S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

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

Том 14, стр. 405–417 (2017) УДК 512.5
DOI 10.17377/semi.2017.14.034 MSC 20D06

ON MAXIMUM ORDERS OF ELEMENTS OF SIMPLE ORTHOGONAL GROUPS IN CHARACTERISTIC 2

M.A. GRECHKOSEEVA, D.V. LYTKIN

Abstract. We give exact formulas for the two largest orders of elements of the simple orthogonal group $\Omega^{\varepsilon}_{2n}(q)$, where $\varepsilon \in \{+,-\}$ and $q > 2$ is even.

Keywords: maximum order of an element, simple orthogonal group.

1. Introduction

Given a finite group G, we write $o_1(G)$ and $o_2(G)$, with $o_1(G) > o_2(G)$, for the two largest orders of elements of G. This paper was motivated by [1], where for algorithmic needs, the exact values of $o_1(S)$ and $o_2(S)$ for S a simple group of Lie type in odd characteristic were determined. As for the groups of Lie type in characteristic 2, there are upper bounds on $o_1(S)$ [2, Lemma 1.3] and even on $o_1(\operatorname{Aut} S)$ [3, Table 3], but determining the exact values encounters obstacles related to orthogonal and symplectic groups (see [1, p. 808] for explanation). The symplectic groups $Sp_{2n}(2^m)$ were handled independently in [4] and [5] (the former gives formulas for $o_1(S)$ and $o_2(S)$, and the latter for $o_1(S)$ and $o_1(\operatorname{Aut} S)$).

Our main result is the exact values of $o_1(S)$ and $o_2(S)$ for $S = \Omega^{\varepsilon}_{2n}(2^m)$, where $n \geqslant 4$ and $m > 1$ (Theorem 1). In particular, we show that these numbers are always odd and that $o_i(\operatorname{Aut} S) = o_i(S)$ for $i = 1, 2$ provided that $S \neq \Omega^{+}_{8}(2^m)$.

The main difficulty with $S = \Omega^{\varepsilon}_{2n}(2)$ is that even $o_1(S)$ is not always odd, and so is not always an order of a semisimple element. The value of $o_1(\Omega^{\varepsilon}_{2n}(2))$ in some cases can be derived from the results of [4]: it turns out that at least one of $o_1(Sp_{2n}(2))$ and $o_2(Sp_{2n}(2))$ is an order of an element of $\Omega^{+}_{2n}(2)$ or $\Omega^{-}_{2n}(2)$.

Grechkoseeva, M.A., Lytkin, D.V. On maximum orders of elements of simple orthogonal groups in characteristic 2.

Received October, 27, 2016, published April, 28, 2017.

However, this does not resolve the problem since $o_1(Sp_{2n}(2))$ and $o_2(Sp_{2n}(2))$ quite rarely coincide with $o_1(\Omega^+_{2n}(2))$ and $o_1(\Omega^-_{2n}(2))$.

The main difficulty with determining the largest orders of elements in $\mathrm{Aut}(\Omega^+_8(q))$ are triality automorphisms, since there are no method to calculate, or at least to satisfactorily bound, the orders of elements in extensions by these automorphisms.

2. Preliminaries

In this section we collect all necessary information about $\Omega^\pm_{2n}(2^m)$. Our number-theoretic notation is mostly standard. In particular, we write $[n_1,\dots,n_s]$ and $(n_1,\dots,n_s)$ for the least common multiple and greatest common divisor of integers $n_1,\dots,n_s$. Also we denote the highest power of 2 dividing a positive integer n by $(n)_2$ and define $(n)_{2'}$ to be $n/(n)_2$.

We write $\omega(G)$ for the set of orders of elements of a group G and $\omega_{2'}(G)$ for the set of odd orders. For $\varepsilon\in\{+,-\}$, we replace $\varepsilon 1$ by ε in arithmetic expressions. In Lemma 1 and Formula (2.1) below, $\pm$ in $[q^{n_1}\pm 1,\dots,q^{n_s}\pm 1]$ means that we can choose $+$ or $-$ for every entry independently.

Lemma 1 ([6, Corollary 4]). *The set $\omega(\Omega^\varepsilon_{2n}(q))$, where q is a power of 2 and $n\geqslant 4$, consists of all divisors of the following numbers:*

(i) $[q^{n_1}-\tau_1,\dots,q^{n_s}-\tau_s]$, *where $s\geqslant 1$, $n_i>0$ and $\tau_i\in\{+,-\}$ for $1\leqslant i\leqslant s$, $n_1+\dots+n_s=n$, and $\tau_1\dots\tau_s=\varepsilon$;*

(ii) $2[q^{n_1}\pm 1,\dots,q^{n_s}\pm 1]$, *where $s\geqslant 1$, $n_i>0$ for $1\leqslant i\leqslant s$, and $2+n_1+\dots+n_s=n$;*

(iii) $2^k[q^{n_1}\pm 1,\dots,q^{n_s}\pm 1]$, *where $k\geqslant 2$, $s\geqslant 1$, $n_i>0$ for $1\leqslant i\leqslant s$, and $2^{k-2}+2+n_1+\dots+n_s=n$;*

