ON THE STRUCTURE OF FINITE GROUPS ISOSPECTRAL TO FINITE SIMPLE GROUPS

MARIYA A. GRECHKOSEEVA

Sobolev Institute of Mathematics and Novosibirsk State University,
Ac. Koptyuga 4, Novosibirsk, 630090, Russia.

ANDREY V. VASIL’EV

Sobolev Institute of Mathematics and Novosibirsk State University,
Ac. Koptyuga 4, Novosibirsk, 630090, Russia.

Abstract. Finite groups are said to be isospectral if they have the same sets of element orders. The present paper is the final step in the proof of the following conjecture due to V.D. Mazurov: for every finite nonabelian simple group \( L \), apart from a finite number of sporadic, alternating and exceptional groups and apart from several series of classical groups of small dimensions, if a finite group \( G \) is isospectral to \( L \) then \( G \) is an almost simple group with socle isomorphic to \( L \). Namely, we prove that a nonabelian composition factor of a finite group isospectral to a finite simple symplectic or orthogonal group \( L \) of dimension at least 10, is either isomorphic to \( L \) or not a group of Lie type in the same characteristic as \( L \).

Keywords. Simple group, symplectic group, orthogonal group, element orders, spectrum of a group.

2010 MSC. 20D06, 20D60.

1. Introduction

The spectrum \( \omega(G) \) of a finite group \( G \) is the set of element orders of \( G \). Groups are isospectral if they have the same spectra. Given a finite group \( G \) with nontrivial soluble radical, one can construct infinitely many different finite groups isospectral to \( G \) [21,28]. On the contrary, there is a conjecture due to Mazurov that in general the set of groups isospectral to a finite nonabelian simple group \( L \) is finite and consists of groups closely related to \( L \). The precise statement of this conjecture is as follows: for every finite nonabelian simple group \( L \), apart from a finite number of sporadic, alternating and exceptional groups and apart from several series of classical groups of small dimensions, if a finite group \( G \) is isospectral to \( L \) then \( G \) is an almost simple group with socle isomorphic to \( L \), and in particular there are only finitely many different finite groups isospectral to \( L \).
The main purpose of this paper is to establish the following theorem, thereby proving Mazurov’s conjecture (our notation for nonabelian simple groups follows [6]).

**Theorem 1.** Let $L$ be one of the following nonabelian simple groups:

1. a sporadic group other than $J_2$;
2. an alternating group $A_n$, where $n \neq 6, 10$;
3. an exceptional group of Lie type other than $^3D_4(2)$;
4. $L_n(q)$, where $n \geq 45$ or $q$ is even;
5. $U_n(q)$, where $n \geq 45$ or $q$ is even and $(n, q) \neq (4, 2), (5, 2)$;
6. $S_{2n}(q), O_{2n+1}(q)$, where either $q$ is odd and $n \geq 28$ or $q$ is even and $n \geq 20$;
7. $O_{2n}^+(q)$, where either $q$ is odd and $n \geq 31$ or $q$ is even and $n \geq 20$;
8. $O_{2n}^-(q)$, where either $q$ is odd and $n \geq 30$ or $q$ is even and $n \geq 20$.

Then every finite group isospectral to $L$ is isomorphic to some group $G$ with $L \leq G \leq \text{Aut } L$. In particular, there are only finitely many pairwise nonisomorphic finite groups isospectral to $L$.

Theorem 1 is undoubtedly a sum of efforts by numerous mathematicians, and a comprehensive list of references covering its proof consists of about hundred papers, so this list is too long to be given here. But for every series of simple groups mentioned in Theorem 1, we cite the work in which the proof for this series was completed, and as a rule this work includes a survey of previous investigations. Thus, see [25] for sporadic groups, [11] for alternating groups, [37] for exceptional groups, and [32, Theorem 1] for linear and unitary groups. The present paper is concerned with symplectic and orthogonal groups.

By [32, Theorem 2], if $L$ is a finite simple symplectic or orthogonal group of Items (6)–(8) of Theorem 1 and $G$ is a finite group with $\omega(G) = \omega(L)$, then $G$ has only one nonabelian composition factor and this factor $S$ is a symplectic or orthogonal group having the same underlying characteristic as $L$. If $S \cong L$, then the soluble radical of $G$ is trivial [13, Theorem 1.1], and hence $G$ is an almost simple group with socle isomorphic to $L$, as required. If $S \not\cong L$, then by [36, Theorem 3] there are at most two possibilities for $S$ (see Lemma 13 below). We eliminate these possibilities by the following theorem, and thus Theorem 1 follows.

**Theorem 2.** Let $q$ be a power of a prime $p$, $L$ one of the groups $S_{2n}(q)$, where $n \geq 2$ and $(n, q) \notin \{(2, 2), (2, 3)\}$, $O_{2n+1}(q)$, where $n \geq 3$, or $O_{2n}^\pm(q)$, where $n \geq 4$, and let $G$ be a finite group with $\omega(G) = \omega(L)$. Suppose that some nonabelian composition factor $S$ of $G$ is a group of Lie type over a field of characteristic $p$. If $S \not\cong L$, then one of the following holds:

1. $L = S_4(q)$, where $q \neq 3^{2k+1}$, and $S = L_2(q^2)$;
2. $L = O_9(q), S_8(q)$ and $S = O_8^+(q)$;
3. $\{L, G\} = \{O_8^+(2), S_6(2)\}$;
4. $\{L, G\} = \{O_8^+(3), O_7(3)\}$.

