S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

Том 11, стр. 823–832 (2014) УДК 512.542
MSC 20D06, 20D60

SPECTRA OF AUTOMORPHIC EXTENSIONS OF FINITE SIMPLE SYMPLECTIC AND ORTHOGONAL GROUPS OVER FIELDS OF CHARACTERISTIC 2

M.A. ZVEZDINA

Abstract. We prove that the spectrum of any nontrivial automorphic extension of a finite simple symplectic or orthogonal group S over a field of characteristic 2 differs from the spectrum of S.

Keywords: Finite simple group, automorphic extension, element order, spectrum of a group.

1. Introduction

Let G be a finite group. The set of its element orders is called the *spectrum* of G and denoted by $\omega(G)$. Let S be a finite non-abelian simple group and let $S \leq G \leq \mathrm{Aut}(S)$ (we will refer to G as an automorphic extension of S). This article is concerned with the problem of finding all S and G such that $\omega(G) = \omega(S)$ [1, Question 17.36]. We solve this problem in the case where S is a finite simple symplectic or orthogonal group over a field of characteristic 2.

Theorem. *Let S be a finite simple symplectic or orthogonal group over a field of characteristic 2. If $S < G \leq \mathrm{Aut}(S)$, then $\omega(G) \neq \omega(S)$.*

Investigation of the spectra of automorphic extensions of simple groups is closely related to the recognition by spectrum problem. Two groups are called *isospectral* if they have the same spectra. A finite group G is called *recognizable by spectrum* if any finite group isospectral to G is isomorphic to G. It turns out that for most non-abelian simple groups S the following holds: if G is a finite group isospectral to S, then $S \leq G \leq \mathrm{Aut}(S)$, where «for most groups» means «for classical groups

Zvezdina, M.A., Spectra of automorphic extensions of finite simple symplectic and orthogonal groups over fields of characteristic 2.

The work is supported by Russian Science Foundation (project 14-21-00065).
Received October, 10, 2014, published November, 15, 2014.

of almost all dimensions and for almost all non-classical groups» (see [2]). Thus, in order to establish whether a simple group S is recognizable by spectrum, in most cases it suffices to examine the spectra of automorphic extensions of S. An example of such an approach is the following result, which is a direct consequence of our theorem and [2, Theorem 1].

Corollary. *Let S be a finite simple symplectic or orthogonal group of dimension at least 40 over a field of characteristic 2. Then S is recognizable by spectrum.*

2. Preliminaries

Our notation of non-abelian simple groups follows [3]. In that notation, $S_{2n}(q)$, $n \geq 2$ is a simple symplectic group, $O_{2n+1}(q)$, $n \geq 3$ is a simple orthogonal group of odd dimension, $O^+_{2n}(q)$ and $O^-_{2n}(q)$, $n \geq 4$ are simple orthogonal groups of even dimension. For short, let us denote simple orthogonal groups of even dimension by $O^\varepsilon_{2n}(q)$, $\varepsilon \in \{+,-\}$. If q is even, then $S_{2n}(q)$ and $O_{2n+1}(q)$ are isomorphic. We will consider these groups as symplectic groups.

Lemma 1. ([4, Corollary 3]) *Let q be a power of 2 and $G = S_{2n}(q)$, $n \geq 2$. Then $\omega(G)$ consists of all divisors of the following numbers:*

1. *$[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ for all $s \geq 1$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, and $n_1, n_2, ..., n_s > 0$ such that $n_1 + n_2 + ... + n_s = n$;*
2. *$2[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ for all $s \geq 1$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, and $n_1, n_2, ..., n_s > 0$ such that $n_1 + n_2 + ... + n_s = n - 1$;*
3. *$2^k[q^{n_1}+\varepsilon_1 1, q^{n_2}+\varepsilon_2 1, ..., q^{n_s}+\varepsilon_s 1]$ for all $s \geq 1$, $k \geq 2$, $\varepsilon_i \in \{+,-\}$, $1 \leq i \leq s$, and $n_1, n_2, ..., n_s > 0$ such that $2^{k-2}+1+n_1+n_2+...+n_s = n$;*
4. *2^k, if $2^{k-2}+1 = n$ for some $k \geq 2$.*

Lemma 2. ([4, Corollary 4]) *Let $G = O^\varepsilon_{2n}(q)$, where $n \geq 4$, $\varepsilon \in \{+,-\}$ and q is a power of 2. Then $\omega(G)$ consists of all divisors of the following numbers:*

