On finite groups isospectral to simple classical groups

A.V. Vasil′ev[1]

Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia

Abstract

The *spectrum* $\omega(G)$ of a finite group G is the set of element orders of G. Finite groups G and H are *isospectral* if their spectra coincide. Suppose that L is a simple classical group of sufficiently large dimension (the lower bound varies for different types of groups but is at most 62) defined over a finite field of characteristic p. It is proved that a finite group G isospectral to L cannot have a nonabelian composition factor which is a group of Lie type defined over a field of characteristic distinct from p. Together with a series of previous results this implies that every finite group G isospectral to L is 'close' to L. Namely, if L is a linear or unitary group, then $L \leqslant G \leqslant \operatorname{Aut} L$, in particular, there are only finitely many such groups G for given L. If L is a symplectic or orthogonal group, then G has a unique nonabelian composition factor S and, for given L, there are at most 3 variants for S (including $S \simeq L$).

Keywords: groups of Lie type, finite classical groups, element orders
2000 MSC: 20D06, 20D20

Introduction

The *spectrum* $\omega(G)$ of a finite group G is the set of element orders of G. Finite groups having the same spectra are said to be *isospectral*. Recently, the following general result was obtained.

Theorem A. *Suppose that L is a finite simple group, and G is a finite group with $\omega(G) = \omega(L)$ and $|G| = |L|$. Then G is isomorphic to L.*

Email address: `vasand@math.nsc.ru` (A.V. Vasil′ev)

[1]The author was supported by the RFBR (project 13-01-00505) and the Target program of SB RAS for 2012-2014 (integration project No. 14).

The statement was conjectured by W. Shi [1] in 1987, while its proof was completed in [2] (see the latter article for background information and complete list of references). It is worth mentioning that Theorem A together with [3, Corollary 5.2] implies that a finite simple group and a finite group with the same Burnside rings are isomorphic as well.

What happens if we omit the condition $|G| = |L|$ in Theorem A? Then G is not necessary isomorphic to L. For example, there are infinitely many groups with the same spectrum as the spectrum of the alternating permutation group of degree six [4]. On the other hand, it turns out that for a bulk of finite nonabelian simple groups L, a finite group isospectral to L is isomorphic to L or, at least, to a group G with $L \leqslant G \leqslant \operatorname{Aut} L$. Investigations on this subject have 30-year history and resulted in more than a hundred papers of numerous authors. We do not intend to give a detailed review, rather prefer to draw an overall picture. In order to do that we formulate the following conjecture attributed to V.D. Mazurov:

Conjecture B. *For every finite nonabelian simple group L, apart from a finite number of sporadic, alternating and exceptional groups and apart from several series of classical groups of small dimensions, if a finite group G is isospectral to L then G is an almost simple group with socle isomorphic to L.*

The conjecture was proved for sporadic groups [5], for alternating groups [6], and very recently for exceptional groups of Lie type [7]. Here we deal with groups isospectral to finite simple classical groups. Observe that there are a lot of results on this topic concerning groups in particular characteristics or dimensions. The peculiarity of our approach is that we sacrifice groups of small dimensions in order to obtain a general result (cf. the theorems below with recent papers [8, 9, 10, 11, 12, 13, 14, 15]). Throughout this paper we use single-letter names for simple classical groups, following [16], i. e., for example, $L_n(q)$ means $PSL_n(q)$, as well as the standard abbreviation $L_n^{\varepsilon}(q)$, where $\varepsilon \in \{+, -\}$, $L_n^{+}(q) = L_n(q)$, and $L_n^{-}(q) = U_n(q)$.

Theorem 1. *Suppose that $L = L_n^{\varepsilon}(q)$ is a finite simple linear or unitary group and $n \geqslant 45$. Then a finite group isospectral to L is isomorphic to a group G with $L \leqslant G \leqslant \operatorname{Aut} L$. In particular, there are only finitely many pairwise non-isomorphic finite groups G with $\omega(G) = \omega(L)$.*

Theorem 2. *Suppose that L is a finite simple symplectic or orthogonal group, where $n \geqslant 28$ for $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, $n \geqslant 31$ for $L = O_{2n}^{+}(q)$, and $n \geqslant 30$*

for $L = O^-_{2n}(q)$. If G is a finite group with $\omega(G) = \omega(L)$, then G has a unique nonabelian composition factor S, and one of the following holds:
(i) $L \simeq S$;
(ii) $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ *and* $S \in \{O_{2n+1}(q), O^-_{2n}(q)\}$;
(iii) *n is even, $L = O^+_{2n}(q)$, and $S \in \{S_{2n-2}(q), O_{2n-1}(q)\}$.*
In particular, there exist at most 3 possibilities for S for given L.

Remark 1. It seems very likely that the conclusion of Theorem 1 is valid under the hypothesis of Theorem 2.

In fact, as shown in the last section, Theorems 1 and 2 are straightforward consequences of a series of previous results [17, 18, 19, 20] and the following theorem whose proof is the main goal of this paper.

Theorem 3. *Let L be a simple classical group over a finite field of characteristic p, and G be a finite group with $\omega(G) = \omega(L)$. Suppose that $n \geqslant 45$ for $L = L^\varepsilon_n(q)$, $n \geqslant 28$ for $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, $n \geqslant 31$ for $L = O^+_{2n}(q)$, and $n \geqslant 30$ for $L = O^-_{2n}(q)$. Then G has a unique nonabelian composition factor S, and S is not isomorphic to a group of Lie type over a field of characteristic distinct from p.*

We strongly believe that the conclusion of Theorem 3 remains true for all simple classical groups except the well-known examples of isomorphic groups in different characteristics such as $L_2(4) \simeq L_2(5)$; three groups $L_3(3)$, $U_3(3)$, and $S_4(3)$, which are the only simple groups of Lie type isospectral to some solvable groups [21, Corollary 1]; and a few exotic cases such as $\omega(U_3(5)) = \omega(2^{18} : L_3(4))$ [22]. Moreover, for many classical groups of small dimensions and specific characteristics the conclusion of the theorem has already been proved. In the article we concentrate on groups of sufficiently large dimensions in order to achieve a generic proof covering classical groups of all types in all characteristics.

A final remark. The determination of properties of a group by means of its element orders is widely applied in computational group theory, especially in development of the so-called black-box algorithms, i. e. algorithms that do not exploit specific features of a group representation. We mention here just one of the numerous results on this subject, which is nearest to our main assertion. Namely, W. Kantor and Á. Seress in [23] proved that the characteristic of a finite simple group G of Lie type can be determined if three greatest element orders of G are known (it is additionally assumed that the characteristic of G is odd). One may observe that Theorem 3 says the same thing but only for classical groups of large dimensions and involving the whole spectrum of G. However, we do not presuppose that G is a simple group, and this is an important distinction between our approach and that of [23]. On the other hand, in contrast to [23] we do not propose here any practical implementation of our results.

1. Preliminaries: arithmetic of Zsigmondy primes

For nonzero integers $n_1, \dots, n_k$, let $(n_1, \dots, n_k)$ and $[n_1, \dots, n_k]$ denote their greatest common divisor and least common multiple, respectively. Given a nonzero integer n, we put $\varphi(n)$ for the Euler totient function of n, $\pi(n)$ for the set of prime divisors of n, and if G is a finite group then, as usual, $\pi(G)$ stands for $\pi(|G|)$. If π is a set of primes, then n_π denotes the π-part of n, that is, the largest divisor k of n with $\pi(k) \subseteq \pi$; and $n_{\pi'}$ denotes the π'-part of n, that is, the ratio $|n|/n_\pi$. If n is a nonzero integer and r is an odd prime with $(r, n) = 1$, then $e(r, n)$ denotes the multiplicative order of n modulo r. Given an odd integer n, we put $e(2, n) = 1$ if $n \equiv 1 \pmod 4$, and $e(2, n) = 2$ otherwise.

Fix an integer a with $|a| > 1$. A prime r is said to be a *primitive prime divisor* of $a^i - 1$ if $e(r, a) = i$. We write $r_i(a)$ to denote some primitive prime divisor of $a^i - 1$, if such a prime exists, and $R_i(a)$ to denote the set of all such divisors. Zsigmondy [24] proved that primitive prime divisors exist for almost all pairs (a, i).

Lemma 1.1 (Zsigmondy). *Let a be an integer and $|a| > 1$. For every natural number i the set $R_i(a)$ is nonempty, except for the pairs $(a, i) \in \{(2, 1), (2, 6), (-2, 2), (-2, 3), (3, 1), (-3, 2)\}$.*

For $i \neq 2$ the product of all primitive divisors of $a^i - 1$ taken with multiplicities is denoted by $k_i(a)$. Put $k_2(a) = k_1(-a)$. The number $k_i(a)$ is said to be the *greatest primitive divisor* of $a^i - 1$. It follows from the definition that $(k_i(a), k_j(a)) = 1$ if $i \neq j$. It is easy to check that $k_1(a) = |a - 1|$ if $a \not\equiv 3 \pmod 4$, and $k_1(a) = |a-1|/2$ if $a \equiv 3 \pmod 4$, as well as $k_2(a) = |a+1|$ if $a \not\equiv 1 \pmod 4$, and $k_2(a) = |a + 1|/2$ if $a \equiv 1 \pmod 4$. It follows from [25] that for $i > 2$,

$$k_i(a) = \frac{|\Phi_i(a)|}{(r, \Phi_{i_{\{r\}'}}(a))}, \tag{1}$$

where $\Phi_i(x)$ is the ith cyclotomic polynomial and r is the largest prime dividing i; moreover, if $i_{\{r\}'}$ does not divide $r-1$ then $(r, \Phi_{i_{\{r\}'}}(a)) = 1$.

Note that for a divisor, the property of being primitive depends on the pair (a, i) and is not determined by the number $a^i - 1$. For example, $k_6(2) = 1$ but $k_3(4) = 7$, and $k_2(2) = 3$ but $k_2(-2) = 1$.

Lemma 1.2. *Suppose that a and i are integers with $|a| > 1$ and $i > 0$, and p is a prime. Then $k_{ip}(a)$ divides $k_i(a^p)$. Furthermore, if p divides i then $k_{ip}(a) = k_i(a^p)$.*

Proof. Let r be odd. Then $r \in R_{ip}(a)$ means that the multiplicative order of a modulo r equals ip. Hence the order of a^p modulo r equals i, that is $r \in R_i(a^p)$. Vice versa, if the order of a^p modulo r is equal to i, and p divides i, then the order of a modulo r is equal to ip. Thus, for odd $k_{ip}(a)$ and $k_i(a^p)$ the assertion holds by the definition of a greatest primitive divisor.

Assume that $2 \in R_{ip}(a)$. Then a is odd, $p = 2$, and $i = 1$. Therefore, $k_{ip}(a) = k_2(a)$ divides $|a+1|$, and so divides $a^2 - 1 = k_1(a^2) = k_i(a^p)$. If $2 \in R_i(a^p)$ and p divides i, then a is odd, $p = 2$, and $i = 2$, so $k_i(a^p) = k_2(a^2) = (a^2+1)/2 = k_4(a) = k_{ip}(a)$.

Lemma 1.3. *Let a and i be integers with $|a| > 1$ and $i > 0$. If i is odd then $k_i(-a) = k_{2i}(a)$, and if i is a multiple of 4 then $k_i(-a) = k_i(a)$.*

Proof. Let i be odd. By the definition of $k_2(a)$, we may assume that $i \geqslant 3$, so both $k_i(-a)$ and $k_{2i}(a)$ are odd. The order of a modulo an odd prime r is equal to $2i$ if and only if the order of $-a$ modulo r is equal to i. Hence $R_i(-a) = R_{2i}(a)$. It follows that $k_i(-a) = k_{2i}(a)$ because $k_{2i}(a)$ divides a^i+1.

The latter assertion follows from Lemma 1.2. Indeed, put $i = 2 \cdot 2j$ and observe that $k_i(-a) = k_{2\cdot 2j}(-a) = k_{2j}(a^2) = k_{2\cdot 2j}(a) = k_i(a)$.

Lemma 1.4. *Suppose that a, i, and γ are integers with $|a| > 1$, $i > 0$, and $\gamma > 1$, r is an odd prime such that $(r, a) = 1$ and r divides $k_i(a) - 1$. The following hold:*

(i) *if $i = 2^\gamma$, then $e(r, a)$ divides $2^{\gamma-1}$;*
(ii) *if $i = 3 \cdot 2^\gamma$, then $e(r, a)$ divides 2^γ;*
(iii) *if $i = 5 \cdot 2^{\gamma+1}$, then $e(r, a)$ divides $2^{\gamma+1}$;*
(iv) *if $i = 7 \cdot 2^\gamma$, then $e(r, a)$ divides $3 \cdot 2^\gamma$;*
(v) *if $i = 9 \cdot 2^\gamma$, then $e(r, a)$ divides $3 \cdot 2^{\gamma-1}$;*
(vi) *if $i = 11 \cdot 2^\gamma$, then $e(r, a)$ divides $5 \cdot 2^\gamma$.*

In particular, $e(r, a) \leqslant i/2$. Moreover, $e(r, a) \leqslant i/3$ in (ii) *and* (v).

Proof. Observe that, by (1), for $\gamma \geqslant 2$ and $i \in \{2^\gamma, 3\cdot 2^\gamma, 5\cdot 2^{\gamma+1}, 7\cdot 2^\gamma, 9\cdot 2^\gamma, 11\cdot 2^\gamma\}$ we have $k_i(a) = k_i(-a) = \Phi_i(a)$. It is easy to verify the following equalities:

if $i = 2^\gamma$, then $\Phi_i(a) - 1 = a^{2^{\gamma-1}}$ for even a, and $\Phi_i(a) - 1 = (a^{2^{\gamma-1}} - 1)/2$ for odd a;

if $i = 3\cdot 2^\gamma$, then $\Phi_i(a) - 1 = a^{2^{\gamma-1}}(a^{2^{\gamma-1}} + 1)$;

if $i = 5\cdot 2^{\gamma+1}$, then $\Phi_i(a) - 1 = a^{2^{\gamma-1}}(a^{2^\gamma} + 1)(a^{2^{\gamma-1}} - 1)$;

if $i = 7\cdot 2^\gamma$, then $\Phi_i(a) - 1 = a^{2^{\gamma-1}}(a^{3\cdot 2^\gamma} - 1)/(a^{2^{\gamma-1}} + 1)$;

if $i = 9\cdot 2^\gamma$, then $\Phi_i(a) - 1 = a^{3\cdot 2^{\gamma-1}}(a^{3\cdot 2^{\gamma-1}} - 1)$;

if $i = 11\cdot 2^\gamma$, then $\Phi_i(a) - 1 = a^{2^{\gamma-1}}(a^{5\cdot 2^\gamma} - 1)/(a^{2^{\gamma-1}} + 1)$.

These equalities yield the lemma.

Lemma 1.5. *Let a and i be integers, and $\varepsilon \in \{+,-\}$. If $a \geqslant 2$, $i \geqslant 3$, and $(a,i) \notin \{(2,3),(2,6)\}$, then $k_i(\varepsilon a) > a^{\varphi(i)/2}$.*

Proof. We prove that $k_i(a) > a^{\varphi(i)/2}$ first. Let r be the greatest prime divisor of i and $i = r^\alpha k$ where $(r,k) = 1$. It follows that $k_i(a) = \Phi_i(a)/(r, \Phi_k(a))$, and if $r-1$ is not a multiple of k, then $(r, \Phi_k(a)) = 1$. If $(r,\Phi_k(a)) = 1$, then the desired inequality holds by [25, Lemma 7], so we assume that r divides $\Phi_k(a)$ and, in particular, k divides $r-1$.

As observed in [25], the inequality

$$\Phi_i(a) \geqslant \left(\frac{b^r+1}{b+1}\right)^{\varphi(k)},$$

where $b = a^{r^{\alpha-1}}$, holds true. Since $\Phi_k(a) \leqslant (a+1)^{\varphi(k)}$, we have

$$k_i(a) \geqslant \frac{(b^r+1)^{\varphi(k)}}{r(b+1)^{\varphi(k)}} \geqslant \frac{(b^r+1)^{\varphi(k)}}{(a+1)^{\varphi(k)}(b+1)^{\varphi(k)}} \geqslant \left(\frac{b^r+1}{(b+1)^2}\right)^{\varphi(k)}. \qquad (2)$$

Let $r \geqslant 5$ and $(r,b) \neq (5,2)$. Then $b^{(r+1)/2} > (b+1)^2$ and, therefore, $k_i(a) > b^{\varphi(k)(r-1)/2} = a^{\varphi(i)/2}$ by (2).

Let $r = 5$ and $b = 2$. Then $a = 2$, $\alpha = 1$. Furthermore, k divides $r-1 = 4$. If $k \in \{1,2\}$, then $(5, \Phi_k(2)) = 1$, so we may assume that $k = 4$ and $i = 20$. In this case the assertion follows because $k_{20}(2) = k_{20}(-2) = 41 > 16 = 2^{\varphi(20)/2}$.

Let $r = 3$. Then $k \in \{1,2\}$ and $\varphi(k) = 1$. If $b \geqslant 4$ then $b^2 > 3(b+1)$. Therefore, by (2),

$$k_i(a) \geqslant \frac{(b^3+1)^{\varphi(k)}}{3(b+1)^{\varphi(k)}} = \frac{b^3+1}{3(b+1)} > b = b^{\varphi(k)} = a^{\varphi(i)/2}.$$

Thus, $b \in \{2,3\}$, so $a \in \{2,3\}$ and $\alpha = 1$. Since $i = r^\alpha k \in \{3,6\}$, the case $a = 2$ is impossible by the hypothesis. If $a = 3$ then $(3, \Phi_k(3)) = 1$.

Let, finally, $r = 2$. Then $k_i(a) = (a^{\varphi(i)} + 1)/(2, a-1) \geqslant a^{\varphi(i)}/2 \geqslant a^{\varphi(i)/2}$, as required. Thus, the inequality $k_i(a) > a^{\varphi(i)/2}$ is proved.

Now we apply Lemma 1.3. If $i \equiv 0 \pmod 4$ then $k_i(-a) = k_i(a)$. If $i \equiv 2 \pmod 4$ then $\varphi(i) = \varphi(i/2)$, so $k_i(-a) = k_{i/2}(a) > a^{\varphi(i/2)/2} = a^{\varphi(i)/2}$. Finally, if i is odd then $\varphi(i) = \varphi(2i)$, hence $k_i(-a) = k_{2i}(a) > a^{\varphi(2i)/2} = a^{\varphi(i)/2}$. The lemma is proved.

Define the following function on positive integers:

$$\eta(k) = \begin{cases} k, & \text{if } k \text{ is odd,} \\ k/2, & \text{if } k \text{ is even.} \end{cases} \tag{3}$$

Lemma 1.6. *Let u be a prime power, $\varepsilon \in \{+,-\}$, p be an odd prime, and j be a natural number with $\eta(j) \geqslant 11$. Then $k_j(\varepsilon u) > u^7$ and $k_{jp}(\varepsilon u) > u^{5p}$.*

Proof. By Lemma 1.5, the assertion holds for sufficiently large j. Indeed, if $\varphi(j) \geqslant 15$, then

$$k_j(\varepsilon u) > u^{\varphi(j)/2} > u^7,$$
$$k_{jp}(\varepsilon u) > u^{\varphi(jp)/2} \geqslant u^{\varphi(j)(p-1)/2} \geqslant u^{15(p-1)/2} \geqslant u^{5p},$$

where the latest inequality follows because $p \geqslant 3$. Therefore, we may assume that $\varphi(j) \leqslant 14$ and, in particular, $j \leqslant \varphi(j)^2 \leqslant 196$.

Let M stand for the set of j, satisfying the hypothesis of the lemma and the inequality $\varphi(j) \leqslant 14$. By brute-force attack, we obtain that $M = \{42, 36, 30, 28, 26, 24, 22, 21, 15, 13, 11\}$. If $j = 21, 15, 13, 11$, then $k_{2j}(\varepsilon u) = k_j(-\varepsilon u)$ by (1), so it is sufficient to prove the assertion for all $j \in M' = \{36, 28, 24, 21, 15, 13, 11\}$.

We use the following inequalities on $\Phi_j(\varepsilon u)$ for $j \in M'$:

$$u^{12} > \Phi_{36}(\varepsilon u) = u^{12} - u^6 + 1 > u^{11},$$

$$u^{12} > \Phi_{28}(\varepsilon u) = \frac{u^{14}+1}{u^2+1} > u^{11},$$
$$u^8 > \Phi_{24}(\varepsilon u) = u^8 - u^4 + 1 > u^7,$$
$$u^{13} > \Phi_{21}(\varepsilon u) = u^{12} - \varepsilon u^{11} + \varepsilon u^9 - u^8 + u^6 - u^4 + \varepsilon u^3 - \varepsilon u + 1 > u^{11},$$
$$u^9 > \Phi_{15}(\varepsilon u) = u^8 - \varepsilon u^7 + \varepsilon u^5 - u^4 + \varepsilon u^3 - \varepsilon u + 1 > u^7,$$

$$u^{13} > \Phi_{13}(\varepsilon u) = \frac{u^{13} - \varepsilon 1}{u - \varepsilon 1} > u^{11},$$

$$u^{11} > \Phi_{11}(\varepsilon u) = \frac{u^{11} - \varepsilon 1}{u - \varepsilon 1} > u^{9}.$$

By (1), for $j = 36,\ 28,\ 24,\ 15$ the equality $k_j(\varepsilon u) = \Phi_j(\varepsilon u)$ holds, so $k_j(\varepsilon u) > u^7$ by the above inequalities. For the other numbers from M' we have:

$$k_{21}(\varepsilon u) = \frac{\Phi_{21}(\varepsilon u)}{(7, \Phi_3(\varepsilon u))} > \frac{u^{11}}{u^2 + u + 1} > u^8,$$

$$k_{13}(\varepsilon u) = \frac{\Phi_{13}(\varepsilon u)}{(13, u - \varepsilon 1)} > \frac{u^{11}}{u + 1} > u^9,$$

$$k_{11}(\varepsilon u) = \frac{\Phi_{11}(\varepsilon u)}{(11, u - \varepsilon 1)} > \frac{u^{9}}{u + 1} > u^7.$$

Thus, the first required inequality is proved.

If p divides j then $k_{jp}(\varepsilon u) = k_j(\varepsilon u^p)$ by Lemma 1.2, so $k_{jp}(\varepsilon u) > u^{7p}$. Therefore, we assume that p does not divide j. Then $\Phi_{jp}(x) = \Phi_j(x^p)/\Phi_j(x)$. Suppose that $p \geqslant 13$. Then p is the greatest prime divisor of jp, hence, using (1), we obtain

$$k_{jp}(\varepsilon u) = \frac{\Phi_j(\varepsilon u^p)}{\Phi_j(\varepsilon u)(p, \Phi_j(\varepsilon u))} \geqslant \frac{\Phi_j(\varepsilon u^p)}{\Phi_j^2(\varepsilon u)} > \frac{u^{7p}}{u^{26}} \geqslant u^{5p}.$$

Suppose that $5 \leqslant p \leqslant 11$. In this case the greatest prime divisor of jp is at most 13. It follows that

$$k_{jp}(\varepsilon u) = \frac{\Phi_j(\varepsilon u^p)}{\Phi_j(\varepsilon u)(p, \Phi_j(\varepsilon u))} \geqslant \frac{\Phi_j(\varepsilon u^p)}{13\Phi_j(\varepsilon u)} > \frac{u^{9p}}{13u^{13}} > \frac{u^{9p}}{u^{17}} > u^{5p},$$

unless j equals 15 or 24. For $j \in \{15, 24\}$, the greatest prime divisor of jp is equal to p, and $p - 1$ is not a multiple of j, hence

$$k_{jp}(\varepsilon u) = \frac{\Phi_j(\varepsilon u^p)}{\Phi_j(\varepsilon u)} > \frac{u^{7p}}{u^9} > u^{5p}.$$

Let $p = 3$. Then $j = 28, 13, 11$, and the assertion follows from the inequalities:

$$k_{54}(\varepsilon u) = \frac{\Phi_{28}(\varepsilon u^3)}{\Phi_{28}(\varepsilon u)} > \frac{u^{33}}{u^{12}} > u^{15},$$

$$k_{39}(\varepsilon u) = \frac{\Phi_{13}(\varepsilon u^3)}{13\Phi_{13}(\varepsilon u)} > \frac{u^{33}}{13u^{13}} > u^{15},$$

$$k_{33}(\varepsilon u) = \frac{\Phi_{11}(\varepsilon u^3)}{\Phi_{11}(\varepsilon u)} > \frac{u^{27}}{u^{11}} > u^{15}.$$

The lemma is proved.

Lemma 1.7. *Let q and m be integers greater than 1, and $\varepsilon \in \{+,-\}$.*

(i) *If an odd prime r divides $\varepsilon q - 1$, then $((\varepsilon q)^m - 1)_{\{r\}} = m_{\{r\}}(\varepsilon q - 1)_{\{r\}}$.*

(ii) *If an odd prime r divides $(\varepsilon q)^m - 1$, then r divides $(\varepsilon q)^{m_{\{r\}'}} - 1$.*

(iii) *If $\varepsilon q - 1$ is a multiple of 4, then $((\varepsilon q)^m - 1)_{\{2\}} = m_{\{2\}}(\varepsilon q - 1)_{\{2\}}$.*

Proof. See, for example, [26, Chapter IX, Lemma 8.1].

Let $[x]$ denote the integer part of a real number x.

Lemma 1.8. *Let a, b be positive integers, $b > a$, and $A = \{i \in \mathbb{N} \mid b - a < \eta(i) \leqslant b\}$. If b is even then $|A| = [3a/2]$. If b is odd then $|A| = [(3a+1)/2]$.*

Proof. Since the equation $\eta(x) = j$ has two integer solutions for odd j and one solution for even j, the cardinality of A is equal to the sum of a and the quantity of odd numbers in the interval $(b-a, b]$. If b is even then this quantity is equal to $[a/2]$, and if b is odd then it equals $[(a+1)/2]$.

Lemma 1.9. *If n is a natural number and $n \geqslant 30$, then the interval $(5n/6, n)$ contains a prime. If, in addition, $n \neq 35, 36, 37, 53$, then the interval $(8n/9, n)$ contains a prime.*

Proof. The first part is proved in [27]. It is shown in [28] that for every natural number $m \geqslant 119$, the interval $[m, 1.073m]$ contains a prime. Since $9/8 > 1.073$, the second part holds for all sufficiently large n (precisely, for $n \geqslant 129$). For smaller n the assertion can be verified directly.

2. Preliminaries: the prime graph and the spectrum of a finite group

The *prime graph* $GK(G)$ of a finite group G is the nonoriented graph with the vertex set $\pi(G)$ and two distinct vertices r and s are adjacent if and only if $rs \in \omega(G)$. The notion of prime graph was introduced by G.K. Gruenberg and O. Kegel (for this reason it is also called the Gruenberg–Kegel graph). They established that a finite group with disconnected prime graph is either Frobenius or 2-Frobenius group, or has a unique nonabelian composition factor with disconnected prime graph. J.S. Williams [29] published this result and started the classification of finite simple groups with disconnected prime graph. The classification was completed by A.S. Kondrat′ev [30]. The full list of nonabelian simple groups with disconnected prime graph can be found, e.g., in [31, Tables 1a-1c].

Recall that an independent set of vertices or a *coclique* of a graph Γ is any subset of pairwise nonadjacent vertices of Γ. We write $t(\Gamma)$ to denote the independence number of Γ, that is the greatest size of coclique in Γ. For a group G, put $t(G) = t(GK(G))$. By analogy, for each prime r, define the r-independence number $t(r, G)$ to be the greatest size of cocliques containing the vertex r in $GK(G)$. For convenience, we refer to a coclique containing r as an $\{r\}$-coclique. In [32] there was proved the following assertion which is, in some sense, a generalization of the Gruenberg–Kegel theorem (below we give the statement of this result from [33, Theorem 1]).

Lemma 2.1. *Let G be a finite group with $t(G) \geqslant 3$ and $t(2, G) \geqslant 2$. Then the following hold:*

(i) *There exists a nonabelian simple group S such that $S \leqslant \overline{G} = G/K \leqslant \operatorname{Aut} S$, where K is the maximal normal soluble subgroup of G.*

(ii) *For every coclique ρ of $GK(G)$ of size at least 3, at most one prime of ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geqslant t(G) - 1$.*

(iii) *One of the following holds:*

(a) *every prime $r \in \pi(G)$ nonadjacent to 2 in $GK(G)$ does not divide the product $|K| \cdot |\overline{G}/S|$; in particular, $t(2, S) \geqslant t(2, G)$;*

(b) *there exists a prime $r \in \pi(K)$ nonadjacent to 2 in $GK(G)$; in which case $t(G) = 3$, $t(2, G) = 2$, and $S \simeq A_7$ or $L_2(q)$ for some odd q.*

Let L and G be isospectral finite groups. It follows by the definition of prime graph that $GK(L) = GK(G)$. Therefore, if L satisfies the hypothesis of Lemma 2.1, then so does G. In [34, 35], for every finite nonabelian simple group, an adjacency criterion of its prime graph is developed and all cocliques and $\{2\}$-cocliques of greatest size in this graph are found, as well as $\{p\}$-cocliques of greatest size for groups of Lie type in characteristic p. This information and Williams–Kondrat′ev's classification, imply the following assertion which is the first step toward a proof of main results of the present paper.