We conclude the introduction with a discussion of what nonabelian simple groups are genuine exceptions to the general law stated in Mazurov’s conjecture. For brevity we will refer to a nonabelian simple group $L$ such that every finite group isospectral to $L$ is an almost simple group with socle isomorphic to $L$, as *almost recognizable by spectrum*. The groups $J_2, A_6, A_{10}, ^3D_4(2), U_4(2) \cong S_4(3)$, and $U_5(2)$ are not almost recognizable by spectrum; moreover, each of them is isospectral to a group with nontrivial soluble radical (see [3, 21, 23, 28]).
All the groups $L_2(q)$, $L_3(q)$ and $U_3(q)$, except for $L_2(9)$, $L_3(3)$, $U_3(5)$ and $U_3(p)$ where $p$ is a Mersenne prime and $p^2 - p + 1$ is a prime too, are almost recognizable (see [3], [26, 41] and [26, 42] respectively). The question is still open for $L_4(q)$ and $U_3(q)$ with $q$ odd, but the conjecture is that there are infinitely many $q$ such that $L_4(q)$ is not almost recognizable (see [43]). Thus, the exceptions of Items (1)–(3) of Theorem 1 are necessary, while the condition $n \geq 45$ in Items (4)–(5) can probably be replaced by $n \geq 5$.

The simple group $S_4(q)$ is almost recognizable if and only if $q = 3^m$ with $m > 1$ odd, and moreover the case (1) of Theorem 2 is possible [22,26]. It is known that $\omega(O^+_8(3)) = \omega(S_6(2))$ and $\omega(O^+_8(3)) = \omega(O_7(3))$ and that there are no other finite groups with such spectra [20,29]. The group $S_8(2)$ is not almost recognizable [24]. In the last section we generalize this result to all groups $S_q(q)$ with $q$ even showing that the case (2) of Theorem 2 is possible when $q$ is even. We suspect that it is also possible when $q$ is odd, at least for $L = O_q(q)$. Thus all exceptions of Theorem 2 are substantial. On the other hand, we believe that all other symplectic and orthogonal groups are almost recognizable by spectrum.

To summarize, we propose the following

**Conjecture 1.** Let $L$ be one of the following groups:

1. $L_n(q)$, where $n \geq 5$;
2. $U_n(q)$, where $n \geq 5$ and $(n, q) \neq (5, 2)$;
3. $S_{2n}(q)$, where $n \geq 3$, $n \neq 4$ and $(n, q) \neq (3, 2)$;
4. $O_{2n+1}(q)$, where $q$ is odd, $n \geq 3$, $n \neq 4$ and $(n, q) \neq (3, 3)$;
5. $O^*_2(q)$, where $n \geq 4$ and $(n, q, \varepsilon) \neq (4, 2, +), (4, 3, +)$.

Then every finite group isospectral to $L$ is isomorphic to some group $G$ with $L \leq G \leq \text{Aut } L$.

In fact, to prove Conjecture 1 it is suffices to show that the only nonabelian composition factor $S$ of a group $G$ isospectral to a simple classical group $L$ under consideration is not a group of Lie type whose underlying characteristic differs from that of $L$. The existing generic proof of this assertion recently obtained in [32] requires that the dimension of $L$ is as large as stated in Theorem 1. It is worth also mentioning that the assertion was proved in some special cases, in particular for many classical groups with disconnected prime graph (see [2,7,8,14–16,19,27,34] for recent research in this area).

2. Preliminaries

By $(a_1, a_2, \ldots, a_k)$ and $[a_1, a_2, \ldots, a_k]$ we denote respectively the greatest common divisor and least common multiple of positive integers $a_1, a_2, \ldots, a_k$. If $a$ is a positive integer and $p$ is a prime then $\pi(a)$ denotes the set of prime divisors of $a$ and $(a)_r$ denotes the highest power of $r$ that divides $a$.

**Lemma 1** (Zsigmondy [44]). Let $q \geq 2$ and $n \geq 3$ be integers with $(q, n) \neq (2, 6)$. There exists a prime $r$ such that $r$ divides $q^n - 1$ but does not divide $q^i - 1$ for $i < n$.

With notation of Lemma 1, we call a prime $r$ a **primitive prime divisor** of $q^n - 1$ and denote it by $r_n(q)$. By $R_n(q)$ we denote the set of all primitive prime divisors of $q^n - 1$. Observe that $R_n(q) \subseteq R_n(q^k)$ if $k$ is coprime to $n$, and $R_{nk}(q) \subseteq R_n(q^k)$ for all $n$ and $k$.

Given a group $G$, we set $\pi(G) = \pi(|G|)$ and define the prime graph $GK(G)$ as follows: its vertex set is $\pi(G)$ and two different primes $r$ and $s$ are adjacent if and only if $G$ has an element of order $rs$. We use standard graph-theoretic terminology: a **coclique** of a graph is a
Lemma 2. Let $L$ be a finite nonabelian simple group of Lie type other than $L_3(3)$, $U_3(3)$, $S_4(3) \cong U_4(2)$ and let $G$ be a finite group with $\omega(G) = \omega(L)$. Then the following hold.

1. There is a nonabelian simple group $S$ such that $S \leq G = G/K \leq \text{Aut} S$, where $K$ is the largest normal soluble subgroup of $G$.

2. If $\rho$ is a coclique of size at least 3 in $GK(G)$, then at most one prime of $\rho$ divides $|K| \cdot |G/S|$.

3. If $r \in \pi(G)$ is not adjacent to 2 in $GK(G)$, then $r$ is coprime to $|K| \cdot |G/S|$.

Proof. If there is a coclique of size 3 in $GK(L)$, then the assertion is the main theorem of [31] supplemented with [33] and [39, Theorem 7.1]. If there are no cocliques of size 3 in $GK(L)$, then we have that $GK(L)$ is disconnected by [18,38,40]. Then the Gruenberg–Kegel theorem [40, Theorem A] implies that either (1) and (3) holds true for $G$, or $G$ is a Frobenius or 2-Frobenius group. Simple groups of Lie type that can be isospectral to a Frobenius or 2-Frobenius group are described in [1], and these groups are precisely $L_3(3)$, $U_3(3)$ and $S_4(3) \cong U_4(2)$.

