ON RECOGNITION BY SPECTRUM OF FINITE SIMPLE LINEAR GROUPS OVER FIELDS OF CHARACTERISTIC 2

A. V. Vasil'ev, M. A. Grechkoseeva

Abstract. A finite group G is said to be recognizable by spectrum, i. e. by the set of element orders, if every finite group H, having the same spectrum as G, is isomorphic to G. We proof that the simple linear groups $L_n(2^k)$ are recognizable by spectrum for $n = 2^m \geq 32$.

Introduction

Given a finite group G, denote by $\omega(G)$ the *spectrum* of G, i. e., the set of its element orders. A group G is said to be *recognizable by spectrum* (briefly, *recognizable*), if every finite group H with $\omega(H) = \omega(G)$ is isomorphic to G. Since a finite group with a nontrivial normal soluble subgroup is not recognizable, of prime interest is the recognition problem for simple and almost simple groups.

At present there is a vast list of finite and almost finite groups with solved recognition problem. The most recent version of this list is presented in [1, Table 1]; references to some new results can be found in [2].

The overwhelming majority of recognizable groups from this list have disconnected prime graphs and this condition is essentially used in proof of recognizability of these groups. This is due to the fact that given a finite simple group with disconnected prime graph one can apply the Gruenberg —Kegel theorem when establishing some property of this group, which is named, in accord to [3], quasirecognizability. A finite nonabelian simple group S is said to be *quasirecognizable* if every finite group H with the same spectrum as S includes a unique nonabelian composition factor and this factor is isomorphic to S.

Unfortunately, among finite simple groups those with disconnected prime graphs are rather the exception than the rule. But the recently published paper [2] contains the structural theorem which allows to start proving quasirecognizability of the considered group under much weaker conditions. In particular, it can be applied to almost all the finite simple groups of Lie type. In the present paper on the basis of this result we proof recognizability of the infinite series of finite simple linear groups over fields of characteristic 2.

Key words and phrases. finite group, finite simple group, linear group, spectrum of group, recognition by spectrum, prime graph.

The authors were supported by the Russian Foundation for Basic Research (Grant 05–01–00797), the State Maintenance Program for the Leading Scientific Schools of the Russian Federation (Grant NSh–2069.2003.1), the Program "Development of the Scientific Potential of Higher School" of the Ministry for Education of the Russian Federation (Grant 8294), the Program "Universities of Russia" (Grant UR.04.01.202), and a grant of the Presidium of the Siberian Branch of the Russian Academy of Sciences (No. 86-197).

Theorem. *Let $L = L_n(q)$ where $n = 2^m \geqslant 32$, $q = 2^k \geqslant 2$. Then L is recognizable by spectrum.*

§ 1. Preliminaries

Let G be a finite group, $\omega(G)$ be its spectrum. The set $\omega(G)$ is ordered by the divisibility relation and we denote by $\mu(G)$ the set of its elements which are maximal under this relation. If p is a prime, then p-period of G is the maximal power of p which belongs to $\omega(G)$.

Let $\pi(G)$ be the set of all prime divisors of the order of G. We define a graph on the set $\pi(G)$ with the following adjacency relation: vertices p and r in $\pi(G)$ are joined by edge if and only if $pr \in \omega(G)$. This graph is called the *Gruenberg — Kegel graph* or *prime graph* of G and denoted by $GK(G)$. Guided by given graph conception, we say that prime divisors p and r of the order of G are *adjacent* if vertices p and r are joined by edge in $GK(G)$. Otherwise primes p and r are said to be *nonadjacent*.

The set of vertices of a graph is called *independent*, if vertices of this set are pairwise nonadjacent. The cardinality of an independent set with maximal number of vertices is usually called the *independence number* of the graph. Denote by $t(G)$ the independence number of the graph $GK(G)$ of G. By analogy we denote by $t(2, G)$ the maximal number of vertices in independent sets of $GK(G)$ containing the vertex 2. We call this number the 2-*independence number*.

The following theorem on connection between the structure of a finite group and the properties of its prime graph is proved in [2].

Lemma 1. *Let G be a finite group satisfying two conditions:*

(a) *there exist three primes in $\pi(G)$ pairwise nonadjacent in $GK(G)$; i. e., $t(G) \geq 3$;*

(b) *there exists an odd prime in $\pi(G)$ nonadjacent to prime 2 in $GK(G)$; i. e., $t(2, G) \geq 2$.*

Then there is a finite nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ for the maximal normal soluble subgroup K of G. Furthermore, $t(S) \geq t(G) - 1$, and one of the following statements holds.

(1) *$S \simeq \mathrm{Alt}_7$ or $L_2(q)$ for some odd q, and $t(S) = t(2, S) = 3$;*

(2) *For every prime $p \in \pi(G)$, nonadjacent to 2 in $GK(G)$ a Sylow p-subgroup of G is isomorphic to a Sylow p-subgroup of S. In particular, $t(2, S) \geq t(2, G)$.*

Proof. See [2].

