S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 2, стр. 253–263 (2005) УДК 512.542
MSC 20D60

ON RECOGNITION OF THE PROJECTIVE SPECIAL LINEAR GROUPS OVER BINARY FIELD

M.A. GRECHKOSEEVA, M.S. LUCIDO, V.D. MAZUROV, A.R. MOGHADDAMFAR, A.V. VASIL'EV

Abstract. The spectrum $\omega(G)$ of a finite group G is the set of element orders of G. Let L be the projective special linear group $L_n(2)$ with $n \geq 3$. First, for all $n \geq 3$ we establish that every finite group G with $\omega(G) = \omega(L)$ has a unique non-abelian composition factor and this factor is isomorphic to L. Second, for some special series of integers n we prove that L is recognizable by spectrum, i. e. every finite group G with $\omega(G) = \omega(L)$ is isomorphic to L.

Introduction

Throughout this paper, all groups are assumed to be finite and all simple groups are non-abelian. Some interesting problems in finite group theory are related to arithmetical characteristics of the group. For example for a group G we can consider the set $\pi(G)$ of prime divisors of $|G|$ and the set $\omega(G)$ of orders of all elements in G. We call this last set the *spectrum* of G, motivating it as follows.

We recall that for an element $A \in \mathrm{GL}(n, \mathbb{C})$, we have

$$\mathrm{Spec}(A) = \{\lambda \in \mathbb{C} : \lambda \text{ is an eigenvalue of } A\}.$$

Grechkoseeva, M.A., Lucido, M.S., Mazurov, V.D., Moghaddamfar, A.R., Vasili'ev, A.V., On recognition of the projective special linear groups over the binary field.

The first, third, and last authors were supported by RFBR (Grant 05–01–00797), the State Maintenance Program for the Leading Scientific Schools of the Russian Federation (Grant NSh–2069.2003.1), 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); the fourth author was partially supported by a grant from IPM (No. 84200039).

Received October 26, 2005; published December 9, 2005 .

We consider the regular representation of a finite group G over $\mathbb{C}$. Then G can be viewed as a subgroup of $GL(|G|, \mathbb{C})$ and we can consider

$$\mathrm{Spec}(G) = \bigcup_{g \in G} \mathrm{Spec}(g).$$

It can be easily seen that

$$\mathrm{Spec}(G) = \{\lambda \in \mathbb{C} : \lambda^m = 1 \text{ for } m \in \omega(G)\}.$$

Thus $\omega(G)$ and $\mathrm{Spec}(G)$ are uniquely determined one by the other and the definition of $\omega(G)$ as the spectrum of G is therefore consistent.

If Ω is a non-empty subset of the set of natural numbers, $h(\Omega)$ stands for the number of isomorphism classes of finite groups G with $\omega(G) = \Omega$ and put $h(G) = h(\omega(G))$. We say that G is *recognizable* (by spectrum) if $h(G) = 1$. The group G is *almost recognizable* (resp. *nonrecognizable*) if $1 < h(G) < \infty$ (resp. $h(G) = \infty$). A list of simple groups recognizable, almost recognizable or nonrecognizable by their spectrum is given in [15, 16].

In the present paper, we focus our attention on the projective special linear groups $L_n(2)$. We have good evidence that these groups are recognizable by their spectrum and therefore we put forward the following conjecture.

Conjecture. The projective special linear groups $L_n(2)$ are recognizable by their spectrum for all integers $n \geq 3$.

It has already been proved that the conjecture is true for $n \leq 8$ and $n = 11, 12$ (see [19, 20, 5, 6, 18, 17]). In [13] the conjecture is proved for the linear groups $L_p(2)$, where p is an odd prime such that 2 is a primitive root modulo p (note that this result implies recognizability of $L_{13}(2)$). In [7, 8] the groups $L_n(2^k)$, where $n = 2^m \geq 16$ and k is an arbitrary natural number, are shown to be recognizable; thus the conjecture also holds for $n = 2^m \geq 16$.

In this paper we first establish that for every $n \geq 3$ the projective special linear group $L = L_n(2)$ has the following property. If G is a finite group with the same spectrum as L, then G has a unique non-abelian composition factor and this factor is isomorphic to L; that is, L is *quasirecognizable* by spectrum.

Theorem 1. *The projective special linear group $L_n(2)$ is quasirecognizable by spectrum for all integers $n \geq 3$.*

Second, we prove the conjecture for some new series of integers n. In particular, we prove it for $n = 9, 10, 14, 15$. Thus Conjecture holds true for all $n < 17$.

Theorem 2. *Let p be a prime such that 2 is a primitive root modulo p and m be a natural number such that $2^m - 1 \geq p$. The projective special linear group $L_n(2)$ is recognizable by spectrum for $n = 2^m + p - 1$. If, in addition, 3 does not divide $p - 1$, then the projective special linear group $L_n(2)$ is recognizable by spectrum for $n = 2^m + p + 2$ and $n = p + 3$.*

1. Preliminaries

Our notation is standard. If n is a natural number, π is a set of primes, then by $\pi(n)$ we denote the set of all prime divisors of n, and by n_π we denote the maximal divisor t of n such that $\pi(t) \subseteq \pi$. Note that for a finite group G, $\pi(G) = \pi(|G|)$ by definition. For a set of integers X, by $\operatorname{lcm} X$ we denote the least common multiple of elements from X. By $[x]$ we denote the integer part of x, i. e., the greatest integer that is less than or equal to x.