Proposition 1. *Let L be a finite simple group of Lie type different from the groups $L_3(3)$, $U_3(3)$, and $S_4(3)$. If G is a finite group isospectral to L, then the following hold true for G:*

(i) *There exists a nonabelian simple group S such that $S \leqslant \overline{G} = G/K \leqslant \operatorname{Aut} S$, where K is the maximal normal soluble subgroup of G.*

(ii) *For every coclique ρ of $GK(G)$ of size at least 3, at most one prime of ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geqslant t(L) - 1$.*

(iii) *Every prime $r \in \pi(G)$ nonadjacent to 2 in $GK(G)$ does not divide the product $|K| \cdot |\overline{G}/S|$. In particular, $t(2, S) \geqslant t(2, L)$.*

Proof. If L is a finite nonabelian simple group with connected prime graph and is different from an alternating group, then it satisfies the hypothesis of Lemma 2.1 by [34]. If L has a disconnected prime graph then the existence and uniqueness of a nonabelian composition factor S follow from the Gruenberg–Kegel theorem and [36]. By [32, Propositions 2,3], the inequality $t(2, G) \geqslant 2$ and the insolubility of G imply that (ii) and (iii) of Lemma 2.1 hold. It remains to observe that the exceptional case (b) of assertion (iii) of Lemma 2.1 does not hold by [33, Theorem 2]. The proposition is proved.

For a classical group L, we put $\operatorname{prk}(L)$ to denote its dimension if L is a linear or unitary group, and its Lie rank if L is a symplectic or orthogonal group. Observe that $n = \operatorname{prk}(L)$ in Theorems 1–3 in Introduction.

Proposition 2. *Suppose that L is a finite simple classical group,* $\operatorname{prk}(L) \geqslant 27$ *if L is linear or unitary, and* $\operatorname{prk}(L) \geqslant 19$ *if L is symplectic or orthogonal. Suppose that G is a finite group isospectral to L, and S is a unique nonabelian composition factor of G. If S is a group of Lie type, then S is a classical group,* $\operatorname{prk}(S) \geqslant 25$ *if S is linear or unitary, and* $\operatorname{prk}(S) \geqslant 16$ *if S is symplectic or orthogonal.*

Proof. Applying [35, Tables 2,3], it is easy to obtain that $t(L) \geqslant 14$ provided the hypothesis of the proposition. By Proposition 1(ii), we have $t(S) \geqslant 13$. On the other hand, it follows from [35, Table 4] that $t(H) \leqslant t(E_8(u)) = 12$ for every simple exceptional group H of Lie type. Thus, S is a classical group. The required inequalities on $\operatorname{prk}(S)$ hold by [35, Tables 2,3]. The proposition is proved.

Given a classical group L over a field of order q, put

$$\delta(L) = \begin{cases} \pi(\varepsilon q - 1), & \text{if } L = L_n^{\varepsilon}(q), \\ \pi((2, q-1)), & \text{if } L \text{ is symplectic or orthogonal.} \end{cases} \tag{4}$$

Lemma 2.2. *Let L be a simple classical group over a field of order q and characteristic p. Suppose that r and s are distinct primes, $r, s \notin \delta(L)$, $r \in R_i(q)$, and $s \in R_j(q)$.*

(i) *If $rs \in \omega(L)$, then $r's' \in \omega(L)$ for every distinct odd primes $r' \in R_i(q)$ and $s' \in R_j(q)$.*

(ii) *If $pr \in \omega(L)$, then $pr' \in \omega(L)$ for every odd prime $r' \in R_i(q)$.*

Proof. It follows from [34].

Thus, for two distinct primes $r, s \in \pi(L) \setminus \delta(L)$, where $r \neq p$, the answer to the question whether they are adjacent in $GK(L)$ depends only on $e(r,q)$, if $s = p$, and $e(r,q)$, $e(s,q)$, if $s \neq p$.

In [34] several functions of natural argument are used to formulate an adjacency criterion, one of them is η defined in (3), and two others we define here.

$$\nu(k) = \begin{cases} k, \text{ if } k \equiv 0 \,(\mathrm{mod}\, 4), \\ k/2, \text{ if } k \equiv 2 \,(\mathrm{mod}\, 4), \\ 2k, \text{ if } k \text{ is odd.} \end{cases} \quad (5)$$

For $\varepsilon \in \{+, -\}$, put

$$\nu_\varepsilon(k) = \begin{cases} k, \text{ if } \varepsilon = +, \\ \nu(k) \text{ if } \varepsilon = -. \end{cases} \quad (6)$$

It is an easy observation that ν_ε is a bijection and ν_ε^2 is an identity.

For linear and unitary groups, we exploit also a reformulation of an adjacency criterion (see [18, Lemmas 2.1–2.3]), if it is more convenient for our goals than an initial formulation from [34] which used the function ν_ε. This reformulation is based on the equality $k_{\nu_\varepsilon(i)}(q) = k_i(\varepsilon q)$, which follows from Lemma 1.3 and the definition of ν_ε.

Now we introduce a new function in order to unify further arguments. Namely, given a simple classical group L over a field of order q and a prime r coprime to q, we put

$$\varphi(r, L) = \begin{cases} e(r, \varepsilon q), \text{ if } L = L_n^\varepsilon(q), \\ \eta(e(r,q)), \text{ if } L \text{ is symplectic or orthogonal.} \end{cases} \quad (7)$$

It follows that

$$e(r,q) = \begin{cases} 2\varphi(r,L), & \text{if either } e(r,q) \text{ is even and } L \text{ is symplectic} \\ & \text{or orthogonal,} \\ & \text{or } e(r,q) \equiv 2 \pmod 4 \text{ and } L \text{ is unitary;} \\ \varphi(r,L)/2, & \text{if } e(r,q) \equiv 1 \pmod 2 \text{ and } L \text{ is unitary;} \\ \varphi(r,L) & \text{otherwise.} \end{cases} \tag{8}$$

Observe that $e(r,-q) = \varphi(r,L)$ in the case of $e(r,q) = \varphi(r,L)/2$.

Lemma 2.3. *Let L be a simple classical group over a field of order q and characteristic p. If r is an odd prime from $\pi(L) \setminus \{p\}$ then $\varphi(r,L)$ divides $r-1$, and if L is a symplectic or orthogonal group then $2\varphi(r,L)$ divides $r-1$.*

Proof. If L is not unitary, then $\varphi(r,L)$ divides $e(r,q)$, which divides $r-1$ by Fermat's little theorem. If L is unitary, then $\varphi(r,L)$ does not divide $e(r,q)$ only when $e(r,q)$ is odd. But then $\varphi(r,L) = e(r,-q) = 2e(r,q)$ and $\varphi(r,L)$ divides $r-1$ because r is odd. Let L be a symplectic or orthogonal group. If $\varphi(r,L)$ is even then $2\varphi(r,L) = e(r,q)$, and if not, then $\varphi(r,L)$ divides $(r-1)/2$.

Lemma 2.4. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n \geqslant 4$.

(i) *If $r \in \pi(L) \setminus \{p\}$, then $\varphi(r,L) \leqslant n$.*

(ii) *If r and s are distinct primes from $\pi(L) \setminus \{p\}$ with $\varphi(r,L) \leqslant n/2$ and $\varphi(s,L) \leqslant n/2$, then r and s are adjacent in $GK(L)$.*

(iii) *If r and s are distinct primes from $\pi(L) \setminus \{p\}$ with $n/2 < \varphi(r,L) \leqslant n$ and $n/2 < \varphi(s,L) \leqslant n$, then r and s are adjacent in $GK(L)$ if and only if $e(r,q) = e(s,q)$.*

(iv) *If r and s are distinct primes from $\pi(L) \setminus \{p\}$ and $e(r,q) = e(s,q)$, then r and s are adjacent in $GK(L)$.*

Proof. It follows from [34, 35].

Let L be a simple classical group over a field of order q and characteristic p. For $\sigma \subseteq \pi(L) \setminus \{p\}$, set $E(\sigma, L) = \{e(r,q) \mid r \in \sigma\}$. If $\mathrm{prk}(L) = n \geqslant 13$ then, by [35], every coclique ρ of greatest size in $GK(L)$ does not contain p, so the set $E(\rho, L)$ is well-defined for ρ. Define $J(L)$ as the union of sets $E(\rho, L)$, and $E(L)$ as the intersection of these sets, where ρ runs over all cocliques of greatest size in $GK(L)$. The next lemma is a particular case of the main theorem of [35].

Lemma 2.5. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n \geqslant 13$. *Let ρ be a coclique of greatest size in $GK(L)$. If $J(L) = E(L)$ then $E(\rho, L) = E(L)$. If $J(L) \neq E(L)$ then $E(\rho, L) = E(L) \cup \{j\}$ for some $j \in J(L) \setminus E(L)$. In particular, $|E(L)| \leqslant t(L) \leqslant |E(L)| + 1$. The sets $E(L)$, $J(L) \setminus E(L)$ and numbers $t(L)$ are listed in Table* 1.

Proof. See [35, Tables 2,3].

Table 1: Cocliques of greatest size

L	Conditions	$t(L)$	$E(L)$	$J(L) \setminus E(L)$
$L_n^{\varepsilon}(q)$	n odd	$\frac{n+1}{2}$	$\{i \mid \frac{n}{2} < \nu_{\varepsilon}(i) \leq n\}$	$\varnothing$
	n even	$\frac{n}{2}$	$\{i \mid \frac{n}{2} < \nu_{\varepsilon}(i) < n\}$	$\{\frac{n}{2}, n\}$
$S_{2n}(q)$ or $O_{2n+1}(q)$	$n \equiv 0 \pmod 4$	$\frac{3n+4}{4}$	$\{i \mid \frac{n}{2} \leqslant \eta(i) \leqslant n\}$	$\varnothing$
	$n \equiv 1 \pmod 4$	$\frac{3n+5}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n\}$	$\varnothing$
	$n \equiv 2 \pmod 4$	$\frac{3n+2}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n\}$	$\{\frac{n}{2}, n\}$
	$n \equiv 3 \pmod 4$	$\frac{3n+3}{4}$	$\{i \mid \frac{n+1}{2} < \eta(i) \leqslant n\}$	$\{\frac{n-1}{2}, n-1, n+1\}$
$O_{2n}^{+}(q)$	$n \equiv 0 \pmod 4$	$\frac{3n}{4}$	$\{i \mid \frac{n}{2} \leqslant \eta(i) \leqslant n, i \neq 2n\}$	$\varnothing$
	$n \equiv 1 \pmod 4$	$\frac{3n+1}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n, i \neq 2n, n+1\}$	$\{n-1, n+1\}$
	$n \equiv 2 \pmod 4$	$\frac{3n-2}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n, i \neq 2n\}$	$\{\frac{n}{2}, n\}$
	$n \equiv 3 \pmod 4$	$\frac{3n+3}{4}$	$\{i \mid \frac{n-1}{2} \leqslant \eta(i) \leqslant n, i \neq 2n, n-1\}$	$\varnothing$
$O_{2n}^{-}(q)$	$n \equiv 0 \pmod 4$	$\frac{3n+4}{4}$	$\{i \mid \frac{n}{2} \leqslant \eta(i) \leqslant n\}$	$\varnothing$
	$n \equiv 1 \pmod 4$	$\frac{3n+1}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n, i \neq n, \frac{n+1}{2}\}$	$\{\frac{n+1}{2}, n-1\}$
	$n \equiv 2 \pmod 4$	$\frac{3n+2}{4}$	$\{i \mid \frac{n}{2} < \eta(i) \leqslant n\}$	$\{\frac{n}{2}, n-2, n\}$
	$n \equiv 3 \pmod 4$	$\frac{3n+3}{4}$	$\{i \mid \frac{n-1}{2} \leqslant \eta(i) \leqslant n, i \neq n, \frac{n-1}{2}\}$	$\varnothing$

Define $J(p, L)$ as the union of sets $E(\rho \setminus \{p\}, L)$, and $E(p, L)$ as the intersection of these sets, where ρ runs over all $\{p\}$-cocliques of greatest size in $GK(L)$.

Table 2: Cocliques containing the characteristic

L	Conditions	$t(p,L)$	$J(p,L)$
$L_n^{\varepsilon}(q)$		3	$\{\nu_{\varepsilon}(n-1), \nu_{\varepsilon}(n)\}$
$S_{2n}(q)$ or	n is even	2	$\{2n\}$
$O_{2n+1}(q)$	n is odd	3	$\{n, 2n\}$
$O_{2n}^{+}(q)$	n is even	3	$\{n-1, 2n-2\}$
	n is odd	3	$\{n, 2n-2\}$
$O_{2n}^{-}(q)$	n is even	4	$\{n-1, 2n-2, 2n\}$
	n is odd	3	$\{2n-2, 2n\}$

Lemma 2.6. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n$. *Suppose that $n \geqslant 4$ and $(n, \varepsilon q) \notin \{(4,-2),(6,2),(7,2)\}$ for $L = L_n^{\varepsilon}(q)$; $n \geqslant 3$ and $(n,q) \neq (3,2)$ for $L \in \{S_{2n}(q), O_{2n+1}(q)\}$; $n \geqslant 4$ and $(n,q) \neq (4,2)$ for $L = O_{2n}^{\pm}(q)$. If ρ is a $\{p\}$-coclique of greatest size in $GK(L)$, then $E(\rho\setminus\{p\}, L) = J(p,L) = E(p,L)$, in particular, $t(p,L) = |J(p,L)|+1$. The sets $J(p,L)$ and numbers $t(p,L)$ are listed in Table 2. In particular, if $n \geqslant 9$ then $t(p,L) < t(L)$. Furthermore, $\varphi(r,L) > n/2$ for every prime r nonadjacent to p in $GK(L)$.*

Proof. It follows from [34, Proposition 6.3, Table 4].

A prime $r \in \pi(L)$ is called *large* (with respect to L), if r lies in some coclique of greatest size in the prime graph $GK(L)$, and *small* (with respect to L) otherwise.

Lemma 2.7. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n \geqslant 13$.

(i) *If $\varphi(r,L) \geqslant n/2$, then r is large with respect to L.*

(ii) *If r is large with respect to L, then $\varphi(r,L) \geqslant n/2 - 1$.*

(iii) *If r is large with respect to L, then*

$$\varphi(r,L) \geqslant \begin{cases} t(L), & \text{if } L \text{ is linear or unitary;} \\ (2t(L)-4)/3, & \text{if } L \text{ is symplectic or orthogonal.} \end{cases} \tag{9}$$

(iv) *If ρ is a coclique in $GK(L)$ and $n/2 < \varphi(r,L)$ for every $r \in \rho$, then $GK(L)$ has a coclique σ of size $t(L)$ with $\rho \subseteq \sigma$.*

Proof. Apply Table 1.

Lemma 2.8. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n \geqslant 13$. *Suppose that $r \in \pi(L)$ and ρ is an $\{r\}$-coclique of greatest size in $GK(L)$. Then every $s \in \rho' = \rho \setminus \{r\}$ is large with respect to L. Further, if r is small with respect to L, then $\varphi(s, L) > n/2$ for every $s \in \rho'$, and $E(\rho', L)$ is uniquely determined by r. If, in addition, $i = e(r, q) > 2$, then $E(\rho', L)$ is uniquely determined by i.*

Proof. If r is large with respect to L, then the assertion is obvious. Suppose that r is small and $s \in \rho'$. If $r = p$ then $\varphi(s, L) > n/2$ and $E(\rho', L) = J(p, L)$ is uniquely determined by Lemma 2.6. Let $r \neq p$. Lemma 2.6 implies that $s \neq p$. Since $\varphi(r, L) < n/2$ by Lemma 2.5, the inequality $\varphi(s, L) > n/2$ follows from Lemma 2.4(ii). Let σ be another $\{r\}$-coclique of greatest size and $\sigma' = \sigma \setminus \{r\}$. Assume that $E(\rho', L) \neq E(\sigma', L)$. Then there is $w \in \sigma'$ with $e(w, q) \notin E(\rho', L)$. It follows from Lemma 2.4(iii) that $\{w\} \cup \rho$ is an $\{r\}$-coclique in $GK(L)$, which contradicts to the maximality of ρ. If $i = e(r, q) > 2$ then $R_i(q)$ and $\delta(L)$ are disjoint. As shown above, ρ' consists of primes large with respect to L, and so ρ' and $\delta(L)$ are disjoint as well. Lemma 2.2 yields that $E(\rho', L)$ depends only on i.

Let L be a simple classical group over a field of order q and characteristic p, and let $\mathrm{prk}(L) = n \geqslant 13$. Let r be small with respect to L and ρ be an $\{r\}$-coclique of greatest size. As shown in Lemma 2.8, the set $E(\rho \setminus \{r\}, L)$ is contained in $J(L)$ and does not depend on a choice of ρ, so we denote it by $J(r, L)$.

Lemma 2.9. *Let L be a simple classical group over a field of order q and characteristic p, and let* $\mathrm{prk}(L) = n \geqslant 13$. *Suppose that $r \in \pi(L)$, $2 \neq r \neq p$, and $t(r, L) \leqslant 4$. Then $e(r, q)$, $t(r, L)$, and $J(r, L)$ are listed in Table* 3.

Proof. The application of an adjacency criterion from [34, 35] reduces the proof to easy arithmetical calculations.

Lemma 2.10. *Suppose that L is a finite simple classical group over a field of characteristic p. Then for every $r \in \pi(L)$ there is $s \in \pi(L)$ such that $p \neq s \neq r$ and $rs \notin \omega(L)$.*

Table 3: Cocliques of size at most 4

L	$e(r,q)$	Conditions	$t(r,L)$	$J(r,L)$
$L_n^{\varepsilon}(q)$	$\nu_\varepsilon(1)$	$\lvert\varepsilon q-1\rvert_r=n_r$	3	$\{\nu_\varepsilon(n-1),\nu_\varepsilon(n)\}$
		$\lvert\varepsilon q-1\rvert_r>n_r$	2	$\{\nu_\varepsilon(n)\}$
		$\lvert\varepsilon q-1\rvert_r<n_r$	2	$\{\nu_\varepsilon(n-1)\}$
	$\nu_\varepsilon(2)$	$n\equiv 0\,(\mathrm{mod}\,2)$	2	$\{\nu_\varepsilon(n-1)\}$
		$n\equiv 1\,(\mathrm{mod}\,2)$	2	$\{\nu_\varepsilon(n)\}$
	$\nu_\varepsilon(3)$	$n\equiv 0\,(\mathrm{mod}\,3)$	3	$\{\nu_\varepsilon(n-2),\nu_\varepsilon(n-1)\}$
		$n\equiv 1\,(\mathrm{mod}\,3)$	3	$\{\nu_\varepsilon(n-2),\nu_\varepsilon(n)\}$
		$n\equiv 2\,(\mathrm{mod}\,3)$	3	$\{\nu_\varepsilon(n-1),\nu_\varepsilon(n)\}$
	$\nu_\varepsilon(4)$	$n\equiv 0\,(\mathrm{mod}\,4)$	4	$\{\nu_\varepsilon(n-3),\nu_\varepsilon(n-2),\nu_\varepsilon(n-1)\}$
		$n\equiv 1\,(\mathrm{mod}\,4)$	4	$\{\nu_\varepsilon(n-3),\nu_\varepsilon(n-2),\nu_\varepsilon(n)\}$
		$n\equiv 2\,(\mathrm{mod}\,4)$	4	$\{\nu_\varepsilon(n-3),\nu_\varepsilon(n-1),\nu_\varepsilon(n)\}$
		$n\equiv 3\,(\mathrm{mod}\,4)$	4	$\{\nu_\varepsilon(n-2),\nu_\varepsilon(n-1),\nu_\varepsilon(n)\}$
$S_{2n}(q)$ or	1		2	$\{2n\}$
$O_{2n+1}(q)$	2	$n\equiv 0\,(\mathrm{mod}\,2)$	2	$\{2n\}$
		$n\equiv 1\,(\mathrm{mod}\,2)$	2	$\{n\}$
	4	$n\equiv 0\,(\mathrm{mod}\,4)$	4	$\{n-1,2n-2,2n\}$
		$n\equiv 1\,(\mathrm{mod}\,4)$	4	$\{n,2n-2,2n\}$
		$n\equiv 2\,(\mathrm{mod}\,4)$	3	$\{n-1,2n-2\}$
		$n\equiv 3\,(\mathrm{mod}\,4)$	3	$\{n,2n\}$
	3	$n\equiv 4\,(\mathrm{mod}\,6)$	4	$\{2n-4,2n-2,2n\}$
	6	$n\equiv 4\,(\mathrm{mod}\,6)$	4	$\{2n-4,n-1,2n\}$
$O_{2n}^{+}(q)$	1		2	$\{2n-2\}$
	2	$n\equiv 0\,(\mathrm{mod}\,2)$	2	$\{n-1\}$
		$n\equiv 1\,(\mathrm{mod}\,2)$	2	$\{n\}$
	4	$n\equiv 0\,(\mathrm{mod}\,4)$	3	$\{n-1,2n-2\}$
		$n\equiv 1\,(\mathrm{mod}\,4)$	4	$\{n-2,2n-2,n\}$
		$n\equiv 2\,(\mathrm{mod}\,4)$	3	$\{n-1,2n-2\}$
		$n\equiv 3\,(\mathrm{mod}\,4)$	3	$\{n-2,n\}$
	3	$n\equiv 4\,(\mathrm{mod}\,6)$	4	$\{2n-6,2n-4,2n-2\}$
	6	$n\equiv 4\,(\mathrm{mod}\,6)$	4	$\{2n-4,n-3,n-1\}$
		$n\equiv 5\,(\mathrm{mod}\,6)$	4	$\{2n-2,n-2,n\}$
$O_{2n}^{-}(q)$	1		2	$\{2n\}$
	2	$n\equiv 0\,(\mathrm{mod}\,2)$	2	$\{2n\}$
		$n\equiv 1\,(\mathrm{mod}\,2)$	2	$\{2n-2\}$
	4	$n\equiv 0\,(\mathrm{mod}\,4)$	4	$\{n-1,2n-2,2n\}$
		$n\equiv 1\,(\mathrm{mod}\,4)$	4	$\{2n-4,2n-2,2n\}$
		$n\equiv 2\,(\mathrm{mod}\,4)$	4	$\{n-1,2n-4,2n-2\}$
		$n\equiv 3\,(\mathrm{mod}\,4)$	3	$\{2n-4,2n\}$
	3	$n\equiv 5\,(\mathrm{mod}\,6)$	4	$\{2n-4,2n-2,2n\}$

PROOF. It follows from [34] (e.g., see [37, Lemma 4] and [20, Lemma 12]).

We note without proof a more general result following from [34]: for every finite nonabelian simple group L, which is not alternating, and for every $r \in \pi(L)$ there exists $s \in \pi(L)$ not equal to r and satisfying $rs \notin \omega(L)$.

Lemma 2.11. *Let r be a prime divisor of the order of a simple classical group L over a field of order q, and let $e(r,q)$ divide $l \cdot 2^k$, where $l \in \{1,3,5\}$, k is a nonnegative integer. If $L = L_n^\varepsilon(q)$, then either $\varphi(r,L) \leqslant 2l$ or $\varphi(r,L) = e(r,q)$. If L is a symplectic or orthogonal group, then either $\varphi(r,L) \leqslant l$ or $\varphi(r,L) = e(r,q)/2$.*

PROOF. It follows from (7) by direct verification.

Lemma 2.12. *Let L be a simple classical group over a field of order q and characteristic p, and let $\mathrm{prk}(L) = n \geqslant 4$. If $r \in \pi(L) \setminus \{p\}$, $i = e(r,q)$, and $n/2 < \varphi(r,L) \leqslant n$, then L includes a cyclic Hall subgroup of order $k_i(q)$.*

PROOF. It follows from formulae for orders of simple classical groups and information on cyclic structure of their maximal tori (see, e.g., [38]).

Our main source on spectra of classical group is a series of papers [38, 39, 40] containing an explicit arithmetical criterion for a natural number to lie in the spectrum of a classical group. In particular, the following lemma is a direct corollary of these results and properties of $e(r,q)$.

Lemma 2.13. *Let L be a simple classical group over a field of order q and characteristic p, and let $\mathrm{prk}(L) = n$. Let k and l be integers, $k \geqslant 0$, $l > 0$, and $\delta = \delta(L)$. For $j = 1, \dots, l$, suppose that pairwise distinct primes r_j lie in $\pi(L) \setminus (\delta \cup \{p\})$ and put $i_j = e(r_j, q)$. The product $p^k r_1 r_2 \cdots r_l$ lies in $\omega(L)$ if and only if the δ'-part of $p^k a$ lies in $\omega(L)$, where*

$$a = \begin{cases} [(\varepsilon q)^{\nu_\varepsilon(i_1)} - 1, (\varepsilon q)^{\nu_\varepsilon(i_2)} - 1, \dots, (\varepsilon q)^{\nu_\varepsilon(i_l)} - 1], & \textit{if } L = L_n^\varepsilon(q), \\ [q^{\eta(i_1)} + (-1)^{i_1}, q^{\eta(i_2)} + (-1)^{i_2}, \dots, q^{\eta(i_l)} + (-1)^{i_l}] & \textit{otherwise.} \end{cases}$$

In particular, if $i_1, i_2, \dots, i_l$ are greater than 2 and pairwise distinct, then $p^k r_1 r_2 \cdots r_l \in \omega(L)$ if and only if $p^k k_{i_1}(q) k_{i_2}(q) \cdots k_{i_l}(q) \in \omega(L)$.

PROOF. See [38, 39, 40].

Remark 2. The last assertion of the lemma in the particular case $k = 0$, $l = 1$ means the following: If r with $e(r, q) = i > 2$ divides $|L|$, then $k_i(q) \in \omega(L)$. If in addition $n \geqslant 4$, then obviously $k_i(q) \in \omega(L)$ for $i = 1, 2$. In particular, it gives another proof of Lemma 2.4(iv).

Lemma 2.14. *Let L be a simple classical group over a field of order q and characteristic p, and let $\operatorname{prk}(L) = n$.*

(i) *If $L = L_n^\varepsilon(q)$ and $n \geqslant 23$, then $\omega(L)$ contains a number k with $k \geqslant q^{4t(L)/3}$ and all prime divisors of k are large with respect to L.*

(ii) *If $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ and $n \geqslant 29$, or $L = O_{2n}^\varepsilon(q)$ and $n \geqslant 30$, then $\omega(L)$ contains a number k with $k \geqslant q^{10t(L)/9}$ and all prime divisors of k are large with respect to L.*

(iii) *The numbers from $\omega(L)$ do not exceed $q^{2t(L)}$.*

(iv) *If $p^\gamma > 2n - 1$, then the exponent of a Sylow p-subgroup of L does not exceed p^γ.*

Proof. (i) Suppose that $L = L_n^\varepsilon(q)$, where $n \geqslant 29$. Then $t(L) = [(n+1)/2] \geqslant 15$ and $n + 1 \geqslant 2t(L)$. By Lemma 1.9, there is a prime j such that $5(n+1)/6 < j < n + 1$. The inequalities $j \leqslant n$ and $j > n/2$ imply that $k_j(\varepsilon q)$ lies in $\omega(L)$ and all its prime divisors are large with respect to L. Furthermore, applying (1) it is easy to get the inequality $k_j(\varepsilon q) > q^{j-3}$ (see, for example, [17, Lemma 3.1]). It follows

$$j - 3 > \frac{5(n+1)}{6} - 3 \geqslant \frac{5t(L)}{3} - 3 \geqslant \frac{4t(L)}{3}.$$

If $23 \leqslant n \leqslant 28$, then we prove the assertion by putting $j = 23$.

(ii) Let L be a symplectic or orthogonal group. To prove the lemma it is sufficient to find a prime j such that $j - 2 \geqslant 10t(L)/9$, and either $j < n$ or $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ and $j \leqslant n$. Indeed, if these conditions hold, then both numbers $k_j(q)$ and $k_j(-q)$ lie in $\omega(G)$, all their prime divisors are large, and at least one of $k_j(q)$ and $k_j(-q)$ is greater than q^{j-2} (applying (1) again). The required assertion will be also proved, if we find j, which is a power of 2, satisfying $n/2 < j < n$ and $k_{2j}(q) = (q^j + 1)/(2, q-1) \geqslant q^{10t(L)/9}$.

Suppose that $n \geqslant 54$. Then $t(L) \geqslant (3n-2)/4 \geqslant 40$. We find desired j applying Lemma 1.9.

Let n be even. Then $t(L) \leqslant (3n+4)/4$ and, therefore, $n + 1 \geqslant (4t(L) - 1)/3$. There exists a prime j with $8(n+1)/9 < j < n + 1$ and, in particular, $j > 8(4t(L) - 1)/27$. Since n is even, we have $j < n$.