The independence and 2-independence numbers for all the finite simple groups are calculated in [4]. Notice that these results and the previous lemma imply

Corollary. *Let L be a finite nonabelian simple group other than $L_3(3)$, $U_3(3)$, $S_4(3)$, Alt_{10}, and Alt_n with n satisfying $\{r \mid n - 3 \leq r \leq n,\ r \ \text{ is prime}\} = \varnothing$. Suppose G be a finite group with $\omega(G) = \omega(L)$. Then the conclusion of Lemma 1 holds true for G.*

Proof. See [4, Corollary 7.2].

We use the following number-theoretic notation. If n is a natural number, then $\pi(n)$ is the set of prime divisors of n. If $p \in \pi(n)$, then n_p is the maximal p-power which divides n. By $[x]$ we denote the integer part of x. If q is a natural number,

r is an odd prime and $(q,r)=1$, then by $e(r,q)$ we denote the smallest natural number m such that $q^m \equiv 1 \pmod r$. For an odd q put $e(2,q)=1$ if $q \equiv 1 \pmod 4$ and put $e(2,q)=2$ if $q \equiv -1 \pmod 4$.

The following number-theoretic result is of fundamental importance for investigations on the structure of prime graphs of the Lie type finite simple groups.

Lemma 2 (Zsigmondy)**.** *Let q be a natural number greater than 1. Then for every natural number m there exists a prime r such that $e(r,q)=m$, except for the following cases:*

(1) *$m=6$ and $q=2$;*

(2) *$m=2$ and $q=2^l-1$ for some natural number l.*

Proof. See [5].

The prime r with $e(r,q)=m$ is called a *primitive prime divisor* of q^m-1. If q is fixed, we denote by r_m any primitive prime divisor of q^m-1 (obviously, q^m-1 can have more than one primitive prime divisor).

Lemma 3. *Let G be a finite group, $K \lhd G$, and G/K be a Frobenius group with core F and cyclic complement C. If $(|F|,|K|)=1$ and F does not lie in $KC_G(K)/K$, then $r \cdot |C| \in \omega(G)$ for some prime divisor r of $|K|$.*

Proof. See [6, Lemma 1].

Lemma 4. *Let L be a finite simple group $L_n(q)$, q be a power of a prime p, and $d=(q-1,n)$. Then*

(1) *$\frac{q^{n-1}-1}{d}$ is in $\mu(L)$;*

(2) *p-period of L is equal to p^m, where m is the smallest natural number such that $n \le p^m$;*

(3) *for every $r \in \pi(L)$ there is a prime $s \in \pi(L)$ nonadjacent to r; furthermore, if $n \ge 4$ and $(n,q) \ne (6,2),(7,2)$, then either a primitive prime divisor r_n of q^n-1 or a primitive prime divisor r_{n-1} of $q^{n-1}-1$ can be taken as a prime s.*

Proof. (1) See [7, Proposition 7].

(2) See [8, Proposition 0.5].

(3) If $n=2$ or 3, then the claim holds since in this case the graph $GK(L)$ is disconnected. For $L_6(2)$, $L_7(2)$ the claim is verified directly. Let $n \ge 4$ and $(n,q) \ne (6,2),(7,2)$. By Lemma 2 there exist primitive prime divisors r_n and r_{n-1} of q^n-1 and $q^{n-1}-1$ respectively. In view of [4, Propositions 2.1, 3.1 and 4.1] the prime r is nonadjacent either to r_n or to r_{n-1}.

Lemma 5. *Let L be a finite simple group $L_n(q)$, $d=(q-1,n)$.*

(1) *If there exists primitive prime divisor r of q^n-1, then L includes a Frobenius subgroup with core of order r and cyclic complement of order n.*

(2) *L includes a Frobenius subgroup with core of order q^{n-1} and cyclic complement of order $\frac{q^{n-1}-1}{d}$.*

Proof. (1) We use the method of constructing maximal tori of a finite group of Lie type on a basis of maximal tori of the corresponding algebraic group, described in [9, Chapter 3]. If X is a group and α is a automorphism of X, then denote by X_α the centralizator of α in X.

Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the field of order q and $\overline{G}=SL_n(\overline{\mathbb{F}}_q)$. Let σ be a Frobenius automorphism of $\overline{G}$ such that $G=\overline{G}_\sigma$ is isomorphic to $SL_n(q)$. Let

$\overline{D}$ be the group of diagonal matrices in $\overline{G}$ and π be the natural homomorphism of $N_{\overline{G}}(\overline{D})$ onto Sym_n. Let w be an element in $N_{\overline{G}}(\overline{D})$ such that $w^\sigma = w$ and $\pi(w)$ is a cycle of length n. Put $\sigma_w = \sigma \circ c_w^{-1}$, where c_w denotes conjugation by w. Then $\overline{T} = \overline{D}_{\sigma_w}$ is a cyclic group of order $\frac{q^n-1}{q-1}$.