1. *$[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1 ... q^{n_s}-1]$ for all $s \geq 1$, even l if $\varepsilon = +$, and odd l if $\varepsilon = -$, and $n_1, n_2, ..., n_s > 0$ such that $n_1 + n_2 + ... + n_s = n$;*
2. *$2^k[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1 ... q^{n_s}-1]$ for all $s \geq 1$ and $n_1, n_2, ..., n_s > 0$ such that $2^{k-2}+2+n_1+n_2+...+n_s = n$;*
3. *$2[q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1 ... q^{n_s}-1]$ for all $s \geq 1$ and $n_1, n_2, ..., n_s > 0$ such that $2+n_1+n_2+...+n_s = n$;*
4. *$2[q \pm 1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1 ... q^{n_s}-1]$ for all $s \geq 1$, even l if $\varepsilon = +$, and odd l if $\varepsilon = -$, and $n_1, n_2, ..., n_s > 0$ such that $2+n_1+n_2+...+n_s = n$;*
5. *$4[q-1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_s}+1]$ for all $s \geq 1$ which is even if $\varepsilon = +$, and odd if $\varepsilon = -$, and $n_1, n_2, ..., n_s > 0$ such that $3+n_1+n_2+...+n_s = n$;*
6. *$4[q+1, q^{n_1}+1, q^{n_2}+1, ..., q^{n_l}+1, q^{n_{l+1}}-1, q^{n_{l+2}}-1 ... q^{n_s}-1]$ for all $s \geq 1$, odd l if $\varepsilon = +$, and even l if $\varepsilon = -$, and $n_1, n_2, ..., n_s > 0$ such that $3+n_1+n_2+...+n_s = n$;*
7. *2^k, if $n = 2^{k-2}+2$ for some $k > 2$.*

Note that the spectrum of a group G is closed under divisibility, and hence it is uniquely determined by its subset of the maximal under divisibility elements. Denote this subset by $\mu(G)$.

Let q be a nonzero integer, r be an odd prime, and assume that $(q,r)=1$. A *multiplicative order* $e(r,q)$ of q modulo r is the minimal natural number m with $q^m \equiv 1 \pmod r$. For an odd q, put $e(2,q)=1$ if $q \equiv 1 \pmod 4$, and $e(2,q)=2$ if $q \equiv 3 \pmod 4$. A prime r with $e(r,q)=m$ is called a *primitive prime divisor* of q^m-1. Given q, denote by $r_m(q)$ a primitive prime divisor of q^m-1 if it exists. The existence of primitive prime divisors for almost all pairs (n,q) is proved by Zsigmondy in [5]. The following is a corollary to Zsigmondy's theorem:

Lemma 3. *Let q be an integer with $|q|>1$. For every natural m there exists a prime r with $e(r,q)=m$ but for the cases*

$$(q,m) \in \{(2,1),(2,6),(-2,2),(-2,3),(3,1),(-3,2)\}.$$

Note that if r is an odd primitive prime divisor of a number q^m-1 and m is even, then r divides $q^{\frac{m}{2}}+1$ and does not divide $q^{\frac{m}{2}}-1$. In this case we will also refer to r as a primitive prime divisor of $q^{\frac{m}{2}}+1$.

Let $\pi(n)$ be the set of all prime divisors of a natural number n. Denote by $\pi(G)$ the set of all prime divisors of the order of a group G. A *prime graph* of a group G is the graph with the set of vertices $\pi(G)$, where different vertices r and s are adjacent if and only if there is an element of order rs in G.

Define a function $\eta : \mathbb{N} \to \mathbb{N}$ by the rule:

$$\eta(m) = \begin{cases} m & \text{if } m \text{ is odd,} \\ \frac{m}{2} & \text{otherwise.} \end{cases} \tag{1}$$

Lemma 4. ([6, Prop. 2.4]) *Let G be one of the simple groups $S_{2n}(q)$ or $O_{2n+1}(q)$ over a field of characteristic p. Let r, s be odd primes with $r,s \in \pi(G)\setminus\{p\}$. Put $k=e(r,q)$ and $l=e(s,q)$, and suppose that $1 \le \eta(k) \le \eta(l)$. Then r and s are non-adjacent in $GK(G)$ if and only if $\eta(k)+\eta(l)>n$, and k, l satisfy the following condition:*

$$\frac{l}{k} \text{ is not an odd natural number.} \tag{2}$$

Condition (2) means that $q^{\eta(k)}+(-1)^k$ does not divide $q^{\eta(l)}+(-1)^l$.

Lemma 5. ([6, Prop. 2.5]) *Let $G=O^{\varepsilon}_{2n}(q)$ be a finite simple group over a field of characteristic p. Suppose r, s are odd primes and $r,s \in \pi(G)\setminus\{p\}$. Put $k=e(r,q)$, $l=e(s,q)$ and $1 \le \eta(k) \le \eta(l)$. Then r ans s are non-adjacent in $GK(G)$ if and only if*

$$2\eta(k)+2\eta(l) > 2n-(1-\varepsilon(-1)^{k+l}),$$

k and l satisfy the condition (2), and, if $\varepsilon=+$, then the chain of equalities

$$n=l=2\eta(l)=2\eta(k)=2k$$

is not true.

Lemma 6. *Let r be an odd prime divisor of a natural number $n \ge 7$. Then there exist natural numbers k and l such that $k+l=n$ and k, l satisfies the following condition:*

$$(k,r)=(l,r)=1;\ k \text{ and } l \text{ do not divide each other.} \tag{3}$$

Proof. Let n be even. Since r is odd, r divides $\frac{n}{2}$. Let $k=\frac{n}{2}-1$, $l=\frac{n}{2}+1$. It is clear that $(k,r)=(l,r)=1$. Since $n>6$, k does not divide l, because $k>\frac{l}{2}$. Let

n be odd. Then $k = \frac{n-1}{2}$, $l = \frac{n+1}{2}$. Again, $(k, r) = (l, r) = 1$ and k, l do not divide each other.

