G \leq G_1$  with  $e = e(G) = 4$  are the  $\varphi(M)$  where  $M$  contains the subgroup  $\mathrm{SL}(2, 3) \times \mathrm{SL}(2, 3)$  of the base group. It is not difficult to check (with [GAP]) that the groups  $G = \varphi(M)$  do not satisfy (P) (precisely, no centralizer has regular orbits) when  $M \not\leq \mathrm{GL}(2, 3) \times \mathrm{SL}(2, 3)$  or  $M \not\leq \mathrm{SL}(2, 3) \times \mathrm{GL}(2, 3)$  (in these cases (P) holds: each centralizer has three regular orbits).

$e = 6$ :

In this case  $p \geq 7$  and by [15, Thm. 20.13],  $C$  is a subgroup of the central product  $N_1 \vee N_2$ , where  $N_1/A \simeq S_4$  and  $N_2/A$  is (isomorphic to) the semidirect product of  $\mathrm{SL}(2, 3)$  and its natural module. Since  $C/A \simeq N_1/A \times N_2/A$ , by Lemma 3.1 it follows that there is a  $K \trianglelefteq C$  with  $K/F$  nilpotent and  $|C : K| \leq 6$  such that  $\nu_2(K) \leq 78$  and  $\nu_3(K) \leq 120$ . As  $x^6 - 78x^4 - 120x^3 > 0$  for  $x \geq 11$ , by Lemma 2.4(4),  $K$  has a regular orbit on  $V$  for all  $p^a \neq 7$ . If  $p^a = 7$ , by Lemma 2.1(6),  $G$  is (linearly) isomorphic to a central product  $G_1 \vee G_2$  where  $G_1$  is the (unique up to conjugation) maximal primitive subgroup of  $\mathrm{GL}(2, 7)$  with  $e(G_1) = 2$  and  $G_2$  is the maximal primitive subgroup of  $\mathrm{GL}(3, 7)$  with  $e(G_2) = 3$ . One checks that  $G_1 \vee G_2$  has just 18 noncentral involutions. Since  $7^6 - 18 \cdot 7^4 - 120 \cdot 7^3 > 0$  the subgroup  $K = F_2(G)$  has a regular orbit on  $V$ .

Since  $p^{6a} - 6ap^{6a\frac{3}{4}} - 6ap > 0$  for all  $p \geq 7$ ,  $a \geq 1$ , (P) holds when  $e = 6$ .

$e = 8$ :

By Proposition 3.3(b), there is a normal subgroup  $K$  of  $C$  such that  $K/F$  is nilpotent,  $|C/K| \leq 48$ ,  $C/K$  has at most 23 prime order subgroups and  $\nu_2(K) \leq 452$  if  $3 \nmid |A| = p^a - 1$  and  $\nu_2(K) \leq 1092$  otherwise. The central product  $D_8 \vee D_8 \vee D_8 \vee C_4$  has 126 noncentral involutions; hence  $\nu(K) \leq 1218$  if  $p \equiv 1 \pmod{3}$  and  $\nu(K) \leq 578$  otherwise. Since  $p^{8a} - 1218p^{4a} > 0$  for  $p^a \geq 7$  and  $5^8 - 578 \cdot 5^4 > 0$ , then by Lemma 2.4(4), when  $p^a \neq 3$  there is a  $v \in V$  such that  $C_G(v) \cap K = 1$ . Hence  $C_G(v)$  has at least  $p$  regular orbits on  $V$ , as  $p^{8a} - 23p^{6a} - 48a(p^{4a} + p) > 0$  for all  $p^a \neq 3$ .

We check the case  $p = 3$ ,  $a = 1$  by [GAP]. The Fitting subgroup  $F$  of  $G$  is isomorphic either to  $E_1 = D_8 \vee D_8 \vee D_8$  or  $E_2 = D_8 \vee D_8 \vee Q_8$ . We consider  $E_1, E_2$  as subgroups of  $\mathrm{GL}(8, 3)$  (using for instance the method in [14, p. 19]). By Lemma 2.1(5) we can assume that, up to conjugation in  $\mathrm{GL}(8, 3)$ ,  $F = E_1$  or  $F = E_2$ .