(iv) $2[q\pm 1,q^{n_1}-\tau_1,\dots,q^{n_s}-\tau_s]$, *where $s\geqslant 1$, $n_i>0$ and $\tau_i\in\{+,-\}$ for $1\leqslant i\leqslant s$, $2+n_1+\dots+n_s=n$, and $\tau_1\dots\tau_s=\varepsilon$;*

(v) $4[q-\tau,q^{n_1}-\tau_1,\dots,q^{n_s}-\tau_s]$, *where $s\geqslant 1$, $\tau\in\{+,-\}$, $n_i>0$ and $\tau_i\in\{+,-\}$ for $1\leqslant i\leqslant s$, $3+n_1+\dots+n_s=n$, and $\tau\tau_1\dots\tau_s=\varepsilon$;*

(vi) 2^k *if $n=2^{k-2}+2$ for $k\geqslant 3$.*

By Lemma 1, the set $\omega_{2'}(\Omega^\varepsilon_{2n}(q))$ consists of all numbers of the form

$$[q^{n_1}-\tau_1,\dots,q^{n_s}-\tau_s],$$

where $n_1+\dots+n_s=n$ and $\tau_1\dots\tau_s=\varepsilon$. In particular, it is a subset of the set $M(n,q)$ of all numbers of the form

$$[q^{n_1}\pm 1,\dots,q^{n_s}\pm 1], \tag{2.1}$$

where $n_1+\dots+n_s=n$. Denote the maximum element of $M(n,q)$ by $m_1(n,q)$.

Lemma 2. *Let q be a power of 2. If $n\geqslant 2$, then*

$$m_1(n,q)\leqslant o_1(Sp_{2n}(q))\leqslant q^{n+1}/(q-1).$$

If $n\geqslant 5$, $a\in\omega(Sp_{2n}(q))$ and a is even, then $a\leqslant 2m_1(n,q)/3$.

Proof. The first assertion is proved in [2, Lemma 1.3] or [3, Lemma 2.9]. The second one is established in the beginning of the proof of [4, Proposition 4]. □

The next formulas are well-known.

Lemma 3. *Let q be an even integer. Then*

(i) $(q^n-1,q^m-1)=q^{(n,m)}-1$;

(ii) $(q^n-1,q^m+1)=\begin{cases}1 & \text{if } (n)_2\leqslant(m)_2\\ q^{(n,m)}+1, & \text{if } (n)_2>(m)_2\end{cases};$

(iii) $(q^n+1,q^m+1)=\begin{cases}1 & \text{if } (n)_2\neq(m)_2\\ q^{(n,m)}+1, & \text{if } (n)_2=(m)_2\end{cases}.$

To work with automorphisms of $\Omega^{\pm}_{2n}(2^m)$, it is convenient to regard these groups as the fixed point sets of Frobenius endomorphisms. In the choice of Frobenius endomorphisms, we follow [7, pp. 70–71]. Let $\overline{V}$ be a $2n$-dimensional vector space over the algebraic closure of the binary field and let $\overline{K}=\Omega(\overline{V},f)$ be the connected component of $O(\overline{V},f)$, where f is the quadratic form $x_1x_{-1}+\dots+x_nx_{-n}$ and x_i are coordinates with respect to a basis of $\overline{V}$ consisting of vectors $v_n,\dots,v_1,v_{-1},\dots,v_{-n}$. Let γ be the involution of $O(\overline{V},f)$ that interchanges v_n and v_{-n} and fixes all other basis vectors, and let φ be the endomorphism of $O(\overline{V},f)$ induced by raising coordinates to the second power. Then γ and φ permute, and for $q=2^m$, we have $\Omega^+_{2n}(q)\simeq S^+(q)=C_{\overline{K}}(\varphi^m)$ and $\Omega^-_{2n}(q)\simeq S^-(q)=C_{\overline{K}}(\varphi^m\gamma)$.

We denote the automorphisms of $S^+(q)$ and $S^-(q)$ induced by γ and φ by the same letters. These automorphisms generate the group of order $2m$, which has the form $\langle\gamma\rangle\times\langle\varphi\rangle$ for $S^+(q)$ and $\langle\varphi\rangle$ for $S^-(q)$. In the latter case $\varphi^m=\gamma$ and every subgroup of $\langle\varphi\rangle$ is generated by either $\varphi^{m/k}$ for some k or $\varphi^{m/k}\gamma$ for some odd k.

Lemma 4. *Let $n\geqslant4$, k divides m, $q=2^m=q_0^k$ and $\beta=\varphi^{m/k}$. Then*
(i) $\omega(S^+(q)\beta)=k\cdot\omega(S^+(q_0))$;
(ii) $\omega(S^+(q)\beta\gamma)=k\cdot\omega(S^-(q_0))$ *if k is even;*
(iii) $\omega(S^+(q)\beta\gamma)=k\cdot\omega(S^+(q_0)\gamma)$ *if k is odd;*
(iv) $\omega(S^-(q)\beta)=k\cdot\omega(S^+(q_0)\gamma)$;
(v) $\omega(S^-(q)\beta\gamma)=k\cdot\omega(S^-(q_0))$ *if k is odd.*

Proof. It is similar to the proof of [8, Lemma 3.3]. □

3. Two largest orders of elements

Throughout this section q is a power of 2, $q>2$ and $S=\Omega^{\varepsilon}_{2n}(q)$. Since $q>2$, we may expect that $o_1(S)$ and $o_2(S)$ are odd and, in particular, are contained in $M(n,q)$. Moreover, if n is sufficiently large, we may expect that they are contained in its subset $M^c(n,q)$ consisting of all numbers of the form (2.1) with pairwise coprime entries $q^{n_i}\pm1$.