The spectrum $\omega(G)$ of a group G determines the prime graph (or Gruenberg — Kegel graph) $GK(G)$ whose vertex set is $\pi(G)$ and two vertices p and q are adjacent if and only if $pq \in \omega(G)$. Denote by $s(G)$ the number of connected components of $GK(G)$.

Suppose that S is a simple non-abelian group with $s(S) > 1$ other than $L_4(3)$, $U_4(3)$, and $S_4(3)$, and G is a finite group with $\omega(G) = \omega(S)$. As follows from the Gruenberg-Kegel theorem on groups with disconnected prime graphs [23] and the main result of [1], the group G has a unique non-abelian composition factor H and $s(H) \geq s(G)$, in particular $s(H) > 1$. Simple groups H with $s(H) > 1$ were classified in [23] and [11]. So this classification may be used in proving that $H \simeq S$.

By [11], we have

$$s(L_n(2)) = \begin{cases} 1 & \text{if } n \neq p,\ p+1; \\ \\ 2 & \text{if } n = p \text{ or } p+1, \end{cases}$$

where $p > 3$ is a prime. Thus the class of linear groups over field of order 2 to which above technique can be applied is quite restricted. A similar situation arises for several families of simple groups. Recently a number of papers appeared, concerning the structure of G with $\omega(G) = \omega(S)$ under weaker conditions on the source group S. First, it is shown that G is generally insoluble.

Lemma 1 ([12, Theorem 2]). *Let S be a finite non-abelian simple group other than $L_4(3)$, $U_4(3)$, $S_4(3)$, and Alt_{10}. Suppose that G is a finite group with $\omega(G) = \omega(S)$. Then G is insoluble.*

More constructive result, generalizing in a certain way the Gruenberg-Kegel theorem, was obtained in [21]. The set of vertices of a graph is called independent if vertices of this set are pairwise nonadjacent. Following [21], we denote by $\rho(G)$ (by $\rho(r, G)$ where $r \in \pi(G)$) some independent set in $GK(G)$ (containing r) with maximal number of vertices. Moreover, we define the independence number $t(G)$ of G as $|\rho(G)|$ and the r-independence number $t(r, G)$ of G as $|\rho(r, G)|$.

Lemma 2 ([21]). *Let G be a finite group satisfying two conditions:*

(a) *there exist three primes in $\pi(G)$ which are pairwise nonadjacent in $GK(G)$, that is $t(G) \geq 3$;*

(b) *there exists an odd prime in $\pi(G)$ which is nonadjacent to prime 2 in $GK(G)$, that is $t(2, G) \geq 2$.*

Then there exists a finite non-abelian simple group S such that $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ for 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 $GK(G)$ the Sylow p-subgroup of G is isomorphic to the Sylow p-subgroup of S. In particular, $t(2, S) \geq t(2, G)$.*

Remark that Condition (a) in the statement of above theorem may be replaced by a weaker condition that G is insoluble (see [21]). The information about values of independence and 2-independence numbers of finite simple groups obtained in [22] together with this remark imply the following corollary of Lemma 2.

Lemma 3 ([22, Corollary 7.2]). *Let S be a finite non-abelian 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 that G is a finite group with $\omega(G) = \omega(S)$. Then the conclusion of Lemma 2 holds true for G.*

Above results were applied to the recognition problem in [7, 8], where a series of linear groups with connected prime graph were proved to be recognizable.

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

Lemma 4 (Zsigmondy[24]). *Let q and m be natural numbers greater than 1. There exists a prime divisor r of $q^m - 1$ such that r does not divide $q^i - 1$ for all $i < m$, except for the following cases:*
(a) $m = 6$ *and* $q = 2$;
(b) $m = 2$ *and* $q = 2^l - 1$ *for some natural number* l.

Such a prime r 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). It is also convenient to use the following notation. 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 $q^m \equiv 1 \pmod r$. Thus for a primitive prime divisor r of $q^m - 1$ we have $e(r, q) = m$.

The last lemma describes the spectrum of $L_n(2)$.

Lemma 5 ([13, Lemma 1]). *Let $n = \sum_{i=1}^{N} k_i d_i$, where $k_1, k_2, \ldots, k_N, d_1, \ldots, d_N$ are natural numbers and $n \geq 3$. Let $e = \operatorname{lcm}\{2^{d_1} - 1, 2^{d_2} - 1, \ldots, 2^{d_N} - 1\}$ and m be the smallest integer with $2^m \geq \max\{k_1, k_2, \ldots, k_N\}$. Then $2^m e \in \omega(L_n(2))$. Moreover, every element of $\omega(L_n(2))$ is a divisor of a such product.*

2. Proof of Quasirecognizability for $L_n(2)$

In this paragraph we establish Theorem 1. Since $L_n(2)$ where $n \leq 8$ or $n = 11, 12, 13$ are proved to be recognizable we can assume that either $n = 9, 10$ or $n \geq 14$.