Let n be odd and $L \in \{S_{2n}(q), O_{2n+1}(q)\}$. Then $t(L) \leqslant (3n+5)/4$, and so $n+2 \geqslant (4t(L)+1)/3$. There is a prime j with $8(n+2)/9 < j < n+2$ and, in particular, $j > 8(4t(L)+1)/27$. Since n is odd, the inequality $j \leqslant n$ holds.

Let, finally, n be odd and $L = O_{2n}^{\varepsilon}(q)$. Then $t(L) \leqslant (3n+3)/4$, and so $n \geqslant (4t(L)-3)/3$. There is a prime j with $8n/9 < j < n$ and, in particular, $j > 8(4t(L)-3)/27$.

In all cases $j > 8(4t(L)-3)/27$, hence

$$j - 2 > \frac{8(4t(L)-3)}{27} - 2 = \frac{32t(L)-78}{27} \geqslant \frac{10t(L)}{9}.$$

For $n \leqslant 53$ we point out j explicitly.

If $48 \leqslant n \leqslant 53$ then $t(L) \leqslant 41$, and if $t(L) = 41$ then $n = 53$ and $L \in \{S_{2n}(q), O_{2n+1}(q)\}$. Put $j = 47$, if $t(L) \leqslant 40$, and $j = 53$, if $t(L) = 41$. If $44 \leqslant n \leqslant 47$, then $t(L) \leqslant 36$ and $j = 43$ can be taken. If $n = 42, 43$, then $t(L) \leqslant 33$ and $j = 41$. If $38 \leqslant n \leqslant 41$, then $t(L) \leqslant 32$ and j equals 41 or 37 according to a type of group. If $n = 32$, then $t(L) \leqslant 25$ and $j = 31$. If either $29 \leqslant n \leqslant 31$ and $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, or $n = 30, 31$ and $L = O_{2n}^{\varepsilon}(q)$, then $t(L) \leqslant 24$ and $j = 29$.

It remains to treat the case $33 \leqslant n \leqslant 37$. It follows that $t(L) \leqslant 29$. If $t(L) = 29$, then $n = 37$ and $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, so we put $j = 37$. Let $t(L) \leqslant 28$. We show that $j = 32$ is suitable in this case. If q is even then $k_{2j}(q) = q^{32} + 1 > q^{280/9}$. If q is odd then $q^{8/9} > 2$, so $k_{2j}(q) > q^{32}/2 > q^{32}/q^{8/9} = q^{280/9}$.

(iii) It follows from [2, Lemma 1.3] that numbers from $\omega(L)$ do not exceed $q^{m+1}/(q-1)$, where m is the Lie rank of L. Now the required assertion can be easily obtained by using the formulae for $t(L)$ from Table 1.

(iv) By [41, Proposition 0.5], the exponent of a Sylow p-subgroup of L is equal to the minimal power of p greater than the maximal height $h(L)$ of a root in the root system of L. Since $h(L) = n-1$ for linear and unitary groups, $h(L) = 2n-3$ for orthogonal groups of even dimension, and $h(L) = 2n-1$ for symplectic groups and orthogonal groups of odd dimension, the required assertion follows.

3. Preliminaries: actions and automorphisms

In this section we collect some facts concerning spectra of covers and automorphic extensions of classical groups. Our main tools are well-known results on Frobenius actions, Hall–Higman type theorems, as well as a description of parabolic subgroups and centralizers of field automorphisms of classical groups.

We start with two known results on covers of finite groups.

Lemma 3.1 ([42, Lemma 10]). *Suppose that K is a normal elementary abelian p-subgroup of a finite group G, $H \simeq G/K$, and $G_1 = K \rtimes H$ is the natural semidirect product under the action of H on K via conjugation. Then $\omega(G_1) \subseteq \omega(G)$.*

Lemma 3.2 ([18, Lemma 1.5]). *Let G be a finite group, K be a normal subgroup of G, and $r \in \pi(K)$. Suppose that the factor group G/K has a section isomorphic to a non-cyclic abelian p-group for some odd prime p distinct from r. Then $rp \in \omega(G)$.*

Now we put a result on a faithful Frobenius action and its corollary for a cover of Frobenius group.

Lemma 3.3. *If a Frobenius group FC with kernel F and cyclic complement $C = \langle c\rangle$ of order n acts faithfully on a vector space V of positive characteristic p coprime to the order of F, then the minimal polynomial of c on V is equal to $x^n - 1$. In particular, the natural semidirect product $V \rtimes C$ contains an element of order pn and $\dim C_V(c) > 0$.*

Proof. See, e.g., [42, Lemma 2].

Lemma 3.4 ([43, Lemma 1]). *Let G be a finite group, K be a normal subgroup of G, and let G/K be a Frobenius group with kernel F and cyclic complement C. If $(|F|, |K|) = 1$ and F does not lie in $KC_G(K)/K$, then $r|C| \in \omega(G)$ for some prime divisor r of $|K|$.*

Next step is to discuss several results based on theorems of Hall–Higman type. Our main source here is Di Martino and Zalesskii's theorem [44] on minimal polynomials of elements of prime-power order lying in proper parabolic subgroups of classical groups. We begin with a direct corollary of this theorem.

Lemma 3.5. *Let L be a simple classical group over a field of order q and characteristic p, $r \in \pi(L)$, $r^s \in \omega(P)$, where P is a proper parabolic subgroup of L, and $(r, 6p(q+1)) = 1$. If L acts faithfully on a vector space V over the field of characteristic t distinct from p, then $tr^s \in \omega(V \rtimes L)$.*

Proof. Let an element $g \in P$ have an order r^s. Since $(r, 6p(q+1)) = 1$, it follows from the main result of [44] that the minimal polynomial of g on V has degree r^s, so the lemma holds.

The proof of Di Martino and Zalesskii's theorem is based on the application of the Hall–Higman theorem and its cross-characteristic analogues to the restriction of faithful representation of a classical group on its parabolic subgroups. Next two lemmas contain very similar arguments, and we include them because their formulations are convenient for our further purposes.

Lemma 3.6. *Let s and p be distinct primes, a group H be a semidirect product of a normal p-subgroup T and a cyclic subgroup $C = \langle g \rangle$ of order s, and let $[T, g] \neq 1$. Suppose that H acts faithfully on a vector space V of positive characteristic t not equal to p. If the minimal polynomial of g on V does not equal $x^s - 1$, then*

(i) $C_T(g) \neq 1$;
(ii) T *is nonabelian*;
(iii) $p = 2$ *and* $s = 2^{2^\delta} + 1$ *is a Fermat prime.*

Proof. If $C_T(g) = 1$, then TC is a Frobenius group and the minimal polynomial of g on V equals $x^s - 1$ by Lemma 3.3. If T is abelian, then $T = [T, g] \times C_T(g)$ and $[T, g]C$ is a Frobenius group acting on V faithfully. Therefore, (ii) also holds. The last assertion follows from the Hall–Higman theorem [45, Theorem 2.1.1] in the case $t = s$, and can be easily derived from [46, Satz 17.13] (see, e.g., [47] and [48]) for $t \neq s$.

Lemma 3.7. *Let L be a simple classical group over a field of order q and characteristic p, and* $\mathrm{prk}(L) > 4$. *Suppose that a prime s divides the order of a proper parabolic subgroup of L, and $(s, p(q^2 - 1)) = 1$. Then L includes a subgroup H such that H is a semidirect product of a normal p-subgroup T and a cyclic subgroup $C = \langle g \rangle$ of order s with $[T, g] \neq 1$, and at least one of three assertions from the conclusion of Lemma* 3.6 *does not hold for H.*

Proof. First of all, observe that $s > 3$ because $(s, p(q^2 - 1)) = 1$. Let g be an element of order s in L. There exists a proper parabolic subgroup P of L admitting the Levi decomposition $A : B$, where A is the unipotent radical, B is the Levi factor, and $g \in B$. By [49, 13.2], we have $g \notin C_L(A)$, so $[A, g] \neq 1$. Suppose that the conclusion of the lemma does not hold. Then $q = 2^\beta$, $s = 2^{2^\delta} + 1$ is a Fermat prime, A is nonabelian, and $C_A(g) \neq 1$. First we assume that s is coprime to the order of a stabilizer of one-dimensional totally isotropic (totally singular) subspace in the natural representation of L. If it occurs, the one of the following holds: $L = U_n(q)$, $e(s, -q)$ is even and $e(s, -q) \geqslant n-1$; $L = S_{2n}(q) = O_{2n+1}(q)$ or $L = O^+_{2n}(q)$ and $e(s, q) = n$ is odd; $L = O^-_{2n}(q)$ and $e(s, q) = n-1$ is odd. However, in all these cases, it follows from [34, Table 4] that s and p are not adjacent in $GK(L)$, and so $C_A(g) = 1$, a contradiction. Thus, we may assume that P is a stabilizer of one-dimensional totally isotropic subspace. Since $p = 2$, the unipotent radical A of P is abelian, unless $L = U_n(q)$ (see, for example, [44, Lemma 3.1]). Therefore, $L = U_n(q)$. Now $s = 2^{2^\delta} + 1$ is a Fermat prime greater than 3, so $e(s, 2) = 2^{\delta+1} \geqslant 4$. Putting $e(s, q) = l$, we have $2^{\delta+1}$ divides βl and does not divide βi for $i < l$. If $l_{\{2\}} \leqslant 2$, then $2^{\delta+1}$ divides 2β, which is impossible because $l > 2$. Hence $e(s, -q) = e(s, q) = l \equiv 0 \,(\mathrm{mod}\, 4)$. Furthermore, as proved, $e(s, -q) < n-1$. By [20, Lemma 5], L has a Frobenius subgroup TC such that its kernel T is a p-subgroup, and a complement C has the order s. This completes the proof.

The subgroup H from the conclusion of Lemma 3.7 is said to be *good in L with respect to a prime s.*

The next lemma gives an easy criterion whether a prime divisor of the order of a classical group divides the order of some its proper parabolic subgroup.

Lemma 3.8. *For a simple classical group L over a field of order q and characteristic p with* $\mathrm{prk}(L) = n \geqslant 4$*, put*

$$j = \begin{cases} n, & \text{if } L \simeq L_n(q); \\ 2n-2, & \text{if either } L \simeq O^+_{2n}(q) \text{ or } L \simeq U_n(q) \text{ and } n \text{ is even,} \\ 2n, & \text{otherwise.} \end{cases}$$

Then $(k_j(q), |P|) = 1$ for every proper parabolic subgroup P of L. If $i \neq j$ and a primitive prime divisor $r_i(q)$ lies in $\pi(L)$, then there is a proper parabolic subgroup P of L such that $k_i(q)$ lies in $\omega(P)$. In particular, if two distinct primes $r, s \in \pi(L)$ do not divide the order of any proper parabolic subgroup of L, then r and s are adjacent in $GK(L)$.

Proof. The order and structure of parabolic subgroups of finite classical groups are well-known (see, for example, [50, Propositions 4.1.17–4.1.20]). So it is easy to verify that $(k_j(q), |P|) = 1$ for every proper parabolic subgroup

P of L. Let $r \in \pi(L)$ and $e(r,q) = i \neq j$. Since $n \geqslant 4$, it is clear that if $i \leqslant 2$ then there is a proper parabolic subgroup P with $k_i(q) \in \omega(P)$. So we may assume that $i > 2$. Applying [50, Propositions 4.1.17–4.1.20] again, we obtain a proper parabolic subgroup P with the Levi factor having a section isomorphic to a simple classical group M over a field of order q (with one exception when M is over a field of order q^2) such that r divides M. If M is over a field of order q, then $k_i(q) \in \omega(M) \subseteq \omega(P)$ by Lemma 2.13. In the exceptional case $L = U_n(q)$, n even, $M \simeq L_{n/2}(q^2)$. Again, using Lemma 2.13, we have $k_{n/2}(q^2) \in \omega(M)$, and $k_n(q) \in \omega(M) \subseteq \omega(P)$ by Lemma 1.2. Finally, if two distinct primes $r, s \in \pi(L)$ do not divide the order of any proper parabolic subgroup of L, then $r, s \in R_j(q)$, so they are adjacent to each other by Lemma 2.4(iv).

In the end of the section we handle the spectra of extensions of classical groups by field automorphisms.

Lemma 3.9. *Let a symbol X be chosen from the set $\{SL_n^\varepsilon, Sp_{2n}, \Omega_{2n+1}, \Omega_{2n}^\varepsilon\}$. Suppose that q is a prime power, and τ is a field automorphism of odd order t of the group $X(q)$. Then*

$$\omega(X(q) \rtimes \langle\tau\rangle) = \bigcup_{k|t} k\omega(X(q^{1/k})). \tag{10}$$

Proof. If $X = SL_n^\varepsilon$, then the assertion is proved in (i) of Corollary 14 in [51]. The proof is based on the general result on connected linear algebraic groups [51, Proposition 13]. So it can be extended to the other cases exactly by the same way as in the proof of Corollary 14 from [51].

Given a finite group G and a prime r, let $\exp_r(G)$ stand for the r-exponent of G, i.e., the exponent of its Sylow r-subgroup.

Lemma 3.10. *Let L be a simple classical group over a field of order q, and $r \in \pi(L)$. Suppose that $(r, q|\operatorname{Inndiag} L/L|) = 1$, and if $L = O_8^\xi(q)$ then $r \neq 3$. If $L \leqslant G \leqslant \operatorname{Aut} L$, then $\exp_r(L) = \exp_r(G)$.*

Proof. It is nothing to prove if $|G/L|_r = 1$. Let $|G/L|_r = r^\kappa > 1$. Since $(r, q|\operatorname{Inndiag} L/L|) = 1$ and $r \neq 3$ for $L = O_8^\xi(q)$, the group G includes a subgroup H isomorphic to the extension of L by the field automorphism τ of order r^κ, and $\exp_r(G) = \exp_r(H)$. Choose the symbol X from the statement of Lemma 3.9 so that L is the nonabelian composition factor of $X(q)$. Then $\exp_r(X(q)) = \exp_r(L)$. Furthermore, τ can be lifted to the field automorphism of $X(q)$, which we denote by the same letter τ. Thus, $\exp_r(X(q)) = \exp_r(L) \leqslant \exp_r(H) \leqslant \exp_r(X(q) \rtimes \langle\tau\rangle)$, and it is sufficient to prove that the r-exponents of $X(q)$ and $X(q) \rtimes \langle\tau\rangle$ are equal.

Put $q_0 = q^{1/r}$. Since $i = e(r, q)$ divides $r - 1$, we have $(r, i) = 1$. It follows from Lemma 1.7(ii) that $i = e(r, q_0)$ and $(q^i - 1)_{\{r\}} = r((q_0)^i - 1)_{\{r\}}$. Applying Lemma 1.7(i), it is easy to see that $\exp_r(X(q)) = (q^{ir^l} - 1)_{\{r\}}$ for some nonnegative integer l. Therefore, $\exp_r(X(q)) = (q^{ir^l} - 1)_{\{r\}} = r^l(q^i - 1)_{\{r\}} = r^{l+1}((q_0)^i - 1)_{\{r\}} = r((q_0)^{ir^l} - 1)_{\{r\}} = r\exp_r(X(q_0))$. The equality $\exp_r(X(q)) = r\exp_r(X(q_0))$ yields the validity of the following chain of equalities:

$$\exp_r(X(q)) = r\exp_r(X(q^{1/r})) = \ldots = r^\kappa \exp_r(X(q^{1/r^\kappa})). \qquad (11)$$

By Lemma 3.9, we have

$$\omega(X(q) \rtimes \langle\tau\rangle) = \bigcup_{0 \leqslant l \leqslant \kappa} r^l \omega(X(q^{1/r^l})). \qquad (12)$$

The lemma follows from (11) and (12).

4. Proof: restrictions on K and $\overline{G}/S$

The following four sections contain the proof of Theorem 3. Throughout L is a simple classical group over a field of order q and characteristic p, and $\mathrm{prk}(L) = n$. We will prove the theorem by contradiction. So we assume that there exists a finite group G isospectral to L with a unique nonabelian composition factor S isomorphic to a simple group of Lie type over a field of order u and characteristic v distinct from p. Further, since the assumptions on $\mathrm{prk}(L)$ in the hypothesis of Proposition 2 are weaker than ones from the hypothesis of Theorem 3, we obtain that S is a classical group and put $\mathrm{prk}(S) = m$. Here and below K is the soluble radical of G, $\overline{G} = G/K$, S is treated as a subgroup of $\overline{G}$, so $S \trianglelefteq \overline{G} \leqslant \operatorname{Aut} S$ and $\overline{G}/S \leqslant \operatorname{Out} S$.

The purpose of this section is to prove the following three propositions under the assumption that the dimension of the natural representation of L, denoted by $\dim L$, is at least 40. Observe that the hypothesis of Theorem 3 yields $\dim L \geqslant 40$, and the later inequality implies the validity of the assumptions on $\mathrm{prk}(L)$ from Proposition 2.

Proposition 3. *Suppose that* $\dim L \geqslant 40$*. Then the soluble radical* K *of* G *is nilpotent. If* $r \in \pi(K) \setminus \{v\}$*, then* $t(r, L) = 2$*, and* $(s, |K| \cdot |\overline{G}/S| \cdot |P|) = 1$ *for every* $s \in \pi(L)$ *nonadjacent to* r *in* $GK(L)$ *and every proper parabolic subgroup* P *of* S*.*

Proposition 4. *Suppose that* $\dim L \geqslant 40$*. If a prime* r *not equal to* p *divides the order of* $\overline{G}/S$*, then either* $\varphi(r, L) \leqslant n/3$*, or* $L = L_n^{\varepsilon}(q)$*,* $n \in [2^{\gamma+3}, 9 \cdot 2^{\gamma})$*, and* $e(r, \varepsilon q) = \varphi(r, L) = 3 \cdot 2^{\gamma}$ *for some integer* $\gamma \geqslant 3$*. In particular,* r *is small with respect to* L*.*

Proposition 5. *Suppose that* $\dim L \geqslant 40$*. If a prime* r *is large with respect to* L*, then* $(r, pv|K| \cdot |\overline{G}/S|) = 1$ *and* $k_{e(r,q)}(q) \in \omega(S)$*. In particular,* $t(S) \geqslant t(L)$*.*

The following six lemmas show that Propositions 3 and 4 hold.

Lemma 4.1. *If* $r \in \pi(L) \setminus \{p\}$ *and* $\varphi(r, L) > n/2$*, then* r *does not divide* $|\overline{G}/S|$*.*

Proof. Assume to the contrary that r divides $|\overline{G}/S|$.

Let L be a linear or unitary group first. Since $\dim L = \mathrm{prk}(L) = n \geqslant 40$ there are integers $\alpha, \beta \geqslant 2$ and $\gamma \geqslant 3$ with $n/2 < 2^{\alpha}, 3 \cdot 2^{\beta}, 5 \cdot 2^{\gamma} \leqslant n$. Set $I = \{2^{\alpha}, 3 \cdot 2^{\beta}, 5 \cdot 2^{\gamma}\}$. Then the numbers $k_i(q)$, where $i \in I$, lie in $\omega(L)$ and, for every prime divisor s of any of these numbers, $\varphi(s, L) > n/2$. By hypothesis $\varphi(r, L) > n/2$, hence Lemma 2.4(iii) implies that r is adjacent to s if and only if $e(r, q) = e(s, q)$. Therefore, there exist at least two numbers a and b from $\{k_i(q) \mid i \in I\}$ such that $rs \notin \omega(L)$ for every prime s dividing ab. If $s \in \pi(a)$, $w \in \pi(b)$, then $\{r, s, w\}$ is a coclique in $GK(L)$, so both a and b lie in $\omega(S)$ by Proposition 1(ii). If at least one prime divisor w of one of these numbers satisfies $\varphi(w, S) \leqslant m/2$, then, for every prime divisor s of the other, we have $\varphi(s, S) > m/2$ by Lemma 2.4(ii). Thus, the set $\{k_i(q) \mid i \in I\}$ contains a number k such that $rs \notin \omega(L)$ and $\varphi(s, S) > m/2$ for every prime s dividing k. Lemma 2.4(iii) implies that $e(s, u)$ is the same for every prime divisor s of k. Therefore, k divides $k_{e(s,u)}(u)$. Since $\varphi(s, S) > m/2$, Lemma 2.12 yields that S has a cyclic Hall subgroup of order $k_{e(s,u)}(u)$. The s-exponent of L equals $k_{\{s\}}$ for every s dividing k, so $(k, k_{e(s,u)}(u)/k) = 1$ and S has a cyclic Hall subgroup H of order k. Let $s \in \pi(k)$. The normalizer $N_{\overline{G}}(P)$ in $\overline{G}$ of a Sylow s-subgroup P of S contains an element x of order r by Frattini argument. Therefore, $H\langle x \rangle$ is a Frobenius group, and so r divides

$|P|-1$. Since the last inference is valid for every prime $s\in\pi(k)$ and H is cyclic of order k, the prime r divides $k-1=k_i(q)-1$ for some $i\in I$. It follows from Lemma 1.4 that $e(r,q)$ divides $c=2^\delta$ with $c\leqslant n/2$. Lemma 2.11 implies that $\varphi(r,L)$ either divides c or equals 2. Both possibilities contradict the hypothesis $\varphi(r,L)>n/2$.

Now let L be a symplectic or orthogonal group. Since $\dim L=2\operatorname{prk}(L)=2n\geqslant 40$, there are integers $\alpha,\beta\geqslant 2$ and $\gamma\geqslant 3$ with $n<2^\alpha,3\cdot 2^\beta,5\cdot 2^\gamma\leqslant 2n$. Put $I=\{2^\alpha,3\cdot 2^\beta,5\cdot 2^\gamma\}$. Exclude the case when $L=O^+_{2n}(q)$ and $2n\in I$ for a while. Then numbers $k_i(q)$, where $i\in I$, lie in $\omega(L)$ and $\varphi(s,L)=i/2>n/2$ for every prime divisor s of any of these numbers. Repeating the arguments of the preceding paragraph word for word, we derive that r divides $k_i(q)-1$ for some $i\in I$. Therefore, $e(r,q)$ divides $c=2^\delta$ with $c\leqslant n$ by Lemma 1.4. Lemma 2.11 yields that $\varphi(r,L)=e(r,q)/2$ divides $c/2$, contrary to $\varphi(r,L)>n/2$. Let, finally, $L=O^+_{2n}(q)$ and $2n\in I$. We consider the set $I'=(I\cup\{n\})\setminus\{2n\}$ instead of I. The numbers $k_i(q)$, where $i\in I'$, lie in $\omega(L)$. By adjacency criterion (see [34] or Table 1), $rs\notin\omega(L)$ for every primes s with $e(s,q)=n$. Therefore, there exist at least two numbers a and b from $\{k_i(q)\mid i\in I'\}$ such that $rs\notin\omega(L)$ for every prime s dividing ab. If $s\in\pi(a)$ and $w\in\pi(b)$, then $\{r,s,w\}$ is the coclique in $GK(L)$ (again see Table 1), so both a and b lie in $\omega(S)$ by Proposition 1(ii). Repeating the preceding arguments once more, we conclude that r divides $k_i(q)-1$ for one of $i\in I'$. Again $e(r,q)$ divides $c=2^\delta$ with $c\leqslant n$, which is impossible because $\varphi(r,L)>n/2$.

Lemma 4.2. *If $r\in\pi(K)\cup\pi(\overline{G}/S)$ and $r\neq v$, then $vr\in\omega(G)$. There exists $s\in\pi(S)\setminus(\pi(K)\cup\pi(\overline{G}/S)\cup\{v\})$ such that $vs\notin\omega(G)$.*

Proof. If $v=2$, then the first assertion of the lemma holds by Proposition 1(iii). Assume that v is odd. It follows from Proposition 1(ii) that the dimension of S is large enough, so $S\not\simeq L_2(v)$ and a Sylow v-subgroup of S includes a noncyclic abelian subgroup. Therefore, by Lemma 3.2, we have $rv\in\omega(G)$ for every $r\in\pi(K)\setminus\{v\}$. Furthermore, it is well-known that the centralizer in S of any outer automorphism of S contains an element of order v. Thus, the first assertion of the lemma is completely proved. On the other hand, Lemma 2.10 yields that there is $s\in\pi(L)\setminus\{v\}$ with $sv\notin\omega(L)$. Now the latter assertion of the lemma follows from the former one.

Lemma 4.3. *If $r,s\in\pi(G)$, r divides $|K|$, s does not lie in $\pi(K)$ and divides the order of some proper parabolic subgroup of S, then $rs\in\omega(G)$.*

Proof. We may assume that $s \neq v$ by Lemma 4.2, and $s \neq 2$ by Proposition 1(iii). Put $C = C_G(K)$ for the centralizer of K in G. If $C \not\subseteq K$, then the preimage of S in G lies in CK, and so the factor group $C/(C \cap K) \simeq CK/K$ has a subgroup isomorphic to S, hence $rs \in \omega(G)$. Therefore, $C \leqslant K$. If S has an elementary abelian subgroup of order s^2, then $rs \in \omega(G)$ by Lemma 3.2, so we may assume that there is no such subgroup in S, in particular, it follows $(s, u^2 - 1) = 1$.

Consider a normal r-series of K:

$$1 = R_0 \leqslant K_1 < R_1 \leqslant K_2 \leqslant \ldots \leqslant R_{t-1} < K_t \leqslant R_t = K,$$

where $K_i/R_{i-1} = O_{r'}(K/R_{i-1})$ and $R_i/K_i = O_r(K/K_i)$.

First we suppose that $R = R_t/K_t \neq 1$. Put $V = R/\Phi(R)$ for the factor group of R by its Frattini subgroup $\Phi(R)$. It follows from Lemma 3.1 that $\omega(V \rtimes S) \subseteq \omega(\overline{G})$, where $V \rtimes S$ is the natural semidirect product under the action of S on V by conjugation. By Lemma 3.7, the group S has a subgroup H which is good in S with respect to s. Since $C \leqslant K$, the action of H on V by conjugation is faithful. Therefore, by Lemma 3.6, there exists an element g of order s in H such that the minimal polynomial of g under this action is equal to $x^s - 1$. Thus, $rs \in \omega(G)$ in this case.

Let $K = R_t = K_t$ and put $\widetilde{K} = K/R_{t-1}$. Assume that v does not divide $|\widetilde{K}|$. Once more we take a subgroup H that is good in S with respect to s. By the Schur–Zassenhaus theorem, the factor group $\widetilde{G} = G/R_{t-1}$ has a subgroup $\widetilde{H}$ isomorphic to H. Put $V = R_{t-1}/\Phi(R_{t-1})$. If $C_{\widetilde{G}}(V)$ does not lie in $\widetilde{K}$, then $C_{\widetilde{G}}(V)\widetilde{K}/\widetilde{K}$ has a subgroup isomorphic to S, hence s divides $C_{\widetilde{G}}(V)$ and $rs \in \omega(G)$. Furthermore, $\widetilde{H} \cap \widetilde{K} = 1$. So $\widetilde{H}$ acts on V faithfully and we derive $rs \in \omega(G)$ by Lemma 3.6.

Finally, suppose that v divides $|\widetilde{K}|$. Let $\widetilde{T}$ be a Sylow v-subgroup of $\widetilde{K}$ and $\widetilde{G} = G/R_{t-1}$. Applying, if necessary, the Frattini argument, we may assume that $\widetilde{T} \trianglelefteq \widetilde{G}$. Let U be a minimal normal in $\widetilde{G}$ subgroup of the center $Z(\widetilde{T})$ of $\widetilde{T}$ and put $V = R_{t-1}/\Phi(R_{t-1})$. If an element g of order s from $\widetilde{G}$ centralizes U, then $C_{\widetilde{G}}(U)\widetilde{K}/\widetilde{K}$ includes a subgroup isomorphic to S, so v is adjacent to every prime divisor of the order of S, which contradicts Lemma 4.2. Thus, $A = [U, g] \neq 1$ and $A\langle g \rangle$ is a Frobenius group with a cyclic complement of order s. Since $C_{\widetilde{G}}(V)$ is normal in $\widetilde{G}$, either $U \leqslant C_{\widetilde{G}}(V)$ or $C_{\widetilde{G}}(V) \cap U = 1$. The former is impossible because $K_{t-1}/R_{t-2} = O_{r'}(K/R_{t-2})$. Therefore, A does not lie in $VC_{\widetilde{K}}(V)$. Lemma 3.3 yields $rs \in \omega(H)$.

Lemma 4.4. *If $r \in \pi(K)\setminus\{v\}$, then $t(r, L) = 2$, and $(s, |K|\cdot|\overline{G}/S|\cdot|P|) = 1$ for every $s \in \pi(L)$ nonadjacent to r in $GK(L)$ and every proper parabolic subgroup P of S.*

Proof. Observe first that $t(r, L) \geqslant 2$ due to Lemma 2.10. Suppose that $t(r, L) > 2$ and ρ is any $\{r\}$-coclique of size at least 3. It follows from Proposition 1(ii) that $(s, |K|\cdot|\overline{G}/S|) = 1$ for every $s \in \rho\setminus\{r\}$. By Lemma 4.3, all such s do not divide the order of any proper parabolic subgroup of S. It contradicts to Lemma 3.8.