We say that a finite group $H$ is a (proper) cover of a finite group $G$ if there is a (nontrivial) normal subgroup $K$ of $H$ such that $H/K \cong G$.

Lemma 3 ([13, Lemma 2.3]). Let $A$ and $B$ be finite groups. The following are equivalent.

1. $\omega(H) \nsubseteq \omega(B)$ for any proper cover $H$ of $A$;

2. $\omega(H) \nsubseteq \omega(B)$ for any split extension $H = K : A$, where $K$ is a nontrivial elementary abelian group.

Lemma 4 ([20, Lemma 1]). Let $G$ be a finite group, $K$ a normal subgroup of $G$ and $G/K$ a Frobenius group with kernel $N$ and cyclic complement $C$. If $(|N|, |K|) = 1$ and $N$ is not contained in $KC_G(K)/K$, then $r|C| \in \omega(G)$ for some $r \in \pi(K)$.

Lemma 5 ([35, Lemma 3]). Let $G$ be a finite group, $K$ a normal soluble subgroup of $G$ and $S \leq G/K \leq \text{Aut} S$ for some nonabelian simple group $S$. Suppose that $\pi(S) \setminus \pi(K)$ contains primes $t$ and $s$ that are not adjacent and have disjoint neighbourhoods in $GK(G)$. If $r \in \pi(K)$ is adjacent to none of $t$ and $s$ in $GK(G)$ and $S$ includes a Frobenius group with cyclic complement $C$ and kernel $N$ such that $(|N|, r) = 1$, then $r|C| \in \omega(G)$.

Lemma 6 ([13, Lemma 2.7]). Let $S$ be a finite simple group of Lie type over a field of characteristic $p$ and let $S$ act faithfully on a vector space $V$ over a field of characteristic $r$, where $r \neq p$. Let $H = V \rtimes S$ be a natural semidirect product of $V$ by $S$. Suppose that $s$ is a power of $r$ and some proper parabolic subgroup $P$ of $S$ contains an element of order $s$. If the unipotent radical of $P$ is abelian or both $p$ and $r$ are odd or $p = 2$ and $r$ is not a Fermat prime or $r = 2$ and $p$ is not a Mersenne prime, then $rs \in \omega(H)$.

We conclude with several lemmas on spectra of symplectic and orthogonal groups. In all these lemmas, $\pm in [a_1 \pm 1, \ldots, a_s \pm 1]$ means that we can choose + or – for every entry independently.

Lemma 7 ([5, Corollaries 2 and 6]). Let $L$ be one of the simple groups $S_{2n}(q)$ and $O_{2n+1}(q)$, where $n \geq 2$ and $q$ is a power of an odd prime $p$. Let $d = 1$ if $L = S_{2n}(q)$ or $n = 2$ and
Lemma 11. Let $d = 2$ if $L = O_{2n+1}(q)$ with $n \geq 3$. Then $\omega(L)$ consists of all divisors of the following numbers:

1. $(q^n \pm 1)/2$;
2. $[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $s \geq 2$, $n_i > 0$ for all $1 \leq i \leq s$ and $n_1 + \cdots + n_s = n$;
3. $p^k(q^n \pm 1)/d$, where $k, n_1 > 0$ and $p^{k-1} + 1 + 2n_1 = 2n$;
4. $p^k[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $k > 0$, $s \geq 2$, $n_i > 0$ for all $1 \leq i \leq s$ and $p^{k-1} + 1 + 2(n_1 + \cdots + n_s) = 2n$;
5. $p^k$ if $2n = p^{k-1} + 1$ for some $k > 0$.

Lemma 8 ([5, Corollary 3]). Let $L = S_{2n}(q)$, where $n \geq 2$ and $q$ is even. Then $\omega(L)$ consists of all divisors of the following numbers:

1. $[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $s \geq 1$, $n_i > 0$ for all $1 \leq i \leq s$ and $n_1 + \cdots + n_s = n$;
2. $[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $s \geq 1$, $n_i > 0$ for all $1 \leq i \leq s$ and $n_1 + \cdots + n_s = n - 1$;
3. $2^k[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$, where $k \geq 2$, $s \geq 1$, $n_i > 0$ for all $1 \leq i \leq s$ and $2^{k-2} + 1 + n_1 + \cdots + n_s = n$;
4. $2^k$ if $n = 2^{k-2} + 1$ for some $k \geq 2$.

Proof. The assertion follows from [5, Corollaries 3 and 9].

Lemma 9. Let $L = O_{8}^\pm(q)$, where $q$ is a power of a prime $p$. Then $\omega(L)$ consists of all divisors of the following numbers:

1. $(q^4 - 1)/(2, q - 1)$, $(q^3 \pm 1)/(2, q - 1)$, $q^2 - 1$, $p(q^2 \pm 1)/(2, q - 1)$;
2. $p^k(q \pm 1)/(2, q - 1)$ if $p = 2, 3$;
3. $25$ if $p = 5$;
4. $8$ if $p = 2$.

Proof. The assertion follows from [5, Corollary 3].