Lemma 7. *Let r be an odd prime divisor of a natural number $n \geq 6$. Then there exist natural numbers k and l such that $k + l = n + 1$, and if $n \neq 9$, then k, l satisfy* (3)*, otherwise, $(k, r) = (l, r) = 1$, $q^k + 1$ and $q^l + 1$ do not divide each other.*

Proof. Let n be even. Then $k = \frac{n-2}{2}$, $l = \frac{n+4}{2}$. Let $n \neq 9$ be odd. If $r > 3$, then $k = \frac{n-1}{2}$, $l = \frac{n+3}{2}$. Let $r = 3$. Then $k = \frac{n-5}{2}$, $l = \frac{n+7}{2}$ if $n > 17$, and $k = 5$, $l = 11$ if $n = 15$. If $n = 9$, then $k = 2$, $l = 8$.

Lemma 8. *Let r be an odd prime divisor of a natural number $n > 9$. Then there exist natural numbers k and l such that $k+l = n-1$ and k, l satisfy the condition* (3)*.*

Proof. Let n be odd. If $r > 3$, then $k = \frac{n-3}{2}$, $l = \frac{n+1}{2}$. Let $r = 3$. Then $k = \frac{n-7}{2}$, $l = \frac{n+5}{2}$ if $n > 19$, and $k = 4$, $l = 10$ if $n = 15$. Let n be even and $n \neq 10$. Then $k = \frac{n-4}{2}$, $l = \frac{n+2}{2}$. Let $n = 10$. Then $r \neq 7$, and we take $k = 2$, $l = 7$.

Our terminology for the automorphisms of finite groups of Lie type follows [7, Def. 2.5.13]. Let G be a nontrivial automorphic extension of a simple symplectic or orthogonal group S over a field of characteristic 2, i.e. $S < G \leq \mathrm{Aut}(S)$. Note that all the simple groups under consideration have no outer diagonal automorphisms, and all their automorphic extensions are split (see, e.g., [7, Theorem 2.5.12]). Also observe that in proving $\omega(G) \neq \omega(S)$, we may assume that the index $|G : S|$ is a prime number, because it is the minimal example (if inequality $\omega(G) \neq \omega(S)$ holds for every extension G of a group S such that $|G : S|$ is prime, then it holds for an arbitrary extension G of a group S).

Lemma 9. ([8, Prop. 13]) *Let G be a connected linear algebraic group over an algebraically closed field of characteristic p. Let τ be a surjective endomorphism of G. Denote $G_r = C_G(\tau^r)$, where r is a natural number. If the group G_r is finite for some r, then τ is an automorphism of order r of G_r, and*

$$\omega(G_r\langle\tau\rangle) = \bigcup_{k|r} \frac{r}{k}\omega(G_k).$$

Lemma 10. *Let a symbol X be chosen from the set $\{S_{2n}, O^+_{2n}, O^-_{2n}\}$ and let q be a power of 2. Let τ be a field automorphism of order r of a group $X(q)$, where r is odd, if $X = O^-_{2n}$. Then*

$$\omega(X(q) \leftthreetimes \langle\tau\rangle) = \bigcup_{k|r} k\omega(X(q^{\frac{1}{k}})).$$

Proof. Suppose that $X = S_{2n}$ or $X = O^+_{2n}$, and let G be $Sp_{2n}(\overline{F})$ or $G = \Omega_{2n}(\overline{F})$ respectively, where $\overline{F}$ denotes the algebraic closure of the binary field. Denote $q^{1/r}$ by q_0 and let φ be the map $(a_{ij}) \to (a^{q_0}_{ij})$ of G. Then φ is a surjective endomorphism of G and $C_G(\varphi^k) = X(q_0^k)$ for all k dividing r.

Suppose that $X = O^-_{2n}$. Let $G = \Omega_{2n}(\overline{F})$ and let φ be as above. Let γ be a graph automorphism of G commuting with φ and define $\tau = \varphi\gamma$. Then $C_G(\tau) = X(q_0)$ and since r is odd, it follows that $C_G(\tau^k) = X(q_0^k)$ for all k dividing r.

The result now follows by Lemma 9.

3. Symplectic groups

Proposition 1. *Let S be the finite simple symplectic group $S_{2n}(q)$, where q is even. If $S < G \leq \operatorname{Aut} G$, then $\omega(G) \neq \omega(S)$.*

Proof. It was shown in [9] that a group with spectrum equal to the spectrum of $S_6(2)$ is isomorphic to either $S_6(2)$ or $O_8^+(2)$. The group $S_6(4)$ is proved to be recognizable by spectrum in [10]. Finally, the main result of [11] yields that a group $S_6(q)$ is recognizable by spectrum if q is even and $q > 4$. So we will consider groups $S_{2n}(q)$, where $n \neq 3$.

Let $S < G \leq \operatorname{Aut}(S)$. We may assume that $G = S \leftthreetimes \langle \tau \rangle$, where τ is an automorphism of prime order r.

Step 1. Assume that τ is a field automorphism. For short, denote $q^{\frac{1}{r}}$ by q_0 and $S_{2n}(q_0)$ by S_0. By Lemma 10, it follows that $r \cdot \omega(S_0) \subseteq \omega(G)$. The idea is to find an element $r_0 \in \omega(S_0)$ such that $rr_0 \notin \omega(S)$.