Let t be an element in $\overline{T}$ of order r. Since $t^w = t^\sigma = t^q$, the element w acts on the group $\langle t\rangle$ by conjugation. Suppose that $t = t^{w^l}$ for some l. Then $t = t^{q^l}$. Hence $t^{q^l-1} = 1$, and therefore r divides $q^l - 1$. In view of primitivity of r, the number l is divisible by n, that is $w^l = 1$. Thus, $F = \langle t, w\rangle$ is a Frobenius group with core of order r and complement of order n. Notice that $F \cap Z(G) = \langle t\rangle \cap Z(G) = 1$.

By the Lang-Steinberg theorem [10], there is an element g in $\overline{G}$ such that $\pi(g^{-1}g^\sigma) = \pi(w)$. By virtue of equalities

$$({}^g t)^\sigma = g^\sigma t^\sigma (g^{-1})^\sigma = gwt^\sigma w^{-1}g^{-1} = gt^{\sigma_w}g^{-1} = {}^g t,$$
$$({}^g w)^\sigma = g^\sigma w(g^{-1})^\sigma = gwww^{-1}g^{-1} = {}^g w$$

${}^g F$ lies in G and its image in $G/Z(G)$ is the desired Frobenius group.

(2) Consider the parabolic subgroup P of $SL_n(q)$ consisting of all matrices of the form

$$M(a,b) = \left(\begin{array}{c|c} a & 0 \\ \hline b & \det a^{-1} \end{array}\right), \quad \text{where} \quad a \in GL_{n-1}(q), \quad b \in \mathbb{F}_q^{n-1}.$$

Denote by A the subgroup of P consisting of all matrices of the form $M(a, \mathbf{0})$, where $\mathbf{0}$ is the null row in $\mathbb{F}_q^{n-1}$. Denote by B the subgroup of all matrices of the form $M(\mathbf{1}, b)$, where $\mathbf{1}$ is the identity matrix in $GL_{n-1}(q)$. The group P is a semidirect product of B by A with $M(\mathbf{1}, b)^{M(a,\mathbf{0})} = M(\mathbf{1}, ba \det a)$.

We again consider the algebraic closure $\overline{\mathbb{F}}_q$ of the field of order q, the algebraic group $\overline{G} = SL_n(\overline{\mathbb{F}}_q)$, and the subgroup $\overline{A}$ of $\overline{G}$, consisting of matrices

$$M(a,b) = \left(\begin{array}{c|c} \bar{a} & 0 \\ \hline \mathbf{0} & \det \bar{a}^{-1} \end{array}\right), \quad \text{where} \quad \bar{a} \in GL_{n-1}(\overline{\mathbb{F}}_q).$$

Let $\overline{D}$ be the group of diagonal matrices in $\overline{A}$ and π be a natural homomorphism of $N_{\overline{A}}(\overline{D})$ onto Sym_{n-1}. Let w be an element in $N_{\overline{A}}(\overline{D})$ such that $\pi(w)$ is a cycle of length $n-1$. Put $\sigma_w = \sigma \circ c_w^{-1}$ where c_w is conjugation by w. Then $\overline{T} = \overline{D}_{\sigma_w}$ is a cyclic group of order $q^{n-1}-1$ generated by $t = \mathrm{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{n-2}}, \lambda^{(1-q^{n-1})/(q-1)})$, where λ is a primitive $q^{n-1}-1$-th root of unity. Just as above, choose $g \in \overline{A}$ such that ${}^g t \in A$ and denote by C the group generated by ${}^g t$.

Suppose that an element $M(c, \mathbf{0})$ of C centralizes some nontrivial element of B. Then $bc \det c = b$ with $b \neq \mathbf{0}$. Therefore, the matrix $c \det c$ has 1 as an eigenvalue. Since c is conjugate to $\mathrm{diag}(\lambda, \lambda^q, \ldots, \lambda^{q^{n-2}})$ where $\lambda^{q^{n-1}-1} = 1$, the eigenvalues of $c \det c$ are equal to $\lambda^{q^i} \cdot \lambda^{(1-q^{n-1})/(q-1)}$, $0 \leq i \leq n-2$. If $\lambda^{q^i} \cdot \lambda^{(1-q^{n-1})/(q-1)} = 1$, then $\lambda^{q^i(q-1)} = 1$. Therefore, $\lambda^{q-1} = 1$. Hence $M(c, \mathbf{0}) \in Z(SL_n(q))$. Thus, the kernel of action of C on B is $Z(SL_n(q))$, and all the other elements of C act on B fixed-point-freely. So the image of BC in $L_n(q)$ is the desired Frobenius group. The lemma is proved.

