S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 7, стр. 435–444 (2010) УДК 512.542

MSC 20D60

QUASIRECOGNIZABILITY OF SIMPLE UNITARY GROUPS OVER FIELDS OF EVEN ORDER

M. A. GRECHKOSEEVA

Abstract. We refer to the set of element orders of a finite group as the spectrum of this group and say that two groups are isospectral if their spectra coincide. We prove that finite simple unitary groups of dimension at least 5 over fields of characteristic 2 other than $U_5(2)$ are quasirecognizable by spectrum, that is every finite group isospectral to such unitary group U has a unique nonabelian composition factor and this factor is isomorphic to U.

Keywords: unitary group, element orders, spectrum.

1. Introduction

For a finite group G, the set of element orders of G is called the *spectrum* of G and denoted by $\omega(G)$. We say that G is *recognizable by spectrum* if every finite group H with $\omega(H) = \omega(G)$ is isomorphic to G. The problem of recognition by spectrum is of primary interest for almost simple groups, in particular, for nonabelian simple groups (see [1, 2]). A nonabelian simple group L is said to be *quasirecognizable by spectrum* if every finite group H with $\omega(H) = \omega(L)$ has a unique nonabelian composition factor and this factor is isomorphic to L.

The present paper deals with quasireconizability of finite simple unitary groups over fields of characteristic 2. The simple unitary groups $U_3(2^\alpha)$, $\alpha \geqslant 2$, and $U_4(2^\alpha)$,

---

Grechkoseeva, M.A., Quasirecognizability of simple unitary groups over fields of even order.

The work is supported by the RFBR (grants 08–01–00322, 10–01–90007–Bel), the Council for Grants under the President of the Russian Federation (grants NSh–3669.2010.1, MK–2136.2010.1), the Program "Development of the Scientific Potential of Higher School" of the Russian Federal Agency for Education (Grant 2.1.1.419), the Federal Target Program "Scientific and Educational Personnel of Innovation Russia" in 2009-2013 (gov. contracts nos. 02.740.11.0429, 14.740.11.0346), and Lavrent′ev Young Scientists Competition (no. 43 on 04.02.2010).

Received November, 17, 2010, published November, 25, 2010.

$\alpha \geqslant 2$, are recognizable [3, 4]. The group $U_3(2)$ is soluble and the groups $U_4(2), U_5(2)$ are not quasirecognizable [5]. Also $U_6(2)$ is known to be recognizable [6]. Recently in [7], the problem of quasirecognizability of a simple linear or unitary group L was reduced to a special case when a group H with $\omega(H) = \omega(L)$ has a nonabelian composition factor isomorphic to a group of Lie type in cross characteristic, that is in characteristic different from the defining characteristic of L. The goal of the present paper is to handle this special case for unitary groups over fields of characteristic 2 and thus prove the following

Theorem. *If $L = U_m(2^\alpha)$, where $m \geqslant 5$, and $L \neq U_5(2)$ then L is quasirecognizable by spectrum.*

Together with the results mentioned above, this theorem implies

Corollary. *If L is a simple unitary group over a field of characteristic 2 other than $U_4(2)$ and $U_5(2)$ then L is quasirecognizable by spectrum.*

2. Preliminaries

Our notation of simple classical groups and exceptional groups of Lie type follows [8]. For brevity, we also use abbreviations $L_n^\varepsilon(q)$ and $E_6^\varepsilon(q)$, where $\varepsilon = \pm$ and $L_n^+(q)$, $L_n^-(q)$, $E_6^+(q)$, and $E_6^-(q)$ stand for $L_n(q)$, $U_n(q)$, $E_6(q)$, and ${}^2E_6(q)$, respectively. In such situations, we identify ε and $\varepsilon 1$.

We write $[x]$ for the integer part of a number x. The set of prime divisors of a natural number m is denoted by $\pi(m)$. For a finite group G, by definition $\pi(G) = \pi(|G|)$. We denote by $[m_1, m_2, \dots, m_s]$ and $(m_1, m_2, \dots, m_s)$ the least common multiple and greatest common divisor of numbers $m_1, m_2, \dots, m_s$, respectively. For a prime r, the r-part of a natural number m is the largest r-power dividing m. We write m_r for the r-part of m and $m_{r'}$ for the quotient m/m_r.

Let G be a finite group and $\omega(G)$ its spectrum. The divisibility relation endows $\omega(G)$ with a partial order; and the subset of elements maximal under this order is denoted by $\mu(G)$. For a prime r, we refer to the largest power of r in $\omega(G)$ as the *r-period* of G.

The *Gruenberg–Kegel graph* (or *prime graph*) of G is a graph $GK(G)$ whose vertex set is $\pi(G)$ and two different vertices p and r are connected by an edge if and only if $pr \in \omega(G)$. The maximal cardinality of independent sets of vertices (or the independence number) of $GK(G)$ is denoted by $t(G)$; the maximal cardinality of independent sets containing the vertex 2 is denoted by $t(2, G)$. The neighborhood of a vertex is the set consisting of the vertex itself and adjacent vertices.