Thus, $t(r, L) = 2$. If $r = 2$, then the lemma holds due to Proposition 1(iii) and Lemma 4.3. So we assume that r is odd. Let $\{r, s\}$ be a coclique in $GK(L)$. Using Table 3, we have $n/2 < \varphi(s, L) \leqslant n$. Therefore, s does not divide $|\overline{G}/S|$ by Lemma 4.1. Furthermore, applying Table 1, we obtain a coclique ρ in $GK(L)$ of size 3 with $s \in \rho$. Suppose that s divides $|K|$. Then t does not divide $|\overline{G}/S| \cdot |K|$ for every $t \in \rho \setminus \{s\}$ by Proposition 1(ii). Now Lemma 3.8 yields that there exists a prime t from $\rho \setminus \{s\}$ dividing the order of some proper parabolic subgroup of S. If $t = v$, then $ts \in \omega(G)$ by Lemma 4.2, and if $t \neq v$, then $ts \in \omega(G)$ by Lemma 4.3, a contradiction with the choice of t. Therefore, s does not divide $|\overline{G}/S| \cdot |K|$. Yet another application of Lemma 4.3 completes the proof.

Lemma 4.5. *The soluble radical K is nilpotent.*

Proof. Assume the contrary. Then the Fitting subgroup $F = F(K)$ is a proper subgroup of K. Put $\widetilde{G} = G/F$, $\widetilde{K} = K/F$, and set $\widetilde{H}$ for the preimage of S in $\widetilde{G}$. Let $\widetilde{T}$ be a minimal normal subgroup of $\widetilde{G}$ lying in $\widetilde{K}$, and put T for its preimage in G. The solubility of $\widetilde{K}$ implies that $\widetilde{T}$ is an elementary abelian t-group for a prime t. Let $r \in \pi(F) \setminus \{t\}$, R be the Sylow r-subgroup of F, $C_r = C_G(R)$ be the centralizer of R in G, and $\widetilde{C}_r$ be the image of this centralizer in $\widetilde{G}$. Since $\widetilde{C}_r$ is a normal subgroup of $\widetilde{G}$, the minimality of $\widetilde{T}$ yields that either $\widetilde{C}_r \cap \widetilde{T} = 1$ or $\widetilde{T} \leqslant \widetilde{C}_r$. If $\widetilde{T} \leqslant \widetilde{C}_r$ for every $r \in \pi(F) \setminus \{t\}$, then T is a normal nilpotent subgroup of K, a contradiction. Thus, there is a prime $r \in \pi(F) \setminus \{t\}$ with $\widetilde{C}_r \cap \widetilde{T} = 1$. If $\widetilde{K}$ does not include $\widetilde{C} = C_{\widetilde{G}}(\widetilde{T})$, then $\widetilde{C}\widetilde{K}$ includes $\widetilde{H}$ and t is adjacent to every prime from $\pi(S)$, which is impossible due to Lemma 4.4. So $\widetilde{C} \leqslant \widetilde{K}$. Lemma 4.4 implies that there exists $s \in \pi(S) \setminus \pi(K)$ with $rs \notin \omega(G)$. Consider a cyclic subgroup $\langle x\rangle$ of order s in $\widetilde{H}$. Observe that $t \neq s$ because $t \in \pi(K)$. Therefore, $\widetilde{T} = [\widetilde{T}, x] \times C_{\widetilde{T}}(x)$ and $C_{\widetilde{T}}(x) \neq \widetilde{T}$. Hence $A = [\widetilde{T}, x] : \langle x\rangle$ is a Frobenius group with a cyclic complement of order s. Since $\widetilde{C}_r \cap \widetilde{T} = 1$, the action of A on $R/\Phi(R)$ is faithful. By Lemma 3.3, we obtain $rs \in \omega(G)$ and so derive a contradiction. The lemma and Proposition 3 are proved.

Lemma 4.6. *If a prime r not equal to p divides the order of $\overline{G}/S$, then either $\varphi(r, L) \leqslant n/3$, or $L = L_n^{\varepsilon}(q)$, $n \in [2^{\gamma+3}, 9 \cdot 2^{\gamma})$, and $e(r, \varepsilon q) = \varphi(r, L) = 3 \cdot 2^{\gamma}$ for some integer $\gamma \geqslant 3$. In particular, r is small with respect to L.*

Proof. We start with two simple observations. First, for all primes $s \in \pi(L)$ treated in the further proof, we have $s \neq p$ and $e(s, q) > 2$, so, by Lemma 2.13, two such primes s and w with distinct $e(s, q)$ and $e(w, q)$ are adjacent if and only if $k_{e(s,q)}(q) \cdot k_{e(w,q)}(q) \in \omega(L)$. Due to this fact, $k_i(q)$ and $k_j(q)$ are said to be adjacent (nonadjacent) if their prime divisors are adjacent (nonadjacent). Second, if $\varphi(s, L) > n/2$ for $s \in \pi(L)$, then $k_{e(s,q)}(q)$ is coprime to $|K| \cdot |\overline{G}/S|$ and $k_{e(s,q)}(q) \in \omega(S)$, hence, if $\varphi(w, L) > n/2$ and $e(w, q) \neq e(s, q)$ for $w \in \pi(L)$, then $k_{e(s,q)}(q) \cdot k_{e(w,q)}(q) \in \omega(L)$ if and only if $k_{e(s,q)}(q) \cdot k_{e(w,q)}(q) \in \omega(S)$. Applying Lemmas 2.4(iii), 2.12 and arguing as in the proof of Lemma 4.1, we obtain the following: if $k_i(q)$ and $k_j(q)$ are distinct and nonadjacent in $GK(L)$, then S includes a cyclic Hall subgroup of order $k_i(q)$ or $k_j(q)$.

We will prove the lemma from the contrary. Given r dividing $|\overline{G}/S|$, put $\varphi(r, L) = l$, and observe that we may assume $n/3 < l \leqslant n/2$ due to Lemma 4.1. The proof is similar to the proof of Lemma 4.1 but more labor-consuming. Its idea is as follows. Suppose that we find out an integer i such that S includes a cyclic Hall subgroup of order $k_i(q)$ and r is nonadjacent to any prime divisor of $k_i(q)$ in $GK(L)$. Then $\overline{G}$ contains a Frobenius subgroup with kernel of order $k_i(q)$ and complement of order r (see proof of Lemma 4.1), so r divides $k_i(q) - 1$. If, according to Lemma 1.4, we take i with $\varphi(s, L) \leqslant n/3$ for every prime divisor s of $k_i(q) - 1$, then the desired contradiction is obtained.

Since the case of symplectic and orthogonal groups is slightly easier than the case of linear and unitary groups, let us assume that L is a symplectic or orthogonal group at first.

If $s \in \pi(L)$ is chosen so that $e(s, q)$ is a multiple of 4 and $n/2 < \varphi(s, L) \leqslant n$, then r and s are nonadjacent provided $\varphi(r, L) + \varphi(s, L) > n$. Indeed, the adjacency criterion for symplectic and orthogonal groups [35, Propositions 2.4 and 2.5] implies that the adjacency of r and s with $\varphi(r, L) + \varphi(s, L) > n$ is possible only if $e(s, q)/e(r, q)$ is an odd integer. Therefore, $e(r, q)$ is also a multiple of 4, and $e(r,q) = 2\varphi(r,L) < n$ cannot be equal to $e(s,q) = 2\varphi(s,L) > n$. So $\varphi(s,L)/\varphi(r,L) = e(s,q)/e(r,q) \geqslant 3$, which leads to the impossible chain of the inequalities: $n \geqslant \varphi(s,L) \geqslant 3\varphi(r,L) > 3n/3 = n$.

Since L is symplectic or orthogonal, it follows that $\dim L = 2n \geqslant 40$. So there is an integer $\gamma \geqslant 3$ with $2n \in J = [5\cdot 2^{\gamma}, 5\cdot 2^{\gamma+1})$. We partition J into six intervals $J = J_1 \cup \ldots \cup J_6$, putting $J_1 = [5\cdot 2^{\gamma}, 11\cdot 2^{\gamma-1})$, $J_2 = [11\cdot 2^{\gamma-1}, 3\cdot 2^{\gamma+1})$, $J_3 = [3\cdot 2^{\gamma+1}, 7\cdot 2^{\gamma})$, $J_4 = [7\cdot 2^{\gamma}, 2^{\gamma+3})$, $J_5 = [2^{\gamma+3}, 9\cdot 2^{\gamma})$, and $J_6 = [9\cdot 2^{\gamma}, 5\cdot 2^{\gamma+1})$.

Suppose that $2n \in J_1 \cup J_2$. Let $a = 9\cdot 2^{\gamma-1}$, and let s be an arbitrary prime divisor of $k_a(q)$. The number a is divided by 4 and satisfies the inequalities $4n/3 < a < 2n$. It follows that $2n/3 < \varphi(s,L) = a/2 < n$, so r and s is nonadjacent due to the inequality $a/2+l > 2n/3+n/3 = n$ and the adjacency criterion (see the observation above). The group L has a cyclic subgroup of order $k_a(q)$, and so does S. If such subgroup of S is a Hall subgroup, then r divides $k_a(q)-1$. In this case Lemma 1.4 yields $\varphi(r,L) \leqslant e(r,q) \leqslant a/6 < n/3$, a contradiction. Thus, we assume that S has not a cyclic Hall subgroup of order $k_a(q)$. Let $b = 2^{\gamma+2}$. The number b is also divided by 4 and satisfies $2n/3 < \varphi(s,L) = b/2 < n$ for every prime divisor s of $k_b(q)$. Since $k_a(q)$ are $k_b(q)$ distinct and nonadjacent, S includes a cyclic Hall subgroup of order $k_b(q)$. It follows from $b/2 + l > n$ that r and $k_b(q)$ are nonadjacent. Hence r divides $k_b(q) - 1$. By Lemma 1.4, $e(r,q)$ divides $2^{\gamma+1}$. If $e(r,q) \neq 2^{\gamma+1}$, then $l = e(r,q)/2 \leqslant 2^{\gamma-1} = 3\cdot 2^{\gamma-1}/3 < n/3$, contrary to our assumption. Therefore, $e(r,q) = 2^{\gamma+1}$.

If $2n \in J_1$ then put $c = 7\cdot 2^{\gamma-1}$. Given $s \in R_c(q)$, we have $\varphi(s,L) = c/2$. Due to the inequalities $n < c < 2n$ and $c/2 + l = 7\cdot 2^{\gamma-2} + 2^{\gamma} = 11\cdot 2^{\gamma-2} > n$ the group S has a cyclic Hall subgroup of order $k_c(q)$ and r is nonadjacent to every prime divisor of $k_c(q)$. Lemma 1.4 implies that $e(r,q) = 2^{\gamma+1}$ divides $3\cdot 2^{\gamma-1}$, a contradiction.

If $2n \in J_2$, set $c = 11\cdot 2^{\gamma-1}$. Then $n < c \leqslant 2n$. If $c = 2n$, let $L \neq O^{+}_{2n}(q)$ at first. Then we may suppose that S has a cyclic Hall subgroup of order $k_c(q)$. It follows from $c/2 + l = 11\cdot 2^{\gamma-2} + 2^{\gamma} = 15\cdot 2^{\gamma-2} > n$ that r is not adjacent to $k_c(q)$, hence r divides $k_c(q) - 1$. By Lemma 1.4, $e(r,q) = 2^{\gamma+1}$ divides $5\cdot 2^{\gamma-1}$, a contradiction. If $c = 2n$ and $L = O^{+}_{2n}(q)$, then L does not contain an element of order $k_c(q)$, which forces us to complicate a little our arguments. Consider the interval $I = (2l+1, n) = (2^{\gamma+1}+1, 11\cdot 2^{\gamma-2})$ and show that it always contains a prime, which we denote by w. If $\gamma = 3$ then $w = 19 \in I$. If $\gamma \geqslant 4$, then $n > 30$ and I contains a prime w due to the inequality $2l+1 < 5n/6$ and Lemma 1.9. Since $(q-1, q+1) \leqslant 2$ and w is odd, there is $\varepsilon \in \{+,-\}$ such that $(w, \varepsilon q-1)=1$. By our assumption, a cyclic subgroup of order $k_a(q)$ is not a Hall subgroup of S. It follows that a subgroup H of order $k_w(\varepsilon q)$ must be a Hall subgroup of S. Hence r divides $k_w(\varepsilon q)-1=\varepsilon q((\varepsilon q)^{w-1}-1)/(\varepsilon q-1)$, so $e(r,\varepsilon q)=e(r,q)=2l$ divides $w-1$, which is impossible because $e(r,q)=2^{\gamma+1}<w-1<11\cdot 2^{\gamma-2}<2e(r,q)$. Thus, the lemma holds in the case $2n\in J_1\cup J_2$.

Suppose that $2n\in J_3\cup J_4\cup J_5$. Put $a=9\cdot 2^{\gamma-1}$ if $2n=3\cdot 2^{\gamma+1}$, and put $a=3\cdot 2^{\gamma+1}$ otherwise. As in the previous case, a is a multiple of 4, $4n/3<a<2n$, and r cannot divide $k_a(q)-1$ by Lemma 1.4. There exists a cyclic subgroup of order $k_a(q)$ in S. If it is a Hall subgroup, then we derive a contradiction immediately.

If $2n\in J_3$, set $b=5\cdot 2^{\gamma}$. Then $2n/3<b/2<n$, so S includes a cyclic Hall subgroup of order $k_b(q)$. It follows from $b/2+l>n$ that r is not adjacent to $k_b(q)$, so r divides $k_b(q)-1$. By Lemma 1.4, $e(r,q)$ divides $2^{\gamma+1}$, and the condition $e(r,q)/2=l>n/3$ yields $e(r,q)=2^{\gamma+1}$. Let $c=11\cdot 2^{\gamma-1}$. Following the same way, we obtain that r divides $k_c(q)-1$. Applying Lemma 1.4, we conclude that $e(r,q)=2^{\gamma+1}$ must divide $5\cdot 2^{\gamma-1}$, which is impossible.

If $2n\in J_4$, put $b=7\cdot 2^{\gamma}$ and $c=11\cdot 2^{\gamma-1}$. Then S has cyclic Hall subgroups of orders $k_b(q)$ (except the case: $2n=b$ and $L=O_{2n}^{+}(q)$, treated separately) and $k_c(q)$. It follows from $b/2+l>n$ that r divides $k_b(q)-1$, so $e(r,q)=3\cdot 2^{\gamma}$. Then $c/2+l=11\cdot 2^{\gamma-2}+3\cdot 2^{\gamma-1}>2^{\gamma+2}>n$, hence $e(r,q)$ divides $5\cdot 2^{\gamma-1}$, a contradiction. Let $b=2n$ and $L=O_b^{+}(q)$. The existence of a cyclic Hall subgroup of order $k_c(q)$ in S yields $e(r,q)=2l=5\cdot 2^{\gamma-1}$. There is a prime w in $I=(2l+1,n)=(5\cdot 2^{\gamma-1}+1, 7\cdot 2^{\gamma})$. Indeed, one can put $w=23$ for $\gamma=3$, and apply Lemma 1.9 for $\gamma\geqslant 4$. Now we choose $\varepsilon\in\{+,-\}$ so that $(w,\varepsilon q-1)=1$. The group S has a cyclic Hall subgroup of order $k_w(\varepsilon q)$, so r divides $k_w(\varepsilon q)-1$. Therefore, $e(r,q)$ divides $w-1$, which is impossible because $e(r,q)<w-1<2e(r,q)$.

If $2n\in J_5$, put $b=2^{\gamma+3}$ and $c=7\cdot 2^{\gamma}$. If $L\neq O_b^{+}(q)$, then there are cyclic Hall subgroups of S having orders $k_b(q)$ and $k_c(q)$. Then r divides $k_b(q)-1$, so $e(r,q)=2^{\gamma+2}$, and r and $k_c(q)$ are nonadjacent due to $c/2+l>n$. However, $2^{\gamma+2}$ does not divide $3\cdot 2^{\gamma}$, a contradiction. Let $L=O_b^{+}(q)$. The existence of a cyclic Hall subgroup of order $k_c(q)$ provides $e(r,q)=2l=3\cdot 2^{\gamma}$. Since $n=b/2=2^{\gamma+2}>30$, there is a prime w in $I=(2l+1,n)$ by Lemma 1.9. Arguing as in the previous case, we obtain that $e(r,q)$ divides $w-1$ and so derive a contradiction.

Suppose, finally, that $2n\in J_6$. Put $a=3\cdot 2^{\gamma+1}$ for $2n=9\cdot 2^{\gamma}$, and $a=9\cdot 2^{\gamma}$

otherwise. By the choice of a, we must assume that a cyclic subgroup of order $k_a(q)$ in S is not a Hall subgroup in order to avoid the immediate contradiction (similarly to the previous cases). Putting $b = 2^{\gamma+3}$, we obtain that S has a cyclic Hall subgroup of order $k_b(q)$, and derive $e(r,q) = 2^{\gamma+2}$. Handling a cyclic Hall subgroup of order $k_c(q)$, where $c = 7 \cdot 2^{\gamma}$, and the inequality $c/2 + l = 11 \cdot 2^{\gamma} > n$, we conclude that $e(r,q)$ divides $3 \cdot 2^{\gamma}$, a contradiction. Thus, the lemma is proved for symplectic and orthogonal groups.

Let $L = L_n^{\varepsilon}(q)$. It follows that $l = \varphi(r,L) = e(r,\varepsilon q)$. If $s \in \pi(L)$ is chosen so that $e(s,q)$ is a multiple of 4, then $e(s,q) = e(s,-q) = \varphi(s,L)$. Unfortunately, unlike the case of symplectic and orthogonal groups, the inequalities $n/2 < \varphi(s,L) \leqslant n$ and $l + \varphi(s,L) > n$ do not guarantee that r and s are nonadjacent, because $\varphi(s,L)/l$ can be an integer greater than 1 (see [18, Lemma 2.1]).

By the hypothesis $\dim L = n \geqslant 40$, so there is an integer $\gamma \geqslant 3$ with $n \in J = [5 \cdot 2^{\gamma}, 5 \cdot 2^{\gamma+1})$. We consider the same partition $J = J_1 \cup \ldots \cup J_6$ as in the case of symplectic and orthogonal groups.

Suppose that $n \in J_1 \cup J_2$. Let $a = 9 \cdot 2^{\gamma-1}$ and $b = 2^{\gamma+2}$. The numbers a and b are divided by 4, and the inequalities $2n/3 < b < a < n$ hold. Therefore, due to the adjacency criterion [18, Lemma 2.1], r is adjacent to $k_a(q)$ ($k_b(q)$ respectively) if and only if l divides a (l divides b). Assume that l does not divide a. The group S has a cyclic subgroup H of order $k_a(q)$. If H is a Hall subgroup, then r divides $k_a(q) - 1$, so $e(r,q)$ divides $3 \cdot 2^{\gamma-2}$ by Lemma 1.4. Then $l \leqslant 3 \cdot 2^{\gamma-2} < n/3$, a contradiction. If H is not a Hall subgroup, then a cyclic subgroup of order $k_b(q)$ in S must be Hall due to the nonadjacency of $k_a(q)$ and $k_b(q)$. If r is adjacent to $k_b(q)$ then l divides b. The inequalities $l > n/3$ and $b < n$ yield $l = b/2 = 2^{\gamma+1}$. Then l is a multiple of 4, and so $e(r,q) = l = 2^{\gamma+1}$. If r is nonadjacent to $k_b(q)$, then r divides $k_b(q) - 1$, and Lemma 1.4 implies that $e(r,q)$ divides $2^{\gamma+1}$. It follows from the inequality $l > n/3$ that $e(r,q) = 2^{\gamma+1}$. Assume, finally, that l divides a, then $l = 9 \cdot 2^{\gamma-2}$ because $n/3 < l \leqslant n/2$. Thus, the following alternative holds: either $l = e(r,q) = 2^{\gamma+1}$ or $l = 9 \cdot 2^{\gamma-2}$. Furthermore, subgroups of orders $k_a(q)$ and $k_b(q)$ in S cannot be Hall simultaneously, otherwise $2^{\gamma+1} = l = 9 \cdot 2^{\gamma-2}$.

If $n \in J_1$, put $c = 7 \cdot 2^{\gamma-1}$. For both of alternative values, l does not divide c and $c + l > n$. Indeed, $7 \cdot 2^{\gamma-1} + 9 \cdot 2^{\gamma-2} > 7 \cdot 2^{\gamma-1} + 2^{\gamma+1} = 11 \cdot 2^{\gamma-1} > n$. Therefore, r is nonadjacent to $k_c(q)$. Furthermore, S includes a cyclic Hall subgroup of order $k_c(q)$, hence r divides $k_c(q) - 1$. It follows that $e(r,q)$

divides $3 \cdot 2^{\gamma-1}$, which is impossible.

If $n \in J_2$, put $c = 11 \cdot 2^{\gamma-1}$. Since l does not divide c and the inequalities $11 \cdot 2^{\gamma-1} + 9 \cdot 2^{\gamma-2} > 11 \cdot 2^{\gamma-1} + 2^{\gamma+1} = 15 \cdot 2^{\gamma-1} > n$ hold, r is nonadjacent to $k_c(q)$. Therefore, r divides $k_c(q) - 1$. Due to Lemma 1.4, $e(r, q)$ must divide $5 \cdot 2^{\gamma-1}$, a contradiction. This completes the proof for $n \in J_1 \cup J_2$.

Let $n \in J_3 \cup J_4 \cup J_5$. Put $a = 3 \cdot 2^{\gamma+1}$ and observe that $2n/3 < a \leqslant n$. If r divides $k_a(q) - 1$, then $e(r, q)$ divides $2^{\gamma+1} \leqslant n/3$ by Lemma 1.4. Therefore, similarly to the previous case, we can avoid the immediate contradiction just in two cases: either a cyclic subgroup H of order $k_a(q)$ is not a Hall subgroup of S or $l = e(r, q) = 3 \cdot 2^{\gamma}$.

Let $n \in J_3$ and $b = 5 \cdot 2^{\gamma}$. If H is not a Hall subgroup, then a cyclic subgroup of order $k_b(q)$ must be a Hall subgroup of S. Therefore, either l divides b and so $l = b/2 = 5 \cdot 2^{\gamma-1}$ or l divides $k_b(q) - 1$ and so $l = e(r, q) = 2^{\gamma+1}$. Thus, one of two subgroups of orders $k_a(q)$ and $k_b(q)$ is not a Hall subgroup of S, and l possesses one of the following values: $3 \cdot 2^{\gamma}, 5 \cdot 2^{\gamma-1}, 2^{\gamma+1}$. If $l \neq 5 \cdot 2^{\gamma-1}$, put $c = 11 \cdot 2^{\gamma-1}$. It follows from $11 \cdot 2^{\gamma-1} + 3 \cdot 2^{\gamma} > 11 \cdot 2^{\gamma-1} + 2^{\gamma+1} = 14 \cdot 2^{\gamma-1} > n$ that r is nonadjacent to $k_c(q)$, so r divides $k_c(q) - 1$. Then $l = e(r, q)$ divides $5 \cdot 2^{\gamma-1}$, contrary to our assumptions. If $l = 5 \cdot 2^{\gamma-1}$, put $c = 9 \cdot 2^{\gamma-1}$. Then $c + l > n$. Hence r divides $k_c(q) - 1$ and l divides $3 \cdot 2^{\gamma-2}$, which is impossible.

Let $n \in J_4$ and $b = 11 \cdot 2^{\gamma-1}$. If H is not a Hall subgroup, then a cyclic subgroup of order $k_b(q)$ is a Hall subgroup of S and, arguing as in the previous paragraph, we obtain that either l divides b and $l = 11 \cdot 2^{\gamma-2}$, or r divides $k_b(q) - 1$ and $l = e(r, q) = 5 \cdot 2^{\gamma-1}$. Thus, at least one of cyclic subgroups of orders $k_a(q)$ and $k_b(q)$ is not Hall in S, and $l \in \{3 \cdot 2^{\gamma}, 5 \cdot 2^{\gamma-1}, 11^{\gamma-2}\}$. If $l = 3 \cdot 2^{\gamma}$, put $c = 5 \cdot 2^{\gamma}$, otherwise put $c = 7 \cdot 2^{\gamma}$. The verification analogous to the one in the previous paragraph leads to a contradiction for every possible value of l.

Let $n \in J_5$ and $b = 2^{\gamma+3}$. If H is not a Hall subgroup, then either l divides b or r divides $k_b(q) - 1$. In both cases, $l = e(r, q) = 2^{\gamma+2}$. Thus, one of two subgroups of orders $k_a(q)$ and $k_b(q)$ is not a Hall subgroup of S, and $l \in \{3 \cdot 2^{\gamma}, 2^{\gamma+2}\}$. If $l = 2^{\gamma+2}$, then r is nonadjacent to $k_c(q)$, where $c = 7 \cdot 2^{\gamma}$. So r divides $k_c(q) - 1$, together with Lemma 1.4 this leads to a contradiction due to l does not divide $3 \cdot 2^{\gamma}$. Therefore, for $n \in J_5$ the number $l = e(r, q)$ must be equal to $3 \cdot 2^{\gamma}$. In this case $l < n/2 - 1$, so Lemma 2.7(ii) yields the conclusion of the lemma for $n \in J_5$.

Let $n \in J_6$, $a = 9 \cdot 2^{\gamma}$, $b = 2^{\gamma+3}$, and $c = 7 \cdot 2^{\gamma}$. By the choice of a, if a cyclic subgroup of order $k_a(q)$ is a Hall subgroup of S, then $l = 9 \cdot 2^{\gamma-1}$.

Similarly, if a cyclic subgroup of order $k_b(q)$ is a Hall subgroup of S, then $l = 2^{\gamma+2}$. Since l cannot be equal to $9 \cdot 2^{\gamma-1}$ and $2^{\gamma+2}$ simultaneously, one of these subgroups is not Hall. Therefore, S has a cyclic Hall subgroup of order $k_c(q)$. It follows from $9 \cdot 2^{\gamma-1} + 7 \cdot 2^{\gamma} > 2^{\gamma+2} = 11 \cdot 2^{\gamma} > n$ that r is nonadjacent to $k_c(q)$. Then l divides $3 \cdot 2^{\gamma}$ by Lemma 1.4, a contradiction. The lemma and Proposition 4 are proved.

It remains to prove Proposition 5.

Since $\dim L \geqslant 40$, it follows from Table 1 that $t(L) \geqslant 15$. Suppose that r is large with respect to L. By Table 2, we have $t(p, L) \leqslant 4$ and $t(v, S) \leqslant 4$. Lemma 4.2 yields that $t(v, L) = t(v, G) \leqslant t(v, S) \leqslant 4$. Hence $p \neq r \neq v$. Propositions 3 and 4 provide $(r, |K| \cdot |\overline{G}/S|) = 1$. Applying Table 3 and [34, Table 6], we obtain that $r \notin \delta(L)$. Therefore, by Lemma 2.2, every prime $w \in R_{e(r,q)}(q)$ is large with respect to L, so $(k_{e(r,q)}(q), |K| \cdot |\overline{G}/S|) = 1$. On the other hand, $k_{e(r,q)}(q) \in \omega(L) = \omega(G)$. Hence $k_{e(r,q)}(q) \in \omega(S)$. Finally, if ρ is a coclique of size $t(L)$ in $GK(L)$, then every $r \in \rho$ is large with respect to L. It follows that $\rho \subseteq \pi(S)$. If ρ is not a coclique in $GK(S)$, then it is not a coclique in $GK(G) = GK(L)$, which is impossible. Thus, $t(S) \geqslant t(L)$. Proposition 5 is proved.

5. Proof: characteristic 2

Here we prove Theorem 3 provided the characteristic p of L equals 2. Since we apply Proposition 5, we preserve the condition on the dimension of L from the previous section.

Proposition 6. *Suppose that* $\dim L \geqslant 40$ *and* $p = 2$. *Then* S *cannot be a group of Lie type over the field of odd characteristic.*

Proof. Given a finite group H, consider cocliques ρ of $GK(H)$ such that $4r \notin \omega(H)$ for every $r \in \rho$. Choose among them a coclique of greatest size and denote it by $\rho^*(4, H)$. Put $t^*(4, H) = |\rho^*(4, H)|$.

Lemma 5.1. *Every prime lying in* $\rho^*(4, L)$ *is large with respect to* L, *and* $t^*(4, L) \geqslant 3$.

Proof. Apply [39, 40].

Lemma 5.2. $t^*(4, S) \leqslant 2$.

Proof. Again apply [39, 40], keeping in mind that $u^2 \equiv 1 \pmod 8$ for odd u.

We are ready to complete the proof of Proposition 6. Consider a coclique $\rho = \rho^*(4, L)$. By Lemma 5.1, all primes from ρ are large with respect to L. Therefore, $\rho \subseteq \pi(S)$ due to Proposition 5. It follows from Lemmas 5.1 and 5.2 that $t^*(4, L) > 2 \geqslant t^*(4, S)$. Thus, for at least one $r \in \rho$, we have $4r \in \omega(S) \subseteq \omega(G) = \omega(L)$, a contradiction.

