

# On orders of elements of finite almost simple groups with linear or unitary socle

Mariya A. Grechkoseeva

Communicated by Christopher W. Parker

**Abstract.** We say that a finite almost simple  $G$  with socle  $S$  is *admissible* (with respect to the spectrum) if  $G$  and  $S$  have the same sets of orders of elements. Let  $L$  be a finite simple linear or unitary group of dimension at least three over a field of odd characteristic. We describe admissible almost simple groups with socle  $L$ . Also we calculate the orders of elements of the coset  $L\tau$ , where  $\tau$  is the inverse-transpose automorphism of  $L$ .

## 1 Introduction

The *spectrum*  $\omega(G)$  of a finite group  $G$  is the set of orders of its elements, and groups with equal spectra are said to be *isospectral*. To solve the *problem of recognition by spectrum* for a given finite group  $G$  is to describe (up to isomorphism) the finite groups that are isospectral to  $G$ . If a finite group  $G$  has a non-trivial normal solvable subgroup, then there are infinitely many finite groups isospectral to  $G$ , cf. [17, Lemma 1]. This implies that a finite group  $G$  with finite set of isospectral groups must satisfy  $P \leq G \leq \text{Aut } P$ , where  $P$  is a product of nonabelian simple groups, and the easiest situation is when  $G$  is just a nonabelian simple group. The problem of recognition of nonabelian simple groups by spectrum has been studied extensively in recent years, and as a working hypothesis of this investigation, it was conjectured that a finite group  $G$  isospectral to a “sufficiently large” simple group  $S$  must be an almost simple group with socle  $S$ , i.e.  $S \leq G \leq \text{Aut } S$ . In 2015, this conjecture was proved with the following precise meaning of the term “sufficiently large”:  $S$  is a linear or unitary group of dimension larger than 44, or  $S$  is a symplectic or orthogonal group of dimension larger than 60, or  $S$  is one of the sporadic, alternating and exceptional groups of Lie type other than  $J_2$ ,  $A_6$ ,  $A_{10}$ , and  ${}^3D_4(2)$  (see [14] and the references therein). Thus for a vast class of simple groups, the initial problem of recognition by spectrum was reduced to a more specific problem of describing (up to isomorphism) almost simple groups with socle  $S$  that are isospectral to  $S$ , and this is the problem we address in this paper.

For brevity, we refer to a finite almost simple group with socle  $S$  that is isospectral to  $S$  as *admissible* for  $S$ . Clearly we are interested in non-trivial admissible groups, i.e. other than  $S$  itself. It is not hard to check that there are no non-trivial admissible groups for the alternating groups. The information collected in [7] allows to verify that the sporadic groups do not possess non-trivial admissible groups either. One of the first examples of non-trivial admissible groups was discovered by Mazurov [16]: he showed that the finite groups isospectral to  $\mathrm{PSL}_3(5)$  are exactly  $\mathrm{PSL}_3(5)$  and its extension by the graph automorphism. Later Zavarnitsine [23] provided an example demonstrating that the number of admissible groups can be arbitrarily large:  $\mathrm{PSL}_3(7^{3^k})$  has exactly  $k + 1$  admissible groups, including itself, and these are precisely extensions by field automorphisms.

Admissible groups are described for all exceptional groups of Lie type (see [27] for references),  $\mathrm{PSL}_2(q)$  (see [2]),  $\mathrm{PSL}_3(q)$  and  $\mathrm{PSU}_3(q)$  (see [23, 24]), classical groups over fields of characteristic 2 (see [11, 13, 26]), and symplectic and odd-dimensional orthogonal groups over fields of odd characteristic (see [12]). It is worth noting that for all of these groups, there is  $\alpha \in \mathrm{Aut} S$  such that  $S_0 = \langle S, \alpha \rangle$  is admissible and any other admissible group is conjugate in  $\mathrm{Aut} S$  to a subgroup of  $S_0$ ; in other words, any admissible group is a cyclic extension of  $S$  and up to isomorphism there is a unique maximal admissible group. Below we will see that not all simple groups satisfy the latter property.

The main result of this paper is a description of admissible groups for linear and unitary groups over fields of odd characteristic (Theorems 1, 2 and 3). Also we explicitly describe spectra of some almost simple groups with linear or unitary socle (Lemmas 3.3, 4.6, and 4.7). In the rest of this section, we introduce the notation used in the theorems and then state our results.

Throughout this paper,  $p$  is a prime,  $F$  is the algebraic closure of the field of order  $p$ ,  $H = \mathrm{GL}_n(F)$ , with matrices acting on row vectors by right multiplication, and  $\tau$  is the inverse-transpose map  $g \mapsto g^{-\top}$  of  $H$ . If  $q$  is a power of  $p$ , then  $F_q$  denotes the subfield of  $F$  of order  $q$ ,  $\lambda_q$  denotes a fixed primitive element of  $F_q$  and  $\varphi_q$  denotes the standard Frobenius endomorphism of  $H$  of level  $q$ , i.e. the endomorphism induced by raising matrix entries to the  $q$ th power. We identify  $\mathrm{GL}_n(q)$  with  $C_H(\varphi_q)$  and  $\mathrm{GU}_n(q)$  with  $C_H(\varphi_q \tau)$ .

We write  $\mathrm{GL}_n^+(q)$  instead of  $\mathrm{GL}_n(q)$  and  $\mathrm{GL}_n^-(q)$  instead of  $\mathrm{GU}_n(q)$  and use a similar agreement for  $\mathrm{PGL}_n(q)$ ,  $\mathrm{SL}_n(q)$ , and  $\mathrm{PSL}_n(q)$ . For  $\varepsilon \in \{+, -\}$ , we shorten  $\varepsilon 1$  to  $\varepsilon$  in arithmetic expressions.

As usual, by  $(a_1, \dots, a_s)$  we denote the greatest common divisor of positive integers  $a_1, \dots, a_s$ , and by  $[a_1, \dots, a_s]$  we denote their least common multiple. If  $a$  and  $b$  are positive integers, then  $\pi(a)$  denotes the set of prime divisors of  $a$ ,  $(a)_b$  denotes the largest divisor  $c$  of  $a$  such that  $\pi(c) \subseteq \pi(b)$  and  $(a)_{b'}$  denotes the number  $a/(a)_b$ .

Let  $L = \text{PSL}_n^\varepsilon(q)$  ( $q = p^m$ ), and define  $d = (n, q - \varepsilon)$ . We write  $\delta = \delta(\varepsilon q)$  to denote the diagonal automorphism of  $L$  induced by  $\text{diag}(\lambda, 1, \dots, 1)$ , where  $\lambda$  is a primitive  $(q - \varepsilon)$ th root of unity in  $F_{q^2}$ . We denote by  $\varphi$  the field automorphism induced by  $\varphi_p$ . The automorphism induced by  $\tau$  is denoted by the same letter. The image of  $\alpha \in \text{Aut } L$  in  $\text{Out } L$  is denoted by  $\bar{\alpha}$ .

When  $n \geq 3$ , the inverse-transpose automorphism is outer and  $\text{Out } L$  has the following presentation (we omit overbars for convenience):

$$\begin{aligned} \langle \delta, \varphi, \tau \mid \delta^d = \varphi^m = \tau^2 = [\varphi, \tau] = 1, \delta^\varphi = \delta^p, \delta^\tau = \delta^{-1} \rangle & \quad \text{if } \varepsilon = +, \\ \langle \delta, \varphi, \tau \mid \delta^d = \tau^2 = [\varphi, \tau] = 1, \varphi^m = \tau, \delta^\varphi = \delta^p, \delta^\tau = \delta^{-1} \rangle & \quad \text{if } \varepsilon = -. \end{aligned}$$

Theorem 1 is concerned with the extension by the inverse-transpose automorphism  $\tau$ . A criterion of admissibility of this extension is not very short, so it seems reasonable to write it up separately.

**Theorem 1.** *Let  $L = \text{PSL}_n^\varepsilon(q)$ , where  $n \geq 3$ ,  $\varepsilon \in \{+, -\}$  and  $q$  is odd, and let  $G = L \rtimes \langle \tau \rangle$ . Then either  $\omega(G) = \omega(L)$  or one of the following holds:*

- (i)  $n = p^{t-1} + 2$  with  $t \geq 1$ ,  $q \equiv -\varepsilon \pmod{4}$  and  $4p^t \in \omega(G) \setminus \omega(L)$ ,
- (ii)  $n = 2^t + 1$  with  $t \geq 1$ ,  $(n, q - \varepsilon) > 1$  and  $2(q^{(n-1)/2} - \varepsilon^{(n-1)/2})$  is an element of  $\omega(G) \setminus \omega(L)$ ,
- (iii)  $n = p^{t-1} + 1$  with  $t \geq 1$  and  $2p^t \in \omega(G) \setminus \omega(L)$ ,
- (iv)  $n$  is even,  $(n)_2 \leq (q - \varepsilon)_2$ ,  $q \equiv \varepsilon \pmod{4}$  and  $q^{n/2} + \varepsilon^{n/2}$  is an element of  $\omega(G) \setminus \omega(L)$ ,
- (v)  $n$  is even,  $(n)_{2'} > 3$ ,  $(n, q - \varepsilon)_{2'} > 1$  and  $2[q^{(n)_2} - 1, q^{n/2 - (n)_2} + \varepsilon^{n/2 - (n)_2}]$  is an element of  $\omega(G) \setminus \omega(L)$ .

Theorems 2 and 3 describe admissible groups in terms of admissibility of  $\tau$ . As we have mentioned, the admissible groups for  $\text{PSL}_3(q)$  and  $\text{PSU}_3(q)$  were determined by Zavarnitsine [23, 24], so we do not consider these groups. However, we include them in the statements of the theorems for completeness. Observe that two almost simple groups with socle  $S$  are isomorphic if and only if their images in  $\text{Out } S$  are conjugate. Thus to describe admissible groups up to isomorphism, it is sufficient to describe their images in  $\text{Out } S$  up to conjugacy. We refer to  $\alpha \in \text{Aut } S$  as admissible if  $\langle S, \alpha \rangle$  is admissible.

**Theorem 2.** *Let  $L = \text{PSL}_n(q)$ , where  $n \geq 3$ ,  $q = p^m$  and  $p$  is an odd prime. Let  $d = (n, q - 1)$ ,  $b = ((q - 1)/d, m)_d$ ,  $\eta = \delta^{(d)_{2'}}$ ,  $\phi = \varphi^{m/(b)_{2'}}$ , and*

$$\psi = \begin{cases} \varphi^{m/(b)_{2'}} & \text{if } n \neq 4 \text{ or } 12 \nmid q + 1, \\ \varphi^{(m)_{3'}} & \text{if } n = 4 \text{ or } 12 \mid q + 1. \end{cases}$$

Conditions on $L$		$\alpha = \gamma\beta = \beta\gamma$	
		$\gamma$	$\beta$
$n = p^t + 1$ , $n \neq 2^u + 2$	$(b)_2 > 2$ or $(n)_2 < (p-1)_2$ $(m)_2 = 2$ , $(n)_2 < (p+1)_2$	1 1	$\varphi^{m/2}\tau\eta$ $\varphi^{m/2}\eta$
$n \neq p^t + 1$ , $b$ odd	$\tau$ not admissible, $ \psi  > 1$ $\tau$ admissible	$\psi$ $\psi$	1 $\tau$
$n \neq p^t + 1$ , $b$ even, $p \equiv \epsilon \pmod{4}$	$n = p^s + 2^u + 1$	$\psi$	$\phi$ , $\phi^i \tau$
	$n \neq p^s + 2^u + 1$ , $(n)_2 \geq (p-\epsilon)_2$	$\psi$	$\phi$ , $\phi^i \tau$ , $\phi^{2j} \tau \eta$
	$n \neq p^s + 2^u + 1$ , $(n)_2 < (p-\epsilon)_2$ , $\epsilon = +$	$\psi$	$\phi$ , $\phi^i \tau$ , $\phi^{2j} \tau \eta$ , $\phi \tau \eta$
	$n \neq p^s + 2^u + 1$ , $(n)_2 < (p-\epsilon)_2$ , $\epsilon = -$	$\psi$	$\phi$ , $\phi^i \tau$ , $\phi^{2j} \tau \eta$ , $\phi \eta$
$t, u > 0$ , $s \geq 0$		$2i \mid (b)_2$ , $4j \mid (b)_2$	

Table 1. Conditions on the automorphism  $\alpha$  of  $L = \text{PSL}_n(q)$  in Theorem 2.

Suppose that  $L < G \leq \text{Aut } L$ . Then  $\omega(G) = \omega(L)$  if and only if  $G/L$  is conjugate in  $\text{Out } L$  to a subgroup of  $\langle \bar{\alpha} \rangle$ , where  $\alpha$  is one of the elements specified in Table 1.

As an example of applying Theorem 2, let us consider admissible groups for  $\text{PSL}_4(25)$ . For this group, we have  $p = 5$ ,  $d = 4$ ,  $b = 2$ ,  $\phi = \varphi$ ,  $n \neq p^t + 1$  and  $n = p^0 + 2^1 + 1$ . Thus up to isomorphism there are two non-trivial admissible groups, namely, the extensions by  $\varphi$  and by  $\varphi\tau$ . Clearly they are both maximal.

**Theorem 3.** Let  $L = \text{PSU}_n(q)$ , where  $n \geq 3$ ,  $q = p^m$  and  $p$  be an odd prime. Let  $d = (n, q + 1)$ ,  $b = ((q + 1)/d, m)_d$  and

$$\psi = \begin{cases} \varphi^{2m/(b)_{2'}} & \text{if } n \neq 4 \text{ or } 12 \nmid q - 1, \\ \varphi^{2(m)_{3'}} & \text{if } n = 4 \text{ and } 12 \mid q - 1. \end{cases}$$

Suppose that  $L < G \leq \text{Aut } L$ . Then  $\omega(G) = \omega(L)$  if and only if  $n - 1$  is not a power of  $p$  and  $G/L$  is conjugate in  $\text{Out } L$  to a subgroup of  $\langle \bar{\alpha} \rangle$ , where

- (i)  $\alpha = \psi$  if  $\tau$  is not admissible and  $|\psi| > 1$ ,
- (ii)  $\alpha = \psi\tau$  if  $\tau$  is admissible,  $(n)_2 > 2$  and  $n \geq 16$ ,
- (iii)  $\alpha = \psi\varphi^{(m)_{2'}}$  if  $\tau$  is admissible and either  $(n)_2 \leq 2$  or  $n \leq 12$ .

Returning now to the initial recognition problem, we state the following consequence of [21, Theorem 1] and the above results.

**Corollary.** Let  $L = \text{PSL}_n^\epsilon(q)$ , where  $n \geq 45$ ,  $\epsilon \in \{+, -\}$  and  $q$  is odd. A finite group is isospectral to  $L$  if and only if it is isomorphic to an almost simple group  $G$  with socle  $L$  and  $G/L = \langle \bar{\alpha} \rangle$ , where  $\alpha$  is an identity or is as specified in Theorems 2 and 3.

## 2 Spectra of classical groups and related number-theoretical lemmas

In this section, we collect necessary information on spectra of classical groups and related number-theoretical lemmas. Our notation for the classical groups follows that of [7]. Recall some well-known isomorphisms between classical groups (see, for example, [15, Proposition 2.9.1]). If  $q$  is odd, then

$$\begin{aligned} \mathrm{PSp}_4(q) &\simeq \Omega_5(q), & \Omega_6^\varepsilon(q) &\simeq \mathrm{SL}_4^\varepsilon(q)/\{\pm 1\}, \\ \mathrm{P}\Omega_6^\varepsilon(q) &\simeq \mathrm{PSL}_4^\varepsilon(q), & \Omega_4^+(q) &\simeq \mathrm{SL}_2(q) \circ \mathrm{SL}_2(q), \\ \mathrm{P}\Omega_4^+(q) &\simeq \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q), & \Omega_4^-(q) &\simeq \mathrm{PSL}_2(q^2), \\ \mathrm{Sp}_2(q) &\simeq \mathrm{SL}_2(q), & \Omega_3(q) &\simeq \mathrm{PSL}_2(q). \end{aligned} \quad (2.1)$$

Given a prime  $r$ , we write  $\omega_{r'}(G)$  to denote the set of orders of elements of  $G$  that are coprime to  $r$ . In particular, if  $G$  is a group of Lie type over a field of characteristic  $p$ , then  $\omega_{p'}(G)$  is the set of orders of semisimple elements of  $G$ . By  $\omega_{\tilde{r}}(G)$  we denote the difference  $\omega(G) \setminus \omega_{r'}(G)$ .