If  $F = E_1$ , then  $G \leq L = N_{\mathrm{GL}(8, 3)}(E_1)$  and  $H = G/F$  is a maximal ([14, 2.5.34]) solvable completely reducible subgroup of  $L/F \simeq \mathrm{O}^+(6, 2)$  ([14, 2.4.12]). As  $|\mathrm{O}^+(6, 2)| = 2^7 \cdot 3^2 \cdot 5 \cdot 7$  and  $O_2(H) = 1$ , then  $O_q(H) \neq 1$  for some  $q \in \{3, 5, 7\}$ . Choose for  $q \in \{3, 5, 7\}$  a Sylow  $q$ -subgroup  $T_q$  of  $L$  and let  $G_q = N_L(FT_q)$ . If  $O_{3'}(H) \neq 1$ , then up to conjugation  $G \leq G_5$  or  $G \leq G_7$ . If  $O_{3'}(H) = 1$ , then  $|O_3(H)| > 3$  by the maximality of  $H$  and hence up to conjugation  $G \leq G_3$ . One now checks by [GAP] that there is a  $v \in V$  such that  $C_{G_q}(v)$  has at least three regular orbits on  $V$ , for  $q = 3, 5, 7$ .

Assume now  $F = E_2$ . Then  $G \leq M = N_{\mathrm{GL}(8, 3)}(E_2)$  and  $H = G/F$  is a maximal solvable completely reducible subgroup of  $M/F \simeq \mathrm{O}^-(6, 2)$ . Recall that  $|\mathrm{O}^-(6, 2)| = 2^7 \cdot 3^4 \cdot 5$ . If  $O_5(H) \neq 1$ , then (up to conjugacy)  $G \leq G_5 = N_M(FT_5)$  where  $T_5$  is a Sylow 5-subgroup of  $M$ . One checks by [GAP] that  $G_5$  satisfies (P). So we can assume  $F(H) = O_3(H)$ . Observe that  $|O_3(H)| \geq 3^2$ . Let  $T_3$  be a Sylow 3-subgroup of  $M$ . One checks by [GAP] that  $N_M(FS)$  verifies (P), for each representative  $S$  of the conjugacy classes of subgroups of  $T_3$  with  $|S| \geq 3^2$ .

$e = 9$ :

In this case  $C/F \leq \mathrm{Sp}(U) \simeq \mathrm{Sp}(4, 3)$ , where  $U = F/A$ . Let  $x$  be an involution of  $\mathrm{Sp}(4, 3)$ . If all eigenvalues of  $x$  are  $-1$ , then  $x$  must be the central involution  $z$  of  $\mathrm{Sp}(4, 3)$ . So if  $x \neq z$ , then  $C_U(x) \neq 0$  and by Lemma 2.2, it follows that  $|C_U(x)| = 3^2$ . Further, by Lemma 3.2, there is an  $N \leq C$  with  $F \leq N$ ,  $N/F$  a 2-group with at most 3 involutions and  $|C : N| \leq 48$ . Assume first  $p \neq 2$ . Observe

that  $\nu_3(N) = \nu_2(N) \leq 2(3^4 + 2 \cdot 3^2) = 198$  and that  $\nu_3(N) = 120$ . Since  $p^a \geq 7$  and  $x^9 - 198x^6 - 120x^3 > 0$  for  $x \geq 7$ , it follows that  $N$  has a regular orbit on  $V$ .