We consider the classical groups of Lie type and denote them according to [3]. Sometimes we use notations $A_l^\varepsilon(q)$, $D_l^\varepsilon(q)$, and $E_6^\varepsilon(q)$, where $\varepsilon \in \{+, -\}$ and $A_l^+(q) = A_l(q)$, $A_n^-(q) = {}^2A_l(q)$, $D_l^+(q) = D_l(q)$, $D_l^-(q) = {}^2D_l(q)$, $E_6^+(q) = E_6(q)$, $E_6^-(q) = {}^2E_6(q)$. We denote the alternating group of degree l by Alt_l to avoid confusing with groups of type A_l.

Let $L = L_n(2) = A_{n-1}(2)$ where $n \geq 9$. By [22, §8] we have $\rho(2, L) = \{2, r_n, r_{n-1}\}$, $t(2, L) = 3$, $t(L) = [(n-1)/2] = 4$ for $n = 9, 10$ and $t(L) = [(n+1)/2] \geq 7$ for $n \geq 14$. Furthermore, Lemma 5 implies that all elements of $\omega(L)$ do not exceed $2^n - 1$.

Let G be a finite group with $\omega(G) = \omega(L)$ and K be the maximal normal soluble subgroup of G. By Lemma 2 there is a finite non-abelian simple group S such that $S \leq \overline{G} = G/K \leq \operatorname{Aut}(S)$. Moreover $t(S) \geq t(G) - 1$ and either $r_n, r_{n-1} \in \pi(S)$ or $S \simeq Alt_7$, $A_1(q)$ where q is odd.

(1) First we consider the exceptions. Let $S \simeq Alt_7$ or $S \simeq A_1(q)$ where $q = p^k > 3$ is odd. Since $t(S) = 3$ it follows that $t(L) \leq 4$ and therefore $n = 9, 10$. By the criterion of adjacency from [22], primes $r_5 = 31$, $r_7 = 127$, $r_8 = 17$, and $r_9 = 73$ are pairwise nonadjacent in $GK(G)$. As follows from [21, Proposition 3], at least

three of these numbers belong to $\pi(S)$. Thus $S \not\simeq Alt_7$. Put $\rho = \{r_5, r_7, r_8, r_9\}$ and $\rho' = \rho \cap \pi(S)$. Since ρ' is an independent set of $GK(S)$ with maximal number of vertices, results of [22, Propositions 2.1,3.1,4.1] give that $\rho' = \{p, r_1', r_2'\}$ where r_1' divides $q-1$ and r_2' divides $q+1$. Thus $p \in \rho'$ and $\rho' \setminus \{p\} \subseteq \pi(q^2-1)$. Therefore $\pi(q^2-1) \cap \rho$ contains two elements. On the other hand, $q = p^k$ must satisfy the inequality $(q+1)/2 \leq 2^{10}-1$, otherwise $\omega(S) \not\subseteq \omega(L)$. Hence if $p = 17$ or 31 then $k \leq 2$; if $p = 73$ or 127 then $k = 1$. We calculate that $\pi(q^2-1) \subseteq \{2, 3, 5, 7, 13, 29, 37\}$ for all possibilities of q. Therefore $\pi(q^2-1) \cap \rho = \varnothing$; a contradiction.

Thus the second statement of Lemma 2 holds and therefore r_n and r_{n-1} divide $|S|$. Moreover, r_n and r_{n-1} are nonadjacent to 2 in $GK(S)$. Therefore $t(2, S) \geq 3$. The simple groups satisfying this condition are described in [22], and we consider them consequently.

(2) S is a sporadic group. Since $r_n, r_{n-1} \in \pi(S)$ there must be two odd primes p_1 and p_2 in $\rho(2, S)$ such that $e(p_1, 2)/e(p_2, 2) = n/(n+1)$. It is false when $n \geq 7$ and $n \neq 11$ (see [22, Table 2] or [4]).

(3) $S \simeq Alt_{n'}$. There are two odd primes among numbers $n', n'-1, n'-2, n'-3$; these are r_n and r_{n-1}. By [2, 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 $4 \cdot r_{n-2}$, it follows that $n' \geq r_{n-2} \geq n'-5$. Thus, there are three odd primes among six consecutive numbers $n', \ldots, n'-5$, which implies $n' = 7$ or $n' = 8$. Hence either $n' = 7, 8$ or $r_{n-2} \in \pi(K)$.

If $n' = 7, 8$ we proceed as in (1). If $n' \geq 9$ and $r_{n-2} \in \pi(K)$ we obtain a contradiction by literally repeating the arguments from the part of [7, § 2] which concerns the alternating groups.

To consider the simple groups of Lie type, it is convenient to separate the case when $n = 9, 10$ from other cases. First we suppose that $n \geq 14$. Then S must satisfy $t(2, S) \geq 3$ and $t(S) \geq t(G)-1 \geq 6$. We obtain such groups from [22, Tables 4–9].

(4) S is a group of Lie type over field of order $q = p^k$, p is odd.