Remark 3. If $L = L_n^\varepsilon(q)$ and q is even, then the conclusion of Theorem 3 has already been obtained under much more weaker hypothesis (see [52, 53] for linear and [54, 55] for unitary groups). Moreover, if L is a finite simple linear or unitary group over a field of even order, $L \notin \{U_4(2), U_5(2)\}$, and G is a finite group with $\omega(G) = \omega(L)$, then $L \leqslant G \leqslant \operatorname{Aut} L$, and all such groups G are determined for every given L.

6. Proof: independence and p-independence numbers of S

Here we prove that $t(L) = t(S)$ provided $t(L) \geqslant 23$. Using this equality, we eliminate the exceptional case of Proposition 4, i.e., we establish that every prime divisor r of the order of L with $\varphi(r, L) > n/3$ does not divide $|K| \cdot |\overline{G}/S|$. In conclusion, we show that under some additional assumptions the p-independence numbers of L and S coincide as well.

Proposition 7. *Suppose that $t(L) \geqslant 23$ and for some positive integer a the number $k_a(u)$ has a prime divisor large with respect to S. Then $k_a(u)$ has a prime divisor large with respect to L. In particular, $t(L) = t(S)$ and every prime r large with respect to L is large with respect to S.*

Proof. Suppose to the contrary that none of prime divisors of $k_a(u)$ is large with respect to L.

Lemma 6.1. *There exists a set J of positive integers of size $d = \max\{1, t(S) - t(L)\}$, satisfying the following:*

(i) *for any $j \in J$, every $r \in R_j(u)$ is large with respect to S and divides the number $|\overline{G}/S| \cdot |K|$;*

(ii) *if $t(S) > t(L)$ and every coclique ρ of the greatest size in $GK(L)$ contains a prime s with $\varphi(s, S) \leqslant m/2$, then $\varphi(r, S) > m/2$ for any $j \in J$ and every $r \in R_j(u)$.*

Proof. First we prove that there is a set J satisfying (i). Put $t = t(S)$ and $t(L) = l$. There exists a set I of positive integers of size t containing a such that for any $i \in I$ every prime from $R_i(u)$ is large with respect to S. Assume that there are $l+1$ numbers $i \in I$ such that $\widetilde{R}_i(u) = R_i(u)\setminus(\pi(K)\cup\pi(\overline{G}/S)) \neq \varnothing$ and put ρ for a set consisting of $l+1$ primes from different $\widetilde{R}_i(u)$. Then ρ is a coclique in $GK(L)$ of size $l+1$, a contradiction. Thus, if $t > l$, then there is a subset J of I with $|J| = t - l \geqslant 1$ and such that for any $j \in J$ every prime from $R_j(u)$ divides $|K| \cdot |\overline{G}/S|$. Let $t = l$ (one may observe that $t(L)$ does not exceed $t(S)$ due to Proposition 5). If for every $i \in I$ we have $\widetilde{R}_i(u) = R_i(u) \setminus (\pi(K) \cup \pi(\overline{G}/S)) \neq \varnothing$, then a set ρ consisting of l primes from different $\widetilde{R}_i(u)$ forms a coclique of greatest size in $GK(L)$. Therefore all primes from ρ are large with respect to L. On the other hand, ρ contains a prime from $R_a(u)$, which is impossible due to our assumption on primes dividing $k_a(u)$.

Now we show that a set J can be chosen to satisfy (ii) as well. It follows from Lemma 2.4(ii) that the set I includes a subset I' of size at least $t-1$ such that for any $i \in I'$ and every prime $w \in R_i(u)$ the inequality $\varphi(w, S) > m/2$ holds. If $|I'| = |I| = t$, then $J \subseteq I = I'$, as required. So we may assume that $|I'| = t - 1$. Suppose that there are l numbers from I' with $\widetilde{R}_i(u) = R_i(u) \setminus (\pi(K) \cup \pi(\overline{G}/S)) \neq \varnothing$. Then a set ρ consisting of l primes from different $\widetilde{R}_i(u)$ forms a coclique in $GK(L)$. However, if the conditions of (ii) hold, then there are at most $l-1$ such numbers in I'. Thus, there exists a subset J of I' such that $|J| = t-1-(l-1) = t-l \geqslant 1$, and for any $j \in J$ every prime r from $R_j(u)$ is large with respect to S, divides $|\overline{G}/S|\cdot|K|$, and satisfies $\varphi(r, S) > m/2$. The lemma is proved.

Lemma 6.2. *Let a set J be as in Lemma 6.1. For each $j \in J$ and every $r \in R_j(u)$ there is a large with respect to L prime s with $rs \in \omega(L) \setminus \omega(S)$.*

Proof. Fix $j \in J$ and $r \in R_j(u)$. Let $\rho = \{s_1, \dots, s_l\}$ be a coclique of greatest size in $GK(L)$. By Proposition 5, every prime from ρ does not divide $|\overline{G}/S|\cdot|K|$, and is not equal to v. It follows that the set $I = E(\rho, S) = \{e(s, u) \mid s \in \rho\}$ is well defined (see Section 2), has the size l, and $j = e(r, u) \notin I$. Choose a coclique σ of size t in $GK(S)$ containing r and put $Y = \{e(w, u) \mid w \in \sigma\}$.

If $t = l$, then ρ is also a coclique of greatest size in $GK(S)$. Lemma 2.5 yields $I \cap Y = Y \setminus \{j\}$. Therefore, ρ includes a subset ρ' of size $l-1$ such that the set $\{r\} \cup \rho'$ is a coclique in $GK(S)$. Since the size of this set equals

l and r is small with respect to L, this set cannot be a coclique in $GK(L)$. Hence there is $s \in \rho$ with $rs \in \omega(L) \setminus \omega(S)$. Thus we may assume that $t > l$.

Suppose that $\varphi(r, S) > m/2$. By Lemma 2.4(ii), the set ρ contains a subset ρ' of size $l - 1$ with $\varphi(s, S) > m/2$ for any $s \in \rho'$. Since $j \notin I$, Lemma 2.4(iii) implies that $\{r\} \cup \rho'$ is a coclique in $GK(S)$, and is not in $GK(L)$. Hence the assertion of the lemma again holds.

Let, finally, $\varphi(r, S) \leqslant m/2$. According to Lemma 6.1(ii), a set ρ can be chosen in a way that $\varphi(s, S) > m/2$ for any $s \in \rho$. Then, by Lemma 2.7(iv), there is a coclique σ' of greatest size in $GK(S)$ with $\rho \subseteq \sigma'$. Set $X = \{e(w, u) \mid w \in \sigma'\}$. Applying Lemma 2.5, we obtain that $Y \cap X \supseteq Y \setminus \{j\}$. Therefore, ρ includes a subset ρ' of size $l - 1$ such that $\{r\} \cup \rho'$ is a coclique in $GK(S)$, and is not in $GK(L)$. The lemma is proved.

Lemma 6.3. *Let a prime r be large with respect to S. If S is linear or unitary, then $\varphi(r, S) \geqslant t(L) \geqslant n/2$ and $r \geqslant n/2 + 1$. If S is symplectic or orthogonal, then $\varphi(r, S) \geqslant (2t(L) - 4)/3 \geqslant (n - 4)/3$ and $r \geqslant (2n - 5)/3 > n/2$.*

Proof. By Lemma 2.7(iii), we have $\varphi(r, S) \geqslant t(S) \geqslant t(L) \geqslant n/2$, if S is linear or unitary, and $\varphi(r, S) \geqslant (2t(S) - 4)/3 \geqslant (2t(L) - 4)/3 \geqslant (n - 4)/3$, if S is symplectic or orthogonal. Lemma 2.3 yields $r \geqslant \varphi(r, S) + 1 \geqslant n/2 + 1$ in the first case, and $r \geqslant 2\varphi(r, S) + 1 \geqslant (2n - 5)/3$ in the second one.

Lemma 6.4. *Let a set J be as in Lemma 6.1. Then for each $j \in J$ and every prime r from $R_j(u)$ the number $(k_j(u))_{\{r\}}$ divides $p(q^2 - 1) \log_v u$. Moreover, the inequality*

$$\frac{\prod_{j \in J} k_j(u)}{\log_v u} \leqslant p(q^2 - 1)$$

holds true.

Proof. Let us fix $j \in J$ and a prime $r \in R_j(u)$. Put $(k_j(u))_{\{r\}} = r^\gamma$. Taking into account that r is large with respect to S and applying Lemma 1.7, one can observe that $r > 3$, $r \neq v$, and r^γ is the r-exponent of S.

Suppose that r divides $|K|$. Since $r \neq v$, Proposition 3 provides a prime $s \in \pi(S)$ nonadjacent to r in $GK(L)$ and coprime to the order of any parabolic subgroup of S. It follows from Lemma 3.8 that r divides the order of some parabolic subgroup P of S and, by the same lemma, $r^\gamma \in \omega(P)$. If R is the Sylow r-subgroup of K (recall that K is nilpotent by Proposition 3), then

S acts on $R/\Phi(R)$ by conjugation. This action must be faithful because r and s are nonadjacent. Furthermore, since r is large with respect to S, we have $(r, 6u(u^2-1)) = 1$. Applying Lemma 3.5, we obtain $r^{\gamma+1} \in \omega(G) = \omega(L)$. On the other hand, Proposition 3 yields that $t(r, L) = 2$, and so r either equals to p or divides q^2-1 by Lemmas 2.6 and 2.9.

Lemma 6.3 provides the inequality $r > n/2$. Suppose $r = p$. Since $n^2/4 > 2n-1$ whenever $n \geqslant 8$, we have $p^2 > 2n-1$. It follows from Lemma 2.14(iv) that the p-exponent of L does not exceed p^2. Then $p^2 \geqslant p^{\gamma+1}$, whence $k_j(u)_{\{p\}} \leqslant p$. Suppose that r divides (q^2-1) and put $(q^2-1)_{\{r\}} = r^\delta$. Using the inequality $r > n/2$ and Lemma 1.7, we obtain that the r-exponent of L does not exceed $r^{\delta+1}$. Therefore, $r^{\delta+1} \geqslant r^{\gamma+1}$. Thus, for any $j \in J$ and every $r \in R_j(u) \cap \pi(K)$ the number $(k_j(u))_{\{r\}}$ divides $p(q^2-1)$.

Suppose now that r does not divide $|K|$. Then $|\overline{G}/S|_{\{r\}} = r^\kappa > 1$. Therefore, $\overline{G}$ includes a subgroup isomorphic to an extension of S by an automorphism τ of order r^κ, where $\kappa \geqslant 1$. Since r is odd and coprime to $|\operatorname{Inndiag}(S)/S|$, we may assume that τ is a field automorphism. If $u = v^\beta$ and $\beta = r^\nu \cdot l$, where $(r, l) = 1$, then $\nu \geqslant \kappa \geqslant 1$. If r does not divide $v^{lj}-1$, then r does not divide $v^{r^\nu \cdot lj} - 1 = u^j - 1$, which is false. So $r^\gamma = (k_j(u))_{\{r\}} = (u^j-1)_{\{r\}} = (v^{r^\nu \cdot lj}-1)_{\{r\}} = r^\nu (v^{lj}-1)_{\{r\}} > r^\kappa$ by Lemma 1.7. Further, r^γ is the greatest power of r lying in $\omega(S)$. Lemma 3.10 yields that r^γ is the r-exponent of $\overline{G}$, so it is the r-exponent of G. If $r \neq p$ and $k = e(r, q) \geqslant 3$, then the inequality $r > n/2$ implies that $(q^k-1)_{\{r\}}$ is the r-exponent of L. By Lemma 6.2, there is a large with respect to L prime s with $rs \in \omega(L) \setminus \omega(S)$. It follows from Lemma 2.13 that $r^\gamma s \in \omega(L)$ as well. Since $(rs, |K|) = 1$, the group $\overline{G}$ contains an element x of order $r^\gamma s$. Then the element $y = x^{r^\kappa}$ is of order $r^{\gamma-\kappa} s$ and belongs to S, which is impossible because $\gamma > \kappa$. Thus, r divides $p(q^2-1)$.

If r divides q^2-1, then again the inequality $r > n/2$ and Lemma 1.7 implies $r^\gamma \leqslant r(q^2-1)_{\{r\}}$. Suppose $r = p$. Then the p-exponent of L does not exceed p^2 because $p > n/2$. Since the product of distinct primes from $R_j(u)$, dividing $|\overline{G}/S|$, divides the number $\log_v u$, we obtain that $k_j(u)$ divides $p(q^2-1)\log_v u$. Finally, since for all $j \in J$ numbers $k_j(u)$ are pairwise coprime, the product $\prod_{j \in J} k_j(u)$ divides $p(q^2-1)\log_v u$.

Lemma 6.5. *Let d be a size of the set J from Lemma* 6.1*. Then*

$$p(q^2-1) > q^{\frac{10t(L)d}{3t(S)}}. \tag{13}$$

Proof. Fix $j \in J$ and let r be a prime from $R_j(u)$. If $S = L_m^{\varepsilon}(u)$, then $k_j(u) = k_{\varphi(r,S)}(\varepsilon u)$ and, by Lemma 6.3, the inequality $\varphi(r, S) \geqslant t(L) \geqslant 23$ holds. If S is symplectic or orthogonal, then $\varphi(r, S) = \eta(j)$ and $\eta(j) \geqslant (2t(L) - 4)/3 \geqslant 13$ by Lemma 6.3. Anyway, Lemma 1.6 yields that

$$k_j(u) > u^6 \log_v u.$$

This equation and Lemma 6.4 imply

$$p(q^2 - 1) > u^{6d}. \tag{14}$$

By Lemma 2.14(i)–(ii), the spectrum of L contains a number b such that $b \geqslant q^{10t(L)/9}$ and all its prime divisors are large with respect to L. It follows from Proposition 5 that $b \in \omega(S)$, so $b \leqslant u^{2t(S)}$ by Lemma 2.14(iii). Thus,

$$u^{2t(S)} \geqslant q^{10t(L)/9}. \tag{15}$$

Finally, (14) and (15) yield the inequality (13). The lemma is proved.

Now we show that the right side of (13) is greater than q^3, which leads us to a contradiction with the conclusion of Lemma 6.5. Recall that $t(L) = l$ and $t(S) = t$.

Assume that $l/t > 9/10$. Then

$$\frac{10ld}{3t} \geqslant \frac{10l}{3t} > \frac{10}{3} \cdot \frac{9}{10} = 3.$$

Let now $l/t \leqslant 9/10$. Then

$$\frac{10ld}{3t} = \frac{10l(t-l)}{3t} = \frac{10l}{3} \cdot \left(1 - \frac{l}{t}\right) \geqslant \frac{10l}{3} \cdot \frac{1}{10} = \frac{l}{3} > 3.$$

Thus, we got a contradiction. It follows that $k_a(u)$ has a prime divisor large with respect to L, so $t(S) \leqslant t(L)$. An application of Proposition 5 completes the proof of Proposition 7.

Proposition 8. *Suppose that $t(L) \geqslant 23$. If a prime r distinct from p divides the order of $\overline{G}/S$, then $\varphi(r, L) \leqslant n/3$.*

PROOF. It follows from Proposition 4 that it remains to prove the assertion: if $L = L_n^{\varepsilon}(q)$, $n \in [2^{\gamma+3}, 9 \cdot 2^{\gamma})$ and $e(r, \varepsilon q) = \varphi(r, L) = 3 \cdot 2^{\gamma}$ for some $\gamma \geqslant 3$, then r does not divide $|\overline{G}/S|$.

Assume to the contrary, that r divides $|\overline{G}/S|$. Let $b = 2^{\gamma+3}$ and $l = e(r, q) = 3 \cdot 2^{\gamma}$. Since b is a multiple of 4, the equality $k_b(q) = k_b(\varepsilon q)$ holds. If $s \in R_b(q)$, then s is large with respect to L and, by Proposition 7, it is also large with respect to S. Therefore, $\varphi(s, S) \geqslant m/2 - 1$ by Lemma 2.7(ii). Denote the s-part of $k_b(q)$ by f, and a Sylow s-subgroup of S by F. Then $|F| \in \{f, f^2\}$. By Frattini argument, the group $N = N_{\overline{G}}(F)$ contains an element x of order r. Since $b + l > n$ and l does not divide b, the primes r and s are nonadjacent in $GK(L)$. Therefore, $F \rtimes \langle x \rangle$ is a Frobenius group. It follows that r divides $f^2 - 1$. This is true for every prime divisor s of $k_b(q)$, so the number $k_b(q)^2 - 1$ is a multiple of r. Further, $k_b(q)^2 - 1 = \Phi_b(q)^2 - 1 = (\Phi_b(q) - 1)(\Phi_b(q) + 1)$. Since $p \neq 2$, it follows that r divides the number

$$\frac{q^{2^{\gamma+2}} - 1}{2} \cdot \frac{q^{2^{\gamma+2}} + 3}{2}.$$

Obviously, r does not divide the first product term because $e(r, q) = 3 \cdot 2^{\gamma}$. Assume that r divides the second term and put $a = q^{2^{\gamma}}$. Then r divides $(a^4 + 3, a^3 - 1) = (a^3 - 1, a + 3) = (a + 3, 28)$. However, $e(r, q) \geqslant 24$, so r cannot divide 28, a contradiction. The proposition is proved.

Proposition 9. *Let $t(L) \geqslant 23$. Suppose that the characteristic p of the group L satisfies the conditions:*

(i) *p does not divide the order of K;*

(ii) *if $S = L_m^{\varepsilon}(u)$, then p does not divide the number $\varepsilon u - 1$.*

Then p divides the order of S and $t(p, S) = t(p, L)$.

PROOF. Recall that $p \neq 2$ by Proposition 6. Assume to the contrary that either p does not divide $|S|$ or $t(p, S) \neq t(p, L)$. Observe that if p divides $|S|$ then $t(p, S) \geqslant t(p, L)$. Indeed, it follows from Lemma 2.6 that every prime r nonadjacent to p in $GK(L)$ is large with respect to L, so r does not divide $|\overline{G}/S| \cdot |K|$.

Lemma 6.6. *The number $|\overline{G}/S|$ is divided by p. Every p-element of $\overline{G}/S$ is conjugated to a field automorphism of S.*

Proof. Suppose that p does not divide $|\overline{G}/S|$. Then p divides $|S|$ and, by our assumption, $t(p,S) > t(p,L)$. Let ρ be a $\{p\}$-coclique of size $t(p,S)$ in $GK(S)$. Put $\rho' = \rho \setminus \{p\}$ and $I = E(p,S) = \{e(r,u) \mid r \in \rho'\}$. Then for any $i \in I$ every prime divisor of $k_i(u)$ is large with respect to S by Lemma 2.8. Proposition 7 yields that for every $i \in I$ there is a prime divisor r_i of $k_i(u)$ being large with respect to L. The set $\{p\} \cup \{r_i \mid i \in I\}$ is a coclique in $GK(S)$. Furthermore, since none of primes from the coclique divides $|K| \cdot |\overline{G}/S|$, then it is also a $\{p\}$-coclique in $GK(L)$ of size $t(p,S)$, a contradiction.

Since $(p, 2|\operatorname{Inndiag}(S)/S|) = 1$, we may assume that every p-element of $\overline{G}/S$ is conjugated to a field automorphism of S.

Lemma 6.7. *There exists a positive integer j satisfying the conditions:*

(i) *for every prime r from $R_j(u)$ the inequality $\varphi(r,S) > m/2$ holds and $rp \notin \omega(S)$;*

(ii) *for every prime s from $R_j(u)$, being large with respect to L, the number sp belongs to $\omega(L)$.*

Proof. First, we suppose that either p does not divide $|S|$ or p is large with respect to S. Let $t = t(L) = t(S)$, and ρ be a coclique in $GK(S)$ of size t with $p \in \rho$ if p divides $|S|$. Put $I = E(\rho, S)$. It is clear that there exists a subset Y of I consisting of at least $t-2$ elements and such that for any $j \in Y$ and every $r \in R_j(u)$ we have $pr \notin \omega(S)$ and $\varphi(r,S) > m/2$. Since $t(p,L) \leqslant 4$, there is a subset J of Y consisting of at least $t-5$ elements and satisfying the condition: for any $j \in J$ every prime s from $R_j(u)$, being large with respect to L (for any $j \in J$ such primes from $R_j(u)$ exist by Proposition 7), is adjacent to p in $GK(L)$. The assumption $t \geqslant 23$ implies that J is not empty.

Suppose now that $t(p,S) < t$, $e(p,u) = a$, and ρ is a $\{p\}$-coclique in $GK(S)$ of size $t(p,S)$. Put $I = \{e(r,u) \mid r \in \rho\} \setminus \{a\}$. Then Lemma 2.8 yields $\varphi(r,S) > m/2$ for any $i \in I$ and every $r \in R_i(u)$. By our assumption, $t(p,S) > t(p,L)$, so there is $j \in I$ such that every s from $k_j(u)$, being large with respect to L, is adjacent to p in $GK(L)$.

Lemma 6.8. *Suppose that p divides β, where $u = v^\beta$, and $u_0 = u^{1/p}$. Then for the number j, defined in Lemma 6.7, the inequality $k_{jp}(u_0) \leqslant (q^2 - 1)\log_v u$ holds.*

PROOF. Since $\overline{G}/S$ contains a field automorphism of order p, the number u_0 is an integer. It follows from Lemma 1.2 that $k_{jp}(u_0)$ divides $k_j(u)$. Fix some prime divisor r of $k_{jp}(u_0)$. Suppose that r does not divide $|\overline{G}/S|\cdot|K|$. Then r is large with respect to L, hence $rp \in \omega(L)$. Since $rp \notin \omega(S)$, the prime r must divide the order of the centralizer $H = C_S(f)$ in S of a field automorphism f of order p. The group H is a classical group of the same type and same dimension as S, but defined over the field of order u_0. Therefore, using $\varphi(r,S) > m/2$, it is easy to check that $k_{jp}(u_0)$ is coprime to the order of H. Indeed, if $S = L_m^{\varepsilon}(u)$, then $\varphi(r,H) = \nu_\varepsilon(jp) = p\nu_\varepsilon(j) = p\varphi(r,S) > pm/2 > m$, and if S is symplectic or orthogonal, then $\varphi(r,H) = \eta(jp) = p\eta(j) > pm/2 > m$.

Thus, every prime divisor r of $k_{jp}(u_0)$ divides $|\overline{G}/S|\cdot|K|$. Furthermore, p does not divide $k_j(u)$. Applying Lemma 6.4, we obtain that $(k_{jp}(u_0))_{\{r\}}$ divides $((q^2-1)\log_v u)_{\{r\}}$ for every prime divisor r of $k_{jp}(u_0)$. The lemma is proved.

Let us complete the proof of Proposition 9. Applying the inequality $t(S) \geqslant 23$, Lemma 6.3, and arguing as in the beginning of the proof of Lemma 6.5, we obtain that $\eta(j) \geqslant 11$ for j defined in Lemma 6.7. It follows from Lemma 1.6 that $k_{jp}(u_0) > u^4 \log_v u$. Lemma 6.8 yields $q^2 - 1 \geqslant k_{jp}(u_0)/\log_v u > u^4$. On the other hand, if we apply the equality $t(L) = t(S)$ to the inequality (15), based on Lemma 2.14 and derived in the proof of Lemma 6.5, we obtain the inequality $u \geqslant q^{5/9}$. Thus, the impossible chain of inequalities $q^2 - 1 > u^4 \geqslant (q^{5/9})^4 > q^2$ arises and leads us to a contradiction. The proposition is proved.

7. Proof: pigeons and holes

In this section we complete the proof of Theorem 3. We write $t = t(L)$ and recall that $t(L) = t(S)$ by Proposition 7.

Lemma 7.1. *Let $t(L) \geqslant 23$. If $s \in \pi(L)$ is chosen so that $\varphi(s,L) > n/3$, then $t(s,L) = t(s,S)$.*

PROOF. If $t(s,L) = t(L)$, then the desired result follows from Proposition 5. We may assume, therefore, that s is small with respect to L. Let ρ be an $\{s\}$-coclique of size $t(s,L)$ in $GK(L)$. Since s is small with respect to L, all other numbers in ρ are large with respect to L by Lemma 2.8, and hence they do not divide $|\overline{G}/S| \cdot |K|$. As $\varphi(s, L) > n/3$, Proposition 8 implies that s does not divide $|\overline{G}/S| \cdot |K|$ either. Thus ρ is a coclique in $GK(S)$, whence $t(s, S) \geqslant t(s, L)$.

Let $\rho = \{s, s_1, \ldots, s_{k-1}\}$ be a coclique of size $k = t(s, S)$ in $GK(S)$. By Lemma 2.8, the numbers $s_1, \ldots, s_{k-1}$ are large with respect to S. By Proposition 7, for every $i \in \{1, \ldots, k-1\}$, there is a prime divisor w_i of $k_{e(s_i,u)}$ that is large with respect to L. Write $\rho' = \{s, w_1, \ldots, w_{k-1}\}$. Then ρ' is a coclique in $GK(S)$. Since no number in ρ' divides $|\overline{G}/S| \cdot |K|$, it follows that ρ' is a coclique in $GK(L)$ of size k, whence $t(s, S) \leqslant t(s, L)$. Thus $t(s, L) = t(s, S)$, and the proof is complete.

Let $r \in \pi(L) \setminus \{p\}$, and suppose that r is small with respect to L. Recall that, by Lemma 2.8, the set $E(\rho', L) = \{e(r, q) \mid r \in \rho'\}$, where ρ is an $\{r\}$-coclique of greatest size and $\rho' = \rho \setminus \{r\}$, is independent of the choice of ρ, and it is denoted by $J(r, L)$.

Lemma 7.2. *Let L be a classical simple group over a field of order q and characteristic p, and suppose that* $\mathrm{prk}(L) = n \geqslant 19$. *If a prime divisor r of $|L|$ other than p is chosen so that $\varphi(r, L) > n/3$ or $t(r, L) > 2t(L)/3$, then $e(r, q) > 2$ and $e(r, q) \neq 6$. In particular, if r is small then $J(r, L)$ depends only on the number $e(r, q)$ and type of L.*

Proof. Let $t = t(L)$. If $\varphi(r, L) > n/3$ then $\varphi(r, L) \geqslant 7$, and therefore $e(r, q) \geqslant 7$ or $e(r, q) = 5$. If $t(r, L) > 2t/3$ then $t(r, L) \geqslant 8$, and hence $e(r, q) > 2$ by Lemma 2.9. Also it is easy to check that for $n \geqslant 19$ and $q \neq 2$ we have $t(r_6(q), L) < 2t/3$ (recall that $k_6(2) = 1$). Now the result follows from Lemmas 2.8 and 1.1.

Define
$$M(L) = \{i \mid \varphi(r_i(q), L) > n/3, t(r_i(q), L) < t\}$$
and
$$N(L) = \{i \mid 2t/3 < t(r_i(q), L) < t\}.$$
Also define a function $\zeta_L : M(L) \cup N(L) \mapsto \mathbb{N}$ by setting
$$\zeta_L(i) = t(r_i(q), L).$$

By Lemma 7.2, the sets $M(L)$ and $N(L)$ and function ζ_L are well-defined. We write $T(L)$ to denote $\zeta_L(M(L) \cap N(L))$. In four further lemmas, we describe the sets $M(L)$, $N(L)$, and $T(L)$, as well as the function ζ_L, for all types of classical groups L.

Lemma 7.3. *Let $L = L_n^\varepsilon(q)$, where $n \geqslant 45$. If $n \not\equiv 5 \pmod 6$, then $N(L) = M(L)$. If $n \equiv 5 \pmod 6$, then $N(L) = M(L) \setminus \{\nu_\varepsilon((n+1)/3)\}$. If $i \in M(L)$, then $\zeta_L(i) = \nu_\varepsilon(i)$. In particular, ζ_L is injective and $t - j \in T(L)$ for every $1 \leqslant j \leqslant 7$.*

Proof. Note that the condition $t(r, L) < t$ is equivalent to the inequality $\varphi(r, L) < n/2$. Suppose that $i \in M(L) \cup N(L)$, and consider the set $J(i) = J(r_i(q), L)$. The adjacency criterion yields $J(i) = J_1(i) \setminus J_2(i)$, where $J_1(i) = \{j \mid n - \nu_\varepsilon(i) < \nu_\varepsilon(j) \leqslant n\}$ and $J_2(i) = \{j \mid \nu_\varepsilon(j) \text{ is a multiple of } \nu_\varepsilon(i)\}$. Since ν_ε is bijective, we have $|J_1(i)| = \nu_\varepsilon(i)$. Thus

$$\zeta_L(i) = 1 + |J(i)| = 1 + |J_1(i)| - |J_1(i) \cap J_2(i)| = 1 + \nu_\varepsilon(i) - |J_1(i) \cap J_2(i)|.$$

Let $i \in M(L)$. Then $n/3 < \nu_\varepsilon(i) < n/2$. Therefore $J_1(i) \cap J_2(i) = \{j\}$, where $\nu_\varepsilon(j) = 2\nu_\varepsilon(i)$, and hence $\zeta_L(i) = \nu_\varepsilon(i)$. If n is even, then $2t/3 = n/3$, and so $\zeta_L(i) > 2t/3$. If n is odd and $i \neq (n+1)/3$, then $\zeta_L(i) \geqslant (n+2)/3 > 2t/3$. If n is odd and $i = (n+1)/3$, then $\zeta_L(i) = 2t/3$ and $i \notin N(L)$. Thus $M(L) \subseteq N(L)$ if $n \not\equiv 5 \pmod 6$, and $M(L) \setminus N(L) = \{(n+1)/3\}$ otherwise.