For  $p = 2$  we need a slightly sharper counting. In this case  $p^a \geq 4$  and  $|A|$  is odd. Let  $T$  be a Sylow 2-subgroup of  $N$ . Then  $T \simeq N/F$  and by the previous observation there is at most a  $z \in T$  such that  $|[z, F]| = 3^5$ . Observe that by Lemma 2.4(3) any of the 81 involutions that are conjugate to  $z$  in  $N$  centralizes at most  $p^{a \cdot 5}$  elements of  $V$ . Further, in  $N$  there are at most  $3 \cdot 3^2$  involutions not conjugate to  $z$  and each one of them by Lemma 2.4(4) centralizes at most  $p^{a \cdot 6}$  elements of  $V$ . Since  $x^9 - 81x^5 - 27x^6 - 120x^3 > 0$  for all  $x \geq 4$ , we have again that, for all  $p \geq 2$ , there exists a  $v \in V$  such that  $C_G(v) \cap N = 1$ .

It follows that  $|C_C(v)| \leq |C : N| \leq 48$ . By Lemma 2.4(5),  $|C_V(x)| \leq p^{a6}$  if  $x \in C$  and  $|C_V(x)| \leq p^{a9/2}$  if  $x \notin C$ . Since  $p^{a9} - 48p^{a6} - (a-1)48p^{a9/2} - 48ap > 0$  for all  $p \geq 7$  if  $a = 1$  and for all  $p \geq 2$  if  $a = 2$ , we are done.

$e = 10$ :

By Table 1, we are left with the case  $a = 1$ . By Lemma 2.1(6),  $G = G_1 \vee G_2$  where  $G_1$  (resp.  $G_2$ ) is isomorphic to primitive maximal soluble subgroups of  $\text{GL}(2, p)$  (resp.  $\text{GL}(5, p)$ ) with  $e_1 = e(G_1) = 2$  (resp.  $e_2 = e(G_2) = 5$ ). Let  $K = F_2(G)$ . Then  $K/A$  is the direct product of a group isomorphic to the alternating group  $A_4$  and an extension of a completely reducible nilpotent subgroup of  $\text{SL}(2, 5)$  by the natural module. Thus  $\pi(K/A) = \{2, 3, 5\}$  and, as the Sylow 2-subgroups of  $\text{SL}(2, 5)$  are quaternion groups and the Sylow 3-subgroups are cyclic, by Lemma 3.1a),  $n_2(K/A) \leq 4(5^2 + 1) - 1 = 103$ ,  $n_3(K/A) \leq 8 \cdot 50 + 50 + 8 = 458$ ,  $n_5(K/A) = 24$ . By Lemma 3.1(b), it follows that  $\nu_2(K) \leq 206$ ,  $\nu_3(K) \leq 687$  and  $\nu_5(K) \leq 30$ .

Observe now that  $p \geq 11$ . Therefore, as  $11^{10} - (206 + 687 + 30)11^{2/3} > 0$  there is a  $v \in V$  such that  $C_K(v) = 1$  and hence  $|C_G(v)| \leq |G : K| = |G_1 : F_2(G_1)||G_2 : F_2(G_2)| \leq 2 \cdot 6$  by Lemma 2.1(7). Since  $p^{10} - 12p^{10 \cdot 3/4} - 12p > 0$  for all  $p \geq 11$ , we have (P).

$e = 12$ :

We can again consider just the case  $a = 1$ . By Lemma 2.1(6) and (7),  $G$  is the central product of groups  $G_1 \simeq (C_{p-1} \vee E_1) \cdot \text{SL}(2, 3)$  where  $E_1$  is extraspecial of order  $3^3$  and  $G_2 \simeq (C_{p-1} \vee E_2) \cdot D$ , with  $E_2$  extraspecial,  $|E_2| = 2^5$  and  $D$  isomorphic to either  $S_3 \wr S_2$  or a Frobenius group of order 20 (see [14, §8.1]). Let  $K = F_2(G)$ . Note that  $|G : K| \leq 3 \cdot 8$  and that  $\pi(K) \subseteq \{2, 3, 5\}$ . Using Lemma 3.1 in  $K/A = F_2(G_1)/A \times F_2(G_2)/A$ , one gets  $n_2(K/A) \leq 159$ ,  $n_3(K/A) \leq 1160$  and  $n_5(K/A) \leq 64$ . Hence  $\nu_2(K) \leq 318$ ,  $\nu_3(K) \leq 1740$  and  $\nu_5(K) \leq 80$ . Since  $p \geq 7$ , because 2 and 3 divide  $p-1$ ,  $p^{12} - (\nu_2(K) + \nu_3(K) + \nu_5(K))p^8$  is certainly positive. Thus  $K$  has a regular orbit on  $V$ . As  $p^{12} - 24p^9 - 24p$  is also positive, (P) follows.