**Lemma 2.1.** *Let  $n \geq 2$ , let  $q$  be a power of a prime  $p$ ,  $\varepsilon \in \{+, -\}$  and let  $G$  be  $\mathrm{PGL}_n^\varepsilon(q)$  or  $\mathrm{PSL}_n^\varepsilon(q)$ . Let  $d = 1$  in the first case and  $d = (n, q - 1)$  in the second case. Then  $\omega(G)$  consists of all divisors of the following numbers:*

- (i)  $(q^n - \varepsilon^n)/((q - \varepsilon)d)$ ,
- (ii)  $[q^{n_1} - \varepsilon^{n_1}, q^{n_2} - \varepsilon^{n_2}]/(n/(n_1, n_2), d)$ , where  $n_i > 0$  and  $n_1 + n_2 = n$ ,
- (iii)  $[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}]$ , where  $s \geq 2$ ,  $n_i > 0$  and  $n_1 + \dots + n_s = n$ ,
- (iv)  $p^t(q^{n_1} - \varepsilon^{n_1})/d$ , where  $t \geq 1$ ,  $n_1 > 0$  and  $p^{t-1} + 1 + n_1 = n$ ,
- (v)  $p^t[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}]$ , where  $t \geq 1$ ,  $s \geq 2$ ,  $n_i > 0$  and  $p^{t-1} + 1 + n_1 + \dots + n_s = n$ ,
- (vi)  $(n, q - 1)p^t/d$  if  $n = p^{t-1} + 1$  for some  $t \geq 1$ .

*Proof.* See [4, Corollaries 2 and 3]. □

**Lemma 2.2.** *Let  $n \geq 1$ , let  $q$  be a power of an odd prime  $p$  and let  $G$  be one of the groups  $\mathrm{Sp}_{2n}(q)$ ,  $\mathrm{PSp}_{2n}(q)$ , and  $\Omega_{2n+1}(q)$ . Let  $d = c = 1$  if  $G = \mathrm{Sp}_{2n}(q)$ ; let  $d = 2$  and  $c = 1$  if  $G = \mathrm{PSp}_{2n}(q)$  or  $G = \Omega_5(q)$ ,  $\Omega_3(q)$ ; and let  $d = c = 2$  if  $G = \Omega_{2n+1}(q)$  and  $n \geq 3$ . Then  $\omega(G)$  consists of all divisors of the following numbers:*

- (i)  $(q^n \pm 1)/d$ ,
- (ii)  $[q^{n_1} \pm 1, \dots, q^{n_s} \pm 1]$ , where  $s \geq 2$ ,  $n_i > 0$  and  $n_1 + \dots + n_s = n$ ,
- (iii)  $p^t(q^{n_1} \pm 1)/c$ , where  $t \geq 1$ ,  $n_1 > 0$  and  $p^{t-1} + 1 + 2n_1 = 2n$ ,

- (iv)  $p^t[q^{n_1} \pm 1, \dots, q^{n_s} \pm 1]$ , where  $t \geq 1$ ,  $s \geq 2$ ,  $n_i > 0$  and  $p^{t-1} + 1 + 2n_1 + \dots + 2n_s = 2n$ ,
- (v)  $2p^t/d$  if  $2n = p^{t-1} + 1$  for some  $t \geq 1$ .

*Proof.* See [5, Corollaries 1, 2 and 6] for  $n \geq 2$  and (2.1) together with Lemma 2.1 for  $n = 1$ .  $\square$

**Lemma 2.3.** *Let  $n \geq 2$ , let  $q$  be a power of an odd prime  $p$  and let  $\varepsilon \in \{+, -\}$ . Then  $\omega_{p'}(\Omega_{2n}^\varepsilon(q))$  consists of all divisors of the following numbers:*

- (i)  $(q^n - \varepsilon)/2$ ,
- (ii)  $[q^{n_1 - \kappa_1}, \dots, q^{n_s - \kappa_s}]$ , where  $s \geq 2$ ,  $\kappa_i \in \{+, -\}$ ,  $n_i > 0$ ,  $n_1 + \dots + n_s = n$  and  $\kappa_1 \kappa_2 \dots \kappa_s = \varepsilon$ ,

and  $\omega_{p'}(\mathbf{P}\Omega_{2n}^\varepsilon(q))$  consists of all divisors of the following numbers:

- (i)  $(q^n - \varepsilon)/(4, q^n - \varepsilon)$ ,
- (ii)  $[q^{n_1 - \kappa}, q^{n_2 - \varepsilon \kappa}]/e$ , where  $\kappa \in \{+, -\}$ ,  $n_1, n_2 > 0$ ,  $n_1 + n_2 = n$ ;  $e = 2$  when  $(q^{n_1} - \kappa)_2 = (q^{n_2 - \varepsilon \kappa})_2$  and  $e = 1$  otherwise,
- (iii)  $[q^{n_1 - \kappa_1}, \dots, q^{n_s - \kappa_s}]$ , where  $s \geq 3$ ,  $\kappa_i \in \{+, -\}$ ,  $n_i > 0$ ,  $n_1 + \dots + n_s = n$  and  $\kappa_1 \kappa_2 \dots \kappa_s = \varepsilon$ .

*Proof.* For  $n \geq 4$ , see [6, Theorem 6]. If  $n = 2, 3$ , the assertion follows from the isomorphisms given in (2.1) and Lemma 2.1.  $\square$

Let  $k \geq 3$  and  $q$  an integer whose absolute value is greater than one. A prime  $r$  such that  $r$  divides  $q^k - 1$  and does not divide  $q^i - 1$  for any  $i < k$  is called a primitive prime divisor of  $q^k - 1$  or a Zsigmondy prime. The set of primitive prime divisors of  $q^k - 1$  is denoted by  $R_k(q)$ , and  $r_k(q)$  denotes some fixed element of  $R_k(q)$ . The following result was proved by Bang [1] in 1886 and, in a more general situation, by Zsigmondy [25] in 1892 (and has been reproved many times as explained in [18, p. 34]). A modern proof of this result can be found in [19].

**Lemma 2.4** (Bang–Zsigmondy). *Let  $q \geq 2$  and  $k \geq 3$  be integers. If  $q > 2$  or  $k \neq 6$ , then  $R_k(q)$  is not empty. In particular, if  $q > 2$  or  $n \neq 3$ , then  $R_k(-q)$  is not empty.*

The two following results are well known.

**Lemma 2.5.** *Let  $q > 1$ ,  $k$  and  $l$  be positive integers, and  $\varepsilon \in \{+, -\}$ . Then:*

- (i)  $(q^k - 1, q^l - 1) = q^{(k,l)} - 1$ ,
- (ii)  $(q^k + 1, q^l + 1)$  is equal to  $q^{(k,l)} + 1$  if  $(k)_2 = (l)_2$  and to  $(2, q + 1)$  otherwise,

- (iii)  $(q^k - 1, q^l + 1)$  is equal to  $q^{(k,l)} + 1$  if  $(k)_2 > (l)_2$  and to  $(2, q + 1)$  otherwise,
- (iv)  $((q^k - \varepsilon^k)/(q - \varepsilon), k) = (q - \varepsilon, k)$ ,
- (v) if  $(k, l) = 1$ , then  $(q^l - \varepsilon^l)/(q - \varepsilon)$  divides  $(q^{lk} - \varepsilon^{kl})/(q^k - \varepsilon^k)$  and  $(q^l - \varepsilon^l)/(n, q - \varepsilon)$  divides  $(q^{lk} - \varepsilon^{lk})/(n, q^k - \varepsilon^k)$  for any positive integer  $n$ .

**Lemma 2.6.** Let  $q > 1$  and  $k$  be positive integers and  $\varepsilon \in \{+, -\}$ .

- (i) If an odd prime  $r$  divides  $q - \varepsilon$ , then  $(q^k - \varepsilon^k)_r = (k)_r(q - \varepsilon)_r$ .
- (ii) If an odd prime  $r$  divides  $q^k - \varepsilon^k$ , then  $r$  divides  $q^{(k)_{r'}} - \varepsilon^{(k)_{r'}}$ .
- (iii) If 4 divides  $q - \varepsilon$  and  $k$  is odd, then  $(q^k - \varepsilon^k)_2 = (k)_2(q - \varepsilon)_2$ .

**Lemma 2.7.** Let  $q$  be odd and let  $n \geq 4$  be even. Then  $q^{n/2} + \varepsilon^{n/2} \in \omega(\text{PSL}_n^\varepsilon(q))$  if and only if  $(n)_2 > (q - \varepsilon)_2$ .

*Proof.* Let  $d = (n, q - \varepsilon)$ . Since  $a = q^{n/2} + \varepsilon^{n/2}$  is divisible by a primitive divisor  $r_n(\varepsilon q)$ , it follows from Lemma 2.1 that  $a \in \omega(\text{PSL}_n^\varepsilon(q))$  if and only if  $a$  divides

$$\frac{q^n - 1}{(q - \varepsilon)d} = \frac{(q^{n/2} + \varepsilon^{n/2})(q^{n/2} - \varepsilon^{n/2})}{(q - \varepsilon)d},$$

that is, if and only if  $d$  divides  $(q^{n/2} - \varepsilon^{n/2})/(q - \varepsilon)$ .

If  $n/2$  is odd, by Lemma 2.6 we have that  $(q^{n/2} - \varepsilon^{n/2})/(q - \varepsilon)$  is odd and, therefore, it is not divisible by  $d$ , which is even. If  $n/2$  is even and  $(n)_2 \leq (q - \varepsilon)_2$ , then  $q \equiv \varepsilon \pmod{4}$  and  $(d)_2 = (n)_2$ , and hence

$$\frac{(q^{n/2} - \varepsilon^{n/2})_2}{(q - \varepsilon)_2} = \frac{(n)_2}{2} < (d)_2.$$

Also, if  $(n)_2 > (q - \varepsilon)_2$ , then

$$\left( \frac{q^{n/2} - \varepsilon}{q - \varepsilon}, d \right) = \left( \frac{q^{n/2} - \varepsilon}{q - \varepsilon}, q - \varepsilon, n \right) = \left( \frac{n}{2}, q - \varepsilon, n \right) = d,$$

where the second equality holds by Lemma 2.5 (iv). □

### 3 Extensions by field and graph-field automorphisms

In this section, we derive some formulas concerning orders of elements in extensions of  $\text{PSL}_n^\varepsilon(q)$  by field or graph-field automorphisms. Following the lines of the proof of [24, Proposition 13], we will exploit a correspondence between  $\sigma$ -conjugacy classes of  $C_K(\sigma^k)$  and conjugacy classes of  $C_K(\sigma)$ , where  $K$  is a connected

linear algebraic group and  $\sigma$  is a Steinberg endomorphism of  $K$ , i.e. a surjective endomorphism with finitely many fixed points. Also we will use a slight modification of this correspondence inspired by [10, Theorem 2.1].

We begin with necessary notation and the Lang–Steinberg theorem. If  $K$  is a group and  $\sigma$  is an endomorphism of  $K$ , then we write  $K_\sigma$  to denote  $C_K(\sigma)$ .

**Lemma 3.1** (Lang–Steinberg). *Let  $K$  be a connected linear algebraic group and let  $\sigma$  be a surjective endomorphism of  $K$  such that  $K_\sigma$  is finite. Then the map  $x \mapsto x^{-\sigma}x$  from  $K$  to  $K$  is surjective.*

Recall that  $F$  is the algebraic closure of the field of order  $p$  and  $\varphi_q$  is the endomorphism of  $\mathrm{GL}_n(F)$  raising matrix entries to the  $q$ th power, where  $q$  is a power of  $p$ . An endomorphism  $\sigma$  of a linear algebraic group  $K$  is said to be a Frobenius endomorphism if there are an identification of  $K$  with a closed subgroup of  $\mathrm{GL}_n(F)$  and a positive integer  $k$  such that  $\sigma^k$  is induced by  $\varphi_q$ . Clearly, if  $\sigma$  is a Frobenius endomorphism, then  $\sigma$  is a Steinberg endomorphism.

**Lemma 3.2.** *Let  $K$  be a connected linear algebraic group over  $F$ , let  $\alpha$  be a Frobenius endomorphism of  $K$  and let  $\tau$  be an automorphism of  $K$  of order 2 that commutes with  $\alpha$ . Let  $k$  be a positive integer,  $l \in \{0, 1\}$  and let  $\beta$  be the automorphism of  $K_{\alpha^k \tau^l}$  induced by  $\alpha$ . Given  $g \in K_{\alpha^k \tau^l}$ , choose  $z \in K$  such that  $g = z^{-\alpha}z$  and define  $\zeta(g) = z^{\tau^l}z^{-\alpha^k}$ . Then  $\zeta(g) \in K_\alpha$ ,  $(\beta g)^k = z^{-1}\tau^l\zeta(g)z$  and the map*

$$[\beta g] \mapsto [\tau^l \zeta(g)]$$

*is a one-to-one correspondence between the  $K_{\alpha^k \tau^l}$ -conjugacy classes in the coset  $\beta K_{\alpha^k \tau^l}$  and the  $K_\alpha$ -conjugacy classes in the coset  $\tau^l K_\alpha$ .*

*Proof.* Observe that  $\alpha^k$  and  $\alpha^k \tau$  are Frobenius endomorphisms of  $K$ .

Let  $g, z \in K$ ,  $g = z^{-\alpha}z$  and  $h = z^{\tau^l}z^{-\alpha^k}$ . Define  $f = \tau^l h = z^{\tau^l}z^{-\alpha^k}$ . Then

$$\begin{aligned} g^{\alpha^k \tau^l} = g &\iff \tau^l z^{-\alpha^{k+1}} z^{\alpha^k} \tau^l = z^{-\alpha} z \\ &\iff z^{\alpha} \tau^l z^{-\alpha^{k+1}} = z^{\tau^l} z^{-\alpha^k} \\ &\iff f^{\alpha} = f. \end{aligned} \tag{3.1}$$

This if  $g \in K_{\alpha^k \tau^l}$ , then  $f \in \tau^l K_\alpha$ . Furthermore,

$$(\beta g)^k = \beta^k g^{\alpha^{k-1}} \dots g = \tau^l z^{-\alpha^k} z = z^{-1} f z.$$

Let  $g_1 = z_1^{-\alpha} z_1 \in K_{\alpha^k \tau^l}$  and  $g_2 = z_2^{-\alpha} z_2 \in K_{\alpha^k \tau^l}$ . Suppose  $x^{-1} \alpha g_1 x = \alpha g_2$  for some  $x \in K_{\alpha^k \tau^l}$ . Then writing  $y = z_1 x z_2^{-1}$ , we have  $y^\alpha = y$  and

$$f_1 = z_1 (\beta g_1)^k z_1^{-1} = z_1 x (\beta g_2)^k x^{-1} z_1^{-1} = y f_2 y^{-1}.$$

Conversely, if  $f_1 = yf_2y^{-1}$  with  $y \in K_\alpha$ , then  $x = z_1^{-1}yz_2$  satisfies  $x^{\alpha^k\tau^l} = x$  and

$$x^{-1}\alpha g_1x = z_2^{-1}y^{-1}z_1\alpha z_1^{-\alpha}z_1z_1^{-1}yz_2 = z_2^{-1}y^{-1}\alpha yz_2 = z_2^{-1}\alpha z_2 = \alpha g_2.$$

It follows that the map under consideration translates conjugacy classes to conjugacy classes and is injective. Furthermore, the conjugacy class  $[f]$  does not depend on the choice of  $z$  in the equality  $g = z^{-\alpha}z$ .

Now let  $h \in K_\alpha$ . By the Lang–Steinberg theorem, there is an element  $z \in K$  such that  $h^{-\tau^l} = z^{\alpha^k\tau^l}z^{-1}$ , and therefore  $\tau^lh = z\tau^lz^{-\alpha^k}$ . Then (3.1) implies that  $g = z^{-\alpha}z$  lies in  $K_{\alpha^k\tau^l}$ , with  $[\beta g]$  mapping to  $[\tau^lh]$ . Thus the map is surjective, and the proof is complete.  $\square$

It should be noted that some special cases of Lemma 3.2 were proved in [8, Lemma 2.10] ( $l = 0$ ) and [10, Theorem 2.1] ( $l = 1$  and  $k = 1$ ).

We use Lemma 3.2 to establish the following result generalizing [24, Corollary 14].