Let $S \simeq E_8(q), E_7(q)$ or $E_6^{\varepsilon}(q)$. If $S \simeq E_8(q)$ then $t(S) = 11$ therefore $n \leq 24$. Since q^8-1 must be less than or equal to $2^{24}-1$, we have that $q \leq 8$. Thus $q = 3, 5$ or 7. If $S \simeq E_7(q)$ then $t(S) = 7$ therefore $n \leq 16$. Since $(q^7-1)/2 \leq 2^{16}-1$, we have that $q = 3, 5$. If $S \simeq E_6^{\varepsilon}(q)$ then $t(S) \leq 6$. Therefore $n \leq 14$ and $(q^6 - \varepsilon 1)/(3, q-\varepsilon 1) \leq 2^{14}-1$, whence $q = 3, 5$. Whatever group S we consider, either a primitive prime divisor r_9' of q^9-1 or a primitive prime divisor r_{18}' of $q^{18}-1$ belongs to $\pi(S) \subseteq \pi(L)$. Suppose that $r_9' \in \pi(L)$. For each $q \in \{3, 5, 7\}$ we calculate r_9' and establish that $e(r_9', 2) \geq 36$. Hence the condition $r_9' \in \pi(L_n(2))$ implies $n \geq 36$, which contradicts to above inequality $n \leq 24$. The case $r_{18}' \in \omega(L)$ can be done similarly.

Let $S \simeq A_{n'-1}^{\varepsilon}(q)$, where $n_2' = (q-\varepsilon 1)_2 > 2$. The inequality $t(S) \geq t(G)-1$ together with $t(S) = [(n'+1)/2]$, $t(G) = [(n+1)/2]$ implies $n' \geq n-3$. The group S contains an element of order $q^{n'-2}-1$, and therefore so does L. Since every element of $\omega(L)$ does not exceed 2^n-1, we have $2^n-1 \geq q^{n'-2}-1$. On the other hand, $q^{n'-2} \geq q^{n-5} \geq 3^{n-5} > 2^n$ for all $n \geq 14$; a contradiction.

Let $S \simeq D_{n'}(q)$, where n' is odd and $q \equiv 5 \pmod 8$. The inequality $t(S) \geq t(G)-1$ together with $t(S) = [(3n'+1)/4]$, $t(G) = [(n+1)/2]$ implies $n' \geq (2n-5)/3$. The group S contains an element of order $(q^{n'}-1)/4$ and therefore $(q^{n'}-1)/4 \leq 2^n-$

1. Whence $q^{n'} \leq 2^{n+2}$. This is impossible, since $q^{n'} \geq q^{(2n-5)/3} \geq 5^{(2n-5)/3} > 2^{n+2}$ for all $n \geq 14$.

Let $S \simeq {}^2D_{n'}(q)$, where n' is odd and $q \equiv 3 \pmod 8$. Since $t(S) = [(3n'+4)/4] = [(3n'+3)/4]$, it follows from $t(S) \geq t(G)-1$ that $n' \geq (2n-7)/3$. Since S contains an element of order $(q^{n'}+1)/4$, we have $(q^{n'}+1)/4 \leq 2^n - 1$. Whence $q^{n'} \leq 2^{n+2}$ and therefore $q^{(2n-7)/3} \leq 2^{n+2}$. The last inequality holds true only if $q = 3$ and $n \leq 100$.

Suppose $S \simeq {}^2D_{n'}(3)$ and $9 \leq n \leq 100$. Since $n' \geq 5$ the group S contains an element of order $(3^5+1)/4 = 61$. Therefore $61 \in \pi(L)$ and $n \geq e(61, 2) = 60$. Since $n \geq 60$, we have $n' \geq (2n-7)/3 > 37$. Therefore S contains an element of order $r'_{36} = 757$. Since $757 \in \pi(L)$, we have $n \geq e(757, 2) = 756$; a contradiction.

(5) S is a group of Lie type over field of order $q = 2^k$. Observe that S is not a simple Suzuki or Ree group, otherwise $t(S) < 6$.

Recall that r_n and r_{n-1} divide $|S|$. Put $e_n = e(r_n, 2^k)$ and $e_{n-1} = e(r_{n-1}, 2^k)$. Since r_n divides $2^{e_n k} - 1$ we have that n divides $e_n k$. By the same reason $n-1$ divides $e_{n-1}k$. Suppose that $e_n k > n$. Then prime r with $e(r, 2) = e_n k$ 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 $e_n k = n$. Suppose that $e_{n-1}k > n-1$. Then $e_{n-1}k \geq 2(n-1) > n$ and the similar argumentation leads us to a contradiction. Thus $e_{n-1}k = n-1$.

If S is a classical group of Lie type other than L then we obtain a contradiction by literally repeating the arguments from the part of [7, § 2] which concerns the corresponding groups.

Let $S \simeq E_8(2^k)$. By [22, Proposition 3.2] an odd prime r is nonadjacent to 2 in $GK(S)$ if and only if $e(r, 2^k) \in \{15, 20, 24, 30\}$. Therefore $e_n, e_{n-1} \in \{15, 20, 24, 30\}$. On the other hand, $e_n/e_{n-1} = n/(n-1)$. These two conditions imply $n \leq 6$; a contradiction.