Let $i \in N(L)$. Suppose that $\nu_\varepsilon(i) \leqslant n/3$. If $\nu_\varepsilon(i) \leqslant (n-3)/3$, then $\zeta_L(i) \leqslant 1 + \nu_\varepsilon(i) \leqslant n/3 \leqslant 2t/3$, which is a contradiction. If $\nu_\varepsilon(i) \geqslant (n-2)/3$, then $3\nu_\varepsilon(i) \in J_1(i) \cap J_2(i)$, therefore, $|J(i)| \leqslant \nu_\varepsilon(i) \leqslant n/3 \leqslant 2t/3$, and again we have a contradiction. Thus $i \in M(L)$, and hence $N(L) \subseteq M(L)$.

We conclude that $T(L) = \{x \in \mathbb{Z} \mid n/3 < x < n/2\}$ if n is even, and $T(L)$ contains $\{x \in \mathbb{Z} \mid (n+1)/3 < x < n/2\}$ if n is odd. It follows easily that $t - 1 < n/2$. If n is even, the inequality $t - 7 > n/3$ is equivalent to $n > 42$. If n is odd, the inequality $t - 7 > (n+1)/3$ is equivalent to $n > 43$. Thus $t - 7 \in T(L)$ when $n \geqslant 44$.

Lemma 7.4. *Let $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, where $n \geqslant 29$. Then $M(L) = N(L)$. If $i \in M(L)$, then*

$$\zeta_L(i) = \begin{cases} [\frac{3\eta(i)+2}{2}] & \textit{if } n \textit{ is even,} \\ [\frac{3\eta(i)+3}{2}] & \textit{if } n \textit{ is odd.} \end{cases}$$

Moreover,

$$T(L) \cap \{x \mid t-6 \leqslant x \leqslant t-1\} = \begin{cases} \{t-2, t-3, t-5, t-6\} & \textit{if } n \equiv 0, 3 \pmod 4, \\ \{t-1, t-3, t-4, t-6\} & \textit{if } n \equiv 2 \pmod 4, \\ \{t-1, t-2, t-4, t-5\} & \textit{if } n \equiv 1 \pmod 4. \end{cases}$$

Proof. Using Table 1, it is easy to see that $[(n+1)/2] \leqslant 2t/3 \leqslant [(n+1)/2] + 2/3$.

Suppose that $i \in M(L) \cup N(L)$, and consider the set $J(i) = J(r_i(q), L)$. The adjacency criterion yields $J(i) = J_1(i) \setminus J_2(i)$, where $J_1(i) = \{j \mid n - \eta(i) < \eta(j) \leqslant n\}$ and $J_2(i) = \{j \mid j = li \text{ for an odd } l\}$. Therefore $\zeta_L(i) = 1 + |J_1(i)| - |J_1(i) \cap J_2(i)|$. By Lemma 1.8, the size of $J_1(i)$ is equal to $[3\eta(i)/2]$ if n is even, and $[(3\eta(i)+1)/2]$ if n is odd.

Let $i \in M(L)$. Then $\eta(i) \geqslant (n+1)/3$. If $j = li$ with $l \geqslant 3$ odd, then $\eta(j) = l\eta(i) > ln/3 \geqslant n$. Therefore $J_1(i) \cap J_2(i) = \varnothing$, and so $\zeta_L(i) = 1 + [3\eta(i)/2] = [(3\eta(i)+2)/2]$ when n is even, and $\zeta_L(i) = 1 + [(3\eta(i)+1)/2] = [(3\eta(i)+3)/2]$ when n is odd. Since $\eta(i) \geqslant (n+1)/3$, we have $3\eta(i)/2 \geqslant (n+1)/2$, and so $\zeta_L(i) \geqslant 1 + [(n+1)/2] > 2t/3$. Thus $M(L) \subseteq N(L)$.

Let $i \in N(L)$. By the above formula, $\zeta_L(i) \leqslant 1 + |J_1(i)| \leqslant [(3\eta(i)+3)/2]$. On the other hand, $\zeta_L(i) > [(n+1)/2]$. Therefore $3\eta(i) + 3 > n + 1$, whence $\eta(i) > (n-2)/3$. Suppose that $i \notin M(L)$, that is $\eta(i) \leqslant n/3$. Then $\eta(3i) = 3\eta(i) \leqslant n$ and $\eta(3i) + \eta(i) = 4\eta(i) > 4(n-2)/3 \geqslant n$. It follows that $3i \in J_1(i) \cap J_2(i)$ and $\zeta_L(i) \leqslant [(3\eta(i)+1)/2] \leqslant [(n+1)/2] \leqslant 2t/3$, a contradiction. Thus $N(L) \subseteq M(L)$.

Let a be the largest element of $\eta(M(L))$. Then $a \geqslant (n-2)/2$ when $n \not\equiv 3 \pmod 4$, and $a = (n-3)/2$ when $n \equiv 3 \pmod 4$. The condition $n \geqslant 29$ yields $(n-3)/2 - 3 > n/3$, and hence $a, a-1, a-2, a-3$ are in $\eta(M(L))$. Let $\eta(i) = a$ and $\eta(j) = a-1$. Write b and c for $\zeta_L(i)$ and $\zeta_L(j)$ respectively. As $[3(x-2)/2] = [3x/2] - 3$, we obtain that the four largest elements of $T(L)$ are b, c, $b-3$, and $c-3$, and $T(L) \cap \{x \mid t-6 \leqslant x \leqslant t-1\} = \{b, c, b-3, c-3\} \cap \{x \mid t-6 \leqslant x \leqslant t-1\}$.

Suppose that $n \equiv 0 \pmod 4$. Then $t = (3n+4)/4$ and $a = n/2 - 1$. If $\eta(i) = n/2 - 1$, then $\zeta_L(i) = [(3n-2)/4] = (3n-4)/4 = t-2$. If $\eta(i) = n/2 - 2$, then $\zeta_L(i) = [(3n-8)/4] = t-3$.

Suppose that $n \equiv 2 \pmod 4$. Then $t = (3n+2)/4$ and $a = n/2 - 1$. If $\eta(i) = n/2 - 1$, then $\zeta_L(i) = [(3n-2)/4] = t-1$. If $\eta(i) = n/2 - 2$, then $\zeta_L(i) = [(3n-8)/4] = t-3$.

Suppose that $n \equiv 1 \pmod 4$. Then $t = (3n+5)/4$ and $a = (n-1)/2$. If $\eta(i) = (n-1)/2$, then $\zeta_L(i) = [(3n+3)/4] = t-1$. If $\eta(i) = (n-3)/2$, then $\zeta_L(i) = [(3n-3)/4] = t-2$.

Suppose that $n \equiv 3 \pmod 4$. Then $t = (3n+3)/4$ and $a = (n-3)/2$. If $\eta(i) = (n-3)/2$, then $\zeta_L(i) = [(3n-3)/4] = t-2$. If $\eta(i) = (n-5)/2$, then $\zeta_L(i) = [(3n-9)/4] = t-3$.

Lemma 7.5. *Let $L = O_{2n}^+(q)$, where $n \geqslant 30$. Then*

$$N(L) = \begin{cases} M(L) \text{ if } n \not\equiv 6, 9 \pmod{12}, \\ M(L) \cup \{2n/3\} \text{ if } n \equiv 6 \pmod{12}, \\ M(L) \cup \{2n/3, n/3\} \text{ if } n \equiv 9 \pmod{12}. \end{cases}$$

If $i \in M(L)$, then

$$\zeta_L(i) = \begin{cases} [\frac{3\eta(i)+1}{2}] \text{ if } n \text{ is even}, \\ [\frac{3\eta(i)+2}{2}] \text{ if } n \text{ is odd and } i \text{ is even}, \\ [\frac{3\eta(i)+3}{2}] \text{ if } n \text{ is odd and } i \text{ is odd}. \end{cases}$$

If $n \equiv 6, 9 \pmod{12}$ and $\eta(i) = n/3$, then $\zeta_L(i) = [(n+1)/2] = (2t+1)/3$.

If n is odd, then ζ_L is injective on $M(L) \cap N(L)$, $t - j \in T(L)$ for every $1 \leqslant j \leqslant 6$, and $\zeta_L^{-1}(t-j) \equiv 4 \pmod 8$ for some $1 \leqslant j \leqslant 6$.

If n is even, then

$$T(L) \cap \{x \mid t-6 \leqslant x \leqslant t-1\} = \begin{cases} \{t-1, t-3, t-4, t-6\} \text{ if } n \equiv 0 \pmod 4, \\ \{t-1, t-2, t-4, t-5\} \text{ if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. It is easy to verify that $[(n+1)/2] - 1/3 \leqslant 2t/3 \leqslant [(n+1)/2]$.

Suppose that $i \in M(L) \cup N(L)$, and consider the set $J(i) = J(r_i(q), L)$. The adjacency criterion yields

$$J(i) = J_3(i) \cup J_1(i) \setminus J_2(i),$$

where $J_1(i) = \{j \mid n - \eta(i) < \eta(j) \leqslant n, j \neq 2n\}$, $J_2(i) = \{j \mid j = li \text{ for an odd } l\}$, and $J_3(i) = \{2(n - \eta(i))\}$ when i is odd, $J_3(i) = \{n - \eta(i)\}$ when i is even and $n - \eta(i)$ is odd, and $J_3(i) = \varnothing$ when both i and $n - \eta(i)$ are even. Note that $J_1(i) \cap J_3(i) = \varnothing$. Therefore $\zeta_L(i) = 1 + |J_3(i)| + |J_1(i)| - |J_1(i) \cap J_2(i)|$. By Lemma 1.8, the size of $J_1(i)$ is equal to $[3\eta(i)/2] - 1$ or $[(3\eta(i)+1)/2] - 1$, depending on whether n is even or odd.

Thus if n is even and $\eta(i)$ is odd, then

$$\zeta_L(i) = 1 + [3\eta(i)/2] - |J_1(i) \cap J_2(i)| = (3\eta(i)+1)/2 - |J_1(i) \cap J_2(i)|.$$

If both n and $\eta(i)$ are even, then

$$\zeta_L(i) = [3\eta(i)/2] - |J_1(i) \cap J_2(i)| = 3\eta(i)/2 - |J_1(i) \cap J_2(i)|.$$

If both n and i are odd, then

$$\zeta_L(i) = 1 + (3\eta(i)+1)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+3)/2 - |J_1(i) \cap J_2(i)|.$$

If n is odd and $\eta(i)$ is even, then

$$\zeta_L(i) = 1 + 3\eta(i)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+2)/2 - |J_1(i) \cap J_2(i)|.$$

Finally, if n is odd, i is even and $\eta(i)$ is odd, then

$$\zeta_L(i) = (3\eta(i)+1)/2 - |J_1(i) \cap J_2(i)|.$$

Let $i \in M(L)$. Then $J_1(i) \cap J_2(i) = \varnothing$, and hence the formulas for ζ_L are proved. The condition $\eta(i) > n/3$ implies that $(3\eta(i)+1)/2 > (n+1)/2$, therefore,

$$\zeta_L(i) \geqslant [(3\eta(i)+1)/2] \geqslant [(n+1)/2] \geqslant 2t/3.$$

Suppose that all non-strict inequalities in the above chain are equalities. Then $(n+1)/2$ is integer and $3\eta(i) = n+1$, and so n is odd and $\eta(i)$ is even. But then the first inequality is strict, a contradiction. Thus $M(L) \subseteq N(L)$.

Let $i \in N(L)$. Then $[(n+1)/2] - 1/3 \leqslant 2t/3 < \zeta_L(i) \leqslant [(3\eta(i)+3)/2]$, and hence $n \leqslant 3\eta(i)+3$. Suppose that $n-3 \leqslant 3\eta(i) \leqslant n-1$. Then $3i \in J_1(i) \cap J_2(i)$. If $3\eta(i) = n-3$ or $3\eta(i) = n-1$, then n and $\eta(i)$ have different parity, whence $\zeta_L(i) \leqslant [3\eta(i)/2] \leqslant [(n-1)/2] < 2t/3$, a contradiction. If $3\eta(i) = n-2$, then n and $\eta(i)$ have the same parity, and so $\zeta_L(i) \leqslant [(3\eta(i)+1)/2] = [(n-1)/2] < 2t/3$, which is not the case. Finally, assume that $\eta(i) = n/3$. If n is odd, then $J_1(i) \cap J_2(i) = \{3i\}$. If n is even, then $J_1(i) \cap J_2(i) = \varnothing$. Furthermore, $n - \eta(i)$ is even. It follows that $\zeta_L(i) = [(3\eta(i)+1)/2] = [(n+1)/2]$. If $n \equiv 0, 3 \pmod 4$, then $[(n+1)/2] = 2t/3$, a contradiction. If $n \equiv 1, 2 \pmod 4$, then $[(n+1)/2] > 2t/3$. Thus if $n \equiv 6, 9 \pmod{12}$ and $\eta(i) = n/3$, then $i \in N(L) \setminus M(L)$.

Let a be the largest element of $\eta(M(L))$. Then $a \geqslant [n/2] - 1$. Since $n \geqslant 30$, we have $a - 3 > n/3$.

Let n be even, and $b = \zeta_L(i)$, with $\eta(i) = a$, and $c = \zeta_L(j)$, with $\eta(j) = a-1$. If $n \equiv 0 \pmod 4$, then $t = 3n/4$, $b = [(3n-4)/4] = t-1$, and $c = [(3n-10)/4] = t-3$. If $n \equiv 2 \pmod 4$, then $t = (3n-2)/4$, $b = [(3n-4)/4] = t-1$, and $c = [(3n-10)/4] = t-2$. Reasoning as in the proof of Lemma 7.4, we obtain that $T(L) \cap \{x \mid t-6 \leqslant x \leqslant t-1\} = \{b, c, b-3, c-3\}$.

Let n be odd. We will show that ζ_L is injective. Suppose that i and j have the same parity and $[3\eta(i)/2] = [3\eta(j)/2]$. Then $3\eta(j) - 1 \leqslant 3\eta(i) \leqslant$

$3\eta(j)+1$, whence $\eta(i)=\eta(j)$. By parity condition, it follows that $i=j$. Now suppose that i is even and j is odd, and $[3\eta(i)/2]=[3\eta(j)/2]+1$. Then $[3i/4]=(3j+1)/2$, and so either $3i/2=3j+1$ or $3i/2=3j+2$. Both equalities are clearly impossible.

If $n\equiv 1\,(\mathrm{mod}\,4)$, then $t=(3n+1)/4$, $a=(n-3)/2$ is odd, and $a,2a\in M(L)$. Therefore $T(L)$ contains the following numbers: $\zeta_L(a)=(3a+3)/2=3(n-1)/4=t-1$, $\zeta_L(2a)=t-2$, $\zeta_L(2(a-1))=(3a+1)/2=t-3$, $\zeta_L(a-2)=t-4$, $\zeta_L(2(a-2))=t-5$, and $\zeta_L(2(a-3))=t-6$. If $n\equiv 3\,(\mathrm{mod}\,4)$, then $t=(3n+3)/4$ and $a=(n-1)/2$ is odd with $a\notin M(L)$. It follows that $T(L)$ contains the following numbers: $\zeta_L(2a)=(3a+1)/2=(3n-1)/4=t-1$, $\zeta_L(2(a-1))=(3(a-1)+2)/2=t-2$, $\zeta_L(a-2)=t-3$, $\zeta_L(2(a-2))=t-4$, and $\zeta_L(2(a-3))=t-5$. Furthermore, $a-4>n/3$, and hence $\zeta_L(a-4)=t-6$ and $\zeta_L(2(a-4))=t-7$ also lie in $T(L)$. Thus the set $X=\{x\mid t-6\leqslant x\leqslant t-1\}$ is a subset of $T(L)$. Moreover, one of the numbers $2(a-1)$ and $2(a-3)$ is congruent to 4 modulo 8 and $\zeta_L(2(a-1)),\zeta_L(2(a-3))\in X$.

Lemma 7.6. *Let $L=O^-_{2n}(q)$, where $n\geqslant 30$. Then*

$$N(L)=\begin{cases} M(L) \text{ if } n\not\equiv 0,6,9\,(\mathrm{mod}\,12),\\ M(L)\cup\{2n/3\} \text{ if } n\equiv 0\,(\mathrm{mod}\,6),\\ M(L)\cup\{2n/3,n/3\} \text{ if } n\equiv 9\,(\mathrm{mod}\,12).\end{cases}$$

If $i\in M(L)$, then

$$\zeta_L(i)=\begin{cases} [\frac{3\eta(i)+4}{2}] \text{ if } n \text{ is odd},\\ [\frac{3\eta(i)+2}{2}] \text{ if both } n \text{ and } i \text{ are odd},\\ [\frac{3\eta(i)+3}{2}] \text{ if } n \text{ is odd and } i \text{ is even}.\end{cases}$$

If $\eta(i)=n/3$, then

$$\zeta_L(i)=\begin{cases}(n+2)/2=(2t+1)/3 \text{ if } n\equiv 0\,(\mathrm{mod}\,12)\\ (n+2)/2=(2t+2)/3 \text{ if } n\equiv 6\,(\mathrm{mod}\,12)\\ (n+1)/2=(2t+1)/3 \text{ if } n\equiv 9\,(\mathrm{mod}\,12)\end{cases}.$$

If n is odd, then ζ_L is injective on $M(L)\cap N(L)$, $t-j\in T(L)$ for every $1\leqslant j\leqslant 6$, and $\zeta_L^{-1}(t-j)\equiv 4\,(\mathrm{mod}\,8)$ for some $1\leqslant j\leqslant 6$.

If $n\equiv 0\,(\mathrm{mod}\,4)$, then

$$T(L)\cap\{x\mid t-7\leqslant x\leqslant t-1\}=\{t-1,t-2,t-4,t-5,t-7\}.$$

If $n \equiv 2 \pmod 4$ *and* $n \geqslant 38$*, then*

$$T(L) \cap \{x \mid t-8 \leqslant x \leqslant t-1\} = \{t-2, t-3, t-5, t-6, t-8\}.$$

If $n = 34$*, then* $T(L) = \{t-2, t-3, t-5, t-6\}$*, and if* $n = 30$*, then* $T(L) = \{t-2, t-3, t-5\}$*.*

Proof. It is easy to verify that $n/2 + 1/6 \leqslant 2t/3 \leqslant n/2 + 2/3$.

Suppose that $i \in M(L) \cup N(L)$, and consider the set $J(i) = J(r_i(q), L)$. The adjacency criterion yields

$$J(i) = J_3(i) \cup J_1(i) \setminus J_2(i),$$

where $J_1(i) = \{j \mid n - \eta(i) < \eta(j) \leqslant n, j \neq n\}$, $J_2(i) = \{j \mid j = li \text{ for an odd } l\}$, and $J_3(i) = \{2(n-\eta(i))\}$ if i is even, $J_3(i) = \{n - \eta(i)\}$ if both i and $n - \eta(i)$ are odd, and $J_3(i) = \varnothing$ if i is odd, $n - \eta(i)$ is even. Note that $J_1(i) \cap J_3(i) = \varnothing$. Therefore $\zeta_L(i) = 1 + |J_3(i)| + |J_1(i)| - |J_1(i) \cap J_2(i)|$. If n is even, then $\eta(n) = n/2 \leqslant n - \eta(i)$, and so the size of $J_1(i)$ is equal to $[3\eta(i)/2]$. If n is odd, then the size of $J_1(i)$ is equal to $[(3\eta(i)+1)/2] - 1$.

Thus if n is even and $\eta(i)$ is odd, then

$$\zeta_L(i) = 1 + 1 + (3\eta(i)-1)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+3)/2 - |J_1(i) \cap J_2(i)|.$$

If both n and $\eta(i)$ are even, then

$$\zeta_L(i) = 1 + 1 + 3\eta(i)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+4)/2 - |J_1(i) \cap J_2(i)|.$$

If n is odd and $\eta(i)$ is even, then

$$\zeta_L(i) = 1 + 3\eta(i)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+2)/2 - |J_1(i) \cap J_2(i)|.$$

If both n and i are odd, then

$$\zeta_L(i) = (3\eta(i)+1)/2 - |J_1(i) \cap J_2(i)|.$$

Finally, if n is odd, i is even, and $\eta(i)$ is odd, then

$$\zeta_L(i) = 1 + (3\eta(i)+1)/2 - |J_1(i) \cap J_2(i)| = (3\eta(i)+3)/2 - |J_1(i) \cap J_2(i)|.$$

Let $i \in M(L)$. Then $J_1(i) \cap J_2(i) = \varnothing$, and so the formulas for ζ_L are proved. Since $\eta(i) > n/3$, it follows that $(3\eta(i)+3)/2 > (n+3)/2$, whence

$$\zeta_L(i) \geqslant [(3\eta(i)+3)/2] \geqslant [(n+3)/2] > 2t/3.$$

Thus $M(L) \subseteq N(L)$.

Let $i \in N(L)$. Then $n/2 + 1/6 \leqslant 2t/3 < \zeta_L(i) \leqslant (3\eta(i)+4)/2$, and hence $n \leqslant 3\eta(i)+3$. Suppose that $n-3 \leqslant 3\eta(i) \leqslant n-1$. Then $3i \in J_1(i) \cap J_2(i)$. If n and $\eta(i)$ have the same parity, then $\zeta_L(i) \leqslant (3\eta(i)+2)/2 \leqslant n/2 < 2t/3$, a contradiction. If n and $\eta(i)$ have different parity, then $\zeta_L(i) \leqslant (3\eta(i)+1)/2 \leqslant n/2 < 2t/3$, which is not the case. Suppose that $\eta(i) = n/3$. If n is even, then $J_1(i) \cap J_2(i) = \{2n\}$, and so $\zeta_L(i) = (3\eta(i)+2)/2 = (n+2)/2 > 2t/3$. It follows that $2n/3 \in N(L) \setminus M(L)$ when $n \equiv 0 \pmod 6$. Assume that n is odd. Then $J_1(i) \cap J_2(i) = \{2n\}$ when $i = 2n/3$ and $J_1(i) \cap J_2(i) = \varnothing$ when $i = n/3$. Therefore $\zeta_L(i) = (3\eta(i)+1)/2 = (n+1)/2$. If $n \equiv 3 \pmod 4$, then $(n+1)/2 = 2t/3$, a contradiction. If $n \equiv 1 \pmod 4$, then $(n+1)/2 > 2t/3$. Thus if $n \equiv 9 \pmod{12}$, then $n/3, 2n/3 \in N(L) \setminus M(L)$.

Let a be the largest element of $\eta(M(L))$. Then $a \geqslant [n/2]-1$ when $n \not\equiv 2 \pmod 4$ and $a = n/2 - 2$ when $n \equiv 2 \pmod 4$. Therefore if $n > 30$, then $a - 3 > n/3$, and if, in addition, n is even and $n \neq 34$, then $a - 4 > n/3$.

If $n \equiv 0 \pmod 4$, then $t = (3n+4)/4$ and $a = n/2 - 1$, whence $\zeta_L(a) = (3a+3)/2 = 3n/4 = t-1$ and $\zeta_L(2(a-1)) = (3a+1)/2 = t-2$. If $n \equiv 2 \pmod 4$, then $t = (3n+2)/4$ and $a = n/2-2$, and hence $\zeta_L(a) = (3a+3)/2 = (3n-6)/4 = t-2$ and $\zeta_L(2(a-1)) = (3a+1)/2 = t-3$. The completion of the proof is similar to that of Lemma 7.5.

Lemma 7.7. *If either $S = O^+_{2m}(u)$ with $m \equiv 6, 9 \pmod{12}$ or $S = O^-_{2m}(u)$ with $m \equiv 0, 9 \pmod{12}$, then $T(L) \subseteq T(S) \cup \{(2t+1)/3\}$. If $S = O^-_{2m}(u)$ with $m \equiv 6 \pmod{12}$, then $T(L) \subseteq T(S) \cup \{(2t+2)/3\}$. In other cases, $T(L) \subseteq T(S)$. In particular, if $x \in T(L)$ and $x > (2t+2)/3$, then $x \in T(S)$.*

Proof. Choose $x \in T(L) \setminus T(S)$. Let $s \in \pi(L)$ and $t(s, L) = x$. As $e(s, q) \in M(L) \cap N(L)$, by Lemma 7.1, we have $t(s, S) = x$, and hence $e(s, u) \in N(S)$. If $e(s, u) \in M(S)$, then $x \in T(S)$. If $e(s, u) \notin M(S)$, then applying Lemmas 7.5 and 7.6, we see that the assertion is true in this case too.

Let $\mathcal{L}$ be the class of all classical groups L with $t(L) \geqslant 23$. In what follows, L is always a group lying in this class. Note that the equality $t(L) = t(S)$ implies that the nonabelian composition factor S of G also lies in $\mathcal{L}$. We divide $\mathcal{L}$ on several subclasses, according to the behavior of the function ζ_L. We write $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where

$$\mathcal{X}_1 = \{L \in \mathcal{X} \mid L = L_n^{\varepsilon}(q)\};$$

$$\mathcal{X}_2 = \{L \in \mathcal{X} \mid L = O^{\varepsilon}_{2n}(q), n \equiv 1 \pmod 2\}.$$

Note that $\mathcal{X}$ joins all groups L from $\mathcal{L}$ such that ζ_L is injective.

Furthermore, put $\mathcal{Y} = \mathcal{L} \setminus \mathcal{X} = \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$, where

$$\begin{aligned}\mathcal{Y}_1 = \{L \in \mathcal{Y} \mid L = S_{2n}(q), O_{2n+1}(q) \text{ and } n \equiv 0, 3 \pmod 4, \text{ or}\\ L = O^{-}_{2n}(q) \text{ and } n \equiv 2 \pmod 4\};\end{aligned}$$

$$\begin{aligned}\mathcal{Y}_2 = \{L \in \mathcal{Y} \mid L = S_{2n}(q), O_{2n+1}(q) \text{ and } n \equiv 2 \pmod 4, \text{ or}\\ L = O^{+}_{2n}(q) \text{ and } n \equiv 0 \pmod 4\};\end{aligned}$$

$$\begin{aligned}\mathcal{Y}_3 = \{L \in \mathcal{Y} \mid L = S_{2n}(q), O_{2n+1}(q) \text{ and } n \equiv 1 \pmod 4, \text{ or}\\ L = O^{+}_{2n}(q) \text{ and } n \equiv 2 \pmod 4, \text{ or } L = O^{-}_{2n}(q) \text{ and } n \equiv 0 \pmod 4\}.\end{aligned}$$

Observe that L belongs to $\mathcal{Y}_i$ if and only if $t(L) - i \notin T(L)$.

It is easy to see that we have the partitions:

$$\mathcal{L} = \mathcal{X} \sqcup \mathcal{Y} = \mathcal{X}_1 \sqcup \mathcal{X}_2 \sqcup \mathcal{Y}_1 \sqcup \mathcal{Y}_2 \sqcup \mathcal{Y}_3.$$

Lemma 7.8. *If $t \geqslant 23$, then for every natural $a \leqslant 6$, we have $t - a > (2t+2)/3$.*

Proof. The inequality $t - a < (2t+2)/3$ is equivalent to $a < (t-2)/3$.

Lemma 7.9. *If $i = 1, 2, 3$ and $S \in \mathcal{Y}_i$, then $L \in \mathcal{Y}_i$. In particular, if $L \in \mathcal{X}$, then $S \in \mathcal{X}$.*

Proof. Assume that the conclusion is false. Choose $i \in \{1, 2, 3\}$ and write $x = t - i$. By assumption, $L \notin \mathcal{Y}_i$, therefore, $x \in T(L)$ by Lemmas 7.3–7.6. On the other hand, $x = t - i > (2t+2)/3$ by Lemma 7.8, and so Lemmas 7.5 and 7.6 yield $x \notin T(S) \cup \{(2t+1)/3, (2t+2)/3\}$. This contradicts Lemma 7.7.

Our next goal is to show that p does not divide $|K|$ and, in the case $S = L^{\varepsilon}_m(u)$, that it does not divide $\varepsilon u - 1$ either. For this purpose, we need the following result.

Lemma 7.10. *Let $j \in N(L) \cap M(L)$. There is a natural number i such that $r_i(q)$ is large with respect to L, $\varphi(r_i(q), L) < 2n/3$, $r_i(q)r_j(q)$ lies in $\omega(L)$, and $pr_i(q)r_j(q)$ does not. If, in addition, $L = L_n^\varepsilon(q)$ and $\nu_\varepsilon(j) < (n-1)/2$, or $L = S_{2n}(q), O_{2n+1}(q)$ and $n-\eta(j)$ is odd, or $L = O_{2n}^\varepsilon(q)$ and $\eta(j) < (n-1)/2$, then there are two distinct i and i' satisfying these conditions, and such that $r_i(q)r_{i'}(q) \notin \omega(L)$.*

Proof. Our proof repeatedly uses Lemma 2.13, and we apply this lemma without further mention.