**Lemma 3.3.** *Let  $L = \text{PSL}_n(q)$  and  $U = \text{PSU}_n(q)$ , where  $n \geq 3$  and  $q = p^m$ . Let  $k$  divide  $m$ ,  $q = q_0^k$  and  $\beta = \varphi^{m/k}$ . Then for any  $i$ , we have the following:*

- (i)  $\omega(\beta\delta^i(q)L) = k \cdot \omega(\delta^i(q_0)\text{PSL}_n(q_0))$ ,
- (ii) if  $k$  is even, then  $\omega(\beta\tau\delta^i(q)L) = k \cdot \omega(\delta^i(-q_0)\text{PSU}_n(q_0))$ ,
- (iii) if  $k$  is odd, then  $\omega(\beta\tau\delta^i(-q)U) = k \cdot \omega(\delta^i(-q_0)\text{PSU}_n(q_0))$ ,
- (iv) if  $k$  is odd, then  $\omega(\beta\tau\delta^i(q)L) = k \cdot \omega(\tau\delta^i(q_0)\text{PSL}_n(q_0))$ ,
- (v)  $\omega(\beta\delta^i(-q)U) = k \cdot \omega(\tau\delta^i(q_0)\text{PSL}_n(q_0))$ .

In particular,  $\omega(\tau\delta^i(q)L) = \omega(\tau\delta^i(-q)U)$ .

*Proof.* Denote the center of  $H = \text{GL}_n(F)$  by  $Z$ . In particular, we write  $|gZ|$  to denote the projective order of a matrix  $g \in H$ , that is, the order of  $g$  modulo scalars. We apply Lemma 3.2 to  $H$  with  $\alpha = \varphi_p^{m/k}$  and  $l = 0$ . Observe that  $H_{\alpha^k} = \text{GL}_n(q)$  and  $H_\alpha = \text{GL}_n(q_0)$ . Let  $g \in \text{GL}_n(q)$  and  $h = \zeta(g)$  be the element of  $\text{GL}_n(q_0)$  defined in Lemma 3.2. Since  $(\beta g)^k$  is conjugate to  $h$  in  $H$ , we see that

$$|\beta gZ| = k \cdot |(\beta gZ)^k| = k \cdot |hZ|,$$

and also

$$\det h = \det(g^{\beta^{k-1}} \dots g) = (\det g)^{q_0^{k-1} + \dots + 1} = (\det g)^{(q-1)/(q_0-1)}.$$

Let  $\lambda = \lambda_q$  and  $\lambda_0 = \lambda_{q_0}$ . The condition  $gZ \in \delta^i L$  is equivalent to

$$\det g \in \langle \lambda^i, \lambda^n \rangle = \langle \lambda^{(i,n)} \rangle.$$

Since  $\lambda^{(q-1)/(q_0-1)}$  is a primitive element of  $F_{q_0}$ , it follows that

$$\det g \in \langle \lambda^{(i,n)} \rangle \iff \det h \in \langle \lambda_0^{(i,n)} \rangle.$$

Thus (i) holds. Similarly, (ii) and (iii) follow from Lemma 3.2 with  $\alpha = \varphi_p^{m/k} \tau$  and  $l = 0$ .

Let  $k$  be odd and  $\alpha = \varphi_p^{m/k} \tau$ . Then  $H_{\alpha^k \tau} = \mathrm{GL}_n(q)$  and  $H_\alpha = \mathrm{GU}_n(q_0)$ . Applying Lemma 3.2 with  $l = 1$ , we construct from an element  $g \in \mathrm{GL}_n(q)$  an element  $h \in \mathrm{GU}_n(q_0)$  such that  $g = z^{-\alpha} z$  and  $h = z^\tau z^{-\alpha^k}$  for some  $z \in H$ . As in the previous case, we deduce that  $|\beta \tau g Z| = k \cdot |\tau h Z|$ . Furthermore, we have  $\det g = (\det z)^{q_0+1}$  and  $\det h = (\det z)^{q-1}$ . Since  $(\det g)^{q-1} = 1$ , it follows that  $(\det z)^{(q_0+1)(q-1)} = 1$ . Let  $\lambda = \lambda_q$  and  $\lambda_0 = \lambda_{q_0}^{q_0-1}$ , and let  $\mu$  be a primitive  $(q_0 + 1)(q - 1)$ st root of unity in  $F$ . Then

$$\det g \in \langle \lambda^{(i,n)} \rangle \iff \det z \in \langle \mu^{(i,n)} \rangle,$$

which is equivalent to  $\det h \in \langle \lambda_0^{(i,n)} \rangle$ . Hence

$$\omega(\beta \tau \delta^i(q) L) = k \cdot \omega(\tau \delta^i(-q_0) \mathrm{PSU}_n(q_0)). \quad (3.2)$$

Similarly, taking  $\alpha = \varphi_p^{m/k}$  and  $l = 1$ , we prove (v). Applying (v) with  $k = 1$  and observing that in this case  $\beta$  acts on  $U$  in the same way as  $\tau$ , we have

$$\omega(\tau \delta^i(q) L) = \omega(\tau \delta^i(-q) U).$$

Now this equality and (3.2) imply (iv). □

Note that for unitary groups, (iii) and (v) of Lemma 3.3 cover all possibilities for an element  $\gamma \in \langle \varphi \rangle$ : if  $|\gamma| = 2k$ , then  $\langle \gamma \rangle = \langle \varphi^{m/k} \rangle$ ; while if  $|\gamma| = k$  with  $k$  odd, then  $\langle \gamma \rangle = \langle \varphi^{m/k} \tau \rangle$  because  $(m + m/k, 2m) = 2m/k$ . Thus Lemma 3.3 expresses the spectrum of an extension by a field or graph-field automorphism in terms of known spectra and the spectrum of the extension by graph automorphism, which we consider in the next section.

## 4 Extension by graph automorphism

This section is largely concerned with matrices, so we need to define some of them. We denote by  $I$  the identity matrix whose size is clear from the context, and by  $J_k$  the  $k \times k$  unipotent Jordan block. As in the previous section, we will calculate the projective orders of matrices, that is, the orders modulo scalars.

Recall that  $\langle \bar{\delta} \rangle \rtimes \langle \bar{\tau} \rangle$  is a dihedral group of order  $2(n, q - \varepsilon)$ . It follows that for odd  $n$ , every  $\tau \delta^i$  is conjugate to  $\tau$  modulo  $L$ , and hence

$$\omega(\tau L) = \omega(\cup_{i=1}^d \tau \delta^i L) = \omega(\tau \text{PGL}_n(q)). \quad (4.1)$$

If  $n$  is even, then for any  $i$ , we have

$$\omega(\tau L) = \omega(\tau \delta^{2i} L) \quad \text{and} \quad \omega(\tau \delta L) = \omega(\tau \delta^{2i-1} L). \quad (4.2)$$

As we saw in Lemma 3.3, the cosets  $\tau \delta^i(q) \text{PSL}_n(q)$  and  $\tau \delta^i(-q) \text{PSU}_n(q)$  have the same orders of elements, so it suffices to describe  $\omega(\tau \delta^i(q) \text{PSL}_n(q))$ .

Since  $|g\tau| = 2|(g\tau)^2| = 2|gg^\tau|$ , it follows that the elements of  $\omega(\tau \text{PGL}_n(q))$  are exactly twice the projective orders of elements of

$$\Gamma_n(q) = \{gg^\tau \mid g \in \text{GL}_n(q)\}.$$

If  $n$  is even, then  $\omega(\tau L)$  and  $\omega(\tau \delta L)$  are analogously related to the projective orders of elements of

$$\Gamma_n^\square(q) = \{gg^\tau \mid g \in \text{GL}_n(q), \det g \in (F_q^\times)^2\}$$

and

$$\Gamma_n^\boxtimes(q) = \{gg^\tau \mid g \in \text{GL}_n(q), \det g \notin (F_q^\times)^2\},$$

respectively.

A comprehensive treatment of the equation  $h = gg^\tau$  for a given matrix  $h$  is provided by Fulman and Guralnick in [9], and we use the terminology and some results of this paper. First of all, it is helpful to note that  $h = gg^\tau$  yields

$$xhx^{-1} = (xgx^\top)(xgx^\top)^\tau \quad (4.3)$$

for any  $x \in \text{GL}_n(q)$ , and hence  $h$  lies in  $\Gamma_n(q)$ ,  $\Gamma_n^\square(q)$  or  $\Gamma_n^\boxtimes(q)$  if and only if the whole conjugacy class  $[h]$  lies in the corresponding set. Thus we may work not with individual matrices but with conjugacy classes. Recall that the conjugacy classes of  $\text{GL}_n(q)$  are parametrized by collections of partitions

$$\{\lambda_\phi \mid \phi \text{ is a monic irreducible polynomial over } F_q\}$$

such that  $|\lambda_z| = 0$  and  $\sum_\phi \deg(\phi) |\lambda_\phi| = n$ . In this parametrization, the collection of partitions  $\{\lambda_\phi\}$  corresponds to the class  $[h]$  such that the multiplicity of  $\phi^k$  as an elementary divisor of  $h$  is equal to the multiplicity of parts of size  $k$  in  $\lambda_\phi$ . We denote the partition corresponding under this parametrization to a class  $[h]$  and a polynomial  $\phi$  by  $\lambda_\phi(h)$ .

A criterion for a matrix  $h$  to lie in  $\Gamma_n(q)$  was obtained by Wall in [22]. In the same paper, Wall described the conjugacy classes of finite symplectic and orthogonal groups over fields of odd characteristic, and it turns out that the matrices of  $\Gamma_n(q)$  are very similar to symplectic and orthogonal ones.

**Lemma 4.1.** *If  $q$  is odd, then  $h \in \Gamma_n(q)$  if and only if  $h$  satisfies the following:*

- (i)  $h$  is conjugate to  $h^{-1}$ ,
- (ii) all even parts of  $\lambda_{z-1}(h)$  have even multiplicity,
- (iii) all odd parts of  $\lambda_{z+1}(h)$  have even multiplicity.

*Proof.* See [22, Theorem 2.3.1]. □

**Lemma 4.2.** *Let  $h \in \mathrm{GL}_n(q)$  and let  $q$  be odd. Then  $h$  is conjugate to an element of  $\mathrm{Sp}_n(q)$  if and only if  $h$  satisfies the following:*

- (i)  $h$  is conjugate to  $h^{-1}$ ,
- (ii) all odd parts of  $\lambda_{z-1}(h)$  and  $\lambda_{z+1}(h)$  have even multiplicity.

*Proof.* See [22, p. 36, case (B) (i)]. □

**Lemma 4.3.** *Let  $h \in \mathrm{GL}_n(q)$  and let  $q$  be odd. Then  $h$  is conjugate to an element of  $\mathrm{GO}_n^\varepsilon(q)$  for some  $\varepsilon$  if and only if  $h$  satisfies the following:*

- (i)  $h$  is conjugate to  $h^{-1}$ ,
- (ii) all even parts of  $\lambda_{z-1}(h)$  and  $\lambda_{z+1}(h)$  have even multiplicity.

Suppose that  $n$  is even and  $h$  is a unipotent element satisfying (ii). If  $\lambda_{z-1}(h)$  has odd parts, then  $h$  is conjugate to an element of  $\mathrm{GO}_n^+(q)$  and also to an element of  $\mathrm{GO}_n^-(q)$ . If there are no odd parts, then  $h$  is not conjugate to an element of  $\mathrm{GO}_n^-(q)$ .

Suppose that  $n$  is even,  $|\lambda_{z-1}(h)| = |\lambda_{z+1}(h)| = 0$  and  $h$  satisfies (i). Then  $h$  is conjugate to an element of only one of the groups  $\mathrm{GO}_n^+(q)$  and  $\mathrm{GO}_n^-(q)$ .

*Proof.* See [22, p. 38, Case (C) (i,i')]. □

Next we establish a necessary and sufficient condition for  $h$  to lie in  $\Gamma_n^\square(q)$  or  $\Gamma_n^\boxtimes(q)$ . Let  $h \in \mathrm{GL}_n(q)$ , let  $f$  be the characteristic polynomial of  $h$ , and suppose that  $f = (z-1)^{n_1}(z+1)^{n_2}f_0$  with  $(f_0, z^2-1) = 0$ . Then  $h$  is conjugate to a block diagonal matrix

$$\mathrm{diag}(h_1, h_{-1}, h_0) \tag{4.4}$$

with blocks of dimension  $n_1$ ,  $n_2$  and  $n - n_1 - n_2$ , respectively, corresponding to this factorization of  $f$ . We refer to the matrix in (4.4) as the normal form of  $h$ .

Let  $h \in \Gamma_n(q)$ . We may replace  $h$  by its normal form  $\mathrm{diag}(h_1, h_{-1}, h_0)$  with blocks of dimensions  $n_1$ ,  $n_2$  and  $n - n_1 - n_2$ , respectively, and denote by  $V_1$  the subspace of  $F_q^n$  spanned by the first  $n_1$  rows. Suppose that  $h = gg^\tau$ . Then  $h^g = g^\tau g = h^\tau$ . It follows that  $V_1 g$  is  $h^\tau$ -invariant and the characteristic poly-

mial of  $h^\tau$  on  $V_1 g$  is equal to  $(z-1)^{n_1}$ , and hence  $V_1 g = V_1$ . The same is true for other blocks, and so  $g$  is also block diagonal with blocks  $g_1$ ,  $g_{-1}$  and  $g_0$  of the same dimensions as  $h_1$ ,  $h_{-1}$  and  $h_0$ , respectively (see also [9, Lemma 8.2]). Since  $h_i = g_i g_i^\tau$  for  $i = 1, -1, 0$  and  $\det g = \det g_1 \det g_{-1} \det g_0$ , it suffices to consider the following special cases:  $f = (z-1)^n$ ,  $f = (z+1)^n$ , and  $(f, z^2-1) = 1$ .

Recall that for odd  $q$ , the group  $\Omega_{2n}^\varepsilon(q)$  is the kernel of the spinor norm

$$\theta : \mathrm{SO}_{2n}^\varepsilon(q) \rightarrow F_q^\times / (F_q^\times)^2.$$

The definition of the spinor norm in [20, pp. 163–165] implies the following way to calculate it (see also [3, Proposition 1.6.11]).

**Lemma 4.4.** *Let  $q$  be odd,  $n$  even,  $h \in \mathrm{SO}_n^\varepsilon(q)$  and let  $B$  be the matrix of the invariant symmetric bilinear form of  $\mathrm{SO}_n^\varepsilon(q)$ . Suppose that  $\det(I-h) \neq 0$ . Then  $\theta(h) \equiv \det((I-h)B) \pmod{(F_q^\times)^2}$ .*

**Lemma 4.5.** *Let  $q$  be odd,  $n$  even,  $h \in \Gamma_n(q)$  and let  $f$  be the characteristic polynomial of  $h$ .*

- (i) *If  $f = (z+1)^n$ , then  $h \notin \Gamma_n^\boxtimes(q)$ .*
- (ii) *Let  $f = (z-1)^n$ . If  $\lambda_{z-1}(h)$  has no odd parts, then  $h \notin \Gamma_n^\boxtimes(q)$ ; otherwise,  $h \in \Gamma_n^\square(q) \cap \Gamma_n^\boxtimes(q)$ .*
- (iii) *Let  $(f, z^2-1) = 1$ . Then  $h$  is conjugate to an element of  $\mathrm{SO}_n^\varepsilon(q)$  for some unambiguously defined  $\varepsilon$ , and  $h \in \Gamma_n^\square(q)$  if and only if  $-h$  is conjugate to an element of  $\Omega_n^\varepsilon(q)$ .*

*Proof.* Let  $h = gg^\tau$ . Possibilities for  $g$  in the first two cases are found in [9, Section 8], and we use this result for calculations. For brevity, we write  $x \equiv y$  to denote that  $x \equiv y \pmod{(F_q^\times)^2}$ .

(i) The group  $\mathrm{GL}_n(q) \rtimes \langle \tau \rangle$  can be embedded into  $\mathrm{GL}_{2n}(q)$ , and we consider the Jordan decomposition of  $g\tau$  in the latter group. So  $g\tau = ug_1\tau = g_1\tau u$ , where  $u$  is unipotent and  $(g_1\tau)^2 = -I$ ; i.e.  $g_1$  is a skew-symmetric matrix. Since the determinant of a skew-symmetric matrix is a square and  $\det u = 1$ , we see that  $\det g$  is also a square.