Since $q^{2l}-1=[q^l-1,q^l+1]$, the representation of $a\in M(n,q)$ in the form $[q^{n_1}\pm1,\dots,q^{n_s}\pm1]$ is ambiguous. For definiteness, we assume that in each entry $q^{n_i}-1$ the exponent n_i is odd. With this assumption, Lemma 3 implies that every element of $M^c(n,q)$ can be written as

$$(q^{n_1}+1)\dots(q^{n_s}+1),\ \text{where } n_1+\dots+n_s=n, \tag{3.1}$$

or

$$(q^{n_1}+1)\dots(q^{n_s}+1)(q^l-1),\ \text{where } l \text{ is odd and } l+n_1+\dots+n_s=n, \tag{3.2}$$

and in both cases $(n_1)_2<(n_2)_2<\dots<(n_s)_2$.

The expressions $(q^{n_1}+1)\dots(q^{n_s}+1)$ and $(q^{n_1}+1)\dots(q^{n_s}+1)(q^l-1)$ in (3.1) and (3.2) can be viewed as polynomials of degree n in q. The condition

$$(n_1)_2<(n_2)_2<\dots<(n_s)_2$$

implies that a sum of some of n_i determines its summands uniquely, and hence the coefficients of the first polynomial lie in $\{0,1\}$. Thus the coefficients of both polynomials lie in $\{1,0,-1\}$. By assumption $q\geqslant 4$, so

$$q^m-q^{m-1}-\dots-1>q^{m-1}+\dots+1.$$

It follows that the ordinary order on numbers of $M^c(n,q)$ is defined by the lexicographic order on n-tuples of their coefficients when they are regarded as polynomials in q. In particular, this order does not depend on q and each number $a\in M^c(n,q)$ is represented by a unique polynomial, which we denote by $a(q)$. These observations allows us to determine largest elements of $M^c(n,q)$, where n is small, by computer calculations: it suffices to calculate elements of $M^c(n,4)$. We will refer to this technique as "computation with $q=4$".

Let $a\in M^c(n,q)$. If the first t coefficients (beginning with the leading one) of $a(q)$ are equal to 1, while the $(t+1)$th coefficient is not, then we say that a has height t and write $h(a)=t$. For example, $h((q^n-1)(q+1))=2$ for $n>2$. Clearly, $h(a_1)>h(a_2)$ yields $a_1>a_2$. Also define $l(a)=0$ if a is as in (3.1) and $l(a)=l$ if a is as in (3.2). By Lemma 1, it follows that $a\in\omega(\Omega^\varepsilon_{2n}(q))$ if and only if $\varepsilon=(-1)^s$ or $n_1=l(a)$. Furthermore, in the latter case a lies in both $\omega(\Omega^+_{2n}(q))$ and $\omega(\Omega^-_{2n}(q))$. We set $sgn(a)=(-1)^s$ if $n_1\neq l(a)$ and $sgn(a)=\circ$ otherwise.

The next lemma shows that for sufficiently large n, the numbers $o_1(S)$ and $o_2(S)$ are contained in the set $\widetilde{M}(n,q)$ consisting of $a\in M^c(n,q)$ with odd $n-l(a)$. Denote the ith largest elements of $\widetilde{M}(n,q)$ and $\widetilde{M}(n,q)\cap\omega(S)$ by $\widetilde{m}_i(n,q)$ and $\widetilde{m}^\varepsilon_i(n,q)$ respectively.

Lemma 5. *Let $n\geqslant 5$ and $a\in\omega(S)$. If a divides an element of $M(n,q)\setminus M^c(n,q)$ or is even, then $a<q^n$. If $n>5$ and $a\in M^c(n,q)\setminus\widetilde{M}(n,q)$, then $a<b$, where $b=(q^{n-1}-1)(q+1)$ for even n and $b=(q^3+1)(q^2+1)(q^{n-5}+1)$ for odd n.*

Proof. Let a be even. Since $S<Sp_{2n}(q)$, it follows from Lemma 2 and the assumption $q\geqslant 4$ that

$$a\leqslant\frac{2m_1(n,q)}{3}\leqslant\frac{2q^{n+1}}{3(q-1)}<q^n.$$

Let a divides $[q^{n_1}-\tau_1,q^{n_2}-\tau_2,\dots]$, where $(q^{n_1}-\tau_1,q^{n_2}-\tau_2)>1$, and set $x=[q^{n_1}-\tau_1,q^{n_2}-\tau_2]$. If $\tau_1=\tau_2=1$, then

$$x\leqslant\frac{(q^{n_1}-1)(q^{n_2}-1)}{q-1}<\frac{q^{n_1+n_2}}{q-1}.$$

If at least one of τ_1, τ_2 is equal to $-$, then

$$x\leqslant\frac{(q^{n_1}+1)}{q+1}\cdot\frac{(q^{n_2}+1)}{q+1}\cdot(q+1)\leqslant q^{n_1+n_2-2}(q+1)<\frac{q^{n_1+n_2}}{q-1}.$$