Suppose that $r = 2$. By Lemma 1, the following holds: $2^m \in \omega(S_0)$ if and only if $2^m \in \omega(S)$. Let 2^m be the maximal power of 2 in $\omega(S_0)$ (and so in $\omega(S)$). Then $2 \cdot 2^m \in 2 \cdot \omega(S_0) \subseteq \omega(G)$, but $2^{m+1} \notin \omega(S)$. So $\omega(G) \neq \omega(S)$.

Now suppose that r is odd. Let $n = 2^{k-2} + 1$ for some $k \geq 2$. By Lemma 1, $2^k \in \mu(S_0)$, and, similarly, $2^k \in \mu(S)$. So $r \cdot 2^k \in r \cdot \omega(S_0) \subseteq \omega(G)$, but $r \cdot 2^k \notin \omega(S)$. Therefore, $\omega(G) \neq \omega(S)$.

Further we assume that $n \neq 2^{k-2} + 1$. Denote $s = e(r, q)$. We will try to find r_0 as a primitive prime divisor of a number $q_0^t - 1$, where $t \leq 2n$ satisfies the following conditions:

$$(t, r) = 1; \tag{4}$$

$$\left(\frac{t}{s}\right)^{sgn(t-s)} \text{ is not an odd natural number;} \tag{5}$$

$$\eta(t) + \eta(s) > n. \tag{6}$$

If (4) holds, then r_0 is also a primitive prime divisor of $q^t - 1$. By Lemma 4, conditions (5) and (6) imply that $rr_0 \notin \omega(S)$.

• $n = 4$. Let $\eta(s) = 1$, i.e. r divides $q - 1$ or $q + 1$. We take a number $r_8(q_0)$ as r_0 (recall that $r_8(q_0)$ denotes a primitive prime divisor of $q_0^8 - 1$). Since $t = 8$ and r is odd, $(t, r) = 1$ and condition (4) holds. So r_0 is a primitive prime divisor of $q^8 - 1$. Conditions (5) and (6) obviously hold: $\eta(t) + \eta(s) = 4 + 1 > n$, and $\frac{t}{s} = 8$ if r divides $q - 1$, $\frac{t}{s} = 4$ if r divides $q + 1$. By Lemma 4, $rr_0 \notin \omega(S)$.

Let $\eta(s) \in \{2, 3\}$. We take $r_0 = r_8(q_0)$. It is easy to check that conditions (4–6) hold.

Let $\eta(s) = 4$. We take $t = 2$, i.e. $r_0 = r_2(q_0)$.

• $n = 6$. Let $\eta(s) = 1$. If $r \neq 3$, then we take $r_0 = r_{12}(q_0)$. Suppose that $r = 3$. Let us obtain r_0 as a product of primitive prime divisors of two different numbers. Namely, we take $r_0 = r_8(q_0)r_4(q_0)$. Since $(r, 8) = (r, 4) = 1$, numbers $r_8(q_0)$ and $r_4(q_0)$ are also primitive prime divisors of $q^8 - 1$ and $q^4 - 1$ respectively. Clearly, $r_8(q_0)r_4(q_0) \in \omega(S)$, and so $rr_8(q_0)r_4(q_0) \in r \cdot \omega(S_0)$. On the other hand, $\eta(s) + \eta(8) + \eta(4) > n$, and numbers $q^4 + 1$ and $q^2 + 1$ are coprime to each other and to $q \pm 1$. By Lemma 1, we obtain that $rr_8(q_0)r_4(q_0) \notin \omega(S)$.

Let $\eta(s) = 2$. Then we take $r_0 = r_8(q_0)r_2(q_0)$. It is easy to show that $rr_0 \in r\omega(S_0)$ and $rr_0 \notin \omega(S)$, and so $\omega(G) \neq \omega(S)$.

Note that r and q are coprime, and so Fermat's little theorem implies that $r > 3$ if $s = e(r, q) > 2$ (or, equivalently, if $\eta(s) \geq 2$).

Let $\eta(s) \in \{3, 5, 6\}$. In all these cases we take $r_0 = r_8(q_0)$.

Let $\eta(s) = 4$. We take $t = 10$ if $r \neq 5$, and $t = 6$ otherwise. Then $r_0 = r_t(q_0)$. Note that if $r = 5$, and we have taken $t = 6$, then a primitive prime divisor of $q_0^6 - 1$ does exist (otherwise, the equality $q_0^6 = 2^6$ would hold by Lemma 3. Since $q = q_0^5 = 2^5$, we have $s = e(r, q) = e(5, 32) = 4$, and so $\eta(s) = 2$. But we assumed that $\eta(s) = 4$. Therefore $q_0^6 \neq 2^6$, and there exists a primitive prime divisor of $q_0^6 - 1$).

• $n \geq 7$. Let $\eta(s) = 1$.

Case 1: r divides $q + 1$. If r does not divide n, we take $t = 2n$ if n is even (then $q + 1$ is coprime to $q^n + 1$), and $t = n$ if n is odd (then $q + 1$ is coprime to $q^n - 1$). Now assume that r divides n. By Lemma 6, the number $n \geq 7$ can be represented as a sum of two different natural numbers k and l, which satisfy condition (3).