Lemma 1 ([9, 10]). *Let G be a finite group satisfying conditions $t(G) \geqslant 3$ and $t(2, G) \geqslant 2$. Then the following assertions hold:*

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

(b) *For every independent set ρ consisting of at least 3 vertices in $GK(G)$, at most one prime of ρ divides $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geqslant t(G) - 1$.*

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

Lemma 2 ([11, Lemma 3]). *Let G be a finite group, K a normal soluble subgroup of G, and $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$ for a simple group S. Suppose there are t and s in $\pi(S) \setminus \pi(K)$ whose neighborhoods in $GK(G)$ disjoint. If $r \in \pi(K)$ is adjacent* *neither to t nor to s in $GK(G)$, while S includes a Frobenius subgroup with cyclic complement C and kernel F such that $(|F|, r) = 1$, then $r|C| \in \omega(G)$.*

Lemma 3. *Let q be odd and let S be isomorphic to one of the groups $L_4^\varepsilon(q)$ with $q - \varepsilon \equiv 4 \pmod 8$, $D_n^\varepsilon(q)$ with odd n and $q - \varepsilon \equiv 4 \pmod 8$, $E_6^\varepsilon(q)$, $G_2(q)$. Then S has the following properties:*

(a) *If r is an odd prime and $2r \in \omega(S)$ then $4r \in \omega(S)$.*

(b) *If $S \leq G \leq \operatorname{Aut} S$, r divides $|G/S|$ and $r > 3$ then $4r \in \omega(G)$.*

(c) *There is a Frobenius subgroup with cyclic complement of order 4 in S.*

Proof. For $S \not\simeq G_2(q)$, the assertion is proved in [12, Lemma 4]. Let $S = G_2(q)$. By [13, Lemma 2.1], there is a Frobenius subgroup with kernel of order q^2 and cyclic complement of order $q^2 - 1$ in S, proving (c). By [14, 2.3], if r is an odd prime and $2r \in \omega(S)$ then r divides $q^2 - 1$. This proves (a). Suppose that $S \leq G \leq \operatorname{Aut} S$ and $|G/S|$ is divisible by an odd prime r greater than 3. Then G contains a field automorphism φ of S of order r. Since $C_S(\varphi) \simeq G_2(q^{1/r})$ and $4 \in \omega(G_2(q^{1/r}))$, assertion (b) follows. □

For a integer m and an odd prime r such that $(m, r) = 1$, we write $e(r, m)$ to denote the multiplicative order of m modulo r. Given an odd m, we put $e(2, m) = 1$ if $m \equiv 1 \pmod 4$ and put $e(2, m) = 2$ if $m \equiv 3 \pmod 4$.

Let m be an integer and $|m| > 1$. A prime r is said to be a *primitive prime divisor* of $m^i - 1$ if $e(r, m) = i$. The existence of primitive divisors for almost all pairs of m and i was established by Zsigmondy.

Lemma 4 ([15])**.** *Let m be an integer and $|m| > 1$. For every natural number $i > 2$, there is a prime r with $e(r, m) = i$, except when $(m, i) \in \{(2, 6), (-2, 3)\}$.*

In what follows, $r_i(m)$ stands for a primitive prime divisor of $m^i - 1$ if such exist. The product of all primitive divisors of $m^i - 1$ taken with multiplicities is said to be the *greatest primitive divisor* and denoted by $k_i(m)$. Note that for a divisor, the property of being primitive depends on the pair (m, i) and is not determined by the number $m^i - 1$. For example, $k_6(2) = 1$ while $k_3(4) = 7$ and $k_6(-2) = 7$. By [16], we have that for $i > 2$

$$(*) \qquad k_i(n) = \frac{|\Phi_i(n)|}{(r, \Phi_{i_{r'}}(n))},$$

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

Lemma 5. *Let q be an integer and $q > 1$. The following assertions hold:*

(a) *If i is an odd prime then*

$$k_i(q) \geqslant \frac{q^{i-1}}{(i, q-1)} \text{ and } k_i(-q) \geqslant \frac{q^{i-1}}{2(i, q+1)}.$$

(b) *If $\varepsilon = \pm 1$ then $[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}] \leqslant q^{(n_1 + \dots + n_s)} + 1$.*

Proof. By $(*)$, we have

$$k_i(q) = \frac{q^i - 1}{(q-1)(i, q-1)} \text{ and } k_i(-q) = \frac{q^i + 1}{(q+1)(i, q+1)}.$$

Since $(q^i - 1)/(q-1) = q^{i-1} + \dots + 1 \geqslant q^{i-1}$ and $(q^i + 1)/(q+1) \geqslant q^i/(q+1) \geqslant q^{i-1}/2$, assertion (a) follows.