We consider the groups $E_7(2^k)$, $E_6^{\varepsilon}(2^k)$, $F_4(2^k)$, and $G_2(2^k)$ in the similar way. Namely, by solving the equation $e_n/e_{n-1} = n/(n-1)$ for each group, we find that all solutions are less than 14.

(6) Now we suppose that $L = L_9(2)$ or $L = L_{10}(2)$. Since $\omega(S) \subseteq \omega(L)$ and $r_9 = 73 \in \pi(S)$, we have $\{73\} \subseteq \pi(S) \subseteq \pi(L_{10}(2)) = \{2, 3, 5, 7, 11, 17, 31, 73, 127\}$.

Let S be a classical group of Lie type of rank n' (or $n'-1$ if S of type A^{ε}) over field of order $q = p^k$ where $p \in \pi(L_{10}(2))$. If $p = 2$ and $S \not\simeq L$ we obtain a contradiction as in (5). So we can assume that p is odd. In view of conditions $t(2, S) \geq 3$ and $t(S) \geq 3$ we have $n' \geq 4$. Therefore $q = 3, 5, 7, 9$, or 11, otherwise there is an element in S of order greater than $2^{10} - 1$. On the other hand, either a primitive prime divisor of $q^4 - 1$ or a primitive prime divisor of $q^4 + 1$ belongs to $\omega(S)$. It follows that $q = 3$ or 7. Since $73 \in \pi(S)$ and $e(73, 7) = 24$, $e(73, 3) = 12$, we infer that $n' \geq 12$ for groups of type A^{ε} and $n' \geq 6$ for other classical groups. Thus $q^5 + 1$ divides $|S|$ and therefore a primitive prime divisor of $q^{10} - 1$ belongs to $\pi(S)$. But primitive prime divisors of $7^{10} - 1$ and $3^{10} - 1$ do not lie in $\pi(L_{10}(2))$.

Let S be an exceptional group of Lie type over field of order q.

If q is odd, then S can be isomorphic to $E_8(q)$, $E_7(q)$, $E_6^{\varepsilon}(q)$, $G_2(q)$, or ${}^2G_2(3^{2k+1})$. The first three types of groups have been considered in (4) without using the assumption that $n \geq 14$.

Let $S \simeq G_2(q)$, $q = p^k$ is odd. If $q > 31$ then $2^{10} - 1 < q^2 + q + 1 \in \omega(S)$. Thus we can assume that $q \leq 31$. If $n = 9$ then $17 \in \pi(S)$ and so $17 \in \pi(p(q^6 - 1))$. If $p = 17$ then $307 = 17^2 + 17 + 1 \in \pi(S) \setminus \pi(L)$. Thus $q^6 \equiv 1 \pmod{17}$, whence $q^2 \equiv 1$

(mod 17) and therefore $q \equiv \pm 1 \pmod{17}$. This implies $q \geq 33$; a contradiction. If $n = 10$ then $11 \in \pi(S)$ and so $11 \in \pi(p(q^6-1))$. If $p = 11$ then prime divisor 19 of 11^2+11+1 lies in $\pi(S) \setminus \pi(L)$. Therefore $q \equiv \pm 1 \pmod{11}$. Thus either $q \geq 32$ or $q = 23$. Since $q \leq 31$, it follows that $q = 23$. Since $73 \notin \pi(G_2(23))$, we have a contradiction.

Let $S \simeq {}^2G_2(q)$, where $q = 3^{2k+1}$. It follows from $73 \in \pi(S)$ that 73 divides $q^6-1 = 3^{6(2k+1)}-1$. Therefore $e(73,3) = 12$ divides $6(2k+1)$; a contradiction.

If q is even and S is not a Suzuki or Ree group, we use a technique described in (5). Solving the equation $e_n/e_{n-1} = n/(n-1)$ we find that $S \simeq E_6(q)$ and $n = 9$. Since $13 \in \omega(S) \setminus \omega(L)$, we have a contradiction.

Let $S \simeq {}^2B_2(q)$, where $q = 2^{2k+1} > 2$. If $k > 4$ then $2^{10}-1 < q-1 \in \omega(S)$, so we can assume that $k \leq 4$. Since $r_n, r_{n-1} \in \pi(S)$, we have that r_n, r_{n-1} divide $q^4-1 = 2^{4(2k+1)}-1$ and therefore $n, n-1$ divide $4(2k+1)$; which contradicts to inequalities $n(n-1) \geq 72$ and $4(2k+1) \leq 36$.

Let $S \simeq {}^2F_4(q)$, $q = 2^{2k+1} > 2$. Again we can assume that $k \leq 4$. Since $r_n, r_{n-1} \in \pi(S)$, we have that r_n, r_{n-1} divide $q^6-1 = 2^{6(2k+1)}-1$ and therefore $n, n-1$ divide $6(2k+1)$; which contradicts to inequalities $n(n-1) \geq 72$ and $6(2k+1) \leq 54$.

Thus $S \simeq L$ and Theorem 1 is proved.