Assume that n is even. If k and l are even, then $q + 1$ is coprime to $q^k + 1$ and $q^l + 1$, and we take $r_0 = r_{2k}(q_0)r_{2l}(q_0)$ (since $(r, k) = (r, l) = 1$, numbers $r_{2k}(q_0)$ and $r_{2l}(q_0)$ are primitive prime divisors of $q^{2k} - 1$ and $q^{2l} - 1$ respectively). If k and l are odd, then $q + 1$ is coprime to $q^k - 1$ and $q^l - 1$, and we take $r_0 = r_k(q_0)r_l(q_0)$. Now assume that n is odd. Then n is a sum of an even number, say k, and an odd number, say l. Then $q + 1$ is coprime to $q^k + 1$ and $q^l - 1$, and we take $r_0 = r_{2k}(q_0)r_l(q_0)$.

Case 2: r divides $q - 1$. If r does not divide n, we take $t = 2n$ (because $q - 1$ is coprime to $q^n + 1$). If r divides n, we take $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, where $k + l = n$ and k, l satisfy condition (3) (because $q - 1$ is coprime to $q^k + 1$ and $q^l + 1$). Note that if $n = 7$ (and so $r = 7$), and we have taken $k = 3$, $l = 4$, then a primitive prime divisor of $q_0^{2k} - 1 = q_0^6 - 1$ does exist. (Otherwise, the equalities $q_0 = 2$ and $q = 2^7$ would hold. But r would not divide $q - 1$ in that case. So, $q_0 \neq 2$).

Let $\eta(s) = 2$, i.e. r divides $q^2 + 1$.

Case 1: r does not divide the odd one of the numbers $\{n, n - 1\}$. If n is odd (i.e. r does not divide n), then we take $r_0 = r_{2n}(q_0)$. If n is even (i.e. r does not divide $n - 1$), then $r_0 = r_{2(n-1)}(q_0)$.

Case 2: r divides the odd one of the numbers $\{n, n - 1\}$. Consider the case when n is even (otherwise, we do the same, with n replaced by $n - 1$). Then r does not divide n. Note that $q^2 + 1$ cannot divide both $q^n - 1$ and $q^n + 1$ (and $q^2 + 1$ is coprime to the one of these two numbers which it does not divide). So we choose r_0 as follows: if $q^2 + 1$ divides $q^n - 1$ (equivalently, if n is divisible by 4), then $r_0 = r_{2n}(q_0)$. If $q^2 + 1$ divides $q^n + 1$ (equivalently, if n is even and not divisible by 4), then $r_0 = r_n(q_0)r_{\frac{n}{2}}(q_0)$ (the equality $\eta(s) + \eta(n) + \eta(\frac{n}{2}) = n + 2 > n$ holds, because $\frac{n}{2}$ is an odd number. Moreover, $q^2 + 1$ is coprime to $q^n - 1$).

Let $\eta(s) = 3$. Condition (6) implies that $\eta(t) \in \{n, n - 1, n - 2\}$. Two of these three numbers are not divisible by $\eta(s) = 3$ (and, consequently, not divisible by 6. That guarantees the existence of primitive prime divisors of the corresponding numbers). Recall that $r > 3$ by Fermat's little theorem. Therefore at least one of the two numbers is coprime to r, and it can be chosen as $\eta(t)$.

Let $\eta(s) \geq 4$. Then $\eta(t) \in \{n, n - 1, n - 2, n - 3\}$. At least three of these four numbers are not divisible by $\eta(s)$. Note that $\eta(t)$ cannot divide $\eta(s)$, because $\eta(t) > \frac{n}{2}$ and $\eta(t) \neq \eta(s)$. Since $r > 3$, at least two of the three numbers that are not divisible by $\eta(s)$ are not divisible by r as well, and at least one of these two numbers is not equal to 6; we take that one as $\eta(t)$.

We found r_0 for all possible n and $\eta(s)$, so Step 1 is completed.

Step 2. The simple symplectic groups $S_{2n}(q)$ with $n > 2$ have neither outer diagonal nor outer graph automorphisms, so for these groups the proposition has already been proved (see Step 1). It remains to consider $S = S_4(q)$, $q = 2^\alpha > 2$. For this group, $\mathrm{Aut}(S) \simeq S \leftthreetimes \langle\gamma\rangle$, where $\langle\gamma\rangle$ is a cyclic group of order 2α generated by a graph-field (in the terminology of [7, Def. 2.5.13]) automorphism γ of a group S. All elements of odd prime order in $\langle\gamma\rangle$ are field automorphisms; they were considered on Step 1. The only involution of $\langle\gamma\rangle$ is the automorphism γ^α. Suppose that α is odd. Then the centralizer of γ^α is isomorphic to a group ${}^2B_2(q)$. If r_0 is a primitive prime divisor of $q^2 + 1$ (i.e. $r_0 = r_4(q)$)), then $2 \cdot r_0 \in \omega(S\langle\gamma^\alpha\rangle)$ and $2 \cdot r_0 \notin \omega(S)$. So $\omega(S\langle\gamma^\alpha\rangle) \neq \omega(S)$. Now suppose that α is even. Then the involution γ^α is a field automorphism of S. Field automorphisms were considered on Step 1, so Proposition 1 is proved.