$e = 14$ :

Again  $a = 1$  and  $G$  is the central product of groups  $G_1 \simeq (C_{p-1} \vee Q_8) \cdot \text{SL}(2, 2)$  and  $G_2 \simeq (C_{p-1} \vee E) \cdot D$ , with  $E$  extraspecial of order  $7^3$  and  $D$  a maximal irreducible soluble subgroup of  $\text{SL}(2, 7)$ . Let  $K = F_2(G)$ . Then  $\pi(K) = \{2, 3, 7\}$  and, arguing as in the case  $e = 10$ ,  $\nu_2(K) \leq 398$  (observe that a Sylow 2-subgroup of  $\text{SL}(2, 7)$  has just one involution; see for instance [7, II.8.10]),  $\nu_3(K) \leq 1335$  and  $\nu_7(K) = 56$ . Since by Lemma 2.1(3),  $p \geq 29$ , certainly  $p^{14} - (\nu_2(K) + \nu_3(K) + \nu_7(K))p^{14 \cdot 2/3} > 0$  and, as by Lemma 2.1(7),  $|G : K| \leq 12$ , (P) follows.

$e = 15$ :

Here  $a = 1$  and  $G$  is the central product of groups  $G_1 \simeq (C_{p-1} \vee E_1) \cdot \text{SL}(2, 3)$  and  $G_2 \simeq (C_{p-1} \vee E_2) \cdot D$ , where  $E_1$  and  $E_2$  are extraspecial groups of order respectively

$3^3$  and  $7^3$ , and  $D$  is a maximal irreducible soluble subgroup of  $\mathrm{SL}(2, 5)$ . Take  $K = F_2(G)$ , so that  $\pi(K) = \{2, 3, 5\}$  and, arguing as above,  $\nu_2(K) \leq 518$ ,  $\nu_3(K) \leq 687$  and  $\nu_5(K) = 30$ . Hence  $K$  has a regular orbit on  $V$  (observe that 3 and 5 divide  $p$ ) and, observing that  $|G : K| \leq 3 \cdot 6$ , (P) follows since  $p^{15} - 18p^{15 \cdot 3/4} - 18p$  is positive.

$e = 16$ :

We have only to check the case  $p = 3$ ,  $a = 1$ . By [14, 2.5.34] no isotropic subspace of  $F/A$  is fixed by  $G/F$ . Hence by Lemma 3.3(c), there is a  $K \trianglelefteq G$  such that  $K \leq F_2(G)$ ,  $\nu_2(K) = \nu_2(K/A) \leq 3280$ ,  $|G/K| \leq 2^7 3$  and  $n_2(G/K) \leq n_2(S_2 \wr S_4) = 75$ . Clearly,  $\nu_2(K) = \nu_2(F) \leq 2|F/A| = 2^9$ . By Lemma 2.4(2),(4) the subgroups of prime order of  $K$  centralize at most  $3^8$  elements. Since  $3^{16} - (3280 + 2^9)3^8 > 0$  there is a  $v \in V$  such that  $C_K(v) = 1$ , and hence  $C_G(v)$  is isomorphic to a subgroup of  $G/K$ . By Lemma 2.4(3) the  $2'$ -elements of  $C_G(v)$  centralize at most  $3^8$  elements in  $V$ . So  $C_G(v)$  has at least three regular orbits on  $V$ , as  $3^{16} - 75 \cdot 3^{12} - 2^7 3 \cdot 3^8 - 2^7 3^2 > 0$ .