Thus

$$a\leqslant x\cdot m_1(n-n_1-n_2,q)\leqslant\frac{q^{n_1+n_2}}{q-1}\cdot\frac{q^{n-n_1-n_2+1}}{q-1}=\frac{q}{(q-1)^2}\cdot q^n<q^n.$$

Let $a\in M^c(n,q)\setminus\widetilde{M}(n,q)$ and let a be defined by $l(a)$, n_1, ..., n_s according to (3.1) or (3.2). Since $n-l(a)$ is even, all n_i are even too, and so

$$(q^{n_1}+1)\dots(q^{n_s}+1)\leqslant m_1((n-l(a))/2,q^2)\leqslant q^{n-l(a)}+q^{n-l(a)-2}+\dots+1.$$

If n is even, then $l(a) = 0$ and we have

$$a \leqslant q^n + q^{n-2} + \cdots + 1 < q^n + q^{n-1} - q - 1 = b.$$

If n is odd, then

$$a < (q^{n-l(a)} + q^{n-l(a)-2} + \cdots + 1)q^{l(a)} < q^n + q^{n-2} + q^{n-3} < b.$$

The proof is complete. □

We proceed with determining $\widetilde{m}_1^\varepsilon(n, q)$ and $\widetilde{m}_2^\varepsilon(n, q)$. The result substantially depends on parity of n, and we begin with the case of even n.

Let n be even. Then $\widetilde{M}(n, q)$ consists of the numbers of the form

$$(q^{n_1} + 1) \cdots + (q^{n_s} + 1)(q^l - 1),$$

where $1 = (n_1)_2 < \cdots < (n_s)_2$ and l is odd.

Denote by C_m the set of those element of $\widetilde{M}(n, q)$ for which $n_1 = 1$, $n_2 = 2$, …, $n_m = 2^{m-1}$ and $n_{m+1} \neq 2^m$. Let $a \in C_m$. All numbers n_{m+1}, …, n_s are divisible by 2^m and not equal to 2^m, therefore, we can write them as $n'_1 2^m$, … $n'_{s'} 2^m$ for some $n'_i \neq 1$. Define $c = c(a) = n'_1 + \cdots + n'_{s'}$. Then $n_1 + \cdots + n_s = 2^m - 1 + c \cdot 2^m$, and hence

$$(c + 1)2^m \leqslant n. \tag{3.3}$$

Since $(n'_i)_2$ are pairwise distinct, it follows that

$$s' = 1 \text{ for } c \leqslant 4. \tag{3.4}$$

This shows that for every $c \leqslant 4$, there is at most one a with such c and we denote this a by $a_{m,c}$. Similarly,

$$\text{if } c = 5, 6, \text{ then either } s' = 1, \text{ or } s' = 2, \{n'_1, n'_2\} = \{2, c - 2\}, \tag{3.5}$$

and we denote the corresponding a by $a_{m,c}$ and $a_{m,c,c-2}$ respectively.

Next we show that

$$h(a) = \min(2^m, n - (c + 1)2^m + 1),$$

or equivalently,

$$h(a) = \begin{cases} 2^m & \text{if } n \geqslant (c + 2)2^m \\ n - (c + 1)2^m + 1 & \text{if } n < (c + 2)2^m \end{cases}. \tag{3.6}$$

Since

$$a = (q + 1) \ldots (q^{2^{m-1}} + 1)(q^{c \cdot 2^m} + \cdots + 1)(q^{n-(c+1)2^m+1} - 1)$$

and

$$(q + 1) \ldots (q^{2^{m-1}} + 1) = q^{2^m - 1} + q^{2^m - 2} + \cdots + 1,$$

the polynomial $a(q)$ is the difference of two polynomial with non-negative coefficients of degrees n and $(c+1)2^m - 1$. The first 2^m coefficients of the first polynomial is equal to 1, that is, the last of them is in term with q^{n-2^m+1}. Thus $h(a) = 2^m$ if $n - 2^m + 1 > (c + 1)2^m - 1$ and $h(a) = n - (c + 1)2^m + 1$ otherwise. It remains to note that $n + 2 > (c + 2)2^m$ is equivalent to $n \geqslant (c + 2)2^m$.