4. Orthogonal groups

Proposition 2. *Let S be the finite simple orthogonal group $O^\varepsilon_{2n}(q)$, $\varepsilon \in \{+, -\}$, where q is even. If $S < G \leq \mathrm{Aut}\, G$, then $\omega(G) \neq \omega(S)$.*

Proof. Information about groups with the spectrum equal to $\omega(O^+_8(2))$ was given in the previous section. The group $O^+_8(4)$ was proved to be recognizable by spectrum in [10]. It was shown in [11] that a group $O^+_8(q)$, where $q > 4$ is even, is recognizable by spectrum. So we will consider groups $O^+_{2n}(q)$ with $n > 4$ and $O^-_{2n}(q)$ with $n \geq 4$. Let S be one of such groups over a field of characteristic 2, and let $S < G \leq \mathrm{Aut}(S)$, where G is a split extension of S by an automorphism τ of prime order r.

Step 1. Assume that τ is a field automorphism of S (if $S = O^-_{2n}(q)$, then r is odd). Let us prove that $\omega(G) \neq \omega(S)$ in that case. We denote $q^{\frac{1}{r}}$ by q_0 and $O^\varepsilon_{2n}(q_0)$ by S_0.

Let τ be a field automorphism of order 2 of $O^+_{2n}(q)$. By Lemma 2, we obtain that 2^m is the maximal power of 2 in $\omega(S_0)$ if and only if 2^m is the maximal power of 2 in $\omega(S)$. It follows from Lemma 10 that $2 \cdot 2^m \in 2 \cdot \omega(S_0) \subseteq \omega(G)$, but $2^{m+1} \notin \omega(S)$. So $\omega(G) \neq \omega(S)$.

Let r be an odd prime. Let $n = 2^{k-2} + 2$ for some $k > 2$. Then $2^k \in \mu(S_0)$ by Lemma 2, so $r \cdot 2^k \in r\omega(S_0) \subseteq \omega(G)$. But $2^k \in \mu(S)$, so $r \cdot 2^k \notin \omega(S)$, and we have $\omega(G) \neq \omega(S)$.

Now we suppose that $n \neq 2^{k-2} + 2$. We need to find a primitive prime divisor r_0 of a number $q_0^t - 1$, where $t \leq 2n$ satisfies conditions (4), (5) and the following conditions:

$$2\eta(t) + 2\eta(s) > 2n - (1 - \varepsilon(-1)^{s+t}); \tag{7}$$

(8) *if $\varepsilon = +$, then none of the chains of equations:*

$$n = t = 2\eta(t) = 2\eta(s) = 2s,\ n = s = 2\eta(s) = 2\eta(t) = 2t \text{ is not true.}$$

Condition (4) implies that r is also a primitive prime divisor of $q^t - 1$. Conditions (5), (7), (8) guarantee that we can apply Lemma 5 and conclude that r and r_0 are non-adjacent in $GK(S)$, and so $rr_0 \notin \omega(S)$.

• $n = 5$. Let $\eta(s) = 1$.

Case 1: r divides $q - \varepsilon 1$ (recall that $\varepsilon = +$ if $S = O^+_{2n}(q)$, and $\varepsilon = -$ if $S = O^-_{2n}(q)$). Then $r_0 = r_8(q_0)$.

Case 2: r divides $q+\varepsilon 1$. If $\varepsilon = -$, then $r_0 = 8r_2(q_0)$. It follows from Lemma 2 that $r_0 \in \omega(S_0)$ and $rr_0 \notin \omega(S)$. If $\varepsilon = +$, and if there exists a primitive prime divisor of $q_0 - 1$, then we take $r_0 = 8r_1(q_0)$. Now assume that $q_0 - 1$ has no primitive prime divisors. Then the only possibility is $q_0 = 2$. Note that r divides $q + 1 = 2^r + 1$ and $2^{r-1} - 1$. The greatest common divisor of these three numbers equals 3, therefore $r = 3$. We take $r_0 = r_5(q_0)$.

Let $\eta(s) = 2$, i.e. r divides $q^2 + 1$. Then we take $r_0 = r_8(q_0)$.

Let $\eta(s) = 3$. It follows from Fermat's little theorem that $r > 3$. If r divides $q^3 - 1$, then $r_0 = r_6(q_0)$. If r divides $q^3 + 1$, then $r_0 = r_3(q_0)$.

Let $\eta(s) \in \{4, 5\}$. Then $r_0 = r_4(q_0)$.

• $n \geq 7$. Let $\eta(s) = 1$.

Case 1: r divides $q - 1$. Denote

$$m = \begin{cases} n-1 & \text{if } \varepsilon = +, \\ n & \text{if } \varepsilon = -. \end{cases} \tag{9}$$

If r does not divide m, then $r_0 = r_{2m}(q_0)$. If r divides m, then there exist natural numbers k, l such that $k + l = m + \varepsilon 1$ and k, l satisfy condition (3) (if $\varepsilon = +$, such k and l exist for every $n \geq 7$ by Lemma 7; if $\varepsilon = -$, then such k and l exist for every $n > 9$ by Lemma 8). Then $r_0 = r_{2k}(q_0)r_{2l}(q_0)$. If $\varepsilon = -$ and $n = 7$, take $r_0 = r_4(q_0)r_8(q_0)$, if $\varepsilon = -$ and $n = 9$, take $r_0 = 4r_4(q_0)r_8(q_0)$. In all cases $rr_0 \notin \omega(S)$.