Remark. The proof of the second assertion of the lemma belongs to A. V. Zavarnitsin and is published in [11, Lemma 3]. Since this source is not widely available, we cite, with the kind permission of the author, the slightly modified proof in this paper.

Table 1. Simple groups S with $t(S) \geq 15$ and $t(2,S) \geq 3$

S	Additional conditions on S	$t(2,S)$	$\rho(2,S) \setminus \{2\}$	$t(S)$
Alt_n	$n, n-2$ are prime	3	$\{n, n-2\}$	
$n \geq 137$	$n-1, n-3$ are prime	3	$\{n-1, n-3\}$	
$A_{n-1}(q)$	$2 < (q-1)_2 = n_2$	3	$\{r_{n-1}, r_n\}$	$\left[\frac{n+1}{2}\right]$
$n \geq 29$	q even	3	$\{r_{n-1}, r_n\}$	
	$2 < (q+1)_2 = n_2$	3	$\{r_{2n-2}, r_n\}$	
${}^2A_{n-1}(q)$	q even $n \equiv 0 \pmod 4$	3	$\{r_{2n-2}, r_n\}$	
$n \geq 29$	$n \equiv 1 \pmod 4$	3	$\{r_{n-1}, r_{2n}\}$	$\left[\frac{n+1}{2}\right]$
	$n \equiv 2 \pmod 4$	3	$\{r_{2n-2}, r_{n/2}\}$	
	$n \equiv 3 \pmod 4$	3	$\{r_{(n-1)/2}, r_{2n}\}$	
$B_n(q), n \geq 19$	q even	3	$\{r_n, r_{2n}\}$	$\left[\frac{3n+5}{4}\right]$
$D_n(q)$	$q \equiv 5 \pmod 8$ $n \equiv 1 \pmod 2$	3	$\{r_n, r_{2n-2}\}$	
$n \geq 20$	q even $n \equiv 0 \pmod 2$	3	$\{r_{n-1}, r_{2n-2}\}$	$\left[\frac{3n+1}{4}\right]$
	$n \equiv 1 \pmod 2$	3	$\{r_n, r_{2n-2}\}$	
${}^2D_n(q)$	$q \equiv 3 \pmod 8$ $n \equiv 1 \pmod 2$	3	$\{r_{2n-2}, r_{2n}\}$	
$n \geq 19$	q even $n \equiv 0 \pmod 2$	4	$\{r_{n-1}, r_{2n-2}, r_{2n}\}$	$\left[\frac{3n+4}{4}\right]$
	$n \equiv 1 \pmod 2$	3	$\{r_{2n-2}, r_{2n}\}$	

§ 2. Proof of the Theorem

Through this paragraph we consider the classical groups of Lie type and denote them according to [12]. Sometimes we use notations $A_n^\varepsilon(q)$ and $D_n^\varepsilon(q)$, where $\varepsilon \in \{+,-\}$ and $A_n^+(q) = A_n(q)$, $A_n^-(q) = {}^2A_n(q)$, $D_n^+(q) = D_n(q)$, $D_n^-(q) = {}^2D_n(q)$.

Let $L = L_n(q) = A_{n-1}(q)$ where $n = 2^m \geq 32$, $q = 2^k \geq 2$. By [4, § 8], we have $t(L) \geq 16$ and $t(2,L) = 3$. Furthermore, item (2) of Lemma 4 implies that 2-period of L is equal to $n = 2^m$.

Let G be a finite group with $\omega(G) = \omega(L)$ and K be the maximal normal soluble subgroup of G. By Lemma 1 there is a finite nonabelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$; moreover, $t(S) \geq t(G) - 1$ and either $t(S) = t(2,S) = 3$, or $t(2,S) \geq t(2,G)$. Since $t(G) = t(L) \geq 16$ and $t(2,G) = t(2,L) = 3$, the group S must satisfy $t(S) \geq 15$ and $t(2,S) \geq 3$. By using [4, § 8], we compose a table of the all finite nonabelian simple groups satisfying these conditions. For every group S the table shows 2-independence number and some independent set $\rho(2,S)$ of $GK(S)$ with maximal number of vertices among those containing the vertex 2. Furthermore, for every group of Lie type the table gives independence number as a function of Lie rank.

If not specified r_n, r_{n-1}, and r_{n-2} are some fixed primitive prime divisors of $q^n - 1$, $q^{n-1} - 1$, and $q^{n-2} - 1$ respectively. By definition of primitive prime divisor, these numbers are pairwise distinct. By [4, Proposition 3.1] primes r_n and r_{n-1} are nonadjacent to 2 in $GK(L)$, and so in $GK(G)$ as well. Consequently, by Lemma 1 these primes divide the order of S.