Lemma 10. Let $L = O_{8}(q)$, where $q$ is even. Then $\omega(L)$ consists of all divisors of the following numbers: $q^4 \pm 1$, $(q^2 \pm q + 1)(q^2 - 1)$, $2(q^2 + 1)(q \pm 1)$, $4(q^2 - 1)$, and $8$.

Proof. The assertion follows from [5, Corollary 3].

Lemma 11. Let $q$ be a power of a prime $p$.

1. Let $q$ be odd and $n \geq 3$. Let $r = r_{2n-2}(q)$ if $q^{n-1} \equiv 1 \pmod{4}$ and $r = r_{n-1}(q)$ if $q^{n-1} \equiv -1 \pmod{4}$. Then $2pr \in \omega(S_{2n}(q)) \setminus \omega(O_{2n+1}(q))$.
2. If $n \geq 4$ and $(n, q) \neq (4, 2)$, then $pr_{2n-2}(q) \in \omega(O_{2n+1}(q)) \setminus \omega(O_{2n+1}(q))$. If $n \geq 4$ is even, then $pr_{n-1}(q) \in \omega(O_{2n+1}(q)) \setminus \omega(O_{2n+1}(q))$.
3. If $q > 3$, then $(q^4 - 1)/(2, q - 1)^2 \in \omega(O_8(q)) \setminus \omega(S_6(q))$.
4. If $q$ is odd, then $p(q^2 + 1) \in \omega(S_6(q)) \setminus \omega(O_8(q))$.
5. $\omega(O_{2n+1}(q)) \subseteq \omega(S_{2n}(q))$ for all $n \geq 2$.
6. $\omega(O_{2n-1}(q)) \subseteq \omega(O_8(q)) \subseteq \omega(O_{2n+1}(q))$ for all $n \geq 3$.

Proof. (1) Let $q^{n-1} \equiv \varepsilon \pmod{4}$. Then $2pr$ divides $p(q^{n-1} + \varepsilon)$, and in particular it belongs to $\omega(S_{2n}(q))$ by Lemma 7. Suppose that $2pr \in O_{2n+1}(q)$. It follows by Lemma 7 that $2pr$ divides either $p^k(q^n \pm 1)/2$ for some $k \geq 1$ and $n_1 > 0$ with $p^{k-1} + 1 + 2n_1 = 2n$, or $p^k[q^{n_1} \pm 1, \ldots, q^{n_s} \pm 1]$ for some $k \geq 1$, $s \geq 2$, $n_1, \ldots, n_s > 0$ with $p^{k-1} + 1 + 2n_1 + \cdots + 2n_s = 2n$. In fact, by the definition of primitive divisor, it cannot divide a number of the latter form since all $n_1, \ldots, n_s$ are less than $n-1$. And if $2pr$ divides $p^k(q^{n_1} + \varepsilon)/2$ with $p^{k-1} + 1 + 2n_1 = 2n$, then by the definition of primitive divisor we have that $k = 1$, $n_1 = n-1$ and $\varepsilon = \pm 1$. But then $(q^{n_1} + \varepsilon)/2$ is odd, a contradiction.
(2) See [39, Prop. 3.1].

(3) Let $$a = (q^4 - 1)/(2, q - 1)^2$$. Lemma 9 implies that $$a \in \omega(O^+_8(q))$$. By Lemmas 7 and 8, the orders of semisimple elements of $$S_0(q)$$ are precisely divisors of $$(q^3 + 1)/(2, q - 1)$$, $$(q^2 + 1)(q + 1)/(2, q - 1)$$ and $$q^2 - 1$$. It is clear that $$a$$ divides none of $$(q^3 + 1)/(2, q - 1)$$ and $$q^2 - 1$$. Furthermore,

$$a = \frac{(q^2 + 1) \cdot (q + 1) \cdot (q - 1)}{(2, q - 1) \cdot (2, q - 1)}.$$

Since $$q > 2$$, both $$(q - 1)/(2, q - 1)$$ and $$(q + 1)/(2, q - 1)$$ are greater than one, and so $$a$$ does not divide $$(q^2 + 1)(q + 1)/(2, q - 1)$$ either.

(4)–(5) See Lemmas 7 and 9.

(6) It is well known that $$\Omega_{2n-1} < \Omega_{2n}(q) < \Omega_{2n+1}(q)$$, and the assertion follows.

\begin{lemma}
Let $$q$$ be even, $$S = S_0(q)$$ and $$L = O^+_8(q)$$. Suppose that $$V$$ is a nontrivial $$S$$-module over a field of characteristic 2 and $$H$$ is a natural semidirect product of $$V$$ and $$S$$. Then $$\omega(H) \not\subseteq \omega(L)$$.

\begin{proof}
In the proof of Lemma 4.1 in [13], it was established that $$\omega(H)$$ contains at least one of the numbers 16, 24, and $$2(q^2 + q + 1)$$. By Lemma 9, none of these numbers belong to $$\omega(L)$$.
\end{proof}
\end{lemma}

3. Proof of Theorem 2

As we mentioned in Introduction, the starting point for our proof of Theorem 2 is the following assertion.

\begin{lemma}[{[30, 36]}]
Let $$q$$ be a power of a prime $$p$$, $$L$$ one of the groups $$S_{2n}(q)$$, where $$n \geq 2$$ and $$(n, q) \notin \{(2, 2), (2, 3)\}$$, $$O_{2n+1}(q)$$, where $$n \geq 3$$, or $$O^\pm_{2n}(q)$$, where $$n \geq 4$$, and let $$G$$ be a finite group with $$\omega(G) = \omega(L)$$. Suppose that some nonabelian composition factor $$S$$ of $$G$$ is a group of Lie type over a field of characteristic $$p$$. If $$S \nsubseteq L$$, then one of the following holds:

1. $$L = S_4(q)$$, where $$q > 3$$, and $$S = L_2(q^2)$$;
2. $$(L, S) \subseteq \{S_6(q), O_7(q), O^+_8(q)\}$$;
3. $$(L, S) \subseteq \{S_{2n}(q), O_{2n+1}(q), O^-_{2n}(q)\}$$ and $$n \geq 4$$;
4. $$L = O^+_{2n}(q)$$, $$S \in \{S_{2n-2}(q), O_{2n-1}(q)\}$$, and $$n \geq 6$$ is even.