In (b) we may assume that $s > 1$ and $\varepsilon = -1$. Then

$$[q^{n_1} - (-1)^{n_1}, \dots, q^{n_s} - (-1)^{n_s}] \leqslant (q+1)\frac{q^{n_1} - (-1)^{n_1}}{q+1} \dots \frac{q^{n_s} - (-1)^{n_s}}{q+1} \leqslant$$
$$\leqslant (q+1)q^{n_1-1} \dots q^{n_s-1} = (q+1)q^{n_1+\dots+n_s-s} \leqslant (q+1)q^{n_1+\dots+n_s-2} \leqslant q^{n_1+\dots+n_s}.$$

□

Lemma 6 ([17])**.** *Let $L = L_n^\varepsilon(q)$, where $n \geqslant 3$, $q = p^\alpha$, and $\varepsilon = \pm$, and let $d = (n, q-\varepsilon)$. Then $\omega(L)$ consists of all divisors of the following numbers:*

(1) $\dfrac{q^n - \varepsilon^n}{d(q-\varepsilon)}$;

(2) $\dfrac{[q^{n_1} - \varepsilon^{n_1}, q^{n_2} - \varepsilon^{n_2}]}{(n/(n_1, n_2), q-\varepsilon)}$, *where $n_1, n_2 > 0$ and $n_1 + n_2 = n$;*

(3) $[q^{n_1} - \varepsilon^{n_1}, q^{n_2} - \varepsilon^{n_2}, \dots, q^{n_s} - \varepsilon^{n_s}]$, *where $s \geqslant 3$, $n_1, n_2, \dots, n_s > 0$ and $n_1 + \dots + n_s = n$;*

(4) $p^\gamma \dfrac{q^{n_1} - \varepsilon^{n_1}}{d}$, *where $\gamma, n_1 > 0$, $p^{\gamma-1} + 1 + n_1 = n$;*

(5) $p^\gamma[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}]$, *where $s \geqslant 2$, $\gamma, n_1, \dots, n_s > 0$ and $p^{\gamma-1} + 1 + n_1 + \dots + n_s = n$;*

(6) p^γ *if $p^{\gamma-1} + 1 = n$ for $\gamma > 0$.*

Lemma 7. *Let $L = L_n^\varepsilon(q)$, where $n \geqslant 3$, $q = p^\alpha$, and $\varepsilon = \pm$. If $a \in \omega(L)$ and $a_p \geqslant p^\delta > 2$ then $n \geqslant p^{\delta-1} + 1$ and $a \leqslant p^\delta(q^{n-p^{\delta-1}-1} + 1)$. If, in addition, $a_{p'} > 1$ then $n \geqslant p^{\delta-1} + 2$.*

Proof. By Lemma 6, there are $\gamma \geqslant \delta$, $s \geqslant 1$ and $n_1, \dots, n_s$ such that $p^{\gamma-1} + 1 + n_1 + \dots + n_s = n$ and a divides $p^\gamma[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}]$. Thus $n \geqslant p^{\delta-1} + 1$. If $a_{p'} > 1$ then $n > p^{\delta-1} + 1$. By Lemma 5, we have

$$a \leqslant p^\gamma[q^{n_1} - \varepsilon^{n_1}, \dots, q^{n_s} - \varepsilon^{n_s}] \leqslant p^\gamma(q^{n_1+\dots+n_s} + 1) = p^\gamma(q^{n-p^{\gamma-1}-1} + 1).$$

If $\gamma = \delta$ then the lemma is proved. Suppose $\gamma - \delta \geqslant 1$. Then

$$\frac{p^\delta(q^{n-p^{\delta-1}-1} + 1)}{p^\gamma(q^{n-p^{\gamma-1}-1} + 1)} \geqslant \frac{q^{n-p^{\delta-1}-1}}{p^{\gamma-\delta}q^{n-p^{\gamma-1}}} \geqslant \frac{q^{n-p^{\delta-1}-1}}{q^{n-p^{\gamma-1}+\gamma-\delta}} = q^{p^{\gamma-1}-p^{\delta-1}-\gamma+\delta-1} \geqslant 1,$$

where the last inequality holds since

$$p^{\gamma-1} - p^{\delta-1} = p^{\delta-1}(p^{\gamma-\delta} - 1) \geqslant 2(\gamma - \delta) \geqslant \gamma - \delta + 1.$$

□

Lemma 8. *Let q be an integer, $q > 1$, and $\varepsilon = \pm 1$. If 4 divides $q - \varepsilon$ then $(q^m - \varepsilon^m)_2 = m_2(q-\varepsilon)_2$.*

Proof. If m is odd then $(q^m - \varepsilon^m)/(q-\varepsilon)$ is odd. Thus we may assume that $m = 2^l$ with $l \geqslant 1$. Then

$$(q^m - \varepsilon^m)_2 = (q^m - 1)_2 = (q-\varepsilon)_2 \prod_{i=0}^{l-1}(q^{2^i} + \varepsilon^{2^i})_2 = 2^l(q-\varepsilon)_2 = m_2(q-\varepsilon)_2.$$

□

3. Auxiliary results

We extract a part of the proof of the theorem as a separate section, since it can be applied not only to unitary groups.

Hypothesis A. L is a nonabelian simple group and there are odd primes t, s and r in $\pi(L)$ such that
(a) $\{t,s,r\}$ and $\{t,s,2\}$ are cocliques in $GK(L)$;
(b) the neighborhoods of t and s in $GK(L)$ disjoint;
(c) $r>3$ and $4r\notin\omega(L)$.

Throughout this section we assume that L satisfies Hypothesis A and adopt notation of this hypothesis. Let G be a finite group such that $\omega(G)=\omega(L)$ and K be the soluble radical of G. By Lemma 1, we have $S\leq\overline{G}=G/K\leq\operatorname{Aut}S$ with S being a nonabelian simple group. Moreover, $t(2,S)\geqslant 3$, the primes t, s divide $|S|$ and does not divide $|K|\cdot|\overline{G}/S|$.