Let $S = \mathrm{Alt}_{n'}$. Then $n' \geq 137$ and there are two primes among numbers n', $n'-1$,

$n'-2$, $n'-3$; these are r_n and r_{n-1}. By [7, Proposition 7] we have $4\cdot r_{n-2}\notin\omega(L)$, although $2\cdot r_{n-2}\in\omega(L)$. Suppose that r_{n-2} divides the order of S. Since S does not contain an element of order $4\cdot r_{n-2}$, then $n'\geq r_{n-2}\geq n'-5$. Thus, there are three primes among six consecutive numbers $n',\dots,n'-5$, which is impossible since $n'\geq 137$. So r_{n-2} lies in $\pi(K)\cup\pi(\mathrm{Out}(S))$. Since $\pi(\mathrm{Out}(S))=\{2\}$, we have $r_{n-2}\in\pi(K)$.

Denote r_{n-2} by r. Let $\widetilde{G}=G/O_{r'}(K)$ and $\widetilde{K}=K/O_{r'}(K)$. Then $R=O_r(\widetilde{K})\neq 1$. Suppose that $\widetilde{K}=R$. The group S acts faithfully on $\widetilde{K}$. Otherwise, in view of its simplicity S centralizes $\widetilde{K}$ and, therefore, G contains an element of order $4\cdot r$. The group Alt_6, and so S as well, includes a Frobenius group F with core of order 9 and cyclic complement of order 4. By applying Lemma 3 to the preimage of F in $\widetilde{G}$, we obtain that $4\cdot r\in\omega(G)$; a contradiction. Suppose $\widetilde{K}\neq R$. There is a prime t such that $T=O_t(\widetilde{K}/R)$ is nontrivial. Since $O_{r'}(\widetilde{K})=1$, the group T acts faithfully on R. Then T acts faithfully on $\widehat{R}=R/\Phi(R)$, where $\Phi(R)$ is the Frattini subgroup of R, as well. Denote by $\widehat{G}$ the factorgroup $\widetilde{G}/\Phi(R)$. By Lemma 4 at least one of the primes r_n and r_{n-1} is nonadjacent to t in $\omega(G)$. Denote this prime by s. Let x be an element of order s in $\widehat{G}/\widehat{R}$. Then $H=T\langle x\rangle$ is a Frobenius subgroup in $\widehat{G}/\widehat{R}$. The preimage of H in $\widehat{G}$ satisfies conditions of Lemma 3, hence G contains an element of order $r\cdot s$, which contradicts [4, Proposition 2.1].

Let $S=A^{\varepsilon}_{n'-1}(q')$ where q' is odd. Then $n'_2=(q'-\varepsilon 1)_2>2$ and $t(S)=n'/2$. Since $t(S)\geq t(G)-1$ and $t(G)=n/2$, we have $n'/2\geq n/2-1$. Whence $n'\geq n-2$. Since $n\geq 32$, we have $n-2\geq n/2+2=2^{m-1}+2$. Thus $n'\geq 2^{m-1}+2$. Therefore, S includes a cyclic subgroup of order $q'^{2^{m-1}}-1$. In view of

$$q'^{2^{m-1}}-1=(q'-1)(q'+1)(q'^2+1)\dots(q'^{2^{m-2}}+1),$$

we have

$$(q'^{2^{m-1}}-1)_2=(q'-1)_2(q'+1)_2(q'^2+1)_2\dots(q'^{2^{m-2}}+1)_2\geq 4\cdot 2^{m-1}=2^{m+1}.$$

Thus $2^{m+1}\in\omega(S)$; a contradiction.

Let $S=D^{\varepsilon}_{n'}(q')$ where q' is odd. Then $q'-\varepsilon 1\equiv 4 \pmod 8$, $n'\equiv 1 \pmod 2$ and $t(S)\leq(3n'+3)/4$. Since $t(S)\geq t(G)-1$ and $t(G)=n/2$, we have $(3n'+3)/4\geq n/2-1$, which implies $n'\geq(2n-7)/3$. Since $n\geq 32$, we have $(2n-7)/3\geq n/2+3$. Thus $n'\geq n/2+3$. As $D^{\varepsilon}_{n'}(q')$ includes the universal covering of $A_{n'-2}(q')$, by repeating the above argumentation we obtain that $2^{m+1}\in\omega(S)$; a contradiction.

Now let S be a group of Lie type over field of order $2^{k'}$. Choose primitive prime divisors r_n and r_{n-1} of q^n-1 and $q^{n-1}-1$ such that $e(r_n,2)=nk$ and $e(r_{n-1},2)=(n-1)k$. As noticed above, r_n and r_{n-1} divide the order of S. Put $e_n=e(r_n,2^{k'})$ and $e_{n-1}=e(r_{n-1},2^{k'})$. Since r_n divides $2^{e_nk'}-1$, we have that nk divides e_nk'. By the same reason, $(n-1)k$ divides $e_{n-1}k'$. Suppose that $e_nk'>nk$. Then a prime r with $e(r,2)=e_nk'$ divides the order of S and does not divide the order of L. Therefore, $r\in\omega(S)\setminus\omega(G)$, which is impossible. Thus, $e_nk'=nk$. Suppose that $e_{n-1}k'>(n-1)k$. Then $e_{n-1}k'\geq 2(n-1)k>nk$, and the similar argumentation leads us to contradiction. Thus, $e_{n-1}k'=(n-1)k$. Notice that $e_n>e_{n-1}$.