3. Proof of Theorem 2

Let G be a finite group with $\omega(G) = \omega(L)$ and K be the maximal normal soluble subgroup of G. We conclude from Theorem 1 that $\overline{G} = G/K$ is an almost simple group with unique non-abelian composition factor isomorphic to L. Thus we can assume that $L \leq \overline{G} \leq \mathrm{Aut}(L)$.

Suppose that $\overline{G} \neq L$. Since $\mathrm{Out}(L) = 2$, we infer that $\overline{G} = \mathrm{Aut}(L) = L\langle\gamma\rangle$ where γ is a graph automorphism. Consider the centralizer $C_L(\gamma)$ of γ in L. If n is odd then $C_L(\gamma)$ contains a subgroup isomorphic to $B_{(n-1)/2}(2)$. Therefore $r_{n-1} \cdot 2 \in \omega(\overline{G}) \subseteq \omega(G)$; a contradiction. If n is even then $C_L(\gamma)$ contains a subgroup isomorphic to $C_{n/2}(2)$. Therefore $r_n \cdot 2 \in \omega(\overline{G}) \subseteq \omega(G)$; a contradiction. Thus $\overline{G} = L$.

Suppose that $K \neq 1$. Then there exists a prime r such that $O^r(K) \neq K$. Denote by $\widetilde{G}$ and $\widetilde{K}$ the factor groups $G/O^r(K)$ 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 factor groups $\widetilde{G}/\Phi(\widetilde{K})$ and $\widetilde{K}/\Phi(\widetilde{K})$ respectively. Since $G/K \simeq \widehat{G}/\widehat{K}$, it is sufficient to proof that $\omega(\widehat{G}) \nsubseteq \omega(L)$. 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 contains L. Therefore $r \cdot \omega(L) \subseteq \omega(C) \subseteq \omega(G) = \omega(L)$. However by [7, Lemma 4(3)] there is $r' \in \pi(L)$ such that $r \cdot r' \notin \omega(L)$. Therefore $r \cdot r' \in r \cdot \omega(L) \setminus \omega(L)$; a contradiction. Thus $C = K$ and L acts faithfully on K.

Thus we can apply results concerning orders of elements arising when a group acts faithfully on an elementary abelian group.

Lemma 6 ([14, Lemma 1])**.** *Let G be a finite group, $K \lhd G$, and 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 $r \cdot |C| \in \omega(G)$ for some prime divisor r of $|K|$.*

Lemma 7 ([7, Lemma 5])**.** *Let L be a finite simple group $L_n(q)$, $d = (q-1, n)$.*

(1) *If there exists a primitive prime divisor r of $q^n - 1$, then L contains a Frobenius subgroup with kernel of order r and cyclic complement of order n;*

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

Suppose that $r \neq 2$. Then we consider the Frobenius subgroup F of L from Lemma 7(2). Applying Lemma 6 to the preimage of F in G we obtain that $r \cdot (2^{n-1}-1) \in \omega(G)$. On the other hand, Lemma 5 implies that $r \cdot (2^{n-1}-1) \notin \omega(L)$; a contradiction.

Thus we can assume that $r = 2$. Observe that the above argumentation does not require a special form of n, as declared in the statement of the Theorem. This form is crucial when K is an elementary abelian 2-group. More precisely, we obtain the following statement.

Proposition 1. *Let $L = L_n(2)$, $n \geq 3$. If a finite group G is a minimal counterexample to the assertion: $\omega(G) = \omega(L) \Rightarrow G \simeq L$, then G is isomorphic to an extension $K \cdot L$ where K is an elementary abelian 2-group on which L acts faithfully.*

Now we fix our attention on groups $L_n(2)$ with n satisfying the conditions of Theorem 2.

Lemma 8. *Let p be a prime such that 2 is a primitive root modulo p and $n = 2^m + p - 1$, $m \geq 1$. If $L = L_n(2)$, then $2^{m+1}p \notin \omega(L)$.*

Proof. Suppose that $2^{m+1}p \in \omega(L)$. By Lemma 5 there exist natural numbers $k_1, \ldots, k_N$ and $d_1, \ldots, d_N$ with $\sum_{i=1}^{N} k_i d_i = n$ satisfying two conditions: (a) $e = \mathrm{lcm}\{2^{d_1}-1, \ldots, 2^{d_N}-1\}$ is divisible by p; (b) the smallest integer l with $2^l \geq \max\{k_1, \ldots, k_N\}$ is greater than or equal to $m+1$. Since p divides e, it follows that p divides $2^{d_i}-1$ for some d_i. By hypothesis, 2 is a primitive root modulo p, therefore d_i is divisible by $p-1$. On the other hand, from $l \geq m+1$ we deduce that there exists j such that $k_j > 2^m$. If $i = j$ then $n \geq k_i d_i > 2^m(p-1) \geq 2^m + p - 1 = n$; a contradiction. If $i \neq j$ then $n \geq k_j + d_i > 2^m + p - 1 = n$; a contradiction. The lemma is proved. □

Lemma 9. *Let p be a prime such that 2 is a primitive root modulo p, $n = 2^m + p - 1$, $2^m - 1 \geq p$ and $L = L_n(2)$. Suppose that K is an elementary abelian 2-group on which L acts faithfully. Then there exists an element of order $2^{m+1}p$ in KL and $\omega(KL) \neq \omega(L)$.*