Lemma 9. *If $p,q\in\pi(K)$, $p^x,q^y\in\omega(K)$, and $pt,qt\notin\omega(L)$ then $p^xq^y\in\omega(G)$.*

Proof. Let H be a Hall $\{p,q\}$-subgroup of K and $N=N_G(H)$. By the Frattini argument, $G=NK$ and hence $N/(N\cap K)\simeq G/K$. An element of order t in N acts on H fix-point-freely. By Thompson's theorem, we have that H is nilpotent. Thus $p^xq^y\in\omega(H)$. □

Proposition 1. *If $8\in\omega(L)$ then $S\not\simeq L_2(q)$, where q is odd.*

Proof. Suppose that $S\simeq L_2(q)$ and $q=p^k$, where p is an odd prime. Then $\mu(S)=\{p,(q+1)/2,(q-1)/2\}$ and $\mu(\operatorname{Inndiag}S)=\{p,q+1,q-1\}$. In particular, $t(2,\operatorname{Inndiag}S)=1$ and thus $\overline{G}$ does not include $\operatorname{Inndiag}S$.

Choose $\varepsilon=\pm1$ such that $q\equiv\varepsilon\pmod 4$. The group S contains elements of order 4 if and only if $q-\varepsilon$ is a multiple of 8. If 8 does not divide $q-\varepsilon$ then k is odd and therefore $2\notin\pi(\overline{G}/S)$. Thus the conditions $q\not\equiv\varepsilon\pmod 8$ and $4\notin\omega(\overline{G})$ are equivalent.

Since t and s divide $|S|$ and $2t,2s\notin\omega(S)$, it follows that one of them is equal to p, while the other divides $(q+\varepsilon)/2$. We may assume that $t=p$ and s divides $q+\varepsilon$.

Let r divides $|\overline{G}/S|$. Since r is odd, it follows that $\overline{G}$ contains a field automorphism φ of S of order r. The centralizer $C_S(\varphi)$ is isomorphic to $L_2(q^{1/r})$ and hence contains an element of order $p=t$. Thus $tr\in\omega(G)$.

Let $r\in\pi(S)$. Then r divides $(q-\varepsilon)/2$ and 8 does not divide $q-\varepsilon$. Therefore $4\notin\omega(\overline{G})$. On the other hand, $8\in\omega(G)$ and so $2\in\pi(K)$. A Borel subgroup B of S is a Frobenius group with kernel of order q and cyclic complement of order $(q-1)/2$. Applying Lemma 2, we infer that $q-1\in\omega(G)$. This yields $4r\in\omega(G)$ for $\varepsilon=1$ and $2s\in\omega(G)$ for $\varepsilon=-1$.

Finally, let $r\in\pi(K)$. Applying Lemma 2 with B as a Frobenius group again, we deduce that $r(q-1)/2\in\omega(G)$. If $\varepsilon=-1$ then $sr\in\omega(G)$. If 8 divides $q-1$ then $4r\in\omega(G)$. If $\varepsilon=1$ and $q-1$ is not a multiple of 8 then $4\notin\omega(\overline{G})$. Hence $4\in\omega(K)$ and $4r\in\omega(G)$ by Lemma 9.

Thus in any case at least one of the numbers tr, sr, $2s$, and $4r$ lies in $\omega(G)$. This contradiction proves the proposition. □

Proposition 2. *Let q be odd. Then S is isomorphic to none of $L_4^{\varepsilon}(q)$, $O_{2n}^{\varepsilon}(q)$, $E_6^{\varepsilon}(q)$, $G_2(q)$. Furthermore, if $q>3$ then S is not isomorphic to $E_7(q)$.*

Proof. Suppose that S is isomorphic to one of the groups $L_4^\varepsilon(q)$, $O_{2n}^\varepsilon(q)$, $G_2(q)$, and $E_6^\varepsilon(q)$. Since $t(2,S) \geqslant 3$, it follows from [19, Tables 4 and 6] that n is odd and $q-\varepsilon 1 \equiv 4 \pmod 8$ when $S \simeq O_{2n}^\varepsilon(q)$; and $q-\varepsilon 1 \equiv 4 \pmod 8$ when $S \simeq L_4^\varepsilon(q)$. We assume these conditions. Then $t(2,S)=3$.

Let $r \in \pi(S)$. The equality $t(2,S)=3$ forces that $2r \in \omega(S)$. Then by Lemma 3(a), there is an element of order $4r$ in S.

Let $r \in \pi(\overline{G}/S)$. Then $4r \in \omega(G)$ by Lemma 3(b).

Finally, let $r \in \pi(K)$. By Lemma 3(c), there is a Frobenius subgroup with cyclic complement of order 4 in S. By the above part of the proof, we may assume that $r \notin \pi(S)$ and so the order of the Frobenius kernel of this subgroup is coprime to r. Then Lemma 2 implies that $4r \in \omega(G)$.

Thus in any case $4r \in \omega(G)$, and this contradiction proves the first part of the proposition.