Since r_n and r_{n-1} are nonadjacent to 2 in $GK(S)$, then [4, Proposition 3.1] imposes some restrictions on e_n and e_{n-1}, which will be used in the further consideration.

If $S = A_{n'-1}(2^{k'})$, then $e_n, e_{n-1} \in \{n', n'-1\}$. Hence $n'k' = nk$ and $(n'-1)k' = (n-1)k$, which implies $k' = k$, $n' = n$, and $S \simeq L$.

Let $S = {}^2A_{n'-1}(2^{k'})$. If $n' \equiv 0 \pmod 4$, then $e_n, e_{n-1} \in \{2n'-2, n'\}$. Hence $2(n'-1)k' = nk$ and $n'k' = (n-1)k$, which implies $2k' = (n-2)k$ and $n'-1 = n/(n-2)$. Since $n \geq 32$, the number $n/(n-2)$ cannot be integer; a contradiction. If $n' \equiv 2 \pmod 4$, then $e_n, e_{n-1} \in \{2n'-2, n'/2\}$. Therefore $2(n'-1)k' = nk$ and $n'k' = 2(n-1)k$, whence $2k' = (3n-4)k$ and $n'-1 = n/(3n-4)$. But $n' = n/(3n-4)+1$ cannot be integer. If $n' \equiv 1 \pmod 4$, then $e_n, e_{n-1} \in \{2n', n'-1\}$. Hence $2n'k' = nk$ and $(n'-1)k' = (n-1)k$, which implies $2k' = (2-n)k$. Since $2-n < 0$, we have $k' < 0$, which is impossible. If $n' \equiv 3 \pmod 4$, then $e_n, e_{n-1} \in \{2n', (n'-1)/2\}$. Therefore, $2n'k' = nk$ and $(n'-1)k' = 2(n-1)k$, whence $2k' = (4-3n)k$ and $k' < 0$; a contradiction.

If $S = B_{n'}(2^{k'})$, then $e_n, e_{n-1} \in \{2n', n'\}$. Thus $2n'k' = nk$ and $n'k' = (n-1)k$, which implies $n = 2$; a contradiction.

If $S = D_{n'}(2^{k'})$ and n' is even, then $e_n, e_{n-1} \in \{2n'-2, n'-1\}$. Just as above we obtain that $n = 2$. If n' is odd, then $e_n, e_{n-1} \in \{2n'-2, n'\}$, but we have already proved that this case is impossible.

If $S = {}^2D_{n'}(2^{k'})$, then $e_n, e_{n-1} \in \{2n', 2n'-2, n'\}$. Above we have examined all possibilities, except for $2n'k' = nk$ and $2(n'-1)k' = (n-1)k$. These equalities implies that $n' = n$, $k' = k/2$, and $S = {}^2D_n(2^{k/2})$. It follows from [8, Proposition 0.5] that 2-period of S is equal to 2^{m+1} and, therefore, is greater than 2-period of G; a contradiction.

Thus $S \simeq L$ and quasirecognizability is proved.

The remaining part of the proof can be carried out under weaker conditions on n and q, so it is arranged as two propositions.

Proposition 1. *Let $L = A_{n-1}(q)$ where $n = 2^m \geq 4$, $q = 2^k \geq 2$. Let G be a finite group and K be its nontrivial normal soluble subgroup satisfying $L \leq G/K \leq \mathrm{Aut}(L)$. Then $\omega(G) \not\subseteq \omega(L)$.*

Proof. There exist a prime r such that $O^r(K) \neq K$. Denote by $\widetilde{G}$ and $\widetilde{K}$ the factorgroups $G/O^r(K)$ and $K/O^r(K)$ respectively. The group $\widetilde{K}$ is a nontrivial r-group. Let $\Phi(\widetilde{K})$ be the Frattini subgroup of $\widetilde{K}$. Denote by $\widehat{G}$ and $\widehat{K}$ the factorgroups $\widetilde{G}/\Phi(\widetilde{K})$ and $\widetilde{K}/\Phi(\widetilde{K})$ respectively. Since $G/K \simeq \widehat{G}/\widehat{K}$, it is sufficient to proof that $\omega(\widehat{G}) \not\subseteq \omega(L)$. Therefore, we may assume that $G = \widehat{G}$ and $K = \widehat{K}$ is a nontrivial elementary abelian r-group.