If $L = L_n^\varepsilon(q)$, then $i = \nu_\varepsilon(n - \nu_\varepsilon(j))$ is the desired number. If, in addition, $\nu_\varepsilon(j) < (n-1)/2$, then $i' = \nu_\varepsilon(n-1-\nu_\varepsilon(j))$ also has the desired properties.

Let $L = S_{2n}(q), O_{2n+1}(q)$ and write $a = n - \eta(j)$. Then $i = 2a$ is the desired number. If a is odd, then $i' = a$ also has the desired properties, since $\eta(i') = \eta(i) = a$.

Let $L = O_{2n}^\varepsilon(q)$ and $\eta(j) < n/2-1$. Writing $a = n-1-\eta(j)$, we see that $i = 2a$ has the desired properties, and if a is odd, then so does $i' = a$. If a is even, then $a+1 = n-\eta(j)$ is odd. If $j = \eta(j)$ and $L = O_{2n}^+$, or $j = 2\eta(j)$ and $L = O_{2n}^-$, then $i' = a+1$ is the desired number. And if $j = 2\eta(j)$ and $L = O_{2n}^+$, or $j = \eta(j)$ and $L = O_{2n}^-$, then so is $i' = 2(a+1)$. Now suppose that $\eta(j) = n/2-1$. If $n \equiv 0 \pmod 4$, then $a = n/2$ is even, and we may choose the required numbers i and i' in a similar manner. If $n \equiv 2 \pmod 4$, then $L = O_{2n}^+$ (otherwise $r_j(q)$ is large with respect to L), and hence $i = n/2$ and $i' = n+1$ are the desired numbers. Finally, let $\eta(j) = (n-1)/2$. Since $r_j(q)$ is small, the only possibility is that $n \equiv 3 \pmod 4$ and, moreover, $L = O_{2n}^+(q)$, $j = 2\eta(j) = n-1$ or $L = O_{2n}^-(q)$, $j = \eta(j) = (n-1)/2$. In both cases $i = n+1 = 2(n-\eta(j))$ has the desired properties.

Lemma 7.11. *The order of K is not divisible by p.*

Proof. We derive a contradiction by assuming that p divides the order of the soluble radical K, which is nilpotent by Proposition 3. Let P be a Sylow p-subgroup of K, and let V be the factor group $P/\Phi(P)$. The group S acts on V via conjugation. If this action is not faithful, then p is adjacent to all primes that are large with respect to L, which is not the case. Thus S acts faithfully on V.

By Proposition 3 and Lemma 2.6, we may assume that $L \in \{S_{2n}(q), O_{2n+1}(q) \mid n \equiv 0 \pmod 2\}$. Suppose first that $n \equiv 0 \pmod 4$, and choose $s \in \pi(L)$ so that $\varphi(s, L) = \eta(e(s,q)) = (n-2)/2$. By Lemma 7.4, it follows that $t(s,L) = [(3\eta(e(s,q)) + 2)/2] = (3n-4)/4 = t-2$. If $n \equiv 2 \pmod 4$, then we choose s so that $\varphi(s,L) = \eta(e(s,q)) = (n-4)/2$, and hence $t(s,L) = [(3e(s,q)+2)/2] = (3n-10)/4 = t-3$. In both cases, we have $e(s,q) \in M(L) \cap N(L)$. By Lemma 7.10, there is a such that $r_a(q)$ is large with respect to L, $\varphi(r_a(q),L) < 2n/3$, $r_a(q)s$ lies in $\omega(L)$, and $pr_a(q)s$ does not, and we write $r = r_a(q)$ and $i = e(r,u)$.

Lemma 7.1 yields $x = t(s,S) = t(s,L) \in \{t-2, t-3\}$, and in particular, $x \in T(S)$. Therefore $j = e(s,u) \in M(S) \cap N(S)$ and $m/3 < \varphi(s,S) < m/2$. Since r is large with respect to L, it is also large with respect to S. As $rs \in \omega(L)$ and rs does not divide $|K| \cdot |\overline{G}/S|$, it follows that $rs \in \omega(S)$.

Suppose first that $\varphi(s,S)+\varphi(r,S) > m$. If S is symplectic or orthogonal, then adjacency of r and s in $GK(S)$ implies that i/j is an odd integer. Since r is large with respect to S and s is small, we have $i \neq j$. Therefore $i \geqslant 3j$, whence $\eta(i) \geqslant 3\eta(j) > 3m/3 = m$, which is a contradiction. Let $S = L_m^{\varepsilon}(u)$. Then adjacency of r and s in $GK(S)$ together with the inequality $\varphi(s,S)+\varphi(r,S) > m$ yields $\nu_\varepsilon(i) = 2\nu_\varepsilon(j)$. In particular, $\nu_\varepsilon(i)$ is even. As s is small with respect to S, we have $\nu_\varepsilon(j) \neq m/2$. If $\nu_\varepsilon(j) = (m-1)/2$, then $t(s,S) = t-1 \notin \{t-2, t-3\}$, which contradicts the choice of s. Thus $\nu_\varepsilon(i) = 2\nu_\varepsilon(j) < m-1$. By [37, Lemma 5] and [20, Lemma 5], there is a subgroup of S that is a Frobenius group with kernel being a v-group and complement being a cyclic group of order $|(\varepsilon u)^{\nu_\varepsilon(i)} - 1|/d$, where $\pi(d) \subseteq \pi(u^2-1)$, and in particular, of order divisible by rs. Applying Lemma 3.4 to this subgroup of S acting on $V = P/\Phi(P)$, we conclude that $prs \in \omega(G)$, which contradicts the choice of r and s. Thus $\varphi(r,S) \leqslant m - \varphi(s,S) < 2m/3$.

Now observe that we chose s so that $n - \eta(e(s,q))$ is odd. By Lemma 7.10, there are at least two large with respect to L and nonadjacent numbers r and w such that sr and sw lie in $\omega(L)$, and psr and psw do not. For definiteness, we assume that $\varphi(r,S) \leqslant \varphi(w,S)$. It follows by the result of the previous paragraph that $\varphi(r,S) \leqslant \varphi(w,S) \leqslant m - \varphi(s,S)$.

Writing $k = \varphi(s,S)$, we have $m/3 < k < m/2$. By [50, Propositions 4.1.3, 4.1.4, 4.1.6], S contains a central product of subgroups $\overline{A}$ and $\overline{B}$ having nonabelian composition factors A and B, respectively, such that A and B are also simple classical groups over the same field of order u. The groups $\overline{A}$ and $\overline{B}$ can be chosen as follows. If $S = L_m^{\varepsilon}(u)$, then $A \simeq L_k^{\varepsilon}(u)$ and $B \simeq L_{m-k}^{\varepsilon}(u)$. If $S = S_{2m}(u)$, then $A \simeq S_{2k}(u)$ and $B \simeq S_{2(m-k)}(u)$. If $S = O_{2m+1}(u)$ and $j = k$, then $A \simeq O_{2k}^{+}(u)$ and $B \simeq O_{2(m-k)+1}(u)$. If $S = O_{2m+1}(u)$ and $j = 2k$, then $A \simeq O_{2k}^{-}(u)$ and $B \simeq O_{2(m-k)+1}(u)$. If $S = O_{2m}^{\varepsilon}(u)$ and $j = k$, then $A \simeq O_{2k}^{+}(u)$ and $B \simeq O_{2(m-k)}^{\varepsilon}(u)$. If $S = O_{2m}^{\varepsilon}(u)$ and $j = 2k$, then

$A \simeq O^-_{2k}(u)$ and $B \simeq O^{-\varepsilon}_{2(m-k)}(u)$.

By our choice, it follows that $s \in \pi(A)$. We claim that $r, w \in \pi(B)$. If $S \neq O^{\varepsilon}_{2m}(u)$, then since $\varphi(r, S) \leqslant \varphi(w, S) \leqslant m-k$, we have $r, w \in \pi(B)$. Let $S = O^+_{2m}(u)$ and $j = k$. If $\varphi(w, S) < m - k$, then $r, w \in \pi(B)$. Suppose that $\varphi(w, S) = m - k$. As $sw \in \omega(S)$, the adjacency criterion yields $e(w, u) = \varphi(w, S)$, and therefore, $w \in \pi(B)$. If $\varphi(r, S) = \varphi(w, S) = m - k$, then by similar reasoning, $e(r, u) = \varphi(r, S) = e(w, u)$, which is not the case because $rw \notin \omega(L)$. Thus $\varphi(r, S) < \varphi(w, S)$ and $r \in \pi(B)$. The other cases can be handled in a similar manner.

The numbers s, r, and w are coprime to $u^2 - 1$, and hence to the orders of the centers of $\overline{A}$ and $\overline{B}$ either. Therefore, s divides $|A|$, while r and w divide $|B|$ and are large with respect to B. As r and w are not adjacent in $GK(L)$, they are not adjacent in $GK(B)$ either, and by Lemma 3.8, at least one of them must divide the order of some proper parabolic subgroup F of B. For definiteness, we assume that this number is r (there is no loss in making this assumption, since we will not use the condition $\varphi(r, S) \leqslant \varphi(w, S)$ or the number w itself). Let y be an element of order r lying in the preimage of F in $\overline{B}$, and let x be an element of order s lying in $\overline{A}$. We again consider the action of S on V via conjugation. By the choice of x, it clearly lies in some proper parabolic subgroup of S. By Lemmas 3.6 and 3.7, the degree of the minimal polynomial of x on V is equal to s, and therefore, its centralizer U in V is nontrivial. Since $\overline{B}$ acting on V normalizes U, we may consider its action on U. If the kernel J of this action does not lie in $Z(\overline{B})$, then its image in the factor group $\overline{B}/Z(\overline{B})$ includes B, so, in particular, y centralizes U. If $J \leqslant Z(\overline{B})$, then B acts faithfully on U, and again by Lemmas 3.6 and 3.7, the centralizer $C_U(y)$ is not trivial. In both cases, there is $z \in U$ such that $z^y = z$. Therefore, the element $g = zxy$ of the natural semidirect product $V \rtimes S$ has order psr. By Lemma 3.1, the group $\widetilde{G} = G/O_{p'}(K)\Phi(P)$ has an element of the same order, and therefore so does G. On the other hand, by our choice of s and r, there is no element of order psr in L, a contradiction.

Lemma 7.12. *If $S = L^{\varepsilon}_m(u)$, then p does not divide $\varepsilon u - 1$.*

Proof. By Lemmas 7.3–7.6, we can choose a prime $s \in \pi(L)$ with $e(s, q) \in M(L) \cap N(L)$ so that $(2t+2)/3 < t(s, L) < t-1$, and if $L \in \{S_{2n}(q), O_{2n+1}(q)\}$, then also $n - \varphi(s, L)$ is odd. By Lemma 7.10, there are at least two large with respect to L and nonadjacent numbers r and w such that $sr, sw \in \omega(L)$, but $psr, psw \notin \omega(L)$.

As in the proof of the previous lemma, if $\varphi(r,S)+\varphi(s,S)>m$, then $\varphi(r,S)=2\varphi(s,S)$. As $t(s,S)=t(s,L)<t-1$, it follows that $i=\varphi(r,S)<m-1$. By [39, Corollary 3], the set $\omega(S)$ contains a number $[(\varepsilon u)^i-1,\varepsilon u-1]$, which is divisible by prs, and this contradicts the choice of r and s. Therefore we may assume that $\varphi(r,S)\leqslant\varphi(w,S)\leqslant m-\varphi(s,S)$. Since $rw\notin\omega(S)$ and S is linear or unitary, we have $\varphi(r,S)<\varphi(w,S)$, and hence $\varphi(r,S)+\varphi(s,S)<m$. Writing $i=\varphi(r,S)$ and $j=\varphi(s,S)$, by [39, Corollary 3] we conclude that S has an element of order $[(\varepsilon u)^i-1,(\varepsilon u)^j-1,\varepsilon u-1]$, which is divisible by prs. This contradiction completes the proof.

Proposition 10. *The number p divides $|S|$, and $l=t(p,S)=t(p,L)\in\{2,3,4\}$. Furthermore, $k=e(p,u)$ lies in the set $K(l,S)$ defined in Table* 4.

PROOF. Lemmas 7.11, 7.12 and Proposition 9 imply that p divides $|S|$ and $l=t(p,S)=t(p,L)$. Lemma 2.6 yields $l\in\{2,3,4\}$. The final assertion follows by Lemma 2.9 and Table 3.

Table 4: The set $K(l,S)$

S	$l=2$	$l=3$	$l=4$
$L_m(u)$	$\{2\}$	$\{3\}$	$\{4\}$
$U_m(u)$	$\{1\}$	$\{6\}$	$\{4\}$
$Sp_{2m}(u)$ $O_{2m+1}(u)$	$\{1,2\}$	$\{4\}$, if $m\equiv 2,3\,(\mathrm{mod}\,4)$	$\{4\}$, if $m\equiv 0,1,5,8,9\,(\mathrm{mod}\,12)$ $\{3,6\}$, if $m\equiv 10\,(\mathrm{mod}\,12)$ $\{3,4,6\}$, if $m\equiv 4\,(\mathrm{mod}\,12)$
$O^+_{2m}(u)$	$\{1,2\}$	$\{4\}$, if $m\not\equiv 1\,(\mathrm{mod}\,4)$	$\{3,6\}$, if $m\equiv 4\,(\mathrm{mod}\,6)$ $\{4\}$, if $m\equiv 1,9\,(\mathrm{mod}\,12)$ $\{6\}$, if $m\equiv 11\,(\mathrm{mod}\,12)$ $\{4,6\}$, if $m\equiv 5\,(\mathrm{mod}\,12)$
$O^-_{2m}(u)$	$\{1,2\}$	$\{4\}$, if $m\equiv 3\,(\mathrm{mod}\,4)$	$\{4\}$, if $m\not\equiv 3,5,7,11\,(\mathrm{mod}\,12)$ $\{3\}$, if $m\equiv 11\,(\mathrm{mod}\,12)$ $\{3,4\}$, if $m\equiv 5\,(\mathrm{mod}\,12)$

Let j and k be natural numbers and $j\geqslant k$. Observe that j/k is an odd integer if and only if $j\equiv k\,(\mathrm{mod}\,2k)$.

Lemma 7.13. *Let $k = e(p, u)$. Suppose that $s, r \in \pi(L) \setminus \{p\}$ are different primes such that $(sr, u(u^2-1) \cdot |K| \cdot |\overline{G}/S|) = 1$, $sr \in \omega(L)$, and $psr \notin \omega(L)$, and suppose that $j = e(s, u)$ and $i = e(r, u)$. If $S = L_n^\varepsilon(u)$, then neither $\nu_\varepsilon(j)$ nor $\nu_\varepsilon(i)$ is divisible by $\nu_\varepsilon(k)$. If S is symplectic or orthogonal, then neither i nor j is congruent to k modulo $2k$. In particular, if $a \in M(L) \cap N(L)$ and $j = e(r_a(q), u)$, then $\nu_\varepsilon(j)$ is not divisible by $\nu_\varepsilon(k)$ when $S = L_n^\varepsilon(u)$, and j is not congruent to k modulo $2k$ when S is symplectic or orthogonal.*

Proof. First, suppose that $S = L_m^\varepsilon(u)$. To avoid unwieldy notation, we assume that S is a linear group, that is ν_ε is the identity function. The proof for unitary groups is analogous, we have only to use the function ν instead. Recall that by Lemma 7.12, the number p does not divide $u-1$, that is we have $k \neq 1$. It follows from the equality $(sr, u(u^2-1) \cdot |K| \cdot |\overline{G}/S|) = 1$ that S has a semisimple element of order sr. Now Lemma 2.13 implies that S has an element of order $[u^j-1, u^i-1]/d$, where d is some divisor of $u-1$. If k divides either of j and i, then prs divides $[u^j-1, u^i-1]/d$, which contradicts the fact that $prs \notin \omega(L)$.

Now let S be a symplectic or orthogonal group. Recall that $p \neq 2$. The equality $(sr, u(u^2-1) \cdot |K| \cdot |\overline{G}/S|) = 1$ implies that S has a semisimple element of order sr. By Lemma 2.13, S has an element of order $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i]/d$, where d divides 4. Assume that one of the numbers j and i, say j, is congruent to k modulo $2k$. Then $u^{\eta(k)} + (-1)^k$ divides $u^{\eta(j)} + (-1)^j$, and hence prs divides $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i]/d$, contrary to the hypothesis.

Let $a \in M(L) \cap N(L)$ and let $j = e(r_a(q), u)$. By Lemma 7.10, there is a number b such that $r_b(q)$ is large with respect to L, $r_a(q)r_b(q)$ lies in $\omega(L)$, and $pr_a(q)r_b(q)$ does not. Writing $s = r_a(q)$, $r = r_b(q)$ and observing that $(sr, u(u^2-1) \cdot |K| \cdot |\overline{G}/S|) = 1$, we see that the assertion of the lemma holds for $j = e(r_a(q), u) = e(s, u)$.

Lemma 7.14. *If $L \in \mathcal{X}$, then the conclusion of Theorem 3 holds.*

Proof. Let $L \in \mathcal{X}$. Then Lemma 7.9 implies that S also lies in $\mathcal{X}$. Suppose that $S = L_m^\varepsilon(u)$. Since $L \in \mathcal{X}$, we have $t(p, L) = 3$, and hence $k = e(p, u) = \nu_\varepsilon(3)$ (see Table 4). One of the numbers $t-1$, $t-2$, $t-3$ is a multiple of 3, and we denote this number by c. By Lemma 7.8, we have $(2t+2)/3 < c < t$, and so $c \in T(L)$. Therefore, there is $a \in M(L) \cap N(L)$ such that $\zeta_L(a) = c$. Then $c = t(r_a(q), L) = t(r_a(q), S)$ due to Lemma 7.1. By Lemma 7.3, the function ζ_S is injective and $\zeta_S(\nu_\varepsilon(c)) = c$, and hence $j = e(r_a(q), u) = \nu_\varepsilon(c)$. Since $\nu_\varepsilon = \nu_\varepsilon^{-1}$, we see that $\nu_\varepsilon(j) = c$ is divisible by $\nu_\varepsilon(k) = 3$, which is a contradiction by Lemma 7.13.

Let S be an orthogonal group lying in $\mathcal{X}$. Then $k = e(p, u) = 4$. By Lemmas 7.5 and 7.6, the set $C = \{t-x \mid x = 1, 2, \dots, 6\}$ contains c such that $t(r_j(u), S) = c$ and $j \equiv 4 \pmod 8$. Since $C \subseteq T(L)$, it follows that $c \in T(L)$. Thus there is $a \in M(L) \cap N(L)$ such that $\zeta_L(a) = c$. Then $t(r_a(q), S) = c$, and hence $e(r_a(q), u) = j$, which is not the case by Lemma 7.13.

Lemma 7.15. *If $S \in \mathcal{X}_1$, then the conclusion of Theorem 3 holds.*

Proof. Let $k = e(p, u)$. Suppose that there is $c \in T(L)$ such that $\nu_\varepsilon(k)$ divides c. As in the previous lemma, there is $a \in M(L) \cap N(L)$ such that $t(r_a(q), S) = c$, and by Lemma 7.3, it follows that $j = e(r_a(q), u) = \nu_\varepsilon(c)$. Hence $\nu_\varepsilon(j) = c$ is divisible by $\nu_\varepsilon(k)$, which is a contradiction due to Lemma 7.13. Thus it suffices to show that there is $j \in T(L)$ that is a multiple of $\nu_\varepsilon(k)$.

By the previous result, we may assume that $L \in \mathcal{Y}$. In this case, an additional difficulty is that the members of $T(L)$ are not consecutive integers. Nevertheless, for each group L we will prove that $T(L)$ contains a number with the desired property.

Let $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ and n be even. Then $t(p, L) = 2$. Since $S = L_m^\varepsilon(u)$, and therefore, the characteristic p of L does not divide $\varepsilon u - 1$ by Lemma 7.12, it follows that $k = e(p, u) = \nu_\varepsilon(2)$, and hence $\nu_\varepsilon(k) = 2$. If $n \equiv 0 \pmod 4$, then $t-2, t-3 \in T(L)$, and if $n \equiv 2 \pmod 4$, then $t-3, t-4 \in T(L)$. In each case, $T(L)$ contains two consequent numbers, and one of them is a multiple of 2, as required.

Let $L = O_{2n}^-(q)$ and n be even. Then $t(p, L) = 4$, whence $k = e(p, u) = \nu_\varepsilon(4) = 4$. Now the proof is somewhat similar to the proof in the previous paragraph if we take into account the following observation: $T(L)$ contains the numbers $t-2, t-4, t-5, t-7$ when $n \equiv 0 \pmod 4$ and $t-2, t-4, t-5, t-7$ when $n \equiv 2 \pmod 4$ and $n > 34$, and the set of the residues of these numbers module 4 is all of $\{0, 1, 2, 3\}$; furthermore, if $n = 30$, then $t-3 = 23-3 = 20$ is a multiple of 4 and lies in $t(L)$, and if $n = 34$, then so does $t-2 = 26-2 = 24$.

The remaining cases are $L = S_{2n}(q)$, $O_{2n+1}(q)$ with n odd and $L = O_{2n}^+(q)$ with n even, where we have $t(p, L) = 3$, whence $k = e(p, u) = \nu_\varepsilon(3)$ and $\nu_\varepsilon(k) = 3$. If $L = S_{2n}(q)$, $O_{2n+1}(q)$ and $n \equiv 1 \pmod 4$, then $t \equiv 2 \pmod 3$. Thus $t-2$ lies in $T(L)$ and is a multiple of 3. If either $L = S_{2n}(q)$, $O_{2n+1}(q)$

with $n \equiv 3 \pmod 4$ or $L = O_{2n}^+(q)$ with $n \equiv 0 \pmod 4$, then $t \equiv 0 \pmod 3$, and $t-3$ lies in $T(L)$ and is a multiple of 3. If $L = O_{2n}^+(q)$ and $n \equiv 2 \pmod 4$, then $t \equiv 1 \pmod 3$, and $t-1$ is the desired number.

Now we may assume that $L \in \mathcal{Y}$ and $S \in \mathcal{Y} \cup \mathcal{X}_2$, and in particular, both L and S are symplectic or orthogonal groups. Moreover, by Lemma 7.9, each $i \in \{1,2,3\}$ satisfies the following condition: if $L \in \mathcal{Y}_i$, then $S \in \mathcal{Y}_i \cup \mathcal{X}_2$. Also observe that $[(3x+2)/2]$ is an injective function, and hence $\eta(i)$ is uniquely determined by $\zeta_L(i)$. Furthermore, if $i \equiv 0 \pmod 4$, then i is uniquely determined by $\eta(i)$, and so by $\zeta_L(i)$ as well.

Lemma 7.16. *If $t(p,L) = 3$, then the conclusion of Theorem 3 holds.*

Proof. Let $t(p,L) = 3$. Then either $L = S_{2n}(q)$, $O_{2n+1}(q)$ with n odd or $L = O_{2n}^+(q)$ with n even. Furthermore, since S is symplectic or orthogonal, we have $k = e(p,u) = 4$. Also note that if $S = S_{2m}(u)$, $O_{2m+1}(u)$, then $m \equiv 2,3 \pmod 4$; if $S = O_{2m}^+(u)$, then $m \not\equiv 1 \pmod 4$; and if $S = O_{2m}^-(u)$, then $m \equiv 3 \pmod 4$ (see Table 4).

Let $L = S_{2n}(q)$, $O_{2n+1}(q)$ and $n \equiv 1 \pmod 4$. Suppose that $S = S_{2m}(u)$ or $S = O_{2m+1}(u)$. Since $t(L) = t(S)$, it follows that $m \in \{n, n+1\}$. Now the congruence $m \equiv 2,3 \pmod 4$ yields $m = n+1$. But then $S \in \mathcal{Y}_2$, which is not the case because $L \in \mathcal{Y}_3$. If $S = O_{2m}^+(u)$, then for every m, we have that $t(S)$ is not congruent to 2 modulo 3. On the other hand, $t(L) \equiv 2 \pmod 3$, and hence $S \neq O_{2m}^+(u)$. Similarly, $S \neq O_{2m}^-(u)$, since otherwise $m \equiv 3 \pmod 4$ and $t(S) \equiv 0 \pmod 3$.

Let $L = S_{2n}(q)$, $O_{2n+1}(q)$ and $n \equiv 3 \pmod 4$. Suppose that $S = S_{2m}(u)$ or $S = O_{2m+1}(u)$. The equality $t(L) = t(S)$ yields $m = n$. Both $n-3$ and $n-7$ are divisible by 4, therefore, one of them is congruent to 4 modulo 8. Denote this number by a. Since $t(r_{n-3}(q), L) = t-2$ and $t(r_{n-7}(q), L) = t-5$, we have $x = t(r_a(q), L) > 2t/3$, whence $x \in T(L)$. Thus $t(r_a(q), S) = x$. As ζ_S is invertible on the set of multiples of 4 and S has the same type as L, it follows that $e(r_a(q), u)$ is equal to a, and so it is congruent to 4 modulo 8. Applying Lemma 7.13, we derive a contradiction. Thus S is an orthogonal group of even dimension. If $m = n$, then $S = O_{2n}^\varepsilon(u)$. By Lemmas 7.4–7.6, both $t(r_{n-3}(q), L)$ and $t(r_{n-3}(u), S)$ are equal to $t-2$, so $t-2 = t(r_{n-3}(u), S) = t(r_{n-3}(q), L) = t(r_{n-3}(q), S)$. Similarly, $t-5 = t(r_{n-7}(u), S) = t(r_{n-7}(q), L) = t(r_{n-7}(q), S)$. Repeating the previous argument we derive a contradiction by Lemma 7.13. If $m \neq n$, then the equality $t(L) = t(S)$ implies that the only remaining possibility is $S = O^+_{2n+2}(u)$. Then $S \in \mathcal{Y}_2$, which is not the case because $L \in \mathcal{Y}_1$.

Let $L = O^+_{2n}(q)$ and $n \equiv 2 \pmod 4$. If $S \in \{S_{2m}(u), O_{2m+1}(u)\}$, then $t(L) = t(S)$ yields $m = n-2$, whence $m \equiv 0 \pmod 4$, which is a contradiction. If $S = O^-_{2m}(u)$, then $m \in \{n-2, n-1\}$, and this is also a contradiction since m must be congruent to 3 modulo 4. If $S = O^+_{2m}(u)$, then $m \in \{n-1, n\}$. Since m cannot be congruent to 1 modulo 4, it follows that $m \neq n-1$. Thus S has the same type and the same Lie rank n as L. Both $n-2$ and $n-6$ are multiples of 4, so one of them is congruent to 4 modulo 8, and we denote this number by a. As $t(L) \geqslant 23$, we have $n \geqslant 31$ and $\eta(n-2) > \eta(n-6) = n/2 - 3 > n/3$. Therefore $a \in M(L) \cap N(L)$, and applying Lemma 7.13, we derive a contradiction.

Let $L = O^+_{2n}(q)$ and $n \equiv 0 \pmod 4$. The equality $t(L) = t(S)$ leaves us with two possibilities: either $m = n-1 \equiv 3 \pmod 4$ or $m = n$ and $S = O^+_{2n}(u)$. If S is a symplectic group or an orthogonal group of odd dimension, then $S \in \mathcal{Y}_1$, while $L \in \mathcal{Y}_2$. Suppose that $S = O^+_{2n}(u)$, that is S has the same type and the same Lie rank n as L. Since $n-4$, $n-8$ are multiples of 4, we can choose a number a of them with $a \equiv 4 \pmod 8$. Furthermore, $\eta(n-4) > \eta(n-8) = n/2 - 4 > n/3$ because $t(L) \geqslant 23$ and so $n \geqslant 31$. Thus $a \in M(L) \cap N(L)$, and applying Lemma 7.13, we derive a contradiction.