Suppose that $S \simeq E_7(q)$. The vertices t and s of $GK(S)$ must have disjoint neighborhoods in $GK(S)$, as they does in $GK(G)$. But for $q>3$, the intersection of neighborhoods of any two vertices of $GK(S)$ nonadjacent to 2 contains some odd prime divisor of q^2-1 (see the compact form of $GK(S)$ in [18]). □

4. Proof of the theorem

Let $L=U_m(u)$, where $u=2^\alpha$ and $m \geqslant 5$. Since $U_5(2)$ is not quasirecognizable [5] and $U_6(2)$ is recognizable [6], we may assume that $(n,\alpha) \neq (5,1),(6,1)$. Then $t(L)=[(m+1)/2]$ by [18, Table 2]. Furthermore, by Lemma 4 there exist primitive prime divisors $r_m=r_m(-u)$, $r_{m-1}=r_{m-1}(-u)$, and $r_{m-2}=r_{m-2}(-u)$. Observe that all these numbers are greater than 3, as 3 divides u^2-1. It follows by [18, Table 2] and Lemma 6 that L satisfies Hypothesis A with $t=r_m$, $s=r_{m-1}$, and $r=r_{m-2}$.

Let G be a finite group such that $\omega(G)=\omega(L)$, K the soluble radical of G, and S a nonabelian simple group such that $S \leq \overline{G}=G/K \leq \operatorname{Aut} S$. By [7, Theorems 1–3], either $S \simeq L$, as required, or S is isomorphic to a group of Lie type over a field of odd characteristic.

Suppose that S is a group of Lie type over a field of odd characteristic. By Lemma 6, we have $8 \in \omega(L)$ and so S is not isomorphic to $L_2(q)$ by Proposition 1. Also S cannot be isomorphic to any of $L_4^\varepsilon(q)$, $O_{2n}^\varepsilon(q)$, $E_6^\varepsilon(q)$, $G_2(q)$, and $E_7(q)$, excepting $E_7(3)$, by Proposition 2. Finally, S is not isomorphic to any of $O_{2n+1}(q)$, $PSp_{2n}(q)$, $F_4(q)$, and ${}^3D_4(q)$ since otherwise $t(2,S)<3$ by [19, Tables 5 and 6]. Thus the only possibilities for S are $L_n^\varepsilon(q)$ with $n \neq 2,4$, $E_8(q)$, ${}^2G_2(q)$ and $E_7(3)$.

By Lemma 1, we have $t(2,S) \geqslant 3$ and $t(S) \geqslant t(L)-1$. Moreover, all prime divisors of $k_m(-u)$ and all prime divisor of $k_{m-1}(-u)$ do not divide $|K|\cdot|\overline{G}/S|$. Hence $k_m=k_m(-u)$ and $k_{m-1}=k_{m-1}(-u)$ lie in $\omega(S)$, and their prime divisors are not adjacent to 2 in $GK(S)$.

1. Suppose that $S \simeq L_n^\varepsilon(q)$ with q odd and $n \neq 2,4$. Since $t(2,S) \geqslant 3$, it follows from [19, Table 5] that $n_2=(q-\varepsilon)_2>2$. In particular, $n \geqslant 8$ and n is a multiple of 4. Using the inequality $t(S) \geqslant t(L)-1$ together with [19, Table 8], we infer that

$$\frac{n}{2}=\left[\frac{n+1}{2}\right]=t(S) \geqslant \left[\frac{m+1}{2}\right]-1.$$

We claim that the 2-period of L is smaller than that of S. By Lemma 6, the 2-period of L is 2^γ, where γ satisfies $2^{\gamma-1}<m \leqslant 2^\gamma$. Observe that $\gamma \geqslant 3$.

Now
$$n \geqslant 2\left[\frac{m+1}{2}\right]-2 > 2\left[\frac{2^{\gamma-1}+1}{2}\right]-2 = 2^{\gamma-1}-2,$$
and since 4 divides n, it follows that $n \geqslant 2^{\gamma-1}$. By Lemma 6, for every $l \leqslant n-2$ there is an element of order q^l-1 in S. If $n > 2^{\gamma-1}$ then $2^{\gamma-1} \leqslant n-4$ and so $(q^{2^{\gamma-1}}-1)_2 \in \omega(S)$. Using Lemma 8, we see that $(q^{2^{\gamma-1}}-1)_2 = 2^{\gamma-1}(q-\varepsilon)_2 > 2^\gamma$. If $n = 2^{\gamma-1}$ then $\gamma \geqslant 4$ and $(q^{2^{\gamma-2}}-1)_2 \in \omega(S)$. Now
$$(q^{2^{\gamma-2}}-1)_2 = 2^{\gamma-2}(q-\varepsilon)_2 = 2^{\gamma-2}n_2 = 2^{2\gamma-3} > 2^\gamma,$$
where the last inequality holds since $\gamma > 3$. Thus $2^\gamma \in \omega(S)\setminus\omega(L)$; a contradiction.