Let $$q = p^m$$ and let $$L$$ be one the groups $$S_{2n}(q)$$, where $$n \geq 2$$ and $$(n, q) \notin \{(2, 2), (2, 3)\}$$, $$O_{2n+1}(q)$$, where $$n \geq 3$$, or $$O^\pm_{2n}(q)$$, where $$n \geq 4$$. Let $$G$$ be a finite group with $$\omega(G) = \omega(L)$$. By Lemma 2, we have

$$S \leq G/K \leq \text{Aut} S,$$

where $$K$$ is a soluble radical of $$G$$ and $$S$$ is a nonabelian simple group. Suppose that $$S$$ is a group of Lie type over a field of characteristic $$p$$ and $$S \nsubseteq L$$. Then $$L$$ and $$S$$ are as in the conclusion of Lemma 13.

Let $$L = S_4(q)$$, where $$q > 3$$. If $$q = 3^m$$ and $$m$$ is odd, then $$G \simeq L$$ by [22], contrary to $$S \nsubseteq L$$. If $$q \neq 3^m$$ with $$m$$ odd, then $$S = L_2(q^2)$$ by Lemma 13, and this is the case (1) of the conclusion of Theorem 2.

For the rest of the proof we assume that $$L \neq S_4(q)$$, and hence Lemma 13 implies that $$S$$ is a symplectic or orthogonal group over the field of the same order $$q$$. In particular,
\[ \pi(\text{Out } S) \subseteq \{2, 3\} \cup \pi(m). \] So if \( k > 2 \) and \( r \in R_m(p) \), then \( r \not\in \pi(\text{Out } S) \). Indeed, by Fermat’s little theorem \( mk \) divides \( r - 1 \) and so \( r > 3 \) and \( r > m \).

Throughout the proof we use the criterion of adjacency in prime graphs of simple groups obtained in [38, 39] and often omit the corresponding reference.

We begin with eliminating a special case where \( L = S_{2n}(q) \) and \( S = O_{2n+1}(q), n \geq 3 \) and \( q \) is odd. It follows by [13, Prop. 1.3] that \( K = 1 \) in this case, and hence \( S \leq G \leq \text{Aut } S \). Let \( r = r_{2(n-1)m}(p) \) if \( q^{n-1} \equiv 1 \pmod{4} \) and \( r = r_{(n-1)m}(p) \) otherwise. By Lemma 11, there is an element \( g \) of order 2 in \( G \setminus S \). By the above remark, \( r \not\in \pi(G/S) \).

Suppose that \( p \in \pi(G/S) \). Then \( G \) contains a field automorphism of \( S \) of order \( p \). By [10, Prop. 4.9.1(a)], the centralizer of this automorphism in \( S \) includes \( O_{2n+1}(q) \), where \( q = q_0^p \). Therefore \( pr_{2n}(q_0) \) and \( p[q_0 + 1, q_0^{p-1} \pm 1] \) lie in \( \omega(G) \). If \( p \) does not divide \( n \), then \( r_{2n}(q_0) \in R_{2n}(q) \) and so \( pr_{2n}(q_0) \notin \omega(L) \) by [39, Prop. 3.1]. Let \( p \) divide \( n \). Then \( r_{2n-2}(q_0) \in R_{2n-2}(q) \). By the definition of primitive divisor and Lemma 7, it follows that \( p(q_0 + 1)r_{2n-2}(q_0) \in \omega(L) \) if and only if \( q_0 + 1 \) divides \( q^{n-1} + 1 \), which implies that \( n \) is even. But then \( q_0 + 1 \) does not divide \( q^{n-1} - 1 \), and by the same reasoning we conclude that \( p(q_0 + 1)r_{n-1}(q_0) \notin \omega(L) \). In any case, \( \omega(G) \not\subseteq \omega(L) \), a contradiction.

Thus \( p, r \not\in \pi(G/S) \), and it follows that \( q^pr \not\in S \). Therefore \( G \setminus S \) contains an involution \( t \) such that \( pr \in \omega(C_S(t)) \). Suppose that \( t \in \text{Inndiag } S \). Then \( \text{Inndiag } S \leq G \) and since \( \text{Inndiag } S \simeq SO_{2n+1}(t) \), it follows that \( q^n + 1 \in \omega(G) \setminus \omega(L) \), which is impossible. Therefore, by [10, Prop. 4.9.1(d)], we have that \( t \) is a field automorphism, and hence \( m \) is even. In particular \( q \equiv 1 \pmod{4} \) and \( r = r_{2(n-1)m}(p) \). By [10, Prop 4.9.1(a,b)], the centralizer \( C_S(t) \) can be embedded into \( SO_{2n+1}(q_0) \), where \( q = q_0^p \), and so \( C_S(t) \) has no elements of order \( r \); a contradiction.

Now we are ready to handle the cases (2)–(4) of Lemma 13.

**Case (2).** Let both \( L \) and \( S \) be in \( \{S_6(q), O_7(q), O_7^+(q)\} \). If \( q = 2 \) or \( q = 3 \), then respectively \( \{L, G\} = \{S_6(2), O_7^+(2)\} \) or \( \{L, G\} = \{O_7(3), O_7^+(3)\} \) [22,29], and these are the cases (3) and (4) of the conclusion of Theorem 2. Hence we may assume that \( q > 3 \).