TABLE 1. The numbers $\widetilde{m}_i(n,q)$, $1 \leqslant i \leqslant 4$, for even $n \geqslant 10$

	$\widetilde{m}_1(n,q)$, sgn	$\widetilde{m}_2(n,q)$, sgn	$\widetilde{m}_3(n,q)$, sgn	$\widetilde{m}_4(n,q)$, sgn
$5 \leqslant n/2^k < 6$	$f_{k+1}(n,q)$, $-\tau$	$f_{k+2}(n,q)$, τ	$g_k(n,q)$, $-\tau$	$f_k(n,q)$, τ
$6 \leqslant n/2^k < 7$	$f_{k+2}(n,q)$, τ	$f_{k+1}(n,q)$, $-\tau$	$g_k(n,q)$, $-\tau$	$f_k(n,q)$, τ
$7 \leqslant n/2^k < 9$	$f_{k+2}(n,q)$, τ	$f_{k+1}(n,q)$, $-\tau$	$g_{k+1}(n,q)$, τ	$g_k(n,q)$, $-\tau$
$9 \leqslant n/2^k < 10$	$f_{k+2}(n,q)$, τ	$f_{k+1}(n,q)$, $-\tau$	$g_{k+1}(n,q)$, τ	$f_{k+3}(n,q)$, $-\tau$

Lemma 6. *Let n be even and $n \geqslant 10$. Suppose that we choose $k \geqslant 1$ so that $5 \cdot 2^k \leqslant n < 5 \cdot 2^{k+1}$, put $\tau = (-1)^k$ and define*

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

$$g_m(n,q) = (q+1)(q^2+1)\dots(q^{2^{m-1}}+1)(q^{2^{m+1}}+1)(q^{n-3\cdot 2^m+1}-1)$$

for every $m \geqslant 1$. Then $\widetilde{m}_i(n,q)$ and $sgn(\widetilde{m}_i(n,q))$ for $1 \leqslant i \leqslant 4$ are as in Table 1. In particular, $\{\widetilde{m}_i(n,q) \mid 1 \leqslant i \leqslant 4\} = \{\widetilde{m}_1^+(n,q), \widetilde{m}_2^+(n,q), \widetilde{m}_1^-(n,q), \widetilde{m}_2^-(n,q)\}$ and $\widetilde{m}_4(n,q) \geqslant (q+1)(q^{n-1}-1)$.

Proof. Since $n < 10 \cdot 2^k$, it follows from (3.3) that $C_m = \varnothing$ for all $m > k+3$. Using the properties of C_m established above, one can easily verify Table 2, in which we describe C_{k+1}, C_{k+2} and C_{k+3} depending on the integer part of $n/2^k$. The column "C_m" gives all elements of C_m in decreasing order together with their signs. Observe that $f_m = f_m(n,q)$ and $g_m = g_m(n,q)$ defined in the statement of the lemma are precisely the unique elements of C_m with $c = 0$ and $c = 2$ respectively (see (3.4)). By h_m we denote the unique element of C_m with $c = 3$.

Consider the set $\mathcal{C} = C_{k+1} \cup C_{k+2} \cup C_{k+3}$.

TABLE 2

$n/2^k$	C_{k+1}	C_{k+2}	C_{k+3}
$[5,6)$	f_{k+1} $h(f_{k+1}) = 2^{k+1}$	f_{k+2} $h(f_{k+2}) = n - 2^{k+2} + 1$ $2^{k+1} > h(f_{k+2}) > 2^k$	$\varnothing$
$[6,7)$	$f_{k+1} > g_{k+1}$ $h(f_{k+1}) = 2^{k+1}$ $h(g_{k+1}) = n - 3 \cdot 2^{k+1} + 1 < 2^k$	f_{k+2} $h(f_{k+2}) = n - 2^{k+2} + 1 > 2^{k+1}$	$\varnothing$
$[7,8)$	$f_{k+1} > g_{k+1}$ $h(f_{k+1}) = 2^{k+1}$ $h(g_{k+1}) = n - 3 \cdot 2^{k+1} + 1 > 2^k$	f_{k+2} $h(f_{k+2}) = n - 2^{k+2} + 1 > 2^{k+1}$	$\varnothing$
$[8,9)$	$f_{k+1} > g_{k+1} > h_{k+1}$ $h(f_{k+1}) = h(g_{k+1}) = 2^{k+1}$ $h(h_{k+1}) = n - 2^{k+3} + 1 < 2^k$	f_{k+2} $h(f_{k+2}) = 2^{k+2}$	f_{k+3} $h = h(h_{k+1})$
$[9,10)$	$f_{k+1} > g_{k+1} > h_{k+1}$ $h(f_{k+1}) = h(g_{k+1}) = 2^{k+1}$ $h(h_{k+1}) = n - 2^{k+3} + 1 > 2^k$	f_{k+2} $h(f_{k+2}) = 2^{k+2}$	f_{k+3} $h = h(h_{k+1})$

Let $9 \cdot 2^k \leqslant n < 10 \cdot 2^k$. Then $\mathcal{C}$ consists of five elements, all of them having height larger than 2^k, and hence $\mathcal{C}$ contains the desired elements. The least height of an element of $\mathcal{C}$ is that of h_{k+1} and f_{k+3}, so it remains to compare these numbers. Since

$$\frac{f_{k+3}}{h_{k+1}} = \frac{(q^{2^{k+1}}+1)(q^{2^{k+2}}+1)}{q^{3\cdot 2^{k+1}}+1} > 1,$$

we see that $f_{k+2} > f_{k+1} > g_{k+1} > f_{k+3}$ are the four largest elements, as claimed. Note that $l(\widetilde{m}_i(n,q)) \geqslant l(f_{k+3}) = n - 8\cdot 2^k + 1 > 1$, and hence $sgn(m_i(n,q)) \neq \circ$.