Proof. The group L contains two subgroups $A \simeq L_p(2)$ and $B \simeq L_{n-p}(2)$ such that $A \times B$ is a subgroup of L. By Lemma 7(1) there is a Frobenius subgroup $F = \langle x, y \rangle$ of A with $|x| = p$, $|y| = r_p$, where r_p is a primitive prime divisor of $2^p - 1$. The group F acts on $M = [K, y]$ in such a way that $C_M(y) = 1$ and $C_M(x) \neq 1$. In particular,

$$K_0 = C_K(x) \not\leq C_K(y). \qquad (*)$$

It is easy to see that $C_L(x) = \langle x \rangle \times N$ where $N \simeq L_{n-p+1}(2) = L_{2^m}(2)$ and N acts on K_0. If this action is not faithful then N centralizes K_0 and hence $C_L(x)$ centralizes K_0. It is obvious that $B \leq N$ contains a subgroup F^z which is a conjugate of F in L. Since $|C_K(x^z)| = |K_0|$ and $K_0 \leq C_K(N) \leq C_K(x^z)$, we see that $C_K(x^z) = K_0$ and hence $C_L(x^z)$ centralizes K_0. Since $y \in C_L(x^z)$, then y

centralizes K_0. This contradicts $(*)$. So N acts faithfully on K_0. By Lemma 7(1), there exists a Frobenius subgroup in N of type $r_{2^m} : 2^m$. By Lemma 6 we have $2^{m+1} \in \omega(K_0N)$. Hence there is an element of order $2^{m+1}p$ in KL. On the other hand, by Lemma 8 there is no element of order $2^{m+1}p$ in L, thus concluding the proof. □

Lemma 10. *Let p be a prime such that 2 is a primitive root modulo p, 3 does not divide $p-1$, $n = 2^m + p - 1$, $2^m - 1 \geq p$ or $n = p$ and $L = L_{n+3}(2)$. Let K be an elementary abelian 2-group on which L acts faithfully. Then $\omega(KL) \neq \omega(L)$.*

Proof. Using [9] or [10] it is easy to verify that every element of order 7 from $L_5(2)$ centralizes some nontrivial element in every irreducible $L_5(2)$-module over a field of characteristic 2 and so the same is true for every $L_5(2)$-module over a field of characteristic 2. If x is an element of order 7 of L contained in a subgroup isomorphic to $L_3(2)$, then its centralizer $K_0 = C_K(x)$ in K is not trivial. It is easy to see that $C_L(x) = \langle x \rangle \times N$ where $N \simeq L_n(2)$ and N acts on K_0. If this action is not faithful, then N centralizes K_0. At first, assume that 3 does not divide n. Using Lemma 5 and arguments as in proof of Lemma 8, we obtain that L does not contain an element of order $2 \cdot 7 \cdot r_n$ where r_n is a primitive prime divisor of $2^n - 1$. On the other hand, since N centralizes K_0, there exists an element of order $2 \cdot r_n$ in K_0N, which implies that there is an element of order $2 \cdot 7 \cdot r_n$ in KL. So $\omega(KL) \neq \omega(L)$ and the lemma is proved in this case. If 3 divides n then using Lemma 5 we obtain that $2 \cdot 7 \cdot r_{n-1} \notin \omega(L)$. But K_0N contains an element of order $2 \cdot r_{n-1}$, and so KL contains an element of order $2 \cdot 7 \cdot r_{n-1}$. Thus $\omega(KL) \neq \omega(L)$ again.

Therefore we can suppose that N acts on K_0 faithfully. We first suppose that $n = 2^m + p - 1$. By Lemma 9 there is an element of order $p \cdot 2^{m+1}$ in K_0N which implies that there is an element of order $7 \cdot p \cdot 2^{m+1}$ in KL. Suppose that $7 \cdot p \cdot 2^{m+1} \in \omega(L_{n+3}(2))$. Since 7 is a primitive prime divisor of $2^3 - 1$, p is a primitive prime divisor of $2^{p-1} - 1$, and 3 does not divide $p - 1$, by Lemma 5 we have that $n + 3 > 2^m + (p-1) + 3 = n + 3$. Thus $7 \cdot p \cdot 2^{m+1} \notin \omega(L)$.

Suppose now that $n = p + 3$. Then by Lemma 6 and Lemma 7, there exists an element of order $p \cdot 2$ in K_0N. Therefore $7 \cdot p \cdot 2 \in \omega(KL)$. Suppose that $7 \cdot p \cdot 2 \in \omega(L_{n+3})$. Since 7 is a primitive prime divisor of $2^3 - 1$, p is a primitive prime divisor of $2^{p-1} - 1$, and 3 does not divide $p - 1$, by Lemma 5 we have that $n + 3 \geq 2 + (p-1) + 3 = n + 4$, a contradiction. The Lemma is thus proved. □

Applying Lemmas 9 and 10 we establish that $K = 1$ and therefore $L = G$. Theorem 2 is proved.