2. Suppose that $S \simeq E_8(q)$, where $q = p^\beta$ and p is odd. Then $t(S) = 12$ by [18, Table 4]. By
$$12 = t(S) \geqslant t(L)-1 = \left[\frac{m+1}{2}\right]-1,$$
we infer that $m \leqslant 26$. Furthermore, $q^8-1 \in \omega(S)$ by [20]. Hence $q^8-1 \in \omega(L)$. Since $(q^8-1)_2 \geqslant 32$ and $(q^8-1)_{2'} > 1$, Lemma 7 implies that $m \geqslant 18$ and $q^8-1 \leqslant 32(u^{m-17}+1)$. On the other hand, k_m and k_{m-1} lie in $\omega(G)$ and their prime divisors are not adjacent to 2 in $GK(S)$. Since $2p \in \omega(S)$, it follows that each of k_m and k_{m-1} divides the period of some maximal torus of S. By [14, 2.10], we infer that the possible periods are q^8-q^4+1, $q^8-q^6+q^4-q^2+1$, $q^8+q^7-q^5-q^4-q^3+q+1$, and $q^8-q^7+q^5-q^4+q^3-q+1$. Thus $k_m, k_{m-1} \leqslant 2(q^8-1)$. Combining the derived inequalities yields $18 \leqslant m \leqslant 26$ and $k_m, k_{m-1} \leqslant 64(u^{m-17}+1)$.

Let one of the numbers m, $m-1$ be equal to a prime i. Exploiting Lemma 5, we calculate
$$64u^{m-16} \geqslant 64(u^{m-17}+1) \geqslant k_i = k_i(-u) \geqslant \frac{u^{i-1}}{2(i,u+1)} \geqslant u^{i-3} \geqslant u^{m-4},$$
whence $64 \geqslant u^{12} \geqslant 2^{12}$; a contradiction. Thus m is one of 21, 22, 25, and 26.

Let $m = 25$. Then
$$64u^9 \geqslant 64(u^8+1) \geqslant k_m = k_{25}(-u) = \frac{u^{25}+1}{(u^5+1)(u+1,5)} = k_5(-u^5) \geqslant \frac{u^{20}}{10},$$
whence $640 \geqslant u^{11} \geqslant 2^{11}$; a contradiction.

Let $m = 21$. Then
$$64u^5 \geqslant 64(u^4+1) \geqslant k_{m-1} = k_{20}(-u) = \frac{u^{10}+1}{(u^2+1)(u^2+1,5)} = k_5(-u^2) \geqslant \frac{u^8}{10},$$
and hence $u \leqslant 8$. Now it is easy to check that the inequality $64(u^4+1) \geqslant k_{20}(-u)$ implies $u = 2$. Then $6560 = 3^8-1 \leqslant q^8-1 \leqslant 32(2^4+1) = 544$; a contradiction.

Finally, let $m = 22$ or $m = 26$. Put $m = 2i$. Then
$$64u^{m-16} \geqslant 64(u^{m-17}+1) \geqslant k_m(-u) = k_i(u) \geqslant \frac{u^{i-1}}{(i,u-1)} \geqslant u^{i-2} = u^{(m-4)/2},$$
whence $64 \geqslant u^{(28-m)/2} \geqslant u$. Since $u \leqslant 64$, it follows that $(i,u-1) = 1$ and therefore $64 \geqslant u^2$. Thus $u \leqslant 8$ and it is not hard to verify that the inequality $64(u^{m-17}+1) \geqslant k_i(u)$ implies $u = 2$. Then $q^8-1 \leqslant 32(2^9+1)$ and hence $q = 3$. It is a routine to check that $\omega(E_8(3)) \not\subseteq \omega(U_{26}(2))$ and $\omega(E_8(3)) \not\subseteq \omega(U_{22}(2))$.

3. Suppose that $S \simeq E_7(3)$. Then $t(S) = 8$ by by [18, Table 4] and hence $m \leqslant 18$. On the other hand, $q^4-1 \in \omega(S)$ by [20] and since $(q^4-1)_2 \geqslant 16$, $(q^4-1)_{2'} > 1$, it follows that $m \geqslant 10$. The periods of odd-order maximal tori of $E_7(3)$ are 757 and 1093. These numbers are prime, therefore, $\{k_m, k_{m-1}\} = \{r_m, r_{m-1}\} = \{757, 1093\}$. By definition, if $r_i(-u) = a$ then $e(a, -u) = i$ and by Fermat's theorem, it follows that i divides $a-1$. Thus $m(m-1)$ divides $[757-1, 1093-1] = 2^4{\cdot}3^4{\cdot}7^2{\cdot}13$. Together with $10 \leqslant m \leqslant 18$, this implies that $m = 13$ or $m = 14$. Then $1093 \geqslant k_{13} \geqslant u^{12}/26$, whence $u = 2$ and $1093 \geqslant k_{13}(-2) = 2731$; a contradiction.

4. It remains to show that $S \not\simeq {}^2G_2(q)$. For $L = L_m(2^\alpha)$, this assertion was was proved in [11, Proposition 4]. But the corresponding proof relies on the false fact that $q + 1 \in \omega({}^2G_2(q))$ and thus is incorrect. To fill this gap, we will prove that $S \not\simeq {}^2G_2(q)$ for both $L_m(2^\alpha)$ and $U_m(2^\alpha)$.