The remaining case for $L = O^+_{2n}(q)$ with $n \equiv 0 \pmod 4$, is $S = O^\varepsilon_{2(n-1)}(u)$, and this case requires the most effort. Let $s = r_{n-4}(q)$ and $a = n-1-\eta(n-4) = (n+2)/2$. Similarly to the proof of Lemma 7.10 we conclude that $r_1 = r_a(q)$ and $r_2 = r_{2a}(q)$ have the following properties: for $i = 1, 2$, the number r_i is large with respect to L, $sr_i \in \omega(L)$, and $psr_i \notin \omega(L)$. Since $n \equiv 0 \pmod 4$, we conclude that $r_3 = r_{n+4}(q) = r_{2(a+1)}(q)$ has the same properties. Now r_1, r_2, r_3 constitute a coclique in $GK(L)$ because for any $i, j \in \{1, 2, 3\}$ we have $\varphi(r_i, L) > n/2$ and $e(r_i, q) \neq e(r_j, q)$ whenever $i \neq j$. Therefore these numbers are large with respect to S and constitute a coclique in $GK(S)$. Since ζ_S is injective and $t(s, S) = t(s, L) = t - 3$, the value of $e(s, u)$ depends only on $e(s, q)$. If $S = O^+_{2(n-1)}(u)$, then $j = e(s, u) = (n-6)/2$, and if $S = O^-_{2(n-1)}(u)$, then $j = e(s, u) = n - 6$. In both cases, $\eta(e(s, u)) = \eta(j)$ is odd. Let $r \in \{r_1, r_2, r_3\}$ and write $i = e(r, u)$. As $rs \in \omega(S)$, we have $\eta(i) \leqslant m - \eta(j)$. If $\eta(i) = m - \eta(j)$, then since m is odd, it follows that i is even. The condition $rs \in \omega(S)$ implies that S has an element of order $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i]/2$, which is not the case because i and j have opposite parity when $S = O^+_{2m}(u)$, and the same parity when $S = O^-_{2m}(u)$. Thus $\eta(i) < m - \eta(j)$. If $\eta(i) < m - \eta(j) - 2$, then S has an element of order $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i, u^2 + 1, u + (-1)^{i+1}]$, which is divisible by prs, contrary to the fact that $prs \notin \omega(L)$. Let $\eta(i) = m - \eta(j) - 2$. Then i is even, and hence S has an element of order $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i, u^2 + 1]$, which is divisible by prs. Finally, let $\eta(i) = m - \eta(j) - 1$. But then $e(r, u)$ has only two different possible values, and this is a contradiction since the numbers $e(r_i, u)$ with $i = 1, 2, 3$ must be distinct.

Lemma 7.17. *If $t(p, L) = 2$, then the conclusion of Theorem 3 holds.*

Proof. If $t(p, L) = 2$, then $L = S_{2n}(q), O_{2n+1}(q)$ and n is even. Since S is symplectic or orthogonal, we have $k = e(p, u) \in \{1, 2\}$.

Suppose $n \equiv 2 \pmod 4$. Then $L \in \mathcal{Y}_2$. The equality $t(L) = t(S)$ implies that $S = S_{2n}(u), O_{2n+1}(u)$. Let $j = n/2 - 2$ and $s = r_j(q)$. Observe that $\eta(j) = j$ is odd. As in the proof of Lemma 7.10, we write $a = n - \eta(j) = n/2 + 2$. Then $r_1 = r_a(q)$ and $r_2 = r_{2a}(q)$ have the following properties: for $i = 1, 2$, the number r_i is large with respect to L, $sr_i \in \omega(L)$, and $psr_i \notin \omega(L)$. Furthermore, r_1 and r_2 are not adjacent in $GK(L)$. Since $t(s, S) = t(s, L)$ and S has the same type and the same Lie rank as L, it follows that $\eta(e(s, u)) = \eta(e(s, q)) = j$. Let $r \in \{r_1, r_2\}$ and write $i = e(r, u)$. As $rs \in \omega(S)$, we have $\eta(i) \leqslant n - \eta(j)$. If $\eta(i) < n - \eta(j)$, then S contains elements of orders $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i, u - 1]$ and $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i, u + 1]$, one of which must be divisible by prs because p divides either $u - 1$ or $u + 1$. But then $prs \in \omega(S) \setminus \omega(L)$, a contradiction. Thus $\eta(i) = n - \eta(j) = a$. Since a is odd, there are two possible values for $e(r, u)$, and these are a and $2a$. As $e(r_1, u) \neq e(r_2, u)$, we have $\{e(r_1, u), e(r_2, u)\} = \{a, 2a\}$. If $k = 1$, then $a \equiv k \pmod{2k}$, and if $k = 2$, then $2a \equiv k \pmod{2k}$. We denote by r the number in the set $\{r_1, r_2\}$ for which $i = e(r, u) \equiv k \pmod{2k}$. Now s and r satisfy the hypothesis of Lemma 7.13, which is a contradiction because $i \equiv k \pmod{2k}$.

Now suppose that $n \equiv 0 \pmod 4$. The conditions $t(L) = t(S)$ and $L \in \mathcal{Y}_1$ leave us with two further possibilities: either $S = S_{2n}(u), O_{2n+1}(u)$ or $S = O^{\varepsilon}_{2m}(u)$ with $m = n+1$. In the first case, we use the argument of the previous paragraph with $j = n/2 - 1$ and $a = n - \eta(j) = n/2 + 1$. Now assume that $S = O^{\varepsilon}_{2(n+1)}(u)$ and write $b = n/2 - 1$, $s = r_b(q)$, $a = n - b = n/2 + 1$, $r_1 = r_a(q)$, and $r_2 = r_{2a}(q)$. Since $\eta(b) = b$ is odd, it follows that r_1 and r_2 satisfy the conclusion of Lemma 7.10, that is r_1 and r_2 are not adjacent in $GK(L)$, they are large with respect to L, and for $i = 1, 2$ the number $r_i s$ belongs to $\omega(L)$, but $pr_i s$ does not. Let $r \in \{r_1, r_2\}$, $i = e(r, u)$, and $j = e(s, u)$. Then the equality $t(s, S) = t(s, L) = t - 2$ yields $j = m - 3$ when $S = O^+_{2m}(u)$, and $j = (m-3)/2$ when $S = O^-_{2m}(u)$. As $rs \in \omega(S)$, it follows that $\eta(i) \leqslant m - \eta(j)$. If $\eta(i) < m - \eta(j)$, then $\omega(S)$ contains $[u^{\eta(j)} + (-1)^j, u^{\eta(i)} + (-1)^i, u + (-1)^{i-1}]$ which is divisible by the odd part of $u^2 - 1$, and so by prs, which is a contradiction. Thus since $m \equiv 1 \pmod 4$, the number $\eta(i) = m - \eta(j) = m - (m-3)/2 = (m+3)/2$ is even, and therefore there is only one possible value for $e(r, u)$, namely, $m+3$. But then $e(r_1, u) = e(r_2, u)$, a contradiction.

Lemma 7.18. *If $t(p, L) = 4$, then the conclusion of Theorem 3 holds.*

Proof. Note that the equality $t(p, L) = 4$ holds if and only if $L = O^-_{2n}(q)$ and n is even.

Suppose that $n \equiv 0 \pmod 4$. If $S = S_{2m}(u)$ or $S = O_{2m+1}(u)$, then $t(L) = t(S)$ yields $m = n$. But then $S \in \mathcal{Y}_1$ and $L \in \mathcal{Y}_3$, a contradiction. If $S = O^-_{2m}(u)$, then $m \in \{n, n+1\}$. Suppose that $m = n$. Then $k = e(p, u) = 4$. Since $a = n-4$ and $b = n-8$ lie in $M(L) \cap N(L)$ and are multiples of 4, it follows that one of the numbers $e(r_a(q), u) = e(r_a(q), q) = a$ and $e(r_b(q), u) = e(r_b(q), q) = b$ is congruent to 4 modulo 8. But this contradicts Lemma 7.13. If $S = O^+_{2m}(u)$, then $m \in \{n+1, n+2\}$. Let $m = n+2$. Then $m \equiv 2 \pmod 4$, and, on the other hand, it follows from Table 4 that $m \equiv 4 \pmod 6$. Thus $m \equiv 10 \pmod{12}$, and hence $m = 12c + 10$, $n = 12c + 8$ for some integer c. Writing $X = \{a \mid n/2 \leqslant \eta(a) < 2n/3\}$ and noting that $n/2 = 6c + 4$ is even, we conclude that $|X| = [3((8c+6) - (6c+4))/2] = 3c + 3$ by Lemma 1.8. There is a coclique ρ of size $|X|$ in $GK(L)$ such that $e(r, q) \in X$ for every $r \in \rho$. Let $r \in \rho$. The prime r is large with respect to L, and so r is large with respect to L too, whence $\varphi(r, S) \geqslant m/2$ (see Table 1). Furthermore, there is $b \in M(L) = N(L)$ such that $rr_b(q) \in \omega(L)$. Since $e(r_b(q), u) \in N(S)$ and $N(S) = M(S)$, we have $\varphi(r, S) \leqslant m - \varphi(r_b(q), S) < 2m/3$. Thus writing $Y = \{a \mid m/2 \leqslant \eta(a) < 2m/3\}$, we see that $e(r, u) \in Y$ for every $r \in \rho$. By Lemma 1.8, the size of Y is equal to $[(3((8c+7) - (6c+5)) + 1)/2] = 3c + 3 = |X|$, and therefore $\{e(r, u) \mid r \in \rho\} = Y$. It follows that ρ contains r and r' such that $e(r, u) = m/2$ and $e(r', u) = m$. But then $rr' \in \omega(S)$, a contradiction.

It remains to consider the situation where $S = O^{\varepsilon}_{2m}(u)$, $m = n + 1$, and either $k = e(p, u) = 4$ or $m \equiv 5 \pmod{12}$ and $(\varepsilon, k) \in \{(+, 6), (-, 3)\}$.

First, assume that $m \equiv 5 \pmod{12}$ and $k \neq 4$. Observe that the congruence and the condition $t \geqslant 23$ imply that $m = n + 1 \geqslant 45$. In particular, we have $(n + 12)/2 > n/3$, and so $n-4, n-8, n-12 \in M(L) \cap N(L)$ with $t(r_{n-4}(q), L) = t - 2$, $t(r_{n-8}(q), L) = t - 5$, and $t(r_{n-12}(q), L) = t - 8$. If $S = O^+_{2m}(u)$, then it follows that the numbers $e(r_{n-4}(q), u) = m - 3$, $e(r_{n-8}(q), u) = m - 7$, and $e(r_{n-4}(q), u) = m - 11$ are congruent to 2 modulo 4. Moreover, they have different residues modulo 3, and hence one of them is congruent to 6 modulo 12. We denote this number by j and take a to be such that $e(r_a(q), u) = j$. Applying Lemma 7.13 to $a \in M(L) \cap N(L)$, we conclude that $j \not\equiv 6 \pmod{12}$, a contradiction. If $S = O^-_{2m}(u)$, then the numbers $e(r_{n-4}(q), u) = (m - 3)/2$, $e(r_{n-8}(q), u) = (m - 7)/2$, and $e(r_{n-4}(q), u) = (m - 11)/2$ are odd and one of them is a multiple of 3. Since $k = 3$, we again derive a contradiction by Lemma 7.13. Thus we may assume that $k = e(p, u) = 4$. Let $s_1 = r_{(n-2)/2}(q)$, $s_2 = r_{n-2}(q)$, $r_1 = r_{n+2}(q)$, $r_2 = r_{(n+2)/2}$, and $w = r_n(q)$. It follows that $(n-2)/2, n-2 \in M(L) \cap N(L)$, the primes r_1, r_2, w are large with respect to L and for $l = 1, 2$, we have $s_l r_l, s_l w \in \omega(L)$, but $p s_l r_l, p s_l w \notin \omega(L)$. Furthermore, $t(s_1, L) = t(s_2, L) = t - 1 = t(s_1, S) = t(s_2, S)$. Therefore, $j = e(s_1, u) = e(s_2, u)$ is equal to $(m - 3)/2$ when $S = O^+_{2m}(u)$ and to $m - 3$ when $S = O^-_{2m}(u)$. Let $r \in \{r_1, r_2, w\}$ and $i = e(r, u)$. As for $l = 1, 2$, we have $s_l r_l, s_l w \in \omega(S)$, it follows that $\eta(i) \leqslant m - \eta(m - 3) = m - \eta((m - 3)/2) = (m + 3)/2$. If $\eta(i) = (m + 3)/2$, then $\eta(i)$ is even, and so $i = m + 3$. But then $i + 2\eta(j) = 2\eta(i) + 2\eta(j) = 2m$ and either $j = \eta(j)$ and $S = O^+_{2m}(u)$ or $j = 2\eta(j)$ and $S = O^-_{2m}(u)$, and by adjacency criterion, r and s_l are not adjacent in S for $l = 1, 2$, which is not the case. Thus $\eta(i) < (m + 3)/2$. If $\eta(i) = (m - 1)/2$, then $O^+_{2m}(u)$ has an element of order $a = [u^{\eta(i)} + 1, u^j - 1, u^2 + 1]$ and $O^-_{2m}(u)$ has an element of order $b = [u^{\eta(i)} + 1, u^j + 1, u^2 + 1]$. This is a contradiction because prs_l divides both a and b for $l = 1, 2$. If $\eta(i) < (m - 1)/2$, then it is easy to construct an element of required order. So $\eta(i) = (m + 1)/2$ and there are only two possible values for $e(r, u)$. This is impossible because $\{r_1, r_2, w\}$ is a coclique in $GK(L)$.

Now suppose that $n \equiv 2 \pmod 4$. The group S cannot be isomorphic to $O^+_{2m}(u)$ since otherwise $t(L)$ is congruent to 2 modulo 3 and $t(S)$ does not. Let $S \in \{S_{2m}(u), O_{2m+1}(u)\}$. Then $t(L) = t(S)$ yields $m \in \{n, n - 1\}$. If $m = n$, then $S \in \mathcal{Y}_2$, and if $m = n - 1$, then $S \in \mathcal{Y}_3$, which contradicts to the fact that $L \in \mathcal{Y}_1$. Thus $S = O^-_{2m}(u)$, and it follows from $t(L) = t(S)$ that $m = n$. Then $m \equiv 2 \pmod 4$, and so $k = e(p, u) = 4$. Assume that $t > 23$, that is $m = n > 30$. Then $\eta(n - 6) > \eta(n - 10) = n/2 - 5 > n/3$, and hence

$n-6, n-10 \in M(L)\cap N(L)$ with one of them being a multiple of 4 but not of 8. Now Lemma 7.13 gives the desired contradiction.

Finally, assume that $L = O_{60}^-(q)$ and $S = O_{60}^-(u)$. Let $s_1 = r_{11}(q)$, $s_2 = r_{22}(q)$, $r_1 = r_{38}(q)$, $r_2 = r_{19}(q)$, and $w = r_{18}(q)$. Then $11, 22 \in M(L)\cap N(L)$, $\{r_1, r_2, w\}$ is a coclique in $GK(L)$ and it consists of numbers large with respect to L, and for $l = 1, 2$, we have $s_lr_l, s_lw \in \omega(L)$, but $ps_lr_l, ps_lw \notin \omega(L)$. Writing $j_1 = e(s_1, u)$, $j_2 = e(s_2, u)$ and using Lemma 7.1, we obtain $\eta(j_1) = \eta(j_2) = 11$. Choose $r \in \{r_1, r_2, w\}$ and take $i = e(r, u)$. Since for $l = 1, 2$, we have $s_lr_l, s_lw \in \omega(S)$, it follows that $\eta(i) \leqslant 19$. It is easy to see that if $\eta(i) \leqslant 16$, then $\omega(S)$ contains a number divisible by prs_l for each $l = 1, 2$, which is impossible. So we assume that $\eta(i) \geqslant 17$. If $\eta(i) = 18$, then $i = 36 \equiv 4 \pmod 8$, and applying Lemma 7.13 either to the pair (s_l, r_l) or to the pair (s_l, w) for some $l \in \{1, 2\}$, we have the desired contradiction. Let $\eta(i) \in \{17, 19\}$ and $j \in \{j_1, j_2\}$. If $j = 11$, then since S has no elements of order $[u^{11}-1, u^{19}-1]/d$ with $d \in \{1, 2, 4\}$ and does have element of order $[u^2+1, u^{11}-1, u^{17}-1]$, it follows that $i \in \{34, 38\}$. Similarly, if $j = 22$ then $i \in \{17, 19\}$. If $j_1 = j_2$, then $i = e(r, u)$ can take at most two different values, but there must be at least three of them as $\{r_1, r_2, w\}$ is a coclique in $GK(L)$. And if $j_1 \neq j_2$, then $e(w, u) \in \{17, 19\} \cap \{34, 38\} = \varnothing$, and this contradiction completes the proof.

If $L = L_n^\varepsilon(q)$ with $n \geqslant 45$, $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ with $n \geqslant 29$, $L = O_{2n}^-(q)$ with $n \geqslant 30$, or $L = O_{2n}^+(q)$ with $n \geqslant 31$, then $t(L) \geqslant 23$. We eliminated all possibilities for the group S under the assumption that $t(L) \geqslant 23$, and so the proof of Theorem 3 is complete.

Remark 4. Although the final part of the proof is technically complicated, its idea is transparent and based on an application of the well-known pigeonhole principle. Here pigeons are from $M(L)\cap N(L)$ and holes are from $N(S)$. The number of pigeons and number of holes are almost the same and, what is sufficient, the difference between them is a small constant which does not depend on $n = \mathrm{prk}(L)$. However, there are prohibited holes, and the number of those holes increases when so does n. It provides a contradiction that becomes evident with the growth of n.

8. Proof of Theorems 1 and 2

As written in Introduction, Theorems 1 and 2 follow from Theorem 3 and a series of previously obtained results. The next assertion summarizes the main results of [17, 18].

Lemma 8.1. *Let L be a finite simple classical group over a field of characteristic p, and $L \notin \{L_2(9), L_3(3), U_3(3), U_3(5), U_5(2), S_4(3)\}$. Suppose that G is a finite group with $\omega(G) = \omega(L)$, and S is a unique nonabelian composition factor of G. Then one of the following holds:*

(1) *$S \simeq L$;*
(2) *$L = S_4(q)$, where $q > 3$, and $S \simeq L_2(q^2)$;*
(3) *$L \in \{S_6(q), O_7(q), O_8^+(q)\}$ and $S \in \{L_2(q^3), G_2(q), S_6(q), O_7(q)\}$;*
(4) *$n \geqslant 4$, $L \in \{S_{2n}(q), O_{2n+1}(q)\}$ and $S \in \{O_{2n+1}(q), O_{2n}^-(q)\}$;*
(5) *$n \geqslant 6$ is even, $L = O_{2n}^+(q)$ and $S \in \{S_{2n-2}(q), O_{2n-1}(q)\}$;*
(6) *S is a group of Lie type over a field of characteristic distinct to p.*

This assertion and Theorem 3 yield Theorem 2 immediately.

A *cover* of a finite group G is a finite group having G as a factor group. A cover is proper if the corresponding factor group is proper. If $\omega(G) \neq \omega(H)$ for every proper cover H of G, then G is said to be *recognizable by spectrum among covers*. It follows from [19, Lemma 9] that a finite group G is recognizable by spectrum among covers if and only if $\omega(G) \neq \omega(H)$ for every splitting extension $H = V \rtimes G$, where V is an absolutely irreducible finite-dimensional G-module over a finite field of characteristic r. For every simple linear and unitary group $L = L_n^\varepsilon(q)$ with $n \neq 4$ and every L-module V, if the characteristic r of V coincides with the characteristic p of L, then it is proved that $\omega(L) \neq \omega(V \rtimes L)$ [19]. If V is defined over the field of characteristic distinct to p and $L = L_n(q)$, then any extension $V \rtimes L$ contains an element whose order does not belong to $\omega(L)$ [19, Lemma 11]. For other classical groups the following general result was recently obtained.

Lemma 8.2 ([20]). *Let L be one of the simple groups $U_n(q)$, where $n \geqslant 4$, $S_{2n}(q)$, where $n \geqslant 3$, $O_{2n+1}(q)$, where $n \geqslant 3$, and $O_{2n}^\pm(q)$, where $n \geqslant 4$. Suppose that V is a finite-dimensional L-module over a field of characteristic r prime to q. Then either $\omega(V \rtimes L) \neq \omega(L)$ or $L = U_5(2)$ and $r = 3$. If $L = U_5(2)$, then there is a 10-dimensional L-module V over a field of characteristic 3 such that $\omega(V \rtimes L) = \omega(L)$.*

If $L = L_n^\varepsilon(q)$, $n \geqslant 45$, and G is a finite group isospectral to L, then Theorem 3 and Lemma 8.1 provide $L \leqslant G/K \leqslant \operatorname{Aut} L$, where K is the soluble radical of G. An application of the aforementioned results on covers of linear and unitary groups completes the proof of Theorem 1.

Acknowledgments

The author is grateful to M.A. Grechkoseeva for her reading earlier drafts of this article. Her valuable comments and helpful suggestions have enabled us to improve the text significantly.

References

[1] W. Shi, A new characterization of the sporadic simple groups, in: Group theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 531–540.

[2] A. V. Vasil′ev, M. A. Grechkoseeva, V. D. Mazurov, Characterization of the finite simple groups by spectrum and order, Algebra Logic 48 (6) (2009) 385–409.

[3] W. Kimmerle, F. Luca, A. G. Raggi-Cárdenas, Irreducible components and isomorphisms of the Burnside ring, J. Group Theory 11 (6) (2008) 831–844.

[4] R. Brandl, W. Shi, Finite groups whose element orders are consecutive integers, J. Algebra 143 (2) (1991) 388–400.

[5] V. Mazurov, W. Shi, A note to the characterization of sporadic simple groups., Algebra Colloq. 5 (3) (1998) 285–288.

[6] I. B. Gorshkov, Recognizability of alternating groups by spectrum, Algebra Logic 52 (1) (2013) 41–45.

[7] A. V. Vasil'ev, A. M. Staroletov, Almost recognizability of simple exceptional groups of Lie type, Algebra Logic 53 (5) (2014), http://arxiv.org/abs/1409.2967.

[8] O. A. Alekseeva, A. S. Kondrat'ev, On recognizability of some finite simple orthogonal groups by spectrum, Proc. Steklov Inst. Math. 266 (suppl. 1) (2009) S10–S23.

[9] A. S. Kondrat'ev, Recognition by spectrum of the groups ${}^2D_{2^m+1}(3)$, Sci. China Ser. A 52 (2) (2009) 293–300.

[10] H. He, W. J. Shi, Recognition of some finite simple groups of type $D_n(q)$ by spectrum, Int. J. Algebra Comput. 19 (5) (2009) 681–698.

[11] R. Shen, W. Shi, M. R. Zinov'eva, Recognition of simple groups $B_p(3)$ by the set of element orders, Siberian Math. J. 51 (2) (2010) 244–254.

[12] H. He, W. Shi, A note on the adjacency criterion for the prime graph and characterization of $C_p(3)$, Algebra Colloq. 19 (3) (2012) 553–562.

[13] M. A. Grechkoseeva, D. V. Lytkin, Almost recognizability by spectrum of finite simple linear groups of prime dimension, Siberian Math. J. 53 (4) (2012) 645–655.

[14] M. Foroudi Ghasemabadi, A. Iranmanesh, N. Ahanjideh, Characterizations of the simple group ${}^2D_n(3)$ by prime graph and spectrum, Monatsh. Math. 168 (3-4) (2012) 347–361.

[15] M. Foroudi Ghasemabadi, A. Iranmanesh, N. Ahanjideh, 2-recognizability of the simple groups $B_n(3)$ and $C_n(3)$ by prime graph, Bull. Iranian Math. Soc. 39 (6) (2013) 1273–1281.

[16] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Clarendon Press, Oxford, 1985.

[17] A. V. Vasil′ev, M. A. Grechkoseeva, V. D. Mazurov, On finite groups isospectral to simple symplectic and orthogonal groups, Siberian Math. J. 50 (6) (2009) 965–981.

[18] A. V. Vasil′ev, M. A. Grechkoseeva, A. M. Staroletov, On finite groups isospectral to simple linear and unitary groups, Siberian Math. J. 50 (6) (2009) 965–981.

[19] A. V. Zavarnitsine, Properties of element orders in covers for $L_n(q)$ and $U_n(q)$, Siberian Math. J. 49 (2) (2008) 246–256.

[20] M. A. Grechkoseeva, On element orders in covers of finite simple classical groups, J. Algebra 339 (1) (2011) 304–319.

[21] A. V. Zavarnitsine, A solvable group isospectral to $S_4(3)$, Siberian Math. J. 51 (1) (2010) 20–24.

[22] V. D. Mazurov, Recognition of finite groups by a set of orders of their elements, Algebra and Logic 37 (6) (1998) 371–379.

[23] W. M. Kantor, Á. Seress, Large element orders and the characteristic of Lie-type simple groups, J. Algebra 322 (3) (2009) 802–832.

[24] K. Zsigmondy, Zur theorie der potenzreste, Monatsh. Math. Phys. 3 (1892) 265–284.

[25] M. Roitman, On Zsigmondy primes, Proc. Amer. Math. Soc. 125 (7) (1997) 1913–1919.

[26] B. Huppert, N. Blackburn, Finite Groups II, Springer-Verlag, Berlin, 1982.

[27] J. Nagura, On the interval containing at least one prime number, Proc. Japan Acad. 28 (4) (1952) 177–181.

[28] H. Rohrbach, J. Weis, Zum finiten fall des bertrandschen postulates, J. Reine Angew. Math. Bd 214/5 (1964/1965) 432–440.

[29] J. S. Williams, Prime graph components of finite groups, J. Algebra 69 (2) (1981) 487–513.

[30] A. S. Kondrat′ev, Prime graph components of finite simple groups, Math. USSR-Sb. 67 (1) (1990) 235–247.

[31] V. D. Mazurov, Recognition of finite simple groups $s_4(q)$ by their element orders, Algebra Logic 41 (2) (2002) 93–110.

[32] A. V. Vasil′ev, On connection between the structure of a finite group and properties of its prime graph, Siberian Math. J. 46 (3) (2005) 396–404.

[33] A. V. Vasil′ev, I. B. Gorshkov, On recognition of finite simple groups with connected prime graph, Siberian Math. J. 50 (2) (2009) 233–238.

[34] A. V. Vasil′ev, E. P. Vdovin, An adjacency criterion for the prime graph of a finite simple group, Algebra Logic 44 (6) (2005) 381–406.

[35] A. V. Vasil′ev, E. P. Vdovin, Cocliques of maximal size in the prime graph of a finite simple group, Algebra Logic 50 (4) (2011) 292–322.

[36] M. R. Aleeva, On finite simple groups with the set of elements orders as that of the Frobenius or double Frobenius group, Math. Notes 73 (3) (2003) 323–339.

[37] A. V. Vasil′ev, M. A. Grechkoseeva, On recognition by spectrum of finite simple linear groups over fields of characteristic 2, Siberian Math. J. 46 (4) (2005) 593–600.

[38] A. A. Buturlakin, M. A. Grechkoseeva, The cyclic structure of maximal tori of the finite classical groups, Algebra Logic 46 (2) (2007) 73–89.

[39] A. A. Buturlakin, Spectra of finite linear and unitary groups, Algebra Logic 47 (2) (2008) 91–99.

[40] A. A. Buturlakin, Spectra of finite symplectic and orthogonal groups, Sib. Adv. Math. 21 (3) (2011) 176–210, http://arxiv.org/abs/1102.3021.

[41] D. Testerman, A_1-type overgroups of order p in semisimple algebraic groups and the associated finite groups, J. Algebra 177 (1) (1995) 34.

[42] A. V. Zavarnitsine, V. D. Mazurov, Element orders in coverings of symmetric and alternating groups, Algebra Logic 38 (3) (1999) 159–170.

[43] V. D. Mazurov, Characterizations of finite groups by sets of orders of their elements, Algebra Logic 36 (1) (1997) 23–32.

[44] L. Di Martino, A. E. Zalesskii, Minimum polynomials and lower bounds for eigenvalues multiplicities of prime-power order elements in representations of quasi-simple groups, J. Algebra 243 (2001) 228–263, Corrigendum, J. Algebra 296 (2006), 249–252.

[45] P. Hall, G. Higman, On the p-length of p-soluble groups and reduction theorem for Burnside's problem, Proc. London Math. Soc. 6 (3) (1956) 1–42.

[46] B. Huppert, Endliche Gruppen I, Vol. 134 of Grundlehren Math. Wiss., Springer-Verlag, Berlin, 1979.

[47] B. Hartely, T. Meixner, Finite soluble groups containing an element of prime order whose centralizer is small, Arch. Math. (Basel) 36 (1981) 211–213.

[48] E. I. Khukhro, V. D. Mazurov, Automorphisms with centralizers of small rank, in: Groups St. Andrews 2005, Vol. 340 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2007, pp. 564–585.

[49] D. Gorenstein, R. Lyons, The local structure of finite groups of characteristic 2 type, Vol. 42 of Memoirs Amer. Math. Soc., Amer. Math. Soc., Providence, 1983.

[50] P. Kleidman, M. Liebeck, The subgroup structure of the finite classical groups, Vol. 129 of London Mathematical Society Lecture Note Series, Univ. Press, Cambridge, 1990.

[51] A. V. Zavarnitsine, Recognition of simple groups $U_3(q)$ by element orders, Algebra Logic 43 (2) (2006) 159–170.

[52] M. Grechkoseeva, Recognition by spectrum for finite linear groups over fields of characteristic 2, Algebra Logic 47 (4) (2008) 229–241.

[53] A. V. Vasil′ev, M. A. Grechkoseeva, Recognition by spectrum for finite simple linear groups of small dimensions over fields of characteristic 2, Algebra Logic 47 (5) (2008) 314–320.

[54] M. A. Grechkoseeva, Quasirecognizability of simple unitary groups over fields of even order, Sib. Élektron. Mat. Izv. 7 (2010) 435–444.

[55] M. A. Grechkoseeva, 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.