Suppose that $n < 9\cdot 2^k$. If $5\cdot 2^k \leqslant n < 7\cdot 2^k$ (or $7\cdot 2^k \leqslant n < 9\cdot 2^k$), then $\mathcal{C}$ contains only two (or three) elements whose height is larger than 2^k, therefore, we need the two (or one) largest elements of C_k. We claim that these are g_k and f_k (or g_k). Since $h(f_k) = h(g_k) = 2^k$, it suffices to compare g_k and f_k with other elements of height 2^k. Let $a \in C_k$, $c = c(a) > 2$ and $h(a) = 2^k$. By (3.6), we have that $(c+2)2^k \leqslant n$ and, in particular, $c \leqslant 6$. By (3.4) and (3.5), we need to consider the elements $h_k = a_{k,3}$ (for all n), $a_{k,4}$ (for $n \geqslant 6\cdot 2^k$), $a_{k,5}$ and $a_{k,2,3}$ (for $n \geqslant 7\cdot 2^k$), $a_{k,6}$ and $a_{k,2,4}$ (for $n \geqslant 8\cdot 2^k$). The inequality $q^c+1 < (q^2+1)(q^{c-2}+1)$ yields $a_{k,c} < a_{k,2,c-2}$ and so eliminates $a_{k,5}$ and $a_{k,6}$. Define $l = n - 2^k + 1$ and $d_k = (q+1)(q^2+1)\dots(q^{2^{k-1}}+1)$. Then

$$\begin{aligned}
f_k &= d_k(q^l - 1),\\
g_k &= d_k(q^{2\cdot 2^k}+1)(q^{l-2\cdot 2^k}-1),\\
h_k &= d_k(q^{3\cdot 2^k}+1)(q^{l-3\cdot 2^k}-1),\\
a_{k,4} &= d_k(q^{4\cdot 2^k}+1)(q^{l-4\cdot 2^k}-1),\\
a_{k,2,3} &= d_k(q^{2\cdot 2^k}+1)(q^{3\cdot 2^k}+1)(q^{l-5\cdot 2^k}-1),\\
a_{k,2,4} &= d_k(q^{2\cdot 2^k}+1)(q^{4\cdot 2^k}+1)(q^{l-6\cdot 2^k}-1).
\end{aligned}$$

Since $(q^a+1)(q^{l-a}-1)$ decreases with respect to a, we see that $g_k > h_k > a_{k,4}$ and $a_{k,2,3} > a_{k,2,4}$. Also $4\cdot 2^k < l < 8\cdot 2^k$, and hence $l - 2\cdot 2^k > 2\cdot 2^k$ and $l - 5\cdot 2^k < 3\cdot 2^k$, which yields $g_k > f_k$ and $g_k > a_{k,2,3}$. Thus g_k is the largest element of C_k for all n with $5\cdot 2^k \leqslant n < 9\cdot 2^k$. Now let $5 \leqslant n/2^k < 7$, or equivalently, $4\cdot 2^k < l < 6\cdot 2^k$. Then $l - 3\cdot 2^k < 3\cdot 2^k$ and $l - 5\cdot 2^k < 2\cdot 2^k$, so $f_k > h_k > a_{k,2,3}$, and hence f_k is the second largest element of C_k.

Thus if $5\cdot 2^k \leqslant n < 6\cdot 2^k$, then the desired elements are $f_{k+1} > f_{k+2} > g_k > f_k$. Similarly, for $6\cdot 2^k \leqslant n < 7\cdot 2^k$ or $7\cdot 2^k \leqslant n < 9\cdot 2^k$, they are $f_{k+2} > f_{k+1} > g_k > f_k$ or $f_{k+2} > f_{k+1} > g_{k+1} > g_k$ respectively. It is easy to see that $q-1$ divides none of these elements, and so their signs are not $\circ$.

In all cases, we have either $h(\widetilde{m}_4(n,q)) = 2^k$, in which case $\widetilde{m}_4(n,q) \geqslant f_k$, or $h(\widetilde{m}_4(n,q)) > 2^k$. Since $h((q+1)(q^{n-1}-1)) = 2$ and $(q+1)(q^{n-1}-1) = f_1(n,q)$, the last inequality of the lemma also follows. □

Now let n be odd. Then $\widetilde{M}(n,q)$ consists of the numbers of the form

$$(q^{n_1}+1)\cdots+(q^{n_s}+1),$$

where $1 = (n_1)_2 < \cdots < (n_s)_2$. Put $t_n = |\widetilde{M}(n,q)|$ and denote by $\widetilde{M}_l(n,q)$ the set of those elements of $\widetilde{M}(n,q)$ for which $n_1 = l$. Note that the smallest element of $\widetilde{M}_l(n,q)$ is $(q^l+1)(q^{n-l}+1)$. It is clear that

$$\widetilde{M}_l(n,q) = (q^l+1)\widetilde{M}((n-l)_{2'}, q^{(n-l)_2}), \tag{3.7}$$

and hence $\widetilde{M}_l(n,q)$ contains $t_{(n-l)_{2'}}$ numbers.