Proposition 3. *Let $L = L_m^\varepsilon(u)$, where $u = 2^\alpha$, $m \geqslant 5$, $\varepsilon = \pm$. Suppose that $(u, \varepsilon) \neq (2, +)$ and $(m, u, \varepsilon) \neq (5, 2, -)$. If $\omega(G) = \omega(L)$, K is a soluble radical of G and $S \leqslant \overline{G} = G/K \leqslant \operatorname{Aut} S$ then $S \not\simeq {}^2G_2(q)$.*

Proof. The hypothesis implies that there exist primitive prime divisors $r_m = r_m(\varepsilon u)$, $r_{m-1} = r_{m-1}(\varepsilon u), \dots, r_{[(m+1)/2]} = r_{[(m+1)/2]}(\varepsilon u)$. All these numbers are greater then 3 since 3 divides $u^2 - 1$ and $[(m + 1)/2] \geqslant 3$. Furthermore, by [18, Table 2], these numbers form a coclique in $GK(L)$ and $t(L) = [(m + 1)/2]$.

By Lemma 1, we have $t(2, S) \geqslant 3$ and $t(S) \geqslant t(L) - 1$. Moreover, all prime divisors of $k_m = k_m(\varepsilon u)$ and all prime divisor of $k_{m-1} = k_{m-1}(\varepsilon u)$ do not divide $|K|{\cdot}|\overline{G}/S|$. Hence k_m and k_{m-1} lie in $\omega(S)$, and their prime divisors are not adjacent to 2 in $GK(S)$.

Suppose that $S \simeq {}^2G_2(q)$, where $q = 3^\beta > 3$ and β is odd. By [18, Table 4], we have $t(S) = 5$ and every coclique of $GK(S)$ of size 5 contains the vertex 3. If $m \geqslant 11$ then there exists a coclique of size 6 in $GK(L)$ consisting of primes larger than 3. By Lemma 1, at least five vertices of this coclique lie in $GK(S)$, which is impossible. Thus $5 \leqslant m \leqslant 10$.

By [21], the periods of maximal tori of S are $q - 1$, $(q + 1)/2$, $q - \sqrt{3q} + 1$, and $q + \sqrt{3q} + 1$. In particular, the 2-period of S is equal to 2. Since $|\operatorname{Out} S| = \beta$, it follows that the 2-period of K is twice less than that of L. The numbers k_m and k_{m-1} are not divisible by 3, therefore, they divides $q \pm \sqrt{3q} + 1$.

Let $5 \leqslant m \leqslant 8$. Then one of m, $m - 1$ is a prime. Denote this prime by i. We claim that $q \leqslant 4(u^{i-2} + 1)$.

Let $m = 6$ or $m = 8$. Since $q-1$, $(q+1)/2$ lie in $\omega(L)$ and $(q-1)_2 = (q+1)_2/2 = 2$, Lemma 6 implies that each of this numbers divides $2^\gamma[u^{m_1} - \varepsilon^{m_1}, \dots, u^{m_s} - \varepsilon^{m_s}]$ for some $\gamma \geqslant 1$ and $m_1, \dots, m_s$ such that $2^{\gamma-1} + 1 + m_1 + \dots + m_s = m$. Choose the largest γ with such property. If $\gamma > 1$ then applying Lemma 5, we infer that $q + 1 \leqslant 4(u^{m-3} + 1)$, as required. Suppose that $\gamma = 1$ and some of $q - 1$ and $(q+1)/2$ divides $2[u^{m_1} - \varepsilon^{m_1}, \dots, u^{m_s} - \varepsilon^{m_s}]$ with $s > 1$ and $m_1 + \dots + m_s = m-2$. Since $m-2 = 4$ or $m-2 = 6$, we may assume that m_s divides m_{s-1}. Then $2[u^{m_1} - \varepsilon^{m_1}, \dots, u^{m_s} - \varepsilon^{m_s}]$ divides $4[u^{m_1} - \varepsilon^{m_1}, \dots, u^{m_{s-1}} - \varepsilon^{m_{s-1}}] \in \omega(L)$, contrary to maximality of γ. This contradiction shows that that both $q-1$ and $(q+1)/2$ divide $2(u^{m-2} + \varepsilon^{m-2})$. Then $(q^2-1)/4 \leqslant 2(u^{m-2}+1)$ and so $q^2 \leqslant 8(u^{m-2}+1)+1 \leqslant 16(u^{m-3}+1)^2$, as required. If $m = 5$ or $m = 7$ then applying Lemma 7 to $(q+1)/2$ yields $(q+1)/2 \leqslant 2(u^{m-2}+1)$ and again $q \leqslant 4(u^{i-2} + 1)$.

Now

$$8(u^{i-2} + 1) \geqslant 2q \geqslant q + \sqrt{3q} + 1 \geqslant k_i = k_i(\varepsilon u) \geqslant \frac{u^{i-1}}{2(i, u - \varepsilon)} \geqslant \frac{u^{i-1}}{14}.$$

Thus $u \leqslant 64$. A direct calculation shows that $8(u^{i-2}+1) < k_i(\varepsilon u)$ for $u = 64$ and hence $u \leqslant 16$. Then $q \leqslant 4(16^5+1) < 3^{15}$.

It is a routine to check that $k_i(\varepsilon u)$ divides $(q+\sqrt{3q}+1)(q-\sqrt{3q}+1)$ with $i = 5, 7$, $u \leqslant 16$ and $q \leqslant 3^{13}$ if and only if $u = 2$ and either $\varepsilon = +$, $i = 5$, $q = 3^5$ or $\varepsilon = -$, $i = 7$, $q = 3^7$. By hypothesis, $(u, \varepsilon) \neq (2, +)$, so $S \simeq {}^2G_2(3^7)$, $L = U_5(2)$ or $L = U_6(2)$, and $2269 \in \omega(S) \setminus \omega(L)$; a contradiction.