$e = 18$ :

Here  $a = 1$ , so by Lemma 2.1(6) and (7),  $G$  is the central product of groups  $G_1 \simeq (C_{p-1} \wr Q_8) \cdot \mathrm{SL}(2, 2)$  and  $G_2 \simeq (C_{p-1} \wr E) \cdot D$ , with  $E$  extraspecial of order  $3^5$  and  $D$  a maximal irreducible soluble subgroup of  $\mathrm{Sp}(4, 3)$ . Working in the direct product  $G/A$  and using Lemma 3.2, it follows that there exist a  $\{2, 3\}$ -subgroup  $K$  of  $G$  such that  $\nu_2(K) \leq 2(4 \cdot 244 - 1) = 1950$ ,  $\nu_3(K) \leq \frac{3}{2}(3^2 3^4 - 1) = 1092$  and  $|G : K| \leq 96$ . Since  $p^{18} - \nu_2(K)p^{12} - \nu_3(K)p^9 > 0$  and  $p^{18} - |G : K|(p^{18 \cdot 3/4} + p) > 0$  for all  $p \geq 7$ , (P) follows.

$e = 27$ :

We have only to consider the case  $p = 2$ ,  $a = 2$ . Then  $F$  is an extraspecial group of order  $3^7$ . By Lemma 3.3(d), there is a  $K \trianglelefteq C$  with  $K/F$  a 2-group,  $|G : K| \leq 2592$  and  $\nu_2(K) \leq 3^8 7$ . Also,  $\nu_3(K) = \nu_3(F) = 1092$ . Hence  $4^{27} - \nu_2(K)4^{18} - \nu_3(K)2^{27} > 0$  and  $K$  has a regular orbit on  $V$ . As  $4^{27} - 2592(4^{27 \cdot 3/4} + 2) > 0$ , (P) holds.

The proof is finished.  $\square$

*Remark 3.5.* We have 11 conjugacy classes, in the respective  $\mathrm{GL}(d, p)$ , of primitive linear groups that have less than  $p$  regular orbits on  $V \oplus V$ , where  $V = V(d, p)$  is the natural module. Six of them are in  $\mathrm{GL}(4, 3)$ .

As an immediate consequence of Theorem 3.4, we have the following.

**Corollary 3.6.** *Let  $G$  be a solvable group and  $V$  be a finite, faithful and primitive  $G$ -module. If  $p = \mathrm{char}(V)$  does not divide  $|G|$ , then  $G$  has at least  $p$  regular orbits on  $V \oplus V$ .*

#### 4. PROOFS OF THE THEOREMS

In order to handle imprimitive linear groups, we need some information on permutation actions on subsets.

If  $G$  is a permutation group on a set  $\Omega$  and  $\Gamma \subseteq \Omega$ , we denote by  $G_\Gamma$  the (setwise) stabilizer of  $\Gamma$  in  $G$ .

**Lemma 4.1.** *Let  $G$  be a solvable permutation group on a finite set  $\Omega$ . Let  $p$  be a prime that does not divide  $|G|$  and  $q = \min\{p, 5\}$ . Then there exist  $\Gamma_1, \Gamma_2, \dots, \Gamma_q$  disjoint subsets of  $\Omega$  such that  $\Omega = \Gamma_1 \cup \Gamma_2 \cup \dots \cup \Gamma_q$  and*

$$\bigcap_{i=1}^q G_{\Gamma_i} = 1.$$

*Proof.* Observe that we do not require that the sets  $\Gamma_i$  are all nonempty. Thus, we can assume that  $p$  is the smallest prime that does not divide  $|G|$ .

If  $|G|$  is odd, then by [5, Corollary 1] (see also [11] for an alternative proof)  $G$  has a regular orbit on  $\Omega$ ; i.e. there exists  $\Gamma \subseteq \Omega$  such that  $G_\Gamma = 1$ .

If 3 does not divide  $|G|$ , the claim follows by [2, Lemma 1a) and Theorem 2].