Lemma 7. *Let $n \geqslant 3$ be odd and $n' = (n-1)_{2'}$. Then*

$$\widetilde{m}_i(n,q) = (q+1)\cdot \widetilde{m}_i\left(n', q^{(n-1)_2}\right) \text{ for } i = 1,\dots,t_{n'}.$$

If in addition $n \geqslant 9$ and $(n-3)_2 = 2$, then

$$\widetilde{m}_{t_{n'}+i}(n,q) = (q^3+1)(q^2+1)\cdot \widetilde{m}_i\left((n-5)_{2'}, q^{(n-5)_2}\right) \text{ for } i = 1,\dots,t_{(n-5)_{2'}}.$$

Proof. If $a \in \widetilde{M}_1(n,q)$, then $h(a) \geqslant 2$, while for $a \in \widetilde{M}_l(n,q)$ with $l \geqslant 3$, we have $h(a) = 1$. Thus $\widetilde{M}_1(n,q) > \widetilde{M}_l(n,q)$ for all $l \geqslant 3$, and so the first assertion follows from (3.7).

Let $n \geqslant 9$ and $(n-3)_2 = 2$. Then $(n-3)_{2'} = (n-3)/2 \geqslant 3$. Since

$$\widetilde{M}_3(n,q) = (q^3+1)\widetilde{M}((n-3)/2, q^2)$$

and $((n-3)/2-1)_{2'} = (n-5)_{2'}$, it follows from the first part that the $t_{(n-5)_{2'}}$ largest numbers of $\widetilde{M}_3(n,q)$ are exactly the elements of $(q^3+1)(q^2+1)\widetilde{M}((n-5)_{2'}, q^{(n-5)_2})$. It remains to check that $a < (q^3+1)(q^2+1)(q^{n-5}+1)$ for any $a \in M_l(n,q)$ with $l \geqslant 5$. Indeed, we have

$$a \leqslant \frac{(q^l+1)(q^{n-l+2}-1)}{q^2-1} \leqslant \frac{(q^5+1)(q^{n-3}-1)}{q^2-1} < (q^3+1)(q^2+1)(q^{n-5}+1),$$

where the strong inequality follows by comparing coefficients in term with q^{n-3}. □

By Lemma 5, if the number $\widetilde{m}_i^{-\varepsilon}((n-1)_{2'}, q)$ exists, then

$$\widetilde{m}_i^{\varepsilon}(n,q) = (q+1)\widetilde{m}_i^{-\varepsilon}((n-1)_{2'}, q^2). \tag{3.8}$$

So, if $(n-1)_{2'}$ is not very small, then all the numbers $m_1^{\pm}(n,q)$ and $m_2^{\pm}(n,q)$ are contained in $(q+1)\widetilde{M}((n-1)_{2'}, q^2)$ and, therefore, can be found by induction. The basis of induction is provided by the next lemma.

Lemma 8. *Let n be odd and suppose that $(n-1)_{2'} \leqslant 5$. Then $\widetilde{m}_i^{\pm}(n,q)$ for $i = 1,2$ are as in Tables 3–6.*

Proof. For $n \leqslant 13$ and $n = 17, 21$, the desired numbers are found by computation with $q = 4$ and given in Table 3. Assume from now that $n \geqslant 15$ and $n \neq 17, 21$. The condition $(n-1)_{2'} \leqslant 5$ is equivalent to the fact that n is of the form 2^t+1, or $3\cdot 2^t+1$, or $5\cdot 2^t+1$.

Let $n = 2^t+1$. Since $n \neq 9, 17$, it follows that $t \geqslant 5$, and in particular $(n-3)_2 = 2$. By (3.8), we have

$$\widetilde{m}_1(n,q) = (q+1)\widetilde{m}_1(1, q^{2^t}) = (q+1)(q^{2^t}+1) = \widetilde{m}_1^{+}(n,q),$$

and this is the only element of $\widetilde{M}_1(n,q)$. Lemma 7 implies that the next largest elements are contained in

$$(q^3+1)(q^2+1)\widetilde{M}((n-5)_{2'}, q^4). \tag{3.9}$$

Furthermore, since $(n-5)_{2'} \geqslant 7$, all the numbers $\widetilde{m}_1^{\pm}((n-5)_{2'}, q^4)$, $\widetilde{m}_2^{\pm}((n-5)_{2'}, q^4)$ exist, and we can choose three of them with necessary number of factors. to obtain $\widetilde{m}_1^{-}(n,q)$ and $\widetilde{m}_2^{\pm}(n,q)$. Using the expansion

$$(n-5)_{2'} = 2^{t-2}-1 = 7\cdot 2^{t-5} + 2^{t-6} + \dots + 1$$

and repeatedly applying Lemma 7, we result in

$$\widetilde{m}_i((n-5)_{2'}, q^4) = (q^4+1)\dots(q^{2^{t-4}}+1)\widetilde{m}_i(7, q^{2^{t-3}}). \tag{3.10}$$