(ii) Similarly,  $g\tau = ug_1\tau = g_1\tau u$ , where  $u$  is unipotent and  $(g_1\tau)^2 = I$ ; i.e.  $g_1$  is a symmetric matrix. Furthermore,  $h = u^2$  and the equality  $ug_1\tau = g_1\tau u$  is equivalent to the condition that  $u$  preserves the bilinear form defined by  $g_1$ . By Lemma 4.3, if  $\lambda_{z-1}(u) = \lambda_{z-1}(h)$  has odd parts, then  $u$  is conjugate both to an element of  $\mathrm{SO}_n^+(q)$  and to an element of  $\mathrm{SO}_n^-(q)$ , and so we can choose  $g_1$  with any determinant, square or non-square. If  $\lambda(u)$  has no odd parts, then  $u$  is conjugate to an element of  $\mathrm{SO}_n^+(q)$  only, and since the multiplicities of even parts are even,  $n$  is divisible by 4. In this case  $\det g_1 \equiv \det I$ .

(iii) The fact that  $h$  is conjugate to an element of  $\mathrm{SO}_n^\varepsilon(q)$ , where  $\varepsilon$  is unambiguously defined, follows from Lemmas 4.1 and 4.3. By Lemma 4.4, we have  $\theta(h) \equiv \det(I - h) \det B$ , where  $B$  is the matrix of the symmetric bilinear form preserved by  $h$ . Observing that  $\theta(-I) \equiv \det B$ , we have

$$\theta(-h) \equiv \det(I - h) = \det(I - gg^\tau) = \det(g^\tau - g) \det g^\tau \equiv \det g,$$

where the final equivalence holds because the determinant of the skew-symmetric matrix  $g^\tau - g$  is a square. The proof is complete.  $\square$

We are ready to find  $\omega(\tau\mathrm{PGL}_n(q))$  and  $\omega(\tau\mathrm{PSL}_n(q))$ .

**Lemma 4.6.** *Let  $q$  and  $n \geq 3$  be odd. Then*

$$\omega(\tau\mathrm{PSL}_n(q)) = \omega(\tau\mathrm{PGL}_n(q)) = 2 \cdot \omega(\mathrm{Sp}_{n-1}(q)).$$

*Proof.* The first equality was established in (4.1). To prove the second one, we need to show that the set of the projective orders of elements of  $\Gamma_n(q)$  is equal to  $\omega(\mathrm{Sp}_{n-1}(q))$ .

Let  $h \in \Gamma_n(q)$ . Since  $n$  is odd, Lemma 4.1 implies that 1 is an eigenvalue of  $h$ . It follows that the projective order of  $h$  is equal to the ordinary order.

We show first that  $|h| \in \omega(\mathrm{Sp}_{n-1}(q))$ . Let  $\mathrm{diag}(h_1, h_{-1}, h_0)$  be the normal form of  $h$  as in (4.4) and denote the dimension of  $h_1$  by  $k$ . Then  $k$  is odd. By Lemmas 4.1 and 4.2, the unipotent matrix  $h_1$  is conjugate to an element of  $\mathrm{SO}_k(q)$  and the matrix  $\mathrm{diag}(h_{-1}, h_0)$  is conjugate to an element of  $\mathrm{Sp}_{n-k}(q)$ . If  $k = 1$ , then there is nothing to prove. If  $k > 1$ , then  $|h_1| \in \omega_p(\mathrm{SO}_k(q)) = \omega_p(\mathrm{Sp}_{k-1}(q))$ , and hence  $|h| \in \omega(\mathrm{Sp}_k(q) \times \mathrm{Sp}_{n-k}(q)) \subseteq \omega(\mathrm{Sp}_{n-1}(q))$ .

It follows from Lemmas 4.1 and 4.2 that a semisimple matrix lies in  $\Gamma_n(q)$  if and only if it is conjugate to a matrix of the form  $\mathrm{diag}(1, h')$  with  $h' \in \mathrm{Sp}_{n-1}(q)$ , and thus  $\omega_{p'}(\Gamma_n(q)) = \omega_{p'}(\mathrm{Sp}_{n-1}(q))$ .

Let  $a \in \omega(\mathrm{Sp}_{n-1}(q))$  and  $|a|_p = p^t > 1$ . If  $a = 2p^t$  and  $n - 1 = p^{t-1} + 1$  (i.e. the condition from (v) of Lemma 2.2 holds), we define  $h = \mathrm{diag}(1, -J_{n-1})$ . If  $a = p^t$  or  $n - 1 > p^{t-1} + 1$ , there is a semisimple matrix  $h_s \in \mathrm{Sp}_l(q)$ , where  $n - 1 = p^{t-1} + 1 + l$ , such that  $a = p^t |h_s|$ , and we define  $h = \mathrm{diag}(J_{p^{t-1}+2}, h_s)$ . It is easy to see that  $h \in \Gamma_n(q)$  and  $|h| = a$ . The proof is complete.  $\square$

**Lemma 4.7.** *Let  $q$  be odd and  $n \geq 4$  be even. Then*

$$\omega(\tau\mathrm{PGL}_n(q)) = 2 \cdot \omega(\mathrm{PSp}_n(q))$$

and

$$\omega_{p'}(\tau\mathrm{PSL}_n(q)) = 2 \cdot \omega_{p'}(\mathrm{P}\Omega_n^+(q)) \cup 2 \cdot \omega_{p'}(\mathrm{P}\Omega_n^-(q)).$$

If  $n > 4$ , then

$$\omega_{\bar{p}}(\tau\mathrm{PSL}_n(q)) = 2 \cdot \omega_{\bar{p}}(\Omega_{n+1}(q)).$$

The set  $\omega_{\bar{p}}(\tau\mathrm{PSL}_4(q))$  consists of all multiples of  $p$  dividing  $p(q \pm 1)$  if  $p > 3$ , and it consists of these multiples together with 18 if  $p = 3$ .

*Proof.* It suffices to find the sets of the projective orders of elements of  $\Gamma_n(q)$  and  $\Gamma_n^\square(q)$ . For brevity, we denote these sets by  $\omega(\mathrm{P}\Gamma_n(q))$  and  $\omega(\mathrm{P}\Gamma_n^\square(q))$ , respectively. Also we denote by  $Z$  the center of  $\mathrm{GL}_n(q)$ .

Let  $h \in \Gamma_n(q)$  and  $\mathrm{diag}(h_1, h_{-1}, h_0)$  be the normal form of  $h$ . Since  $n$  is even, it follows from Lemma 4.1 that the dimension of  $h_1$  is even too. We denote this dimension by  $2k$  and define  $h_2 = \mathrm{diag}(h_{-1}, h_0)$ . Then  $h_1$  is conjugate to an element of  $\mathrm{SO}_{2k}^+(q)$  and  $h_2$  is conjugate to an element of  $\mathrm{Sp}_{n-2k}(q)$ .

Let  $k > 0$ . Then  $|h_1| \in \omega_p(\mathrm{SO}_{2k}^+(q)) = \omega_p(\mathrm{Sp}_{2k-2}(q))$ , and hence

$$|h| \in \omega(\mathrm{Sp}_{2k-2}(q) \times \mathrm{Sp}_{n-2k}(q)) \subseteq \omega(\mathrm{Sp}_{n-2}(q)).$$

Using Lemmas 2.2 and 2.3, it is easy to check that

$$\omega_{p'}(\mathrm{Sp}_{n-2}(q)) \subseteq \omega_{p'}(\mathrm{P}\Omega_n^+(q)) \cup \omega_{p'}(\mathrm{P}\Omega_n^-(q)) \subseteq \omega(\mathrm{PSp}_n(q))$$

and

$$\omega_{\bar{p}}(\mathrm{Sp}_{n-2}(q)) \subseteq \omega_{\bar{p}}(\Omega_{n+1}(q)) \subseteq \omega_{\bar{p}}(\mathrm{PSp}_n(q)).$$

Thus the projective order of  $h$  lies in the required sets.

Let  $k = 0$ . Then  $h = h_2$  and  $|hZ| \in \omega(\mathrm{PSp}_n(q))$ . It follows that

$$(\mathrm{P}\Gamma_n(q)) \subseteq \omega(\mathrm{PSp}_n(q)).$$

Suppose, in addition, that  $h \in \Gamma_n^\square(q)$ . Denote the dimension of  $h_{-1}$  by  $2l$ . By Lemma 4.5, we deduce that  $h_{-1} \notin \Gamma_{2l}^\boxtimes(q)$ , and so  $-h_0$  is conjugate to an element of  $\Omega_{n-2l}^\varepsilon(q)$  for some  $\varepsilon$ . Observe that  $|hZ| = |-hZ|$ .

Assume that  $|-h_{-1}| > 1$ . Then

$$|-hZ| = |-h| = |-h_{-1}| \cdot |-h_0|.$$

Since  $|-h_{-1}| \in \omega_p(\mathrm{Sp}_{2l}(q)) = \omega_p(\Omega_{2l+1}(q))$ , we have

$$|hZ| \in \omega_{\bar{p}}(\Omega_{2l+1}(q) \times \Omega_{n-2l}^\varepsilon(q)) \subseteq \omega_{\bar{p}}(\Omega_{n+1}(q)).$$

Furthermore, if  $n = 4$ , then either  $|hZ| = 9$  and  $p = 3$ , or  $|hZ|$  lies in  $p \cdot \Omega_2^\varepsilon(q)$  and, therefore, divides  $p(q - \varepsilon)/2$ .

If  $|-h_{-1}| = 1$ , then either  $l = 0$  and  $h = h_0$ , or  $l > 0$  and  $|-hZ| = |-h_0|$ . In either case,  $|-hZ| \in \omega(\mathrm{P}\Omega_n^\varepsilon(q)) \subseteq \omega(\Omega_{n+1}(q))$ . In particular, if  $n = 4$  and the order  $|-hZ|$  is a multiple of  $p$ , then it divides  $p(q \pm 1)/2$ .

Now we prove the reverse containments. If  $h$  is semisimple, then  $h \in \Gamma_n(q)$  if and only if  $h$  is conjugate to an element of  $\mathrm{Sp}_n(q)$ , and hence

$$\omega_{p'}(\mathrm{PSp}_n(q)) \subseteq \omega(\mathrm{P}\Gamma_n(q)).$$

Let  $a \in \omega(\mathrm{PSp}_n(q))$ ,  $|a|_p = p^t > 1$ . Lemma 2.2 implies that there is a semisimple matrix  $h_s \in \mathrm{Sp}_l(q)$ , where  $n = p^{t-1} + 1 + l$ , such that  $a = p^t |h_s|$ , and we define  $h = \mathrm{diag}(-J_{p^{t-1}+1}, -h_s)$ . It is easy to see that  $h \in \Gamma_n(q)$  and

$$|hZ| = |-hZ| = |-h| = a.$$

Thus

$$\omega_{\bar{p}}(\mathrm{PSp}_n(q)) \subseteq \omega(\mathrm{P}\Gamma_n(q)),$$

and the assertion concerning  $\tau\mathrm{PGL}_n(q)$  follows.

Let  $h \in \Omega_n^\varepsilon(q)$  be semisimple and let  $\mathrm{diag}(h_1, h_{-1}, h_0)$  be the normal form of  $h$ , with  $h_1, h_{-1}$  of dimension  $k$  and  $l$ , respectively. If  $k > 0$ , then  $h \in \Gamma_n^\square(q)$  by Lemma 4.5 (ii). If  $k = 0$ , then applying (i) or (iii) of Lemma 4.5 according as  $l > 0$  or  $l = 0$ , we deduce that  $-h \in \Gamma_n^\square(q)$ . In any case,  $|hZ| \in \omega(\mathrm{P}\Gamma_n^\square(q))$ .

Suppose  $n > 4$  and  $a \in \omega_{\bar{p}}(\Omega_{n+1}(q))$ , or  $n = 4$  and  $a = pc$  with  $c$  dividing  $(q \pm 1)/2$ , or  $n = 4$ ,  $p = 3$  and  $a = 9$ . Let  $|a|_p = p^t$ . By Lemmas 2.2 and 2.3, there are  $\varepsilon \in \{+, -\}$  and a semisimple matrix  $h_s \in \Omega_l^\varepsilon(q)$ , where  $n = p^{t-1} + 1 + l$ , such that  $a = p^t |h_s|$ . Defining  $h = \mathrm{diag}(-J_{p^{t-1}+1}, -h_s)$ , we see that  $h \in \Gamma_n^\square(q)$  and  $|hZ| = |-hZ| = |-h| = a$ . The proof is complete.  $\square$

In contrast to the sets of the projective orders of elements of  $\Gamma_n(q)$  and  $\Gamma_n^\square(q)$ , the corresponding set for  $\Gamma_n^\boxtimes(q)$ , where  $n$  is even, is not in general closed under taking divisors. So we do not give an explicit description of the set  $\omega(\tau\delta\mathrm{PSL}_n(q))$  for even  $n$ . However, we derive some properties of this set.

**Lemma 4.8.** *Let  $q$  be odd and  $n \geq 4$  even. Then  $\omega(\tau\delta\mathrm{PSL}_n(q)) \not\subseteq \omega(\mathrm{PSL}_n(q))$ . If  $k = 2^s$ , where  $s \geq 0$ , and  $q = q_0^k$ , then  $k \cdot \omega(\tau\delta(q_0)\mathrm{PSL}_n(q_0)) \not\subseteq \omega(\mathrm{PSU}_n(q))$ . In particular,  $\omega(\tau\delta(-q)\mathrm{PSU}_n(q)) \not\subseteq \omega(\mathrm{PSU}_n(q))$ .*

*Proof.* Recall that  $\omega(\tau\delta\mathrm{PSL}_n(q))$  consists of the projective orders of matrices of  $\Gamma_n^\boxtimes(q)$  multiplied by 2.

There is an element  $h \in \mathrm{SO}_n^\varepsilon(q) \setminus \Omega_n^\varepsilon(q)$  whose projective order is equal to  $(q^{n/2} - \epsilon)/2$ . By Lemma 4.5, it follows that  $-h \in \Gamma_n^\boxtimes(q)$ , and so we obtain that  $q^{n/2} \pm 1 \in \omega(\tau\delta\mathrm{PSL}_n(q))$ .

Assume that  $n > 4$  and  $l = (n - 2)/2$  is odd. Then Lemma 2.2 together with the existence of primitive divisors  $r_l(\pm q)$  implies that

$$p(q^l \pm 1) \in \omega(\mathrm{PSp}_n(q)) \setminus \omega(\Omega_{n+1}(q)).$$

Applying Lemma 4.7, we see that

$$2p(q^l \pm 1) \in \omega(\tau\mathrm{PGL}_n(q)) \setminus \omega(\tau\mathrm{PSL}_n(q)) \subseteq \omega(\tau\delta\mathrm{PSL}_n(q)). \quad (4.5)$$

Assume now that  $n = 4$  and  $q \equiv \epsilon \pmod{4}$ . The numbers  $p(q+1)$  and  $p(q-\epsilon)$  lie in  $\omega(\mathrm{PSp}_4(q))$  and do not divide  $p(q \pm 1)/2$  (if  $q-1$  divides  $(q+1)/2$ , then  $q = 3$ ), and hence

$$2p(q+1), 2p(q-\epsilon) \in \omega(\tau\delta\mathrm{PSL}_4(q)). \quad (4.6)$$

We prove the first assertion of the lemma and the second assertion for  $k = 1$  together. To this end, suppose that  $\omega(\tau\delta\mathrm{PSL}_n(q)) \subseteq \omega(\mathrm{PSL}_n^\epsilon(q))$  and as usual define  $d = (n, q - \epsilon)$ . Then  $q^{n/2} + \epsilon^{n/2} \in \omega(\mathrm{PSL}_n^\epsilon(q))$ . By Lemma 2.7, this is equivalent to  $(n)_2 > (q - \epsilon)_2$ . It follows that  $l = (n - 2)/2$  is odd and

$$(d)_2 = (q - \epsilon)_2,$$

and so  $(q^l - \epsilon)/d$  is odd. Then  $2(q^l + \epsilon)$  does not divide  $(q^{n-2} - 1)/d$  and, therefore,  $2p(q^l + \epsilon) \notin \omega(\mathrm{PSL}_n^\epsilon(q))$ . If  $n > 4$ , this contradicts (4.5). If  $n = 4$ , then  $q \equiv -\epsilon \pmod{4}$  and (4.6) implies that  $2p(q + \epsilon) \in \omega(\tau\delta\mathrm{PSL}_4(q))$  yielding a contradiction.