Since \( \omega(S) \subseteq \omega(L) \), it follows from Lemma 11 that \( S \neq S_6(q) \) if \( q \) is odd and \( S \neq O_7^+(q) \). The preceding discussion implies that \( (L, S) \neq (S_6(q), O_7(q)) \). Thus \( L = O_7^+(q) \) and \( S = O_7(q) \). Observe that \( r_3(q) \) and \( r_6(q) \) have the following properties with respect to \( GK(L) \):

\[
\begin{align*}
(1) & \quad (q^4 - 1)/(2, q - 1)^2, (q^3 \pm 1)/(2, q - 1), q^2 - 1 \\
(2) & \quad (q^2 + 1)(q \pm 1)/(2, q - 1), (q^3 \pm 1)/(2, q - 1), q^2 - 1
\end{align*}
\]

respectively.

We claim that \( K \neq 1 \) yields \( \omega(G) \not\subseteq \omega(L) \). By Lemma 3 we may assume that \( K \) is an elementary abelian \( r \)-group for some prime \( r \) and \( G \) includes a semidirect product of \( K \) and \( S \). Also we may assume that \( S \) acts on \( K \) faithfully. Otherwise \( S \) centralizes \( K \), and hence all primes of \( \pi(S) = \pi(L) = \pi(G) \) other than \( r \) are adjacent to \( r \) in \( GK(G) \), contrary to the fact that \( r_3(q) \) and \( r_6(q) \) have disjoint neighbourhoods in \( GK(L) \).

Let \( r \neq p \). Since \( r_3(q) \) divides the order of a proper parabolic subgroup of \( S \) with Levi factor of type \( A_2 \) and \( pr_3(q) \not\in \omega(S) \), the group \( S \) includes a Frobenius subgroup whose
kernel is a \( p \)-group and whose complement has order \( r_3(q) \). Furthermore, \( S \) includes a Frobenius subgroup with kernel of order \( q^2 \) and cyclic complement of order \((q^2 - 1)/(2, q - 1)\) by [12, Lemma 5]. Applying Lemma 4, we conclude that \( G \) has elements of orders \( rr_3(q) \) and \( r(q^2 - 1)/(2, q - 1) \). If \( r(q^2 - 1)/(2, q - 1) \in \omega(L) \), then keeping in mind that \( q > 3 \) and consulting (1), we see that either \( r \) divides \((q^2 + 1)/(2, q - 1) \) or \( r = 2 \). In the former case \( rr_3(q) \notin \omega(L) \). Let \( r = 2 \). Then the highest power of 2 in \( \omega(L) \) is equal to \((q^2 - 1)/2 \). Let us consider a parabolic subgroup \( P \) of \( SO_7(q) \) with Levi factor of type \( B_2 \). The Levi factor of \( P \) is \( A \times B \) where \( A \simeq GL_1(q) \), \( B \simeq SO_5(q) \) and both \( A \) and \( B \) contain elements with spinor norm a non-square (see [17, p. 98]). Since \( SO_5(q) \) has elements of order \( q^2 - 1 \), it follows that \( P \cap S \) also has elements of order \( q^2 - 1 \). Furthermore, the unipotent radical of \( P \) is abelian (see, for example, [4, Table 8.39]). Applying Lemma 6 we obtain that \( 2(q^2 - 1)/2 \in \omega(G) \setminus \omega(L) \).

Now let \( r = p \). If \( p = 2 \) then we apply Lemma 12. If \( p \) is odd then \( pr_3(q) \in \omega(G) \) by \([13, \text{Lemma 3.2}]\), and so \( \omega(G) \subset \omega(L) \).

Thus \( K = 1 \) and hence \( S \subset G \subset \text{Aut} S \). Consulting (1) and (2), we see that \( r_{nm}(p)(q^2 - 1)/(2, q - 1) \) lies in \( \omega(G) \setminus \omega(S) \). Since \( r_{4m}(p) \notin \pi(G/S) \), it follows from (2) that at least one of the numbers \((q + 1)/(2, q - 1) \) and \((q - 1)/(2, q - 1) \) belongs to \( \omega(G/S) \). The group \( \text{Out} S \) is a direct product of \( \text{Outdiag} S \) of order \((2, q - 1) \) and a cyclic group of order \( m \). If \( q \) is odd then \( q^3 + 1 \in \omega(\text{Inndiag} S) \setminus \omega(L) \), and so \( G \cap \text{Inndiag} S = S \) for both even and odd \( q \). Therefore the exponent of \( G/S \) divides \( m \). However \((q + 1)/(2, q - 1) = (p^m + 1)/(2, p - 1) \) for \( q > 3 \), a contradiction.

**Case (3).** Let \( n \geq 4 \) and both \( L \) and \( S \) be in \( \{S_{2n}(q), O_{2n+1}(q), O_{2n}^{-}(q)\} \). Since \( \omega(S) \subset \omega(L) \), it follows by Lemma 11 that \( S \neq S_{2n}(q) \) and \( (L, S) \neq (O_{2n+1}(q), O_{2n}^{-}(q)) \). Also we proved that \( (L, S) \neq (S_{2n}(q), O_{2n+1}(q)) \). Therefore \( L \in \{O_{2n+1}(q), S_{2n}(q)\} \) and \( S = O_{2n}^{-}(q) \). If \( n = 4 \), then the case (2) of the conclusion of Theorem 2 holds. So we may assume that \( n \geq 5 \). Let \( t = r_{2n}(q) \) and \( s = r_{2n-2}(q) \). Both of \( t \) and \( s \) exist and divide \(|S| \). Furthermore, \( t \) and \( s \) are not adjacent in \( GK(L) \) and their neighbourhoods in \( GK(L) \) are disjoint. In addition, \( s \) divides the order of a parabolic subgroup of \( S \) with Levi factor of type \( \text{2D}_{n-1} \) and \( ps \notin \omega(S) \). So \( S \) includes a Frobenius subgroup \( F \) whose kernel is a \( p \)-group and whose complement has order \( s \).