Case 2: r divides $q + 1$. Assumme that r does not divide n. Let $\varepsilon = +$. If n is odd, then $r_0 = r_n(q_0)$. If n is even, and r does not divide $n-1$, then $r_0 = r_{n-1}(q_0)$. If $n \geq 7$ is even, and r divides $n-1$, then there exist k and l satisfying condition (3) such that $k + l = n$ (by Lemma 7). If k and l are even, then $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, otherwise, $r_0 = r_k(q_0)r_l(q_0)$.

Let $\varepsilon = -$. If n is odd, and r does not divide $n - 1$, then $r_0 = r_{2(n-1)}(q_0)$. If n is odd, and r divides $n - 1$, then by Lemma 7 there exist k and l satisfying condition (3) such that $k + l = n$. One of these numbers, say k, is even, another one is odd. Then $r_0 = r_{2k}(q_0)r_l(q_0)$. If n is even, then $r_0 = r_{2n}(q_0)$.

Now assume that r divides n.

Let $\varepsilon = +$. Suppose that n is odd. By Lemma 8, for every $n > 9$ there exist k and l satisfying condition (3) such that $k+l = n-1$. If k and l are even, then $r_0 = r_{2k}(q_0)r_{2l}(q_0)$, otherwise, $r_0 = r_k(q_0)r_l(q_0)$. If $n = 7$, then $r_0 = r_4(q_0)r_8(q_0)$, and if $n = 9$, then $r_0 = 4r_4(q_0)r_8(q_0)$. Now suppose that n is even. Then $r_0 = r_{n-1}(q_0)$.

Let $\varepsilon = -$. If n is odd, then $r_0 = r_{2(n-1)}(q_0)$. Now let n be even. Obviously, $n \neq 8$, because r is odd and divides n, so $n > 9$. By Lemma 8, there exist k and l satisfying condition (3) such that $k + l = n - 1$. If k is even, and l is odd, then $r_0 = r_{2k}(q_0)r_l(q_0)$.

Let $\eta(s) = 2$. Denote by n' the odd one of the numbers $\{n, n-1\}$. Suppose that r does not divide n'. Then r_0 is a primitive prime divisor of $q_0^{n'} - \varepsilon 1$. Now suppose that r divides n'. If n is odd, then r_0 is a primitive prime divisor of $q_0^{n-2} - \varepsilon 1$. If n is even, then r divides $n-1$. Let $\varepsilon = +$. Since $n-1 \geq 7$, there exist k and l satisfying condition 3 such that $k + l = n - 1$ (by Lemma 6). As in the proof of Lemma 6, put $\{k, l\} = \{\frac{n-2}{2}, \frac{n}{2}\}$. Let k be the odd one of these two numbers. If $n \equiv 0 \pmod 8$ or $n \equiv 2 \pmod 8$, then l is divisible by 4. Then we take $r_0 = r_{2k}(q_0)r_{2l}(q_0)$. If $n \equiv 4 \pmod 8$ or $n \equiv 6 \pmod 8$, then l is even and not divisible by 4, i.e. $\frac{l}{2}$ is an odd number. Then we take $r_0 = r_{2k}(q_0)r_{\frac{l}{2}}(q_0)r_l(q_0)$ (it is easy to show that the

numbers k and $\frac{l}{2}$ do not divide each other as well). Let $\varepsilon = -$. If n is divisible by 4, then q^2+1 does not divide q^n+1. We take $r_0 = r_{2n}(q_0)$. If $n \equiv 2 \pmod 4$, then q^2+1 does not divide $q^{n-2}+1$. We take $r_0 = r_{2(n-2)}(q_0)$.

Let $\eta(s) = 3$.

Case 1: r divides q^3-1. Denote by n' one of the numbers $\{n-1, n-2\}$ which is coprime to r. Note that numbers q^3-1 and $q^{n'}+1$ are coprime for every n'. We take $r_0 = r_{2n'}(q_0)$.

Case 2: r divides q^3+1. Let $\varepsilon = +$. If there exists a number $n' \in \{n-1, n-2\}$ coprime to r and 3, then $r_0 = r_{2n'}(q_0)$. Otherwise we choose an odd number $n'' \in \{n, n-3\}$. It is coprime to r and 3. We take $r_0 = r_{n''}(q_0)$. Let $\varepsilon = -$. We choose a number $n' \in \{n, n-1, n-2\}$, which is coprime to r and 3, and we take $r_0 = r_{2n'}(q_0)$.

Let $\eta(s) \geq 4$. Let $\varepsilon = +$. If there exists an odd number $n' \in \{n, n-1, n-2, n-3\}$ coprime to r and not divisible by s, then $r_0 = r_{n'}(q_0)$. Otherwise, we choose the smallest even number $n' \in \{n, n-1, n-2, n-3\}$ coprime to r and not divisible by s. Then $r_0 = r_{2n'}(q_0)$. Let $\varepsilon = -$. There exists a number $n' \in \{n, n-1, n-2, n-3\}$ coprime to r and s and not equal to 6. We take $r_0 = r_{2n'}(q_0)$.