Suppose that  $k > 1$  and  $k \cdot \omega(\tau\delta(q_0)\mathrm{PSL}_n(q_0)) \subseteq \omega(\mathrm{PSU}_n(q))$ . Observe that  $(q+1)_2 = 2$  and choose  $\epsilon$  so that  $q_0 \equiv \epsilon \pmod{4}$ . Let  $n/2$  be odd. By assumption, we have  $a = k(q_0^{n/2} - \epsilon) \in \omega(\mathrm{PSU}_n(q))$ . Since  $a$  is a multiple of  $r_{n/2}(\epsilon q_0)$  and  $r_{n/2}(\epsilon q_0) \in R_{n/2}(q) = R_n(-q)$ , it follows that  $a$  divides

$$c = \frac{q^n - 1}{(q+1)(n, q+1)}.$$

This is a contradiction because

$$(a)_2 = (q^{n/2} - 1)_2 > (c)_2 = \frac{(q^n - 1)_2}{4}.$$

Thus  $l = (n - 2)/2$  is odd and by (4.5) and (4.6), we have

$$2p(q_0^l - \epsilon) \in \omega(\tau\delta\mathrm{PSL}_n(q_0)).$$

Then  $a = 2kp(q_0^l - \epsilon) \in \omega(\mathrm{PSU}_n(q))$ , and hence  $a$  divides  $p(q^{n-2} - 1)/(n, q+1)$ . This contradicts  $(a)_2 = (q^{n-2} - 1)_2$ .

The final assertion follows from the second one and Lemma 3.3.  $\square$

We close this section with a proof of Theorem 1 and one of its consequences.

*Proof of Theorem 1.* Recall that  $L = \mathrm{PSL}_n^\epsilon(q)$ ,  $d = (n, q - \epsilon)$  and consider the difference  $\omega(\tau L) \setminus \omega(L)$ . We analyze separately two cases according as  $n$  is odd or even.

Let  $n$  be odd. By Lemma 4.6, the difference under consideration is equal to  $2 \cdot \omega(\text{Sp}_{n-1}(q)) \setminus \omega(L)$ . We consider the numbers from Lemma 2.2 defining  $\omega(\text{Sp}_{n-1}(q))$  in turn.

Let  $a = 2p^t$ , where  $p^{t-1} + 1 = n - 1$ . Any element of  $\omega(L)$  that is a multiple of  $p^t$  divides  $p^t(q - \varepsilon)/d$ . Since  $d$  is odd,  $2a$  divides  $p^t(q - \varepsilon)/d$  if and only if 4 divides  $q - \varepsilon$ . Thus  $4p^t \in \omega(\tau L) \setminus \omega(L)$  if and only if  $n = p^{t-1} + 2$  for some  $t \geq 1$  and  $q \equiv -\varepsilon \pmod{4}$ .

Let

$$a = p^t[q^{n_1} \pm 1, q^{n_2} \pm 1, \dots, q^{n_s} \pm 1],$$

where  $p^{t-1} + 1 + 2n_1 + 2n_2 + \dots + 2n_s = n - 1$ , or

$$a = [q^{n_1} \pm 1, q^{n_2} \pm 1, \dots, q^{n_s} \pm 1],$$

where  $s \geq 2$  and  $2(n_1 + n_2 + \dots + n_s) = n - 1$ . Then  $2a$  divides  $p^t[q^{2n_1} - 1, q^{2n_2} - 1, \dots, q^{2n_s} - 1, q - \varepsilon]$  or  $[q^{2n_1} - 1, q^{2n_2} - 1, \dots, q^{2n_s} - 1, q - \varepsilon]$ , respectively.

The remaining possibility is  $a = q^l \pm 1$ , where  $l = (n - 1)/2$ . If  $a = q^l + \varepsilon^l$ , then  $2a$  divides

$$\frac{q^{n-1} - 1}{d} = (q^l + \varepsilon^l) \frac{q^l - \varepsilon^l}{d}$$

since  $d$  is odd. Let  $a = q^l - \varepsilon^l$ . Assume that  $l$  is not a 2-power. Then  $(l)_2 \leq l/3$ , and hence  $l + 2(l)_2 < n$ . It follows that  $L$  has an element of order

$$c = [q^l - \varepsilon^l, q^{2(l)_2} - 1, q - \varepsilon].$$

Since  $2(a)_2 = 2(q^l - \varepsilon^l)_2 \leq (q^{2l} - 1)_2 = (q^{2(l)_2} - 1)_2$ , we have that  $2a$  divides  $c$ . Finally, assume that  $l$  is a 2-power. Then the 2-exponent of  $L$  is equal to  $(q^{2l} - 1)_2$  and any element of  $\omega(L)$  that is a multiple of  $(q^{2l} - 1)_2$  divides  $(q^{2l} - 1)/d$ . Clearly,  $2a$  divides  $(q^{2l} - 1)/d$  if and only if  $d$  divides  $q^l + \varepsilon^l$ , which is equivalent to  $d = 1$ . Thus  $2(q^l - \varepsilon^l) \in \omega(\tau L) \setminus \omega(L)$  if and only if  $n - 1 = 2^t$  and  $d \neq 1$ .

Let  $n$  be even. By Lemma 4.7, the set  $\omega_{\bar{p}}(\tau L)$  is equal to  $2 \cdot \omega_{\bar{p}}(\Omega_{n+1}(q))$  if  $n > 4$ , it consists of divisors of  $p(q \pm 1)$  if  $n = 4$  and  $p > 3$ , and it consists of divisors of  $p(q \pm 1)$  together with 18 if  $n = 4$  and  $p = 3$ . We can consider the numbers from Lemma 2.2 defining  $\omega_{\bar{p}}(\Omega_{n+1}(q))$  for  $n \geq 6$  and the numbers defining  $\omega_{\bar{p}}(\tau L)$  for  $n = 4$  together.

If  $a = p^t$  and  $n = p^{t-1} + 1$ , then  $2a \notin \omega(L)$ .

Let

$$a = p^t[q^{n_1} \pm 1, q^{n_2} \pm 1, \dots, q^{n_s} \pm 1],$$

where  $s \geq 2$  and  $p^{t-1} + 1 + 2n_1 + 2n_2 + \dots + 2n_s = n$ . Then we have that  $2a$  divides  $p^t[q^{2n_1} - 1, q^{2n_2} - 1, \dots, q^{2n_s} - 1] \in \omega(L)$ .

Let  $a = p^t(q^{n_1} - \epsilon)/2$ , where  $p^{t-1} + 1 + 2n_1 = n$ . If  $\epsilon = \varepsilon^{n_1}$ , then  $2a$  divides  $p^t(q^{n_1} - \varepsilon^{n_1}) \in \omega(L)$ , while if  $\epsilon = -\varepsilon^{n_1}$ , then  $2a$  divides

$$p^t \frac{q^{2n_1} - 1}{d} = p^t (q^{n_1} + \varepsilon^{n_1}) \frac{q^{n_1} - \varepsilon^{n_1}}{d}.$$

Thus

$$\omega_{\tilde{p}}(\tau L) \subseteq \omega(L),$$

whenever  $n \neq p^{t-1} + 1$ .

To handle  $\omega_{p'}(\tau L) = 2 \cdot \omega(\text{P}\Omega_{2n}^+(q)) \cup 2 \cdot \omega(\text{P}\Omega_{2n}^-(q))$ , we consider the numbers from Lemma 2.3 that define  $\omega_{p'}(\text{P}\Omega_{2n}^\pm(q))$ .

Let

$$a = [q^{n_1} \pm 1, q^{n_2} \pm 1, \dots, q^{n_s} \pm 1],$$

where  $s \geq 3$  and  $2(n_1 + n_2 + \dots + n_s) = n$ . In this case, we have that  $2a$  divides  $[q^{2n_1} - 1, q^{2n_2} - 1, \dots, q^{2n_s} - 1] \in \omega(L)$ .

Let  $a = (q^{n/2} - \epsilon)/(4, q^{n/2} - \epsilon)$ . If  $\epsilon = \varepsilon^{n/2}$ , then  $2a$  divides

$$q^{n/2} - \varepsilon^{n/2} \in \omega(L).$$

If  $\epsilon = -\varepsilon^{n/2}$  and  $(4, q^{n/2} + \varepsilon^{n/2}) = 4$ , then  $2a$  divides

$$\frac{q^n - 1}{(q - \varepsilon)d} = \frac{(q^{n/2} + \varepsilon^{n/2})(q^{n/2} - \varepsilon^{n/2})}{(q - \varepsilon)d}$$

because  $d/2$  divides  $(n/2, q - \varepsilon) = ((q^{n/2} - \varepsilon^{n/2})/(q - \varepsilon), q - \varepsilon)$ . If  $\epsilon = -\varepsilon^{n/2}$  and  $(4, q^{n/2} + \varepsilon^{n/2}) = 2$ , then Lemma 2.7 implies that  $2a = q^{n/2} + \varepsilon^{n/2}$  does not lie in  $\omega(L)$  if and only if  $(n)_2 \leq (q - \varepsilon)_2$ . Assuming the last inequality, the condition  $(4, q^{n/2} + \varepsilon^{n/2}) = 2$  is equivalent to  $q \equiv \varepsilon \pmod{4}$ .

Finally, let  $a = [q^{n_1} - \epsilon_1, q^{n_2} - \epsilon_2]/e$ , where  $2(n_1 + n_2) = n$  and with  $e = 2$  if  $(q^{n_1} - \epsilon_1)_2 = (q^{n_2} - \epsilon_2)_2$  and  $e = 1$  if  $(q^{n_1} - \epsilon_1)_2 \neq (q^{n_2} - \epsilon_2)_2$ . We define  $n_0 = n/(2n_1, 2n_2)$ . We may assume that  $(q^{n_1} - \epsilon_1)_2 \geq (q^{n_2} - \epsilon_2)_2$ .

If  $\epsilon_2 = \varepsilon^{n_2}$ , then  $2a$  divides  $[q^{2n_1} - 1, q^{n_2} - \varepsilon^{n_2}] \in \omega(L)$  since

$$2(a)_2 \leq 2(q^{n_1} - \epsilon_1)_2 \leq (q^{2n_1} - 1)_2.$$

Similarly, we obtain that if  $\epsilon_1 = \varepsilon^{n_1}$  and  $(q^{n_1} - \epsilon_1)_2 = (q^{n_2} - \epsilon_2)_2$ , then  $2a$  divides  $[q^{2n_2} - 1, q^{n_1} - \varepsilon^{n_1}]$ .

Let  $\epsilon_2 = -\varepsilon^{n_2}$  and  $\epsilon_1 = -\varepsilon^{n_1}$ . If  $e = 2$ , then  $2a$  divides

$$\frac{[q^{2n_1} - 1, q^{2n_2} - 1]}{q - \varepsilon}.$$

If  $e = 1$ , then  $n_1$  and  $n_2$  have opposite parity, therefore,  $n/2$  is odd. It follows that  $n_0$  is odd too, and  $2a$  divides  $[q^{2n_1} - 1, q^{2n_2} - 1]/(n_0, q - \varepsilon)$ .

Let  $\epsilon_2 = -\epsilon^{n_2}$  and  $\epsilon_1 = \epsilon^{n_1}$ . We may assume that  $(q^{n_1} - \epsilon^{n_1})_2 > (q^{n_2} + \epsilon^{n_2})_2$ . If  $n_1 \neq (n_1)_2$ , then

$$n_1 + 2(n_1)_2 + 2n_2 < n$$

and  $2a$  divides  $[q^{n_1} - \epsilon^{n_1}, q^{2(n_1)_2} - 1]$ . If  $2(q^{n_1} - \epsilon^{n_1})_2 \leq (q^{2n_2} - 1)_2$ , then  $2a$  divides  $[q^{2n_2} - 1, q^{n_1} - \epsilon^{n_1}]$ . If  $q^{n_2} + \epsilon^{n_2}$  divides  $q^{2n_1} - 1$ , then  $2a$  divides  $q^{2n_1} - 1$  too. Finally, if  $(n_0, q - \epsilon) = 1$ , then  $2a$  divides  $[q^{2n_1} - 1, q^{2n_2} - 1]$ .

Thus it remains to consider the case when  $n_1 = (n_1)_2$ ,  $2(q^{n_1} - \epsilon^{n_1})_2 > (q^{2n_2} - 1)_2$ ,  $q^{n_2} + \epsilon^{n_2}$  does not divide  $q^{2n_1} - 1$  and  $(n_0, q - \epsilon) \neq 1$ . The two first conditions yield  $n_1 > (n_2)_2$ . In particular,  $(n/2)_2 = (n_2)_2$  and  $n_0 = n/(2n_2)_2 = (n)_{2'}$ . Then the third condition is equivalent to  $n_2$  not being a 2-power. Observe that

$$(n)_{2'} = \frac{n}{(2n_2)_2} = \frac{n_1 + n_2}{(n_2)_2} = \frac{n_1}{(n_2)_2} + (n_2)_{2'}.$$

It follows that  $(n)_{2'}$  is a sum of a non-identity 2-power and an odd number greater than 1 and also  $((n)_{2'}, q - \epsilon) \neq 1$ . In particular,  $(n)_{2'} > 3$  and  $(n, q - \epsilon)_{2'} \neq 1$ .

Conversely, suppose that  $n = 2^t \cdot l$ , where  $t \geq 1$ ,  $l \geq 5$  is odd and  $(n, q - \epsilon)$  is divisible by an odd prime  $r$ . Writing  $n_1 = (n)_2 = 2^t$ ,  $n_2 = n/2 - n_1 = 2^{t-1}(l-2)$  and  $a = [q^{n_1} - 1, q^{n_2} + \epsilon^{n_2}]$ , we see that

$$(q^{n_1} - 1)_2 = 2^{t-1}(q^2 - 1)_2 > (n_2)_2(q + \epsilon)_2 \geq (q^{n_2} + \epsilon^{n_2})_2$$

and hence  $2a \in \omega(\tau L)$ . Assume that  $2a \in \omega(L)$  and let

$$c = \frac{[q^{l_1} - \epsilon^{l_1}, \dots, q^{l_s} - \epsilon^{l_s}]}{f},$$

where  $l_1 + \dots + l_s = n$ , be a number from Lemma 2.1 that  $2a$  divides. Since  $2(a)_2 = 2(q^{n_1} - 1)_2 = (q^{2n_1} - 1)_2$ , it follows that at least one of the numbers  $l_1, \dots, l_s$  is a multiple of  $2n_1$ . Also  $r_{2n_2}(\epsilon q)$  divides  $a$ , and hence at least one of them is a multiple of  $2n_2$ . Observing that  $[2n_1, 2n_2] = 2^{t+1}(l-2) > 2^t l = n$ , we deduce that those are different numbers, which yields  $s = 2$ ,  $l_1 = 2n_1$  and  $l_2 = 2n_2$ . Then  $f = (n/(2n_1, 2n_2), q - \epsilon)$ , and so  $(f)_r > 1$ . Since  $(r, q + \epsilon) = (r, n_1) = (r, n_2) = 1$ , it follows that

$$(c)_r = \frac{(q - \epsilon)_r}{(f)_r} < (q - \epsilon)_r = (a)_r.$$

This is a contradiction, therefore,  $2a \notin \omega(L)$ , and the proof is complete.  $\square$

An interesting consequence of Theorem 1 is that whenever  $\tau$  is admissible as an automorphism of  $\text{PSL}_n^\epsilon(q)$ , it is also admissible as an automorphism of  $\text{PSL}_n^\epsilon(q^{1/k})$  for every odd  $k$ .

**Lemma 4.9.** *Let  $k$  be odd and  $q = q_0^k$ . If  $\omega(\tau L) \subseteq \omega(L)$ , then*

$$\omega(\tau \text{PSL}_n^\varepsilon(q_0)) \subseteq \omega(\text{PSL}_n^\varepsilon(q_0)).$$

*In particular, if  $\varepsilon = +$ ,  $\tau$  and  $\beta = \varphi^{m/k}$  are admissible for  $L$ , then  $\beta\tau$  is also admissible.*

*Proof.* Assume that  $\omega(\tau \text{PSL}_n^\varepsilon(q_0)) \not\subseteq \omega(\text{PSL}_n^\varepsilon(q_0))$ . This implies that the numbers  $n$  and  $q_0$  satisfy the conditions of one of items (i)–(v) of Theorem 1. Since  $k$  is odd, it follows that  $(n, q_0 - \varepsilon)$  divides  $(n, q - \varepsilon)$  and  $(q - 1)_2 = (q_0 - 1)_2$ , and thus the numbers  $n$  and  $q$  satisfy the same conditions. This contradicts the hypothesis that  $\omega(\tau L) \subseteq \omega(L)$ .