Suppose that \( n \) is odd and let \( r = r_{nm}(p) \), where \( q = p^m \). Since \( r \in \pi(L) \setminus \pi(S) \) and \( r \notin \pi(\text{Out} S) \), it follows that \( r \in \pi(K) \). Observe that \( \{t, s, r\} \) is a coclique in \( GK(L) \), and so \( t, s \notin \pi(K) \) by Lemma 2. Applying Lemma 5 to \( r \) and the Frobenius group \( F \), we conclude that \( rs \in \omega(G) \), a contradiction.

Suppose that \( n \) is even. Let \( r_1 = r_{(n-2)m}(p) \), \( r_2 = r_{(n+2)m}(p) \) if \( (n, q) \neq (8, 2) \) and \( r_1 = r_3(2) \), \( r_2 = r_5(2) \) otherwise. Then \( r_1 r_2 \in \omega(L) \setminus \omega(S) \) and \( r_1, r_2 \notin \pi(\text{Out} S) \). Therefore at least one of \( r_1 \) and \( r_2 \) divides \(|K| \). Denote this number by \( r \). If \( n > 6 \), then \( \{t, s, r\} \) is a coclique in \( GK(L) \), and we derive a contradiction by applying Lemma 5 similarly to the case of odd \( n \).

Now let \( n = 6 \). Then \( 2t \notin GK(L) \) by [39, Prop. 4.4], and so \( t \in \pi(S) \) by Lemma 2. Observe that \( \{r, s, r_5(q)\} \) is a coclique in \( GK(L) \), and hence \( s \) does not divide \(|K| \) by Lemma 2. We claim that at least one of the products \( rs \) and \( pt \) belongs to \( \omega(G) \), contrary to \( \omega(G) = \omega(L) \). Construct a normal \( r \)-series of \( K \) as follows:

\[
1 = R_0 \leq K_1 \leq R_1 \leq \ldots \leq K_{l-1} \leq R_{l-1} \leq K_l \leq R_l = K,
\]

where \( K_i/R_{i-1} = O_r(K/R_{i-1}) \) and \( R_i/K_i = O_r(K/K_i) \) for \( 1 \leq i \leq l \).
Suppose first that $K/K_i \neq 1$ and let $\tilde{K} = G/K_i$ and $\tilde{G} = G/K_i$. Since the group $C_{\tilde{G}}(\tilde{K})\tilde{K} / \tilde{K}$ is a normal subgroup of $\tilde{G} / \tilde{K} \simeq G / K_i$, it either includes $S$ or is trivial. In the former case $C_{\tilde{G}}(\tilde{K})$ has an element of order $s$, and so $rs \in \omega(G)$. In the latter case we apply Lemma 4 to the Frobenius group $F$, and again obtain $rs \in \omega(G)$.

Now suppose that $K = K_i$ and let $\tilde{R} = R_i / K_i$, $\tilde{K} = K_i / K_{i-1}$, and $\tilde{G} = G / K_{i-1}$. Since $O_r(\tilde{K}) = 1$, it follows that $C_{\tilde{K}}(\tilde{R}) \leq \tilde{R}$. Furthermore, we may assume that $C_{\tilde{G}}(\tilde{R}) \leq \tilde{K}$ as above. Thus $C_{\tilde{G}}(\tilde{R}) \leq \tilde{R}$. If $p$ does not divide $|\tilde{K}|$, then $(|\tilde{K}|, |F|) = 1$ and the Schur–Zassenhaus theorem implies that $\tilde{G}$ has a subgroup isomorphic to $F$. In this case we apply Lemma 4 and derive that $rs \in \omega(G)$. Let $p$ divides $|\tilde{K}|$, and let $\tilde{P}$ be a Sylow $p$-subgroup of $\tilde{K}$, $\tilde{Z} = Z(\tilde{P})$ and $\tilde{N} = N_{\tilde{G}}(\tilde{P})$. By Frattini argument, $\tilde{G} / \tilde{K} = \tilde{N} \tilde{K} / \tilde{K}$, and therefore $\tilde{N}$ has an element $g$ of order $s$. Furthermore, since $C_{\tilde{N}}(\tilde{Z})$ is normal in $\tilde{N}$, this group either has $S$ as a section or is contained in $\tilde{K}$. In the former case $pt \in \omega(G)$. In the latter case $g$ does not centralize $\tilde{Z}$, and then $\tilde{Z} = [\tilde{Z}, \langle g \rangle] \times C_{\tilde{Z}}(\langle g \rangle)$ yields $[\tilde{Z}, \langle g \rangle] \neq 1$. Thus $[\tilde{Z}, \langle g \rangle] \vartriangleleft \langle g \rangle$ is a Frobenius group that acts on $\tilde{R}$ faithfully, and applying Lemma 4 once again, we have $rs \in \omega(G)$.