Suppose that $C = C_G(K) \neq K$. Since C is normal in G and L is simple, C/K includes L. Therefore, $r \cdot \omega(L) \subseteq \omega(C) \subseteq \omega(G)$, which contradicts item (3) of Lemma 4. Thus, $C = K$ and L acts faithfully on K.

Let $r = 2$. By item (1) of Lemma 5 the group L includes a Frobenius subgroup with core of odd order and cyclic complement of order n. By applying Lemma 3, we obtain that $2 \cdot n = 2^{m+1} \in \omega(G)$. By item (2) of Lemma 4 we have that 2-period of L is equal to 2^m, i. e., $2^{m+1} \notin \omega(L)$.

Let $r \neq 2$. By item (2) of Lemma 5 the group L includes a Frobenius subgroup with core of order q^n and cyclic complement of order $(q^{n-1}-1)/d$. By applying Lemma 3, we obtain that $r \cdot (q^{n-1}-1)/d \in \omega(G)$. On the other hand, by item (1) of Lemma 4 we have $r \cdot (q^{n-1}-1)/d \notin \omega(L)$. The proposition is proved.

Proposition 2. *Let $L = A_{n-1}(q)$ where $n \geq 10$, $q = 2^k \geq 2$, and $(q-1, n) = 1$. Suppose that $L < G \leq \mathrm{Aut}(L)$. Then $\omega(G) \not\subseteq \omega(L)$.*

Proof. The group G includes a subgroup $G_1 = L\langle\alpha\rangle$ such that the image of α in $\mathrm{Out}(L)$ is of a prime order r. It is sufficient to show that $\omega(G_1) \not\subseteq \omega(L)$. So we may assume that $G = G_1$.

The group $\mathrm{Aut}(L)$ has a normal series $L \leq \widetilde{L} \leq \mathrm{Aut}(L)$, where the factor $\widetilde{L}/L$ is isomorphic to the group of field automorphisms, a cyclic group of order k, and the factor $\mathrm{Aut}(L)/\widetilde{L}$ is isomorphic to the group of graph automorphisms, a cyclic group of order 2.

Let $r = 2$. If $\alpha \notin \widetilde{L}$, then α is either a graph automorphism or a product of a graph and an involutive field automorphisms. In the first case $C_L(\alpha) \simeq C_{n/2}(q)$ if n is even and $C_L(\alpha) \simeq B_{(n-1)/2}(q)$ if n is odd. Therefore, $2 \cdot r_n \in \omega(G)$ or $2 \cdot r_{n-1} \in \omega(G)$. In the second case $q = q_0^2$, $C_L(\alpha)$ includes a subgroup isomorphic to ${}^2A_{n-1}\big(q_0\big)$, and we have, again depending on evenness of n, either $2 \cdot r_{n-1} \in \omega(G)$ or $2 \cdot r_n \in \omega(G)$. Since r_n and r_{n-1} are nonadjacent to 2 in $\omega(L)$, the claim holds for $\alpha \notin \widetilde{L}$.

Now let α be an involutive field automorphism induced by an automorphism φ of field $\mathbb{F}_q$ and u be an element of $\mathbb{F}_q$ such that $u + u^\varphi \neq 0$. Consider the product of α and the unipotent element $x \in L$ of the form $x_1(u)x_2(u)\dots x_{n-1}(u)$ where $x_1, x_2, \dots, x_{n-1}$ are root elements corresponding to the fundamental roots of system A_{n-1}. The element

$$(x\alpha)^2 = x_1(u)x_2(u)\dots x_{n-1}(u)x_1(u^\varphi)x_2(u^\varphi)\dots x_{n-1}(u^\varphi)$$

lies in L and, in virtue of the Chevalley commutator formula [12, Theorem 5.2.2], can be reduced to the form $x_1(u + u^\varphi)\dots x_{n-1}(u + u^\varphi)y$, where y is a product of root elements corresponding to nonfundamental positive roots. Since $u + u^\varphi \neq 0$, by [9, Proposition 5.1.3] the element $(x\alpha)^2$ is regular and, therefore, its order equals to 2-period of L (see the proof of Proposition 0.5 in [8]). Hence the order of $x\alpha$ is twice larger than 2-period of L. Thus $\omega(G) \not\subseteq \omega(L)$.

Let $r \neq 2$. Then α is a field automorphism and $C_L(\alpha) \simeq A_{n-1}(q_0)$ where $q_0 = 2^{k/r}$. Put $s = e(r, q)$. We remind that s is the smallest natural number such that $q^s - 1$ is divisible by r. If $s > n$, then $r \in \omega(G) \setminus \omega(L)$; if $s = n, n-1$, then $2r \in \omega(G) \setminus \omega(L)$. Thus we may assume that $1 \leq s \leq n-2$. Before we begin consideration of cases depending on s, let us observe that if $e(p, q_0)$ equals t and $(t, r) = 1$, then $e\big(p, q_0^r\big)$ equals t as well. In other words, if $t \neq 6$ and $(t, r) = 1$, there is a primitive prime divisor of $q^t - 1$ which divides $q_0^t - 1$.