To prove the second assertion, it suffices to show that  $\omega(\beta\tau L) \subseteq \omega(L)$ . By Lemma 3.3, the proved containment and admissibility of  $\beta$ , we see that

$$\omega(\beta\tau L) = k \cdot \omega(\tau \text{PSL}_n(q_0)) \subseteq k \cdot \omega(\text{PSL}_n(q_0)) = \omega(\beta L) \subseteq \omega(L),$$

and the proof is complete.  $\square$

## 5 Admissible groups

In this section, we prove Theorems 2 and 3. As we have mentioned, the theorems with  $n = 3$  were proved in [23, 24], and so we assume that  $n \geq 4$ . Throughout this section,  $q = p^m$  is odd,  $L = \text{PSL}_n^\varepsilon(q)$  and  $G$  is a group such that  $L < G \leq \text{Aut } L$ . Also, we fix the numbers  $d = (n, q - \varepsilon)$  and  $b = ((q - \varepsilon)/d, m)_d$ .

We begin with lemmas that hold for both linear and unitary groups. We say that a subgroup of  $\text{Out } L$  is admissible if it is the image of an admissible group.

**Lemma 5.1.** *If  $G \cap \text{Inndiag } L > L$ , then  $\omega(G) \neq \omega(L)$ . In particular, admissible groups of  $\text{Out } L$  are abelian and any non-trivial admissible subgroup of the group  $\langle \bar{\delta} \rangle \rtimes \langle \bar{\tau} \rangle$  is conjugate in this group to  $\langle \bar{\tau} \rangle$ .*

*Proof.* By Lemma 2.1, if  $|G \cap \text{Inndiag } L|/|L| = i > 1$ , then  $G$  has an element of order  $(q^n - \varepsilon^n)i/(q - \varepsilon)d$ , which does not lie in  $\omega(L)$ . Thus admissible groups of  $\text{Out } L$  can be embedded into the image of the group generated by  $\varphi$  and  $\gamma$ , which is abelian. The group  $\langle \bar{\delta} \rangle \rtimes \langle \bar{\tau} \rangle$  is dihedral, and so all of its non-trivial subgroups that intersect trivially with  $\langle \bar{\delta} \rangle$  are conjugate to  $\langle \bar{\tau} \rangle$  or  $\langle \bar{\delta}\bar{\tau} \rangle$ , and in the latter case we may assume that  $n$  is even. But Lemma 4.8 says that  $\langle \bar{\delta}\bar{\tau} \rangle$  is not admissible.  $\square$

**Lemma 5.2.** *Suppose that  $n \geq 5$  and  $|G/L|$  is odd. Then  $\omega(G) = \omega(L)$  if and only if  $n - 1$  is not a  $p$ -power,  $G/L$  is conjugate in  $\text{Out } L$  to a subgroup of  $\langle \bar{\varphi} \rangle$  and  $|G/L|$  divides  $((q - \varepsilon)/d, m)_d$ .*

*Proof.* If  $\varepsilon = +$ , the assertion is proved in [11, Propositions 6,7], and if  $\varepsilon = -$ , it is proved in [13, Proposition 6].  $\square$

**Lemma 5.3.** *Let  $n = 4$  and  $|G/L|$  is odd. Then  $\omega(G) = \omega(L)$  if and only if 12 divides  $q + \varepsilon$  and  $G/L$  is a 3-group.*

*Proof.* Let  $\omega(G) = \omega(L)$  and  $r \in \pi(G/L)$ . Then  $G$  contains a field automorphism of order  $r$ , and hence by Lemma 3.3,  $\omega(G)$  includes  $r \cdot \omega(\text{PSL}_4^\varepsilon(q_0))$ , where  $q = q_0^r$ . It follows that  $rr_4(q_0), rr_3(\varepsilon q_0) \in \omega(L)$ . Since  $r_4(q_0) \in R_4(q)$ , we see that  $r$  divides  $a = (q^2 + 1)(q + \varepsilon)/d$  and, in particular, it does not divide  $q - \varepsilon$ . If  $r \neq 3$ , then  $r_3(\varepsilon q_0) \in R_3(\varepsilon q)$ , and so  $r$  divides  $c = (q^3 - \varepsilon)/d$ , which is a contradiction because  $(a, c) = 1$ . Let  $r = 3$ . Then 3 divides  $q + \varepsilon$ . Since  $3p(q_0 - \varepsilon)$  is an element of  $\omega(L)$ , we have that  $3(q_0 - \varepsilon)$  divides  $(q^2 - 1)/d$ , and thus 4 divides  $q + \varepsilon$ .

Conversely, let 12 divide  $q + \varepsilon$  and  $G/L$  be a 3-group. We may assume that  $G$  is the extension of  $L$  by a field automorphism of order dividing  $(m)_3$ . To prove that  $\omega(G) \subseteq \omega(L)$ , it suffices to check  $k \cdot \omega(\text{PSL}_4^\varepsilon(q_0)) \subseteq \omega(\text{PSL}_4^\varepsilon(q))$  with  $q = q_0^k$  for every divisor  $k$  of  $(m)_3$ . Note that 12 divides  $q_0 + \varepsilon$ ,  $(q + \varepsilon)_3 = k(q_0 + \varepsilon)_3$  and  $(4, q_0 - \varepsilon) = 2 = d$ . Since  $p \neq 3$ , the set  $\omega(\text{PSL}_4^\varepsilon(q_0))$  consists of divisors of  $(q_0^2 + 1)(q_0 + \varepsilon)/2$ ,  $(q_0^3 - \varepsilon)/2$ ,  $q_0^2 - 1$  and  $p(q_0^2 - 1)/2$ . Observing that

$$k(q_0^2 + 1)(q_0 + \varepsilon) \mid (q^2 + 1)(q + \varepsilon)$$

and

$$k(q_0^3 - \varepsilon), k(q_0^2 - 1) \mid q^2 - 1,$$

we obtain the desired containment.  $\square$

By Lemmas 5.2 and 5.3, it follows that up to conjugacy  $\text{Out } L$  has only one maximal admissible subgroup of odd order, and we can take this subgroup to be  $\langle \bar{\psi} \rangle$ , where  $\psi \in \langle \varphi \rangle$  has order  $(b)_{2'}$  if  $n > 4$  or  $q \not\equiv 1 \pmod{12}$ , and order  $(m)_3$  if  $n = 4$  and  $q \equiv -\varepsilon \pmod{12}$ .

Let  $\eta = \delta^{(d)_{2'}}$  and  $S_2$  be the Sylow 2-subgroup of  $\text{Out } L$  generated by  $\bar{\eta}, \bar{\varphi}^{(m)_{2'}}$  and  $\bar{\tau}$ .

**Lemma 5.4.** *If  $\omega(G) = \omega(L)$ , then  $G/L$  is conjugate in  $\text{Out } L$  to a subgroup of  $\langle \bar{\psi} \rangle \times S_2$ .*

*Proof.* By Lemma 5.1, the group  $G/L$  is abelian, and hence is the direct product of its Hall  $2'$ -subgroup  $A_1$  and Sylow 2-subgroup  $A_2$ . Since  $A_1$  is admissible, it is conjugate to a subgroup of  $\langle \bar{\psi} \rangle$ . Replacing  $G/L$  by a conjugate if necessary, we may assume that  $A_1 \leq \langle \bar{\psi} \rangle$ .

Note that  $\bar{\eta}$  centralizes  $\bar{\psi}$ . Indeed, if  $\varepsilon = +$ , then  $\bar{\eta}^{\bar{\psi}} = \bar{\eta}^{q_0}$ , where  $q = q_0^{|\psi|}$ . Since  $|\psi|$  is odd, we have

$$(q-1)_2 = (q_0-1)_2,$$

and hence  $(d)_2$  divides  $q_0-1$ . If  $\varepsilon = -$ , then  $\bar{\eta}^{\bar{\psi}} = \bar{\eta}^{q^2}$ , where  $q^2 = q_0^{|\psi|}$ . Now  $(q+1)_2 < (q^2-1)_2 = (q_0-1)_2$ , and again  $(d)_2$  divides  $q_0-1$ . It follows that the whole group  $S_2$  centralizes  $\bar{\psi}$ . Thus  $A_2$  is conjugate in  $C_{\text{Out } L}(A_1)$  to a subgroup of  $S_2$ , and the whole group  $G/L$  is conjugate to a subgroup of  $\langle \bar{\psi} \rangle \times S_2$ .  $\square$

The structure of the group  $S_2$  varies according to whether linear or unitary groups are under consideration, so in the rest of this section we consider the cases  $\varepsilon = +$  and  $\varepsilon = -$  separately. We begin with the case of unitary groups, in which  $S_2 = \langle \bar{\eta} \rangle \rtimes \langle \bar{\varphi}^{(m)_{2'}} \rangle$ .

**Lemma 5.5.** *Let  $\varepsilon = -$  and  $1 < G/L \leq S_2$ . If  $\omega(G) = \omega(L)$ , then  $G/L$  is conjugate to a subgroup of  $\langle \bar{\varphi}^{(m)_{2'}} \rangle$ .*

*Proof.* We may assume that  $n$  is even. If  $m$  is odd, then  $S_2 = \langle \bar{\eta} \rangle \rtimes \langle \bar{\tau} \rangle$  and by Lemma 5.1, the group  $G/L$  is conjugate to  $\langle \bar{\tau} \rangle$ .

Let  $m$  be even. Then  $|\bar{\eta}| = 2$  and  $S_2 = \langle \bar{\eta} \rangle \times \langle \bar{\varphi}^{(m)_{2'}} \rangle$ . Suppose  $G \not\leq \langle \bar{\varphi}^{(m)_{2'}} \rangle$ . Then  $G$  contains  $\varphi^{m/k} \eta$  for some  $k > 1$  dividing  $(m)_2$ . Let  $q = q_0^k$ . By Lemmas 3.3 and 4.8 together with Lemma 4.2, we have

$$\begin{aligned} \omega(\varphi^{m/k} \eta L) &= k \cdot \omega(\tau \delta^{d/2}(q_0) \text{PSL}_n(q_0)) \\ &= k \cdot \omega(\tau \delta(q_0) \text{PSL}_n(q_0)) \not\subseteq \omega(L), \end{aligned}$$

which is a contradiction.  $\square$

Thus if  $\varepsilon = -$  and  $\tau$  is not admissible, then  $S_2$  has no non-trivial admissible subgroups.

**Lemma 5.6.** *Suppose  $\varepsilon = -$ ,  $\tau$  is admissible,  $k > 1$  divides  $(m)_2$  and  $\beta = \varphi^{m/k}$ . Then  $\beta$  is admissible if and only if  $(n)_2 \leq 2$  or  $n = 4, 8, 12$ . If  $\beta$  is admissible and  $\gamma \in \langle \varphi \rangle$  is admissible and has odd order, then  $\gamma\beta$  is also admissible.*

*Proof.* We show first that  $\omega(\beta L) \subseteq \omega(L)$  if and only if  $(n)_2 \leq 2$  or  $n = 4, 8, 12$ . By Lemma 3.3, the set  $\omega(\beta L)$  is equal to  $k \cdot \omega(\tau \text{PSL}_n(q_0))$ , where  $q = q_0^k$ .

Let  $n$  be odd. Since  $\tau$  is admissible and  $q \equiv 1 \pmod{4}$ , Theorem 1 implies that  $n-2$  is not a power of  $p$ . Then using Lemmas 2.2 and 2.6, it is not hard to check that  $k \cdot \omega(\text{Sp}_{n-1}(q_0)) \subseteq \omega(\text{Sp}_{n-1}(q))$ . Now applying Lemma 4.6 yields

$$\begin{aligned} k \cdot \omega(\tau \text{PSL}_n(q_0)) &= 2k \cdot \omega(\text{Sp}_{n-1}(q_0)) \\ &\subseteq 2 \cdot \omega(\text{Sp}_{n-1}(q)) = \omega(\tau L) \subseteq \omega(L). \end{aligned}$$

Let  $n$  be even. Observe that  $(d)_2 = (q + 1)_2 = 2$ . By the admissibility of  $\tau$  and Theorem 1, it follows that  $n - 1$  is not a  $p$ -power. Also it is not hard to verify that  $k \cdot \omega(\Omega_{n+1}(q_0)) \subseteq \omega(\Omega_{n+1}(q))$  (cf. [12, Theorem 1]). Applying Lemma 4.7, we see that  $k \cdot \omega_{\bar{p}}(\tau \text{PSL}_n(q_0)) \subseteq \omega_{\bar{p}}(\tau L)$  for  $n > 4$ . Since  $k(q_0 \pm 1)$  divides  $q - 1$ , the same is true for  $n = 4$ . Thus it remains to examine when  $2k \cdot \omega_{p'}(\text{P}\Omega_n^{\pm}(q_0))$  is a subset of  $\omega(L)$ , and we consider the numbers from Lemma 2.3 in turn.

Let

$$a = [q_0^{n_1} \pm 1, q_0^{n_2} \pm 1, \dots, q_0^{n_s} \pm 1],$$

where  $s \geq 3$  and  $2(n_1 + n_2 + \dots + n_s) = n$ . Then  $2ka$  divides

$$[q^{2n_1} - 1, q^{2n_2} - 1, \dots, q^{2n_s} - 1] \in \omega(L).$$

Let

$$a = \frac{(q_0^{n/2} - \epsilon)}{(4, q_0^{n/2} - \epsilon)}.$$

If  $n/2$  is even, then  $2ka$  divides  $q^{n/2} - 1 \in \omega(L)$ . Suppose that  $n/2$  is odd. Then  $r_{n/2}(\epsilon q)$  divides  $a$  and lies in  $R_{n/2}(q) = R_n(-q)$ , and so  $2ka \in \omega(L)$  if and only if  $2ka$  divides

$$c = \frac{q^n - 1}{(q + 1)d} = \frac{(q^{n/2} - 1)(q^{n/2} + 1)}{(q + 1)d}.$$

Clearly,  $(a)_{2'}$  divides  $(c)_{2'}$ . Since  $(d)_2 = 2$ , we see that  $(c)_2 = (q - 1)_2/2$ . If  $(4, q_0 - \epsilon) = 4$ , then  $2k(a)_2 = k(q_0 - \epsilon)_2/2 = (q - 1)_2/2$ . If  $(4, q_0 - \epsilon) = 2$ , then  $2k(a)_2 = 2k \leq (q - 1)_2/2$ .

Finally, let  $a = [q_0^{n_1} - \epsilon_1, q_0^{n_2} - \epsilon_2]/e$ , where  $2(n_1 + n_2) = n$ , and with  $e = 2$  if  $(q^{n_1} - \epsilon_1)_2 = (q^{n_2} - \epsilon_2)_2$  and  $e = 1$  if  $(q^{n_1} - \epsilon_1)_2 \neq (q^{n_2} - \epsilon_2)_2$ .

Suppose that  $n/2$  is odd. We may assume that  $(q^{n_1} - \epsilon_1)_2 \geq (q^{n_2} - \epsilon_2)_2$ . If  $n_2$  is even, then  $2ka$  divides  $[q^{2n_1} - 1, q^{n_2} - 1]$ . Let  $n_2$  be odd. Then  $n_1$  is even. If  $n_1 \neq (n_1)_2$ , then  $2ka$  divides  $[q^{n_1} - 1, q^{(n_1)_2} - 1, q^{2n_2} - 1]$ . If  $n_1 = (n_1)_2$  and  $n_2 = 1$ , then  $2ka$  divides  $q^{2n_1} - 1$ . If  $(n_1) = (n_1)_2$  and  $n_2 > 1$ , then by the admissibility of  $\tau$ , we have  $(n, q + 1)_{2'} = 1$  and, therefore,  $(n/(2n_1, 2n_2), q + 1) = 1$ . So  $[q^{2n_1} - 1, q^{2n_2} - 1]$  lies in  $\omega(L)$ , and it is divisible by  $2ka$ .