Let $9 \leqslant m \leqslant 10$. Then $16 \in \omega(L)$ and hence $8 \in \omega(K)$. The numbers r_m, r_{m-1}, r_{m-2}, r_{m-4}, and r_{m-5} form a coclique in $GK(L)$. Since every coclique of $GK(S)$ of size 5 contains the vertex 3, it follows that one of the numbers r_{m-3}, r_{m-4}, and r_{m-5}, say r_l, does not divide $|S|$. Moreover, every prime divisor of $k = k_l(\varepsilon u)$ does not divide $|S|$. If $a \in \pi(k)$ and $a \in \pi(K)$ then by Lemma 3, we have $8a \in \omega(G)$, contrary to Lemma 6. Thus k is coprime to $|S|{\cdot}|K|$ and hence $k \in \omega(\overline{G}/S)$. Therefore $k \geqslant \beta$ and $q \geqslant 3^k$.

Since $k_8(\varepsilon u) = u^4+1$, $k_7(\varepsilon u) \geqslant u^5$, $k_6(\varepsilon) = (u^2-\varepsilon u+1)/(3, u-\varepsilon)$, and $k_5 \geqslant u^3/2$, it follows that $k \geqslant (u^2-u+1)/3$.

Applying Lemma 7 to $(q+1)/2$ yields $(q+1)/2 \leqslant 2(u^{m-2}+1)$. Thus

$$4(u^8+1) \geqslant 4(u^{m-2}+1) \geqslant q+1 \geqslant 3^k \geqslant 3^{(u^2-u+1)/3},$$

whence $u \leqslant 4$. Since $(u, \varepsilon) \neq (2, +)$, it follows that $k \geqslant 7$. On the other hand, $q \leqslant 4(u^8+1)$ and so $q \leqslant 3^{11}$. Thus $u \in \{2, 4\}$ and $q \in \{3^7, 3^9, 3^{11}\}$. Now we can directly check that $k_9(\varepsilon u)$ does not divide either $q+\sqrt{3q}+1$ or $q+\sqrt{3q}+1$; a contradiction. □

Thus $S \simeq L$ and the theorem is proved.

References

[1] V.D. Mazurov, *Groups with prescribed spectrum*, Izv. Ural. Gos. Univ., **36** (2005), 119–138 [in Russian].

[2] M.A. Grechkoseeva, W.J. Shi, and A.V. Vasil′ev, *Recognition by spectrum of finite simple groups of Lie type*, Front. Math. China, **3**: 2 (2008), 275–285.

[3] V.D. Mazurov, M.C. Xu, and H.P. Cao, it Recognition of finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders, Algebra and Logic, **39**: 5 (2000), 324–334.

[4] V.D. Mazurov and G.Y. Chen, *Recognizability of finite simple groups $L_4(2^m)$ and $U_4(2^m)$ by spectrum*, Algebra and Logic, **47**: 1 (2008), 49–55.

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

[6] W.J. Shi and H.L.Li, *A characteristic property of M_{12} and $PSU(6,2)$*, Acta Math. Sin., **32** (1989), 758–764 [in Chinese].

[7] A. V. Vasil′ev, M.A. Grechkoseeva, and A.M. Staroletov, *On finite groups isospectral to simple linear and unitary groups*, Siberian Math. J., to appear.

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

[9] 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), 511–522.

[10] A.V. Vasilyev and I. B. Gorshkov, *On recognition of finite simple groups with connected prime graph*, Siberian Math. J., **50**: 2 (2009), 233–238.

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

[12] M.A. Grechkoseeva, *Recognition of finite linear groups over fields of characteristic* 2 *by spectrum*, Algebra and Logic, **47**: 4 (2008), 229–241.

[13] A.V. Vasilyev, *Recognizing groups $G_2(3^n)$ by their element orders*, Algebra and Logic, **41**: 2 (2002), 74–80.

[14] W.M. Kantor and A. Seress, *Prime power graphs for groups of Lie type*, J. Algebra, **427** (2002), 370–434.
[15] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3** (1892), 265–284.
[16] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc., **125** (1997), 1913–1919.
[17] A.A. Buturlakin, *Spectra of finite linear and unitary groups*, Algebra and Logic, **47**: 2 (2008), 157–173.
[18] A. V. Vasil′ev and E. P. Vdovin, *Cocliques of maximal size in the prime graph of a finite simple group*, Preprint No. 225, Sobolev Insitute of Mathematics, Novosibirsk (2009). See also http://arxiv.org/abs/0905.1164v1.
[19] A.V. Vasiliev and E.P. Vdovin, *An adjacency criterion for the prime graph of a finite simple group*, Algebra and Logic, **44**: 6 (2005), 381–406.
[20] D.I. Deriziotis and A.P. Fakiolas, *The maximal tori of the finite Chevalley groups of type E_6, E_7 and E_8*, Comm. Algebra, **19** (1991), 889–903.
[21] H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc., **121** (1966), 62–89.

Maria Aleksandrovna Grechkoseeva
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: grechkoseeva@gmail.com