Remark. Since 2 is a primitive root modulo p for $p = 3, 5, 11$, Theorem 2 yields that groups $L_n(2)$ are recognizable for $n = 4 + (3-1) + 3 = 9$, $n = 8 + (3-1) = 10$, $n = 11 + 3 = 14$, and $n = 8 + (5-1) + 3 = 15$. Together with previous results it implies that groups $L_n(2)$ are recognizable by spectrum for all $n < 17$.

References

[1] M.R. Aleeva, *On finite simple groups with the set of element orders as in a Frobenius group or a double Frobenius group*, Math. Notes, **73** (2003), 299–313.

[2] R.W. Carter, *Centralizers of semisimple elements in the finite classical group*, Proceedings of London Mathematical Society (3), **42** (1981), 1–41.

[3] R.W. Carter, *Simple groups of Lie type*, John Wiley & Sons, London, 1972.

[4] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[5] M.R. Darafsheh and A.R. Moghaddamfar, *Characterization of the groups* $PSL_5(2)$*,* $PSL_6(2)$ *and* $PSL_7(2)$, Comm. in Algebra, **29** (2001), 465–475. *Corrigendum to: Characterization of the groups* $PSL_5(2)$*,* $PSL_6(2)$ *and* $PSL_7(2)$, Comm. in Algebra, **32** (2003), 4651–4653.

[6] M.R. Darafsheh and A.R. Moghaddamfar, *A characterization of groups related to the linear groups* $PSL(n, 2)$*,* $n = 5, 6, 7, 8$, Pure Mathematics and Application, **11** (2000), 629–637.

[7] M.A. Grechkoseeva and A.V. Vasil'ev, *On recognition by spectrum of finite simple linear groups over fields of characteristic* 2, Sib. Math. J., **46** (2005), 593–600.

[8] M.A. Grechkoseeva, W.J. Shi and A.V. Vasil'ev, *Recognition by spectrum of* $L_{16}(2^m)$, to appear in Algebra Colloquium.

[9] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4, 2004; (http://www.gap-system.org).

[10] C. Jansen, K. Lux, R.A. Parker and R.A. Wilson, *An atlas of Brauer characters*, Clarendon Press, Oxford, 1995.

[11] A.S. Kondratév, *On prime graph components of finite simple groups*, Math. USSR Sbornik, **180** (1989), 787–797.

[12] M.S. Lucido andA. R. Moghaddamfar,*Groups with complete prime graph connected components*, J. Group Theory, **7** (2004), 373–384.

[13] M.S. Lucido and A.R. Moghaddamfar, *Recognition of some linear groups over the binary field through their spectrum*, to appear in Siberian Math. J., **46** (2005).

[14] V.D. Mazurov, *Characterizations of finite groups by sets of element orders, Algebra and Logic*, **36** (1997), 23–32.

[15] V.D. Mazurov, *Recognition of finite simple groups* $S_4(q)$ *by their element orders*, Algebra and Logic, **41** (2002), 93–110.

[16] V.D. Mazurov, *Characterization of groups by arithmetic properties*, Algebra Colloquium, **11** (2004), 129–140.

[17] A.R. Moghaddamfar, *On spectrum of linear groups over the binary field and recognizability of* $L_{12}(2)$, to appear in International Journal of Algebra and Computation.

[18] A.R. Moghaddamfar, A.R. Zokayi and M. Khademi, *A characterization of the finite simple group* $L_{11}(2)$ *by its element orders*, Taiwanese J. Math., **9** (2005), 445–455.

[19] W.J. Shi, *A characteristic property of* $PSL_2(7)$, J. Austral Math. Soc., Ser. A., **36** (1984), 354–356.

[20] W.J. Shi, *A characteristic property of* A_8, Acta Math. Sin. New Ser. **3** (1987), 92–96.

[21] A.V. Vasil'ev, *On connection between the structure of finite group and properties of its prime graph*, Sib. Math. J., **46** (2005), 396–404.

[22] A.V. Vasil'ev and E.P. Vdovin, *An adjacency criterion for two vertices of the prime graph of a finite simple group*, to appear in Algebra and Logic (See also Preprint No. 152, Sobolev Institute of Mathematics, Novosibirsk, 2005).

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

[24] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3**(1892), 265–284.

Maria Alexandrovna Grechkoseeva
Novosibirsk State University,
Pirogova st. 2,
630090, Novosibirsk, Russia
E-mail address: `grechkoseeva@gorodok.net`

Maria Silvia Lucido
Universitá degli Studi di Udine,
Udine, Italy
E-mail address: `mslucido@dimi.uniud.it`

Victor Danilovich Mazurov
Sobolev Institute of Mathematics,
prospect ak. Koptyuga 4,
630090, Novosibirsk, Russia
E-mail address: `mazurov@math.nsc.ru`

Ali Reza Moghaddamfar
Department of Mathematics, Faculty of Science,
K. N. Toosi University of Technology,
P. O. Box 16315 – 1618, Tehran, Iran,
Institute for Studies in Theoretical Physics and Mathematics (IPM)
E-mail address: moghadam@kntu.ac.ir, moghadam@ipm.ir

Andrei Victorovich Vasili'ev
Sobolev Institute of Mathematics,
prospect ak. Koptyuga 4,
630090, Novosibirsk, Russia
E-mail address: vasand@math.nsc.ru