Suppose that  $n/2$  is even and  $n/2 \geq 8$ . We can take  $n_1$  and  $n_2$  to be odd coprime numbers larger than 1. Also we take  $\epsilon_1 = +$  and  $\epsilon_2 = -$ . Then

$$a = [q_0^{n_1} - 1, q_0^{n_2} + 1]$$

and  $2k(a)_2 = k(q_0^2 - 1)_2 = (q^2 - 1)_2$ . Since  $a$  is a multiple of both  $r_{n_1}(q_0)$  and  $r_{n_2}(-q_0)$  and  $r_{n_i}(\pm q_0) \in R_{2n_i}(-q)$  for  $i = 1, 2$ , it follows that  $2ka \in \omega(L)$  if and only if  $2ka$  divides  $c = [q_{2n_1} - 1, q^{2n_2} - 1]/(n/(2n_1, 2n_2), q + 1)$ . But we have  $(c)_2 = (q^2 - 1)_2/2 < (a)_2$  because  $n/2$  is even. Thus  $\omega(\beta L) \not\subseteq \omega(L)$ .

We are left with the cases  $n = 4, 8, 12$ . If  $n = 4$ , then  $2a$  divides  $q_0^2 - 1$ , and hence  $2ka$  divides  $q^2 - 1$ . If  $n = 8$ , then  $a$  divides  $[q_0^3 \pm 1, q_0 \pm 1]$  or  $(q_0^4 - 1)/2$ ,

and so  $2ka$  divides  $q^6 - 1$  or  $q^4 - 1$ . If  $n = 12$ , then  $a$  divides  $[q_0^5 \pm 1, q_0 \pm 1]$ ,  $[q_0^4 \pm 1, q_0^2 \pm 1]$ , or  $(q_0^6 - 1)/2$ , and  $2ka$  divides  $q^{10} - 1$ ,  $q^8 - 1$ , or  $q^6 - 1$ .

We established that the condition for  $\omega(\beta L)$  to be a subset of  $\omega(L)$  depends only on  $n$  and not on  $q_0$ , and thus  $\beta$  is admissible if and only if  $\omega(\beta L) \subseteq \omega(L)$ .

Next, suppose that  $\beta$  is admissible,  $\gamma \in \langle \varphi \rangle$  is admissible and has odd order  $l$  and let  $q_0 = q_1^l$ . To prove that  $\gamma\beta$  is admissible, it suffices to show the inclusion  $\omega(\gamma\beta L) \subseteq \omega(L)$ . By Lemma 4.9, if we regard  $\tau$  as an automorphism of  $\text{PSU}_n(q_1^k)$ , it is still be admissible, and so by the above result, it follows that

$$k \cdot \omega(\tau \text{PSL}_n(q_1)) \subseteq \omega(\text{PSU}_n(q_1^k)).$$

By Lemma 3.3, we have

$$\omega(\gamma\beta L) = lk \cdot \omega(\tau \text{PSL}_n(q_1)) \subseteq l \cdot \omega(\text{PSU}_n(q_1^k)) = \omega(\gamma L) \subseteq \omega(L),$$

as desired.  $\square$

We are now in a position to prove Theorem 3.

*Proof of Theorem 3.* Suppose that  $\omega(G) = \omega(L)$ . By Lemmas 5.4 and 5.5, it follows that  $G/L$  is conjugate to a subgroup in  $\langle \bar{\psi} \rangle \times \langle \bar{\varphi}^{(m)2'} \rangle$ . If  $n - 1$  is a  $p$ -power, Lemmas 4.7, 5.2 and 5.3 imply that any non-trivial element of  $G/L$  is not admissible. If  $n - 1$  is not a  $p$ -power, then  $\psi$  is admissible, and applying Lemma 5.6 completes the proof.  $\square$

Now we assume that  $\varepsilon = +$ , and so we have  $S_2 = \langle \bar{\eta} \rangle \rtimes (\langle \bar{\varphi}^{m2'} \rangle \times \langle \bar{\tau} \rangle)$ . Given an element  $1 \neq \beta \in \langle \varphi^{(m)2'} \rangle$ , we define  $\beta_\epsilon$  with  $\epsilon \in \{+, -\}$  by setting  $\beta_+ = \beta$  and  $\beta_- = \beta\tau$ .

**Lemma 5.7.** *Let  $\varepsilon = +$ ,  $k > 1$  divide  $(m)_2$  and  $q = q_0^k$ . Then for any  $\epsilon \in \{+, -\}$ , the following hold:*

(i) *If  $n$  is odd or  $k$  does not divide  $(q - 1)/d$ , then*

$$k \cdot \omega(\text{PSL}_n^\epsilon(q_0)) \not\subseteq \omega(L).$$

(ii) *If  $n$  is even,  $k$  divides  $(q - 1)/d$  and  $n = 1 + p^{t-1}$ , then*

$$k \cdot \omega(\text{PSL}_n^\epsilon(q_0)) \setminus \{kp^t\} \subseteq \omega(L).$$

(iii) *If  $n$  is even,  $k$  divides  $(q - 1)/d$  and  $n - 1$  is not a  $p$ -power, then*

$$k \cdot \omega(\text{PSL}_n^\epsilon(q_0)) \subseteq \omega(L).$$

*In particular, if  $\beta = \varphi^{m/k}$ , then  $\beta_\epsilon$  is admissible if and only if  $n$  is even,  $k$  divides  $(q - 1)/d$  and  $n - 1$  is not a  $p$ -power. If  $\beta_\epsilon$  is admissible and  $\gamma \in \langle \varphi \rangle$  is admissible and has odd order, then  $\gamma\beta_\epsilon$  is also admissible.*

*Proof.* If  $n$  is odd, then  $2r_n(\epsilon q_0)$  is not an element of  $\omega(L)$  since  $r_n(\epsilon q_0) \in R_n(q)$  and  $(q^n - 1)/(q - 1)$  is odd. If  $n$  is even and  $k$  does not divide  $(q - 1)/d$ , then  $kr_{n-1}(\epsilon q_0) \notin \omega(L)$ . Indeed, otherwise the fact that  $r_{n-1}(\epsilon q_0) \in R_{n-1}(q)$  implies that  $k$  divides  $(q^{n-1} - 1)/d$ . But  $(q^{n-1} - 1)_2/(d)_2 = (q - 1)_2/(d)_2$ , and thus (i) follows.

Let  $n$  be even and suppose that  $k$  divides  $(q - 1)/d$ . We claim that  $ka \in \omega(L)$  for all  $a \in \omega(\text{PSL}_n^\epsilon(q_0))$  except  $a = p^t$  for  $n = 1 + p^{t-1}$ . The number  $a$  divides one of the numbers in items (i)–(v) of Lemma 2.1, and we consider these possibilities in turn.

If we have  $a = (q_0^n - 1)/(q_0 - \epsilon)(n, q_0 - \epsilon)$ , then  $ka$  divides  $q^{n/2} - 1$ . Similarly, if  $a = [q_0^{n_1} - \epsilon^{n_1}, q_0^{n_2} - \epsilon^{n_2}]/(n/(n_1, n_2), q_0 - \epsilon)$ , where  $n_1 + n_2 = n$  and both  $n_1, n_2$  are even, then  $ka$  divides  $[q^{n_1/2} - 1, q^{n_2/2} - 1]$ . If  $a = [q^{n_1} - \epsilon^{n_1}, q^{n_2} - \epsilon^{n_2}]/(n/(n_1, n_2), q_0 - \epsilon)$ , where  $n_1$  and  $n_2$  are odd, then  $ka$  divides the element  $c = [q^{n_1} - 1, q^{n_2} - 1]/(n/(n_1, n_2), q - 1)$ . Indeed, if  $q_0 \equiv -\epsilon \pmod{4}$ , then

$$k(a)_2 = k \leq (c)_2,$$

while if  $q_0 \equiv \epsilon \pmod{4}$ , then

$$k(q_0 - \epsilon)_2 = (q - 1)_2 \geq (k)_2(n)_2,$$

which implies that  $(q_0 - \epsilon)_2 \geq (n)_2$  and  $k(a)_2 = (q - 1)_2/(n)_2 = (c)_2$ . Also,  $a$  divides  $c$  by Lemma 2.5. Finally, if  $a = [q_0^{n_1} - \epsilon^{n_1}, \dots, q_0^{n_s} - \epsilon^{n_s}]$ , where  $s \geq 3$  and  $n_1 + \dots + n_s = n$ , or  $a = p^t[q_0^{n_1} - \epsilon^{n_1}, \dots, q_0^{n_s} - \epsilon^{n_s}]$ , where  $s \geq 2$  and  $1 + p^{t-1} + n_1 + \dots + n_s = n$ , we have that  $ka$  divides  $[q^{n_1} - 1, \dots, q^{n_s} - 1]$  or  $p^t[q^{n_1} - 1, \dots, q^{n_s} - 1]$ , respectively.

Let  $\beta = \varphi^{m/k}$ . By Lemma 3.3, we have  $\omega(\beta_\epsilon L) = k \cdot \omega(\text{PSL}_n^\epsilon(q_0))$ . Thus if  $\beta_\epsilon$  is admissible, then  $n$  is even,  $k$  divides  $(q - 1)/d$  and  $n - 1$  is not a  $p$ -power. Conversely, if all these three conditions are satisfied, then by the above

$$\omega(\beta^{k_1} L) = (k/k_1) \cdot \omega(\text{PSL}_n(q_0^{k_1})) \subseteq \omega(L)$$

for every divisor  $k_1$  of  $k$ , and hence  $\beta_\epsilon$  is admissible.

To prove the final assertion, it suffices to check  $\omega(\gamma\beta_\epsilon L) \subseteq \omega(L)$  for admissible  $\gamma$  and  $\beta_\epsilon$ . Let  $|\gamma| = l$  and  $q_0 = q_1^l$ . Observing that  $(q - 1)_2 = (q_1^k - 1)_2$ , we see that  $k$  divides  $(q - 1)/d$  if and only if it divides  $(q_1^k - 1)/(n, q_1^k - 1)$ . Thus the admissibility of  $\beta_\epsilon$  yields

$$k \cdot \omega(\text{PSL}_n^\epsilon(q_1)) \subseteq \omega(\text{PSL}_n(q_1^k)).$$

Applying Lemma 3.3, we have

$$\omega(\gamma\beta_\epsilon L) = lk \cdot \omega(\text{PSL}_n^\epsilon(q_1)) \subseteq l \cdot \omega(\text{PSL}_n(q_1^k)) = \omega(\gamma L) \subseteq \omega(L),$$

and the proof is complete.  $\square$

**Lemma 5.8.** *Let  $\varepsilon = +$ , let  $n$  be even,  $k > 1$  divide  $(m)_2$ ,  $\beta = \varphi^{m/k}$  and  $q = q_0^k$ . If  $\alpha = \beta_\varepsilon \eta^j$  is admissible, then  $\bar{\alpha}$  is conjugate in the group  $S_2$  to either  $\bar{\beta}_\varepsilon$  or  $\bar{\beta}_\varepsilon \bar{\eta}$ , with  $q_0 \equiv -\varepsilon \pmod{4}$  and  $2k \leq (q-1)_2/(d)_2$  in the latter case. Furthermore, if  $q_0 \equiv -\varepsilon \pmod{4}$  and  $2k \leq (q-1)_2/(d)_2$ , then the following statements hold:*

- (i)  *$\beta_\varepsilon \eta$  is admissible if and only if  $n$  cannot be represented as  $1 + p^{t-1} + 2^u$  with  $t, u \geq 1$  and, in addition,  $k = 2$  whenever  $n-1$  is a  $p$ -power,*
- (ii) *If  $\beta_\varepsilon \eta$  is admissible and  $\gamma \in \langle \varphi \rangle$  is admissible and has odd order, then  $\gamma \beta_\varepsilon \eta$  is admissible.*

*Proof.* Note that  $\bar{\eta}^{\bar{\beta}_\varepsilon} = \bar{\eta}^{\varepsilon q_0}$ , and so

$$\bar{\beta}_\varepsilon^{\bar{\eta}} = \bar{\eta}^{-1} \bar{\beta}_\varepsilon \bar{\eta} = \bar{\beta}_\varepsilon \bar{\eta}^{1-\varepsilon q_0}. \quad (5.1)$$

Suppose that  $\alpha = \beta_\varepsilon \eta^j$  is admissible and  $\bar{\alpha}$  is not conjugate in  $S_2$  to  $\bar{\beta}_\varepsilon$ . Then (5.1) implies that  $(q_0 - \varepsilon, (d)_2)$  does not divide  $j$ , or in other words

$$(j)_2 < (q_0 - \varepsilon, d)_2. \quad (5.2)$$

Since  $\eta = \delta^{(d)_{2'}}$ , applying Lemma 3.3 yields

$$\omega(\alpha L) = k \cdot \omega(\delta^{j(d)_{2'}}(\varepsilon q_0) \text{PSL}_n^\varepsilon(q_0)). \quad (5.3)$$

The index of  $\delta^{j(d)_{2'}}(\varepsilon q_0) \text{PSL}_n^\varepsilon(q_0)$  in  $\text{PGL}_n^\varepsilon(q_0)$  is equal to  $(j(d)_{2'}, q_0 - \varepsilon)$ . There is an element of order  $q_0^{n-1} - \varepsilon$  in the group  $\text{PGL}_n(q_0)$ , and hence writing  $a = (q_0^{n-1} - \varepsilon)/(j(d)_{2'}, q_0 - \varepsilon)$ , we see that  $ka \in \omega(\alpha L)$ . Since  $a$  is a multiple of  $r_{n-1}(\varepsilon q_0) \in R_{n-1}(q)$  and lies in  $\omega(L)$ , it follows that  $a$  divides  $c = (q^{n-1} - 1)/d$ . If  $q_0 \equiv \varepsilon \pmod{4}$ , then by (5.2), we deduce that

$$(a)_2 = \frac{k(q_0 - \varepsilon)_2}{(j)_2} = \frac{(q-1)_2}{(j)_2} > \frac{(q-1)_2}{(d)_2} = (c)_2.$$

Thus  $q_0 \equiv -\varepsilon \pmod{4}$ . Then  $(q_0 - \varepsilon, d)_2 = 2$ , and so  $j$  is odd. In particular, (5.1) shows that  $\alpha$  is conjugate to  $\beta_\varepsilon \eta$ . Also,  $(a)_2 = 2k \leq (c)_2 = (q-1)_2/(d)_2$ , and the first assertion is proved.

Next, let  $\alpha = \beta_\varepsilon \eta$ ,  $q_0 \equiv -\varepsilon \pmod{4}$  and  $2k \leq (q-1)_2/(d)_2$ . Observing that  $(q-1)_2 = k(q_0 + \varepsilon)_2$ , we deduce from the last inequality that  $2(d)_2 \leq (q_0 + \varepsilon)_2$ , and hence

$$\bar{\alpha}^2 = \bar{\beta}_\varepsilon^2 \bar{\eta}^{1+\varepsilon q_0} = \bar{\beta}_\varepsilon^2.$$

Since  $2k \leq (q-1)_2/(d)_2$ , it follows from Lemma 5.7 that  $\beta^2$  is admissible if and only if  $k = 2$  or  $n-1$  is not a  $p$ -power.

Suppose  $n = 1 + p^{t-1} + 2^u$  with  $t, u \geq 1$ . Then  $\text{PGL}_n^\epsilon(q_0)$  has an element of order  $p^t(q_0^{2^u} - 1)$ , and so  $ka \in \omega(\alpha L)$ , where  $a = p^t(q_0^{2^u} - 1)/(d, q_0 - \epsilon)_{2'}$ . Since  $ka$  is a multiple of  $kp^t(q_0^{2^u} - 1)_2 = p^t(q^{2^u} - 1)_2$ , it lies in  $\omega(L)$  only if it divides  $p^t(q^{2^u} - 1)/d$ , which is not the case.

To prove (i), it remains to verify that  $\omega(\alpha L) \subseteq \omega(L)$  whenever  $n$  cannot be represented as  $1 + p^{t-1} + 2^u$  with  $t, u \geq 1$ . Since  $((d)_{2'}, q_0 - \epsilon) = (n, q_0 - \epsilon)_{2'} = (n, q_0 - \epsilon)/2$ , it follows from (5.3) that

$$\omega(\alpha L) = k \cdot \omega(2\text{PSL}_n^\epsilon(q_0) \setminus \text{PSL}_n^\epsilon(q_0)),$$

where  $2\text{PSL}_n^\epsilon(q_0)$  is the unique subgroup of  $\text{PGL}_n^\epsilon(q_0)$  that contains  $\text{PSL}_n(q_0)$  as a subgroup of index 2. Denote  $\omega(2\text{PSL}_n^\epsilon(q_0) \setminus \text{PSL}_n(q_0))$  by  $\omega$ .