TABLE 3. The numbers $\widetilde{m}_1^{\pm}(n,q)$ and $\widetilde{m}_2^{\pm}(n,q)$ for small odd n

n	$\widetilde{m}_1^{+}(n,q)$	$\widetilde{m}_2^{+}(n,q)$
1	–	–
3	$(q+1)(q^2+1)$	–
5	$(q+1)(q^4+1)$	$(q^3+1)(q^2+1)$
7	$(q+1)(q^6+1)$	$(q^5+1)(q^2+1)$
9	$(q+1)(q^8+1)$	$(q^7+1)(q^2+1)$
11	$(q+1)(q^{10}+1)$	$(q^9+1)(q^2+1)$
13	$(q+1)(q^{12}+1)$	$(q^{11}+1)(q^2+1)$
17	$(q+1)(q^{16}+1)$	$(q^3+1)(q^2+1)(q^4+1)(q^8+1)$
21	$(q+1)(q^{20}+1)$	$(q^7+1)(q^2+1)(q^4+1)(q^8+1)$
n	$\widetilde{m}_1^{-}(n,q)$	$\widetilde{m}_2^{-}(n,q)$
1	$q+1$	–
3	q^3+1	–
5	q^5+1	–
7	$(q+1)(q^2+1)(q^4+1)$	q^7+1
9	$(q^3+1)(q^2+1)(q^4+1)$	q^9+1
11	$(q+1)(q^2+1)(q^8+1)$	$(q+1)(q^4+1)(q^6+1)$
13	$(q+1)(q^4+1)(q^8+1)$	$(q^3+1)(q^2+1)(q^8+1)$
17	$(q^3+1)(q^2+1)(q^{12}+1)$	$(q^{11}+1)(q^2+1)(q^4+1)$
21	$(q+1)(q^4+1)(q^{16}+1)$	$(q+1)(q^8+1)(q^{12}+1)$

Table 3 says that $\widetilde{m}_1^{+}(7,q)=(q+1)(q^6+1)$ and $\widetilde{m}_1^{-}(7,q)=(q+1)(q^2+1)(q^4+1)$. Combining this with (3.9) and (3.10), we conclude that the set $\{\widetilde{m}_2^{+}(n,q),\widetilde{m}_1^{-}(n,q)\}$ consists of

$$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{3\cdot 2^{t-2}}+1),$$
$$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{2^{t-2}}+1)(q^{2^{t-1}}+1).$$

Similarly, $\widetilde{m}_2^{-}(n,q)$ is equal to

$$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{7\cdot 2^{t-3}}+1)$$

or

$$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{5\cdot 2^{t-3}}+1)(q^{2^{t-2}}+1)$$

depending on the parity of t.

Let $n=3\cdot 2^t+1$, where $t\geqslant 3$. By (3.8), we have

$$\widetilde{m}_1^{\varepsilon}(n,q)=(q+1)\widetilde{m}_1^{-\varepsilon}(3,q^{2^{t-1}}), \tag{3.11}$$

and there are no other elements in $\widetilde{M}_1(n,q)$. Since $(n-5)_{2'}\geqslant 5$, both numbers $\widetilde{m}_1^{\pm}((n-5)_{2'},q)$ exist and by Lemma 7

$$\widetilde{m}_2^{\varepsilon}(n,q)=(q^3+1)(q^2+1)\widetilde{m}_1^{\varepsilon}((n-5)_{2'},q^4).$$

TABLE 4. The numbers $\widetilde{m}_1^{\pm}(n,q)$ and $\widetilde{m}_2^{\pm}(n,q)$ for $n=2^t+1$, $t\geqslant 5$

	$\widetilde{m}_1^{+}(n,q)$
	$(q+1)(q^{2^t}+1)$
	$\widetilde{m}_2^{+}(n,q), \widetilde{m}_1^{-}(n,q), \widetilde{m}_2^{-}(n,q)$
t odd	$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{3\cdot 2^{t-2}}+1)$, $(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{2^{t-2}}+1)(q^{2^{t-1}}+1)$, $(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{7\cdot 2^{t-3}}+1)$
t even	$(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{2^{t-2}}+1)(q^{2^{t-1}}+1)$, $(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{2^{t-3}}+1)(q^{3\cdot 2^{t-2}}+1)$, $(q^3+1)(q^2+1)\dots(q^{2^{t-4}}+1)(q^{5\cdot 2^{t-3}}+1)(q^{2^{t-2}}+1)$

TABLE 5. The numbers $\widetilde{m}_1^{\pm}(n,q)$ and $\widetilde{m}_2^{\pm}(n,q)$ for $n=3\cdot 2^t+1$, $t\geqslant 3$

$\widetilde{m}_1^{+}(n,q), \widetilde{m}_1^{-}(n,q)$
$(q+1)(q^{3\cdot 2^t}+1)$, $(q+1)(q^{2^t}+1)(q^{2^{t+1}}+1)$
$\widetilde{m}_2^{\tau}(n,q), \widetilde{m}_2^{-\tau}(n,q)$, where $\tau=(-1)^{t-1}$
$(q^3+1)(q^2+1)\dots(q^{2^{t-2}}+1)(q^{2^{t-1}}+1)(q^{2^{t+1}}+1)$ $(q^3+1)(q^2+1)\dots(q^{2^{t-2}}+1)(q^{5\cdot 2^{t-1}}+1)$

TABLE 6. The numbers $\widetilde{m}_1