We found r_0 for all possible n and s. So, if τ is a field automorphism of S, then $\omega(S \leftthreetimes \langle\tau\rangle) \neq \omega(S)$. Since a group $O_8^+(q)$ is not under our consideration, all the outer automorphisms of odd prime order of S are field automorphisms. In particular, further we can assume that $|G:S| = 2$.

Step 2. Consider involutive automorphisms of $S = O_{2n}^{\varepsilon}(q)$, $q = 2^\alpha$. Let σ be a graph automorphism of $O_{2n}^{\varepsilon}(q)$ of order 2. If α is even, let τ be a field automorphism of $O_{2n}^{+}(q)$ of order 2.

Let $S = O_{2n}^{+}(q)$. Then $\mathrm{Aut}(S) = S \leftthreetimes (\langle\varphi\rangle \times \langle\sigma\rangle)$, where $\langle\varphi\rangle$ is a group of field automorphisms of order α. So involutive automorphisms of S are σ, $\tau \in \langle\varphi\rangle$ (if α is even), $\tau\sigma$ (if α is even). The involutive field automorphism of $O_{2n}^{+}(q)$ was already considered on Step 1. For the graph automorphism σ, the equality $C_S(\sigma) = S_{2(n-1)}(q)$ holds by [7, Prop. 4.9.2]. Let us find a number $r_0 \in \omega(S_{2(n-1)}(q))$ such that $2 \cdot r_0 \notin \omega(S)$. Let r_0 be a primitive prime divisor of $q^{n-1}+1$. By Lemma 2, we obtain that $2 \cdot r_0 \notin \omega(S)$.

For $\tau\sigma$, the equality $C_S(\tau\sigma) = O_{2n}^{-}(q^{1/2})$ holds by [7, Prop. 4.9.1]. Let us find an odd number r_0 in the spectrum of that centralizer such that $2 \cdot r_0 \notin \omega(S)$. Choose an odd number $n' \in \{n, n-1\}$. Let $r_0 \in \omega(O_{2n}^{-}(q^{1/2}))$ be a primitive prime divisor of $(q^{\frac{1}{2}})^{n'}+1$. Then r_0 is a primitive prime divisor of $q^{n'}-1$, and hence $2 \cdot r_0 \notin \omega(S)$.

Let $S = O_{2n}^{-}(q)$. Then $\mathrm{Aut}(S)$ is a split extension of S by a cyclic subgroup of order 2α, which has the only involution, a graph automorphism σ. By [7, Prop. 4.9.2], the equality $C_S(\sigma) = S_{2(n-1)}(q)$ holds. Let $r_0 \in \omega(S_{2(n-1)}(q))$ be a primitive prime divisor of $q^{n-1}+1$ (or of $q^{n-1}-1$ if $q = 2$ and $n = 4$). It follows from Lemma 2 that $2 \cdot r_0 \notin \omega(S)$.

Now Propositions 1 and 2 are proved, and so is the theorem.

Proof of Corollary. Assume that G is a finite group isospectral to S. If the dimension of S is at least 40, then [2, Theorem 1] implies that $S \leq G \leq \mathrm{Aut}(S)$. By our Theorem, we obtain that $G = S$. Thus, S is recognizable by spectrum.

References

[1] V. D. Mazurov and E.I. Khukhro (eds.), *The Kourovka notebook. Unsolved problems in group theory*, 18 ed., Institute of Mathematics, Russian Academy of Sciences, Siberian Div., Novosibirsk, 2014.

[2] A. V. Vasil'ev, M. A. Grechkoseeva, *On the structure of finite groups isospectral to finite simple groups* (2014), arXiv:1409.8086.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985. MR0827219

[4] A. A. Buturlakin, *Spectra of finite symplectic and orthogonal groups*, Siberian Adv. Math. **21**:3 (2011), 176–210.

[5] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284. MR1546236

[6] A. V. Vasil'ev and E. P. Vdovin, *Cocliques of maximal size in the prime graph of a finite simple group*, Algebra and Logic **50**:4 (2011), 291–322. MR2893582

[7] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 3*, Mathematical Surveys and Monographs, vol. 40.3, American Mathematical Society, Providence, RI, 1998. MR1490581

[8] A. V. Zavarnitsine, *Recognition of the simple groups $U_3(q)$ by element orders*, Algebra and Logic **45**:2 (2006), 106–116. Zbl 1115.20011

[9] V. D. Mazurov, *Characterizations of finite groups by sets of orders of their elements*, Algebra and Logic **36**:1 (1997), 23–32. MR1454690

[10] I. B. Gorshkov, *Recognition of finite simple groups with orders having prime divisors at most* 17 *by the spectrum*, Sib. Élektron. Mat. Izv. **7** (2010), 14–20. MR2586671

[11] A. M. Staroletov, *On recognition by spectrum of the simple groups $B_3(q)$, $C_3(q)$ and $D_4(q)$*, Siberian Math. J. **53**:3 (2012), 532–538. MR2978582

Maria Anatol'evna Zvezdina
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: maria.a.zvezdina@gmail.com