We can hence assume  $p \geq 5$ . By [13, Theorem 1.2] or [2, Corollary 6], there is a partition  $\Omega = \Gamma_1 \cup \Gamma_2 \cup \dots \cup \Gamma_5$  of  $\Omega$  such that  $\bigcap_{i=1}^5 G_{\Gamma_i} = 1$ .  $\square$

In the proof of Theorem 1.1, we are going to use the following result by Hartley and Turull ([6], Lemma 2.6.2).

**Lemma 4.2.** *Let  $G$  be a solvable group that acts on a group  $K$  and assume that  $(|G|, |K|) = 1$ . Then there exists a solvable group  $K_1$  such that  $G$  acts on  $K_1$  and  $K$  and  $K_1$  are isomorphic as  $G$ -sets.*

We remark that Hartley and Turull prove that  $K_1$  can even be chosen to be a product of elementary abelian groups. We do not, however, need this stronger statement in the following.

*Proof of Theorem 1.1.* By the Hartley-Turull Lemma, we can assume that  $K$  is solvable.

Since  $F(K) = F(K \rtimes G)$ ,  $G$  acts faithfully on  $V = F(K)/\Phi(F(K))$ . By induction on  $|K|$  we can assume that  $K = V$ , a completely reducible  $G$ -module (possibly of mixed characteristic).

If  $V$  is reducible, say  $V = V_1 \oplus V_2$ , for proper  $G$ -modules  $V_i$ , then by induction on  $|V|$  there exist  $x_i, y_i \in V_i$  such that  $C_G(x_i) \cap C_G(y_i) = C_G(V_i)$ , for  $i = 1, 2$ , and we are done by considering  $x = x_1 + x_2$  and  $y = y_1 + y_2$ .

Therefore, we can assume that  $V$  is irreducible. We prove that  $G$  has a regular orbit on  $V \oplus V$  that is clearly equivalent to the existence of  $x, y \in V$  with  $C_G(x) \cap C_G(y) = 1$ .

Let  $V = W_1 \oplus W_2 \oplus \dots \oplus W_n$  be an imprimitivity decomposition of  $V$  with a maximal number  $n$  of blocks and let  $H = N_G(W_1)$ . Then  $W = W_1$  is a primitive  $H$ -module. (Observe that we also allow  $n = 1$ : in that case  $V$  is primitive.)

As  $p = \text{char}(W)$  does not divide  $|H|$ , by Corollary 3.6 there exist  $w_1, w_2, \dots, w_p \in W \oplus W$  belonging to distinct regular orbits of  $H/C_H(W)$  on  $W \oplus W$ .

Let  $T$  be a (right) transversal of  $H$  in  $G$ . Then, writing actions (multiplicatively) on the right,  $V \oplus V = \bigoplus_{\alpha \in T} (W \oplus W)\alpha$  and there is a homomorphism  $\varphi : G \rightarrow \text{Sym}(T)$ , defined by  $\alpha\varphi(g) = \beta$ , where  $\alpha, \beta \in T$ ,  $g \in G$  and  $\alpha g = h_\alpha \beta$  for some  $h_\alpha \in H$  ( $h_\alpha$  depending also on  $g$ ).

By Lemma 4.1, there are  $\Gamma_1, \dots, \Gamma_p \subseteq T$  (with possibly some of the  $\Gamma_i$ 's empty) such that  $T$  is the disjoint union of the  $\Gamma_i$ 's and  $\bigcap_{i=1}^p G_{\Gamma_i} = \text{Ker}(\varphi)$ .

Define  $v \in V \oplus V$  by

$$v = \sum_{\alpha \in T} u_\alpha \alpha$$

where  $u_\alpha = w_i$  whenever  $\alpha \in \Gamma_i$ .

Observe that, if  $g \in G$  fixes  $v$ , then  $g$  stabilizes all the sets  $\Gamma_i$  and hence  $g \in \text{Ker}(\varphi)$ . Therefore,  $\alpha g \alpha^{-1} = h_\alpha \in C_H(W)$  for all  $\alpha \in T$ .