**Case (4).** Finally let $L = O^+_{2n}(q)$, where $n \geq 6$ is even, and $S \in \{S_{2n-2}(q), O_{2n-1}(q)\}$. Let $t = r_{2n-2}(q)$ and $s = r_{n-1}(q)$. Both of $t$ and $s$ exist and divide $|S|$; $t$ and $s$ are not adjacent in $GK(L)$ and their neighbourhoods in $GK(L)$ are disjoint. In addition, $s$ divides the order of a parabolic subgroup of $S$ with Levi factor of type $A_{n-2}$ and $ps \notin \omega(S)$, therefore, $S$ includes a Frobenius subgroup $F$ whose kernel is a $p$-group and whose complement has order $s$. Let $r_1 = r_{n-2m}(p)$, $r_2 = r_{n-2m}(p)$ if $(n, q) \neq (8, 2)$, and $r_1 = r_3(2)$, $r_2 = r_5(2)$ otherwise. Then $r_1 r_2 \in \omega(L) \setminus \omega(S)$, thus at least one of the numbers $r_1$ and $r_2$ divides $|K|$. Furthermore, \{r_1, t, s\} and \{r_2, t, s\} are cocliques in $GK(L)$. By Lemma 5, one of $r_1 s$ and $r_2 s$ lies $\omega(G)$, a contradiction.

The proof of Theorem 2 is complete.

4. **New Examples of Non-Quasirecognizable Simple Groups**

A finite nonabelian simple group $L$ is said to be quasirecognizable by spectrum if every finite group isospectral to $L$ has only one nonabelian composition factor and this factor is isomorphic to $L$. Clearly quasirecognizability is a necessary condition for being almost recognizable.

Recall that for even $q$, the simple group $S_{2n}(q)$ is equal to $Sp_{2n}(q)$ and the simple group $O^+_{2n}(q)$ is $\Omega^+_{2n}(q)$, a subgroup of index $2$ in $GO^+_{2n}(q)$ (see, for example, [6, p. xii]). Mazurov and Moghaddamfar [24] noted that $\omega(Sp_{8}(2)) = \omega(GO^-_{8}(2))$, and thereby $Sp_{8}(2)$ is not quasirecognizable by spectrum. We generalize this result to all even $q$.

**Proposition 1.** Let $q$ be even. Then $\omega(Sp_{8}(q)) = \omega(GO^-_{8}(q))$ and in particular $Sp_{8}(q)$ is not quasirecognizable by spectrum.

**Proof.** Denote $Sp_{8}(q)$, $GO^{-}_{8}(q)$, and $\Omega^+_{8}(q)$ by $L$, $G$, and $S$ respectively. Since $G$ is a subgroup in $GO_{9}(q) \simeq Sp_{8}(q)$, it follows that $\omega(G) \subseteq \omega(L)$. Thus it is suffices to show that $\omega(L) \setminus \omega(S) \subseteq \omega(G)$. It follows from Lemma 8 that $\omega(L)$ consists of all divisors of the numbers $q^4 \pm 1$, $(q^2 \pm q + 1)(q^2 - 1)$, $2(q^3 \pm 1)$, $2(q^2 + 1)(q \pm 1)$, $4(q^2 \pm 1)$, and $8(q \pm 1)$. Supplementing this by Lemma 10, we see that every number of $\omega(L) \setminus \omega(S)$ is a divisor of one of the numbers $2(q^3 \pm 1)$, $4(q^2 + 1)$, and $8(q \pm 1)$. 
It is well known that $GO_{2n}^\tau(q)$ includes a subgroup of the form $GO_{2k}^\tau(q) \times GO_{2n-2k}^\tau(q)$ for every $1 \leq k \leq n-1$ and $\tau \in \{+,-\}$. Thus $G$ includes $GO_6^+(q) \times GO_2^-(q)$, $GO_4^+(q) \times GO_4^-(q)$, and $GO_2^+(q) \times GO_6^-(q)$.

It can be verified by means of [9] that $4 G_2^+ (q^2)$. Since $G_2^+ (q^2) \leq G_4^+ (q)$ and $SL_2(q^2) < GO_4^+ (q)$, it follows that $8(q^2 + 1) \in \omega(G)$. Since $q^2 - 1 \in \omega(G)$ and $GO_2^+(q)$ is dihedral of order $2(q - 1)$, we conclude that $2(q^2 + 1) \in \omega(G)$. Furthermore, $G_8 \simeq GO_6^+ (2) \leq GO_6^+ (q)$, and hence $8(q + 1) \in \omega(G)$.

The group $GO_6^- (q)$ is isomorphic to a split extension of $SU_4(q)$ by a graph automorphism. We identify $SU_4(q)$ with $H = \{ A \in SL_4(q^2) \mid A \bar{J} \bar{A}^T = J \}$, where $J$ is a matrix with 1's on antidiagonal and 0's elsewhere and $\bar{a}_{ij} = (a_{ij})$. Then $\gamma$ defined by $A = \bar{A}$ is a graph automorphism of $H$. Choose $t \in GF(q^2)$ such that $t^q \neq t$ and let

$$B = \begin{pmatrix}
1 & t & 0 & 0 \\
0 & 1 & 1 & 0 \\
0 & 0 & 1 & t^q \\
0 & 0 & 0 & 1
\end{pmatrix}.$$ 

It is not hard to verify that $B \in H$ and

$$(B\gamma)^4 = \begin{pmatrix}
1 & 0 & 0 & t^2 + t^{2q} \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.$$ 

Since $t^2 + t^{2q} \neq 0$, the order of $B\gamma$ is equal to 8, and hence $8 \in \omega(GO_6^- (q))$. □

References


[26] V. D. Mazurov, M. C. Xu, and H. P. Cao, Recognition of the finite simple groups $L_3(2^m)$ and $U_3(2^m)$ by their element orders, *Algebra Logic* **39** (2000), no. 5, 324–334.