Let $s = 1$, i. e., $r \mid q - 1$. By hypothesis, we have $(n, r) = 1$. Therefore, there exists a primitive prime divisor r_n of $q^n - 1$ which divides $q_0^n - 1$. It follows from [4, Proposition 4.1] that $r \cdot r_n \notin \omega(L)$. On the other hand, $r \cdot r_n \in r \cdot \omega(A_{n-1}(q_0)) \subseteq \omega(G)$.

Let $2 \leq s \leq n-2$. Among numbers $n, n-1, \dots, n-s+1$ there is only one divisible by s. Among the remaining $s-1$ numbers we can choose a number t coprime to r and not equal to 6, except for the case when $s = 2$ and $r \mid n-1$. We consider this case later and for the present we assume that such t is chosen. Since $(t, r) = 1$, there is a primitive prime divisor r_t of $q^t - 1$ dividing $q_0^t - 1$. Since $t + s > n$ and $s \nmid t$, by [4, Proposition 2.1] we have $r \cdot r_t \notin \omega(L)$. On the other hand, $r \cdot r_t \in r \cdot \omega(A_{n-1}(q_0)) \subseteq \omega(G)$.

Let $s = 2$ and $r \mid n-1$. As follows from [13, Proposition 4.3], if C is a centralizer of involution in L, then $\omega(C) \subseteq \omega(SL_{n-2}(q))$. Let n be even. Since $(n-3, r) = 1$ and $2 \nmid n-3$, by repeating above argumentation we can find a prime divisor r_{n-3} of

$q_0^{n-3}-1$ such that $r_{n-3}\cdot r \notin \omega(A_{n-3}(q))$. Since the order of the center of $SL_{n-2}(q)$ is coprime to both r_{n-3} and r, we have $r_{n-3}\cdot r \notin \omega(SL_{n-2}(q))$. Thus, $2\cdot r_{n-3}\cdot r \notin \omega(L)$. On the other hand, $2 \cdot r_{n-3} \in \omega(A_1(q_0) \times A_{n-3}(q_0)) \subseteq \omega(A_{n-1}(q_0))$, therefore, $2 \cdot r_{n-3} \cdot r \in \omega(G)$. Let n be odd. In the similar way we can find a prime divisor r_{n-2} of $q_0^{n-2}-1$ such that $2\cdot r_{n-2}\cdot r \notin \omega(L)$ and $2\cdot r_{n-2}\cdot r \in \omega(G)$. The proposition is proved.

Now we return to the proof of the theorem. In view of Proposition 1 the soluble radical K of G is trivial. If G is not isomorphic to L, then by Proposition 2 we have $\omega(G) \not\subseteq \omega(L)$. This contradiction completes the proof of the theorem.

References

1. Mazurov V. D., *Characterizations of groups by arithmetic properties*, Algebra Colloq. **11** (2004), no. 1, 129–140.
2. Vasil'ev A. V., *On connection between the structure of finite group and properties of its prime graph*, Sib. Math. J. **46** (2005), no. 3, 396–404.
3. Alekseeva O. A., Kondrat'ev A. S., *On recognition of the group $E_8(q)$ by the set of element orders*, Ukrain. Math. J. **54** (2002), no. 7, 1200–1206.
4. Vasil'ev A. V., Vdovin E. P. An adjacency criterion for two vertices of the prime graph of a finite simple group (2005), no. 152, Sobolev Institute of Mathematics, Novosibirsk.
5. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
6. Mazurov V. D., *Characterization of finite groups by sets of element orders*, Algebra and Logic **36** (1997), no. 1, 23–32.
7. Carter R. W., *Centralizers of semisimple elements in the finite classical group*, Proc. London Math. Soc. (3) **42** (1981), no. 1, 1–41.
8. Testerman D. M., *A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups*, J. Algebra **177** (1995), 34–76.
9. Carter R. W., *Finite groups of Lie type: Conjugacy classes and complex characters*, John Wiley & Sons, New York, 1985.
10. *Steinberg R.* Endomorphisms of algebraic groups. Providence RI: Amer. Math. Soc., 1986. (Mem. Amer. Math. Soc.; 80)
11. Zavarnitsin A. V. Element orders in coverings of the groups $L_n(q)$ and recognition of the alternating group A_{16} (2000), no. 48, NII Diskret. Mat. Inform., Novosibirsk.
12. Carter R. W., *Simple groups of Lie type*, John Wiley & Sons, London, 1972.
13. Aschbacher M., Seitz G. M., *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.