If  $n = p^{t-1} + 1$ , then any element of  $\text{GL}_n(q)$  whose order is divisible by  $p^t$  is conjugate to a scalar multiple of the  $n \times n$  unipotent Jordan block, therefore,  $p^t \notin \omega$ . By Lemma 5.7, we have

$$k \cdot (\omega \cap \omega(\text{PSL}_n^\epsilon(q_0))) \subseteq \omega(L),$$

and hence we are left with elements of  $\omega \setminus \omega(\text{PSL}_n^\epsilon(q_0))$ . By Lemma 2.1, it follows that this difference consists of some divisors of the following numbers:

- $2(q_0^n - 1)/((q_0 - \epsilon)(n, q_0 - \epsilon))$ ,
- $[q_0^{n_1} - \epsilon^{n_1}, q^{n_2} - \epsilon^{n_2}]/(n/(n_1, n_2), q_0 - \epsilon)$ , where  $n_1, n_2$  are odd,  $n_1 + n_2 = n$ ,
- $2p^t(q_0^{n_1} - \epsilon^{n_1})/(n, q_0 - \epsilon)$ , where  $n_1 > 0$  and  $p^{t-1} + 1 + n_1 = n$ .

Let  $a = 2(q_0^n - 1)/((q_0 - \epsilon)(n, q_0 - \epsilon))$ . Then

$$k(a)_2 = 2k \frac{(q_0^n - 1)_2}{(q_0 - \epsilon)_2(q_0 - \epsilon, n)_2} = \frac{(q^n - 1)_2}{2} = (q^{n/2} - 1)_2,$$

and so  $ka$  divides  $q^{n/2} - 1 \in \omega(L)$ .

Let  $a = 2[q_0^{n_1} - \epsilon^{n_1}, q^{n_2} - \epsilon^{n_2}]/(n/(n_1, n_2), q_0 - \epsilon)$ , where  $n_1, n_2$  are odd and  $n_1 + n_2 = n$ . Consider the number  $c = [q^{n_1} - 1, q^{n_2} - 1]/(n/(n_1, n_2), q - 1)$  lying in  $\omega(L)$ . By Lemma 2.5, both numbers  $(q^{n_i} - 1)/(n/(n_1, n_2), q_0 - \epsilon)$ ,  $i = 1, 2$ , divide  $c$ . Also,  $k(a)_2 = 2k \leq (q - 1)_2/d_2 = (c)_2$ , and hence  $ka$  divides  $c$ .

Let  $a = 2p^t(q_0^{n_1} - \epsilon^{n_1})/(n, q_0 - \epsilon)$ , where  $n_1 > 0$  and  $p^{t-1} + 1 + n_1 = n$ . Note that  $n_1$  is even and by hypothesis,  $(n_1)_2 \neq n_1$ . Since

$$k(a)_2 = \frac{2k(q_0^{n_1} - 1)_2}{(q_0 - \epsilon)_2} = (q^{n_1} - 1)_2 = (q^{(n_1)_2} - 1)_2,$$

we see that  $ka$  divides  $p^t[q^{n_1/2} - 1, q^{(n_1)_2} - 1] \in \omega(L)$ .

To prove part (ii), take admissible  $\gamma$  and  $\alpha$ . We may assume that  $n - 1$  is not a  $p$ -power because otherwise  $\gamma = 1$  by Lemmas 5.2 and 5.3. Then by the equality

$$\bar{\alpha}^2 = \bar{\beta}^2$$

and Lemma 5.8, to prove that  $\gamma\alpha$  is admissible, it suffices to check the inclusion  $\omega(\gamma\alpha L) \subseteq \omega(L)$ . Denote  $|\gamma|$  by  $l$  and let  $q_0 = q_1^l$ . Observe that

$$q_1 \equiv q_0 \equiv -\epsilon \pmod{4}$$

and  $2k$  divides  $(q_1^k - 1)_2 / (n, q_1^k - 1)_2$ .

By Lemma 3.3, we have

$$\omega(\gamma\alpha L) = lk \cdot \omega(\delta^{(d)2'}(\epsilon q_1) \text{PSL}_n^\epsilon(q_1)).$$

Using the fact that  $(d, q_1 - \epsilon)_{2'} = (q_1 - \epsilon)/2$  and the above results, we deduce that

$$k \cdot \omega(\delta^{(d)2'}(\epsilon q_1) \text{PSL}_n^\epsilon(q_1)) = k \cdot \omega(2\text{PSL}_n^\epsilon(q_1) \setminus \text{PSL}_n^\epsilon(q_1)) \subseteq \omega(\text{PSL}_n(q_1^k)).$$

Thus

$$\omega(\gamma\alpha L) \subseteq l \cdot \omega(\text{PSL}_n(q_1^k)) = \omega(\gamma L) \subseteq \omega(L),$$

and the proof is complete.  $\square$

We are now ready to describe admissible 2-subgroups of  $\text{Out } L$  in the case of linear groups, and then prove Theorem 2. Recall that  $b = ((q - \epsilon)/d, m)_d$  and define  $\phi = \varphi^{m/(b)_2}$ .

**Lemma 5.9.** *Let  $\epsilon = +$  and let  $1 < G/L \leq S_2 = \langle \bar{\eta} \rangle \rtimes (\langle \bar{\varphi}^{(m)2'} \rangle \times \langle \bar{\tau} \rangle)$ . Then  $\omega(G) = \omega(L)$  if and only if  $G/L$  is cyclic and up to conjugacy in  $S_2$  is generated by the image of one of the following elements:*

- (i)  $\tau$  if  $b$  is odd and  $\tau$  is admissible,
- (ii)  $\beta_\pm$ , where  $1 \neq \beta \in \langle \phi \rangle$ , if  $b$  is even and  $n - 1$  is not a  $p$ -power,
- (iii)  $\beta\tau\eta$ , where  $1 \neq \beta \in \langle \phi^2 \rangle$ , if  $(b)_2 > 2$  and  $n$  cannot be represented as  $1 + p^{t-1}$  or  $1 + p^{t-1} + 2^u$  with  $t, u \geq 1$ ,
- (iv)  $\phi_{-\kappa}\eta$ , where  $p \equiv \kappa \pmod{4}$ , if  $(p - \kappa)_2 > (n)_2$  and  $n$  cannot be represented as  $1 + p^{t-1}$  or  $1 + p^{t-1} + 2^u$  with  $t, u \geq 1$ ,
- (v)  $\varphi^{m/2}\tau\eta$ , if  $(b)_2 > 2$ ,  $n = 1 + p^{t-1}$  for some  $t \geq 1$  and  $n$  cannot be represented as  $2 + 2^u$  with  $u \geq 1$ ,
- (vi)  $(\varphi^{m/2})_{-\kappa}\eta$ , where  $p \equiv \kappa \pmod{4}$ , if  $(m)_2 = 2$ ,  $(p - \kappa)_2 > (n)_2$ ,  $n = 1 + p^{t-1}$  for some  $t \geq 1$  and  $n$  cannot be represented as  $2 + 2^u$  with  $u \geq 1$ .

*Proof.* Observe that  $b$  is even if and only if all the numbers  $n$ ,  $m$  and  $(q - 1)/d$  are even.

Suppose that  $n$  is odd. Then  $S_2 = \langle \bar{\varphi}^{(m)2'} \rangle \times \langle \bar{\tau} \rangle$ . By Lemma 5.7, any non-trivial element of  $\langle \varphi^{(m)2'} \rangle$  is not admissible and thus the only potentially admissible subgroup of  $S_2$  is  $\langle \bar{\tau} \rangle$ .

Suppose that  $n$  is even but at least one of  $m$  and  $(q-1)/d$  is odd. It follows from Lemmas 5.7 and 5.8 that every admissible subgroup of  $S_2$  is contained in  $\langle \bar{\eta} \rangle \rtimes \langle \bar{\tau} \rangle$ . Then by Lemma 5.1, it is conjugate to a subgroup of  $\langle \bar{\tau} \rangle$ , and we are done in the case of odd  $b$ .

Suppose now that all the numbers  $n$ ,  $m$  and  $(q-1)/d$  are even. In particular,  $(q-1)_2 > (d)_2 = (n)_2$  and so  $\tau$  is not admissible by Theorem 4.7. Then by Lemma 5.1, we obtain that all non-trivial elements of  $\langle \bar{\eta} \rangle \rtimes \langle \bar{\tau} \rangle$  are not admissible. It follows that every admissible subgroup of  $S_2$  is isomorphic to a subgroup of  $\langle \bar{\varphi}^{(m)_{2'}} \rangle$ , and hence is cyclic.

Let  $\bar{\alpha} \in S_2 \setminus \langle \bar{\eta} \rangle \rtimes \langle \bar{\tau} \rangle$  be admissible. We may assume that  $\alpha = \beta_\epsilon \eta^j$ , where  $\beta = \varphi^{m/k}$  for some  $1 < k = 2^l \leq (m)_2$ . By Lemmas 5.7 and 5.8, admissibility of  $\alpha$  yields  $k \leq (q-1)_2/(d)_2$  or, equivalently,  $\beta \in \langle \phi \rangle$ . Moreover, all conjugates of  $\bar{\beta}_\epsilon$  are admissible whenever  $n-1$  is not a  $p$ -power, and this gives the automorphisms in (ii).

It remains to consider the case when  $\bar{\alpha}$  is not conjugate to  $\bar{\beta}_\epsilon$ . In this case by Lemma 5.8, we may assume that  $\alpha = \beta_\epsilon \eta$ ,

$$2k \leq \frac{(q-1)_2}{(d)_2} \quad (5.4)$$

and  $q_0 \equiv -\epsilon \pmod{4}$ , where  $q = q_0^k$ . Moreover, we have  $k = 2$  whenever  $n-1$  is a  $p$ -power. Note that  $(q-1)_2 = (m)_2(p-\kappa)_2$ , where  $p \equiv \kappa \pmod{4}$ .

Suppose that  $(q-1)_2/(d)_2 \leq (m)_2$  or, in other words,  $(p-\kappa)_2 \leq (n)_2$ . Then  $k \leq (m)_2/2$ , so  $q_0 \equiv 1 \pmod{4}$  and condition (5.4) is equivalent to  $\beta \in \langle \phi^2 \rangle$ . Thus  $(b)_2 > 2$  and  $\alpha = \beta\tau\eta$  with  $\beta \in \langle \phi^2 \rangle$ . In particular, if  $n-1$  is a  $p$ -power, then  $\alpha = \varphi^{m/2}\tau\eta$ .

Suppose that  $(q-1)_2/(d)_2 > (m)_2$  or, equivalently,  $(p-\kappa)_2 > (n)_2$ . Then condition (5.4) holds for all  $\beta \in \langle \phi \rangle$ . Also, we have  $q_0 \equiv 1 \pmod{4}$  if  $k < (m)_2$  and  $q_0 \equiv \kappa \pmod{4}$  if  $k = (m)_2$ . Thus  $\alpha = \beta\tau\eta$  with  $\beta \in \langle \phi^2 \rangle$  or  $\alpha = \phi_{-\kappa}\eta$ . In particular, if  $n-1$  is a  $p$ -power, then  $\alpha = \varphi^{m/2}\tau\eta$  when  $(b)_2 = (m)_2 > 2$  and  $\alpha = \phi_{-\kappa}\eta$  when  $(b)_2 = (m)_2 = 2$ .

Conversely, let  $\alpha$  be one of the resulting automorphisms and let the associated conditions be satisfied. Then by Lemma 5.8,  $\alpha$  is admissible unless  $n$  cannot be represented as  $1 + p^{t-1} + 2^u$ . If  $n = 1 + p^{t-1}$  and  $n = 1 + p^{s-1} + 2^u$ , then we have  $p^{t-1} = p^{s-1} + 2^u$  or, equivalently,  $p^{s-1}(p^{t-s} - 1) = 2^u$ , and so  $s = 1$  and  $n = 2 + 2^u$ . Thus we obtain the automorphisms in (iii)–(vi), and the proof is complete.  $\square$

*Proof of Theorem 2.* Let  $\omega(G) = \omega(L)$ . By Lemma 5.4, it follows that  $G/L$  is conjugate to a subgroup of  $\langle \bar{\psi} \rangle \times S_2$ . Admissible subgroups of  $\langle \bar{\psi} \rangle$  and  $S_2$  are described in Lemmas 5.2, 5.3 and Lemma 5.9, respectively. These descriptions

together with Lemmas 5.7 and 5.8 imply that the product of an admissible subgroup of  $\langle \bar{\psi} \rangle$  and an admissible subgroup of  $S_2$  is also admissible, and this completes the proof.  $\square$

## Bibliography

- [1] A. S. Bang, Taltheoretiske undersøgelser, *Tidsskrift Math.* **4** (1886), 70–80, 130–137.
- [2] R. Brandl and W. J. Shi, The characterization of  $\mathrm{PSL}(2, q)$  by its element orders, *J. Algebra* **163** (1994), no. 1, 109–114.
- [3] J. Bray, D. Holt and C. Roney-Dougall, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 407, Cambridge University Press, Cambridge, 2013.
- [4] A. A. Buturlakin, Spectra of finite linear and unitary groups, *Algebra Logic* **47** (2008), no. 2, 91–99.
- [5] A. A. Buturlakin, Spectra of finite symplectic and orthogonal groups, *Siberian Adv. Math.* **21** (2011), no. 3, 176–210.
- [6] A. A. Buturlakin and M. A. Grechkoseeva, The cyclic structure of maximal tori of the finite classical groups, *Algebra Logic* **46** (2007), no. 2, 73–89.
- [7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
- [8] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023–3070.
- [9] J. Fulman and R. Guralnick, Conjugacy class properties of the extension of  $\mathrm{GL}(n, q)$  generated by the inverse transpose involution, *J. Algebra* **275** (2004), no. 1, 356–396.
- [10] R. Gow and C. R. Vinroot, Extending real-valued characters of finite general linear and unitary groups on elements related to regular unipotents, *J. Group Theory* **11** (2008), no. 3, 299–331.
- [11] M. A. Grechkoseeva, Recognition by spectrum for finite linear groups over fields of characteristic 2, *Algebra Logic* **47** (2008), no. 4, 229–241.
- [12] M. A. Grechkoseeva, On spectra of almost simple groups with symplectic or orthogonal socle, *Sib. Math. J.* **57** (2016), no. 4, 582–588.
- [13] M. A. Grechkoseeva and W. J. Shi, On finite groups isospectral to finite simple unitary groups over fields of characteristic 2, *Sib. Élektron. Mat. Izv.* **10** (2013), 31–37.
- [14] M. A. Grechkoseeva and A. V. Vasil’ev, On the structure of finite groups isospectral to finite simple groups, *J. Group Theory* **18** (2015), no. 5, 741–759.

- [15] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge, 1990.
- [16] V. D. Mazurov, On the set of orders of elements of a finite group, *Algebra Logic* **33** (1994), no. 1, 49–55.
- [17] V. D. Mazurov, Recognition of finite groups by a set of orders of their elements, *Algebra Logic* **37** (1998), no. 6, 371–379.
- [18] P. Ribenboim, *The Little Book of Bigger Primes*, 2nd ed., Springer, New York, 2004.
- [19] M. Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997), no. 7, 1913–1919.
- [20] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Ser. Pure Math. 9, Heldermann, Lemgo, 2009.
- [21] A. V. Vasil'ev, On finite groups isospectral to simple classical groups, *J. Algebra* **423** (2015), 318–374.
- [22] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Aust. Math. Soc.* **3** (1963), 1–62.
- [23] A. V. Zavarnitsine, Recognition of the simple groups  $L_3(q)$  by element orders, *J. Group Theory* **7** (2004), no. 1, 81–97.
- [24] A. V. Zavarnitsine, Recognition of the simple groups  $U_3(q)$  by element orders, *Algebra Logic* **45** (2006), no. 2, 106–116.
- [25] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.
- [26] M. A. Zvezdina, Spectra of automorphic extensions of finite simple symplectic and orthogonal groups over fields of characteristic 2, *Sib. Élektron. Mat. Izv.* **11** (2014), 823–832.
- [27] M. A. Zvezdina, Spectra of automorphic extensions of finite simple exceptional groups of Lie type, *Algebra Logic* **55** (2016), 354–366.

Received September 7, 2016; revised February 6, 2017.

### Author information

Mariya A. Grechkoseeva, Sobolev Institute of Mathematics and Novosibirsk State University, Ac. Koptyuga 4, Novosibirsk, 630090, Russia.  
E-mail: gma@math.nsc.ru