It follows that

$$g \in \bigcap_{\alpha \in T} C_G(W)^\alpha = \bigcap_{\alpha \in T} C_G(W\alpha) = C_G(V) = 1,$$

and hence  $C_G(v) = 1$ .  $\square$

*Proof of Theorem 1.3.* We want to show that there are  $H_1, H_2, H_3 \in \text{Hall}_\pi(G)$  such that  $H_1 \cap H_2 \cap H_3 = O_\pi(G)$ . By factoring out  $O_\pi(G)$ , we can assume  $O_\pi(G) = 1$ .

Let  $L = O_{\pi'(G)}$ . If  $L < G$ , by induction there exist  $H'_1, H'_2, H'_3 \in \text{Hall}_\pi(L)$  such that  $\bigcap_{i=1}^3 H'_i = 1$ . Further, as  $L \neq 1$  and  $O_\pi(G/L) = 1$ , there exist  $H_1, H_2, H_3 \in \text{Hall}_\pi(G)$  such that  $\bigcap_{i=1}^3 H_i L = L$ . Since  $H_i \cap L \in \text{Hall}_\pi(L)$  and hence it is  $L$ -conjugate to  $H'_i$ , we can assume  $H_i \cap L = H'_i$ , for  $i = 1, 2, 3$ .

As  $\bigcap_{i=1}^3 H_i \leq L$ , we hence have

$$\bigcap_{i=1}^3 H_i = \bigcap_{i=1}^3 H_i \cap L = \bigcap_{i=1}^3 H'_i = 1.$$

Therefore, we can assume  $G = L = KH$  with  $K$  a normal  $\pi$ -complement of  $G$  and  $H \in \text{Hall}_\pi(G)$ . As  $O_\pi(G) = 1$ ,  $H$  acts faithfully on  $K$  and hence by Theorem 1.1 there exist  $x, y \in K$  such that

$$1 = C_H(x) \cap C_H(y) = (H \cap H^x) \cap (H \cap H^y) = H \cap H^x \cap H^y.$$

$\square$

In proving Theorem 1.4, we use the following elementary result:

**Lemma 4.3.** *Let  $V$  be a finite  $G$ -module and  $k$  a positive integer. If  $G$  has  $k$  regular orbits on  $V \oplus V$ , then  $G$  has at least  $k(|V| + 2)$  regular orbits on  $V \oplus V \oplus V$ .*

*Proof.* Let  $\{(x_i, y_i) \mid i = 1, 2, \dots, k\}$  be a set of representatives for the regular  $G$ -orbits of  $V \oplus V$ . Then

$\{(x_i, y_i, u) \mid i = 1, \dots, k, u \in V, u \neq 0\} \cup \{(x_i, y_i, 0), (x_i, 0, y_i), (0, x_i, y_i) \mid i = 1, \dots, k\}$  is a (not necessarily complete) set of representatives of distinct regular orbits of  $G$  on  $V \oplus V \oplus V$ .  $\square$

*Proof of Theorem 1.4.* By the reduction method used in the proof of Theorem 1.1 and by Lemma 4.1, it is enough to prove that if  $G$  is a solvable group and  $V$  is a primitive, finite and faithful  $G$ -module, then  $G$  has at least 5 regular orbits on  $V \oplus V \oplus V$ .

By Lemma 4.3, we are hence left to check the exceptional groups (1)–(4) in Theorem 3.4. It is also enough to consider the maximal groups in that list.

If  $G = \text{GL}(2, 2)$  or  $G = \text{GL}(2, 3)$  and  $V$  is the corresponding natural module, then  $G$  has exactly one regular orbit on  $V \oplus V$  and hence, by Lemma 4.3,  $G$  has at least five regular orbits on  $V \oplus V \oplus V$ .

If  $G = 3^{1+2}.\text{GL}(2, 3) \leq \text{GL}(6, 2)$  or  $G = (Q_8 \times Q_8).O^+(4, 2) \leq \text{GL}(4, 3)$ , one checks by [GAP] that  $G$  has at least five regular orbits on  $V \oplus V \oplus V$ , where  $V$  is the natural  $G$ -module.  $\square$

**Added in proof.** In the paper “Regular orbits of induced modules of finite groups”, Finite groups 2003 (Thompson Conference), de Gruyter, Berlin, 2004, T. Wolf gives a systematic and accurate way to count regular orbits of induced

modules. This result, which was not available to the author at the time of his writing, could be used to replace some arguments in the proof of Theorem 1.1.

## REFERENCES

1. J. Dixon, *The Fitting subgroup of a linear solvable group*, J. Austr. Math. Soc., **7** (1967), 419–424. MR0230814 (37:6372)
2. S. Dolfi, *Orbits of permutation groups on the power set*, Arch. Math., **75** (2000), 321–327. MR1785438 (2001g:20002)
3. A. Espuelas, *Regular orbits on symplectic modules*, J. Algebra, **138** (1991), 1–12. MR1102565 (92b:20007)
4. S. Dolfi, *Intersections of odd order Hall subgroups*, Bull. London Math. Soc. **37** (2005), 61–66. MR2105819 (2005h:20041)
- GAP. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*; 2002, (<http://www.gap-system.org>).
5. D. Gluck, *Trivial set stabilizers in finite permutation groups*, Canad. J. Math., **35** (1983), 59–76. MR685817 (84c:20008)
6. B. Hartley and A. Turull, *On characters of coprime operator groups and the Glauberman character correspondence*, J. Reine Angew. Math. **451** (1994), 175–219. MR1277300 (95d:20010)
7. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin - Heidelberg - New York, 1967. MR0224703 (37:302)
8. B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin - Heidelberg - New York, 1982. MR650245 (84i:20001a)
9. I. M. Isaacs, *Large orbits in actions of nilpotent groups*, Proc. Amer. Math. Soc. **127** (1999), 45–50. MR1469413 (99b:20035)
10. O. Manz and T. Wolf, *Representations of solvable groups*, Cambridge Univ. Press, Cambridge, 1993. MR1261638 (95c:20013)
11. H. Matsuyama, *Another proof of Gluck’s theorem*, J. Algebra, **274** (2002), 703–706. MR1877870 (2002j:20004)
12. D. S. Passman, *Groups with normal solvable Hall  $p'$ -subgroups*, Trans. Amer. Math. Soc. **123** (1966), 99–111. MR0195947 (33:4143)
13. A. Seress, *The minimal base size of primitive permutation groups*, J. London Math. Soc., **53** (1996), 243–255. MR1373058 (96k:20003)
14. M. W. Short, *The primitive soluble permutation groups of degree less than 256*, Lecture Notes in Mathematics 1519, Springer-Verlag, Berlin-Heidelberg, 1992. MR1176516 (93g:20006)
15. D. A. Suprunenko, *Matrix groups*, Translations of Mathematical Monographs **45**, Amer. Math. Soc., Providence RI, 1976. MR0390025 (52:10852)
16. T. Wolf, *Indices of centralizers for Hall-subgroups of linear groups*, Illinois J. Math., **43** (1999), 324–337. MR1703191 (2000e:20023)
17. T. Wolf, *Large orbits of supersolvable linear groups*, J. Algebra **215** (1999), 235–247. MR1684166 (2000d:20047)
18. V. I. Zenkov, *The structure of intersections of nilpotent  $\pi$ -subgroups in finite  $\pi$ -solvable groups*, Siberian Math. J. **34** (1993), 683–687. MR1248794 (94g:20023)

DIPARTIMENTO DI MATEMATICA “U. DINI”, UNIVERSITÀ DEGLI STUDI DI FIRENZE, FIRENZE, 50134 ITALY

*E-mail address:* `dolfi@math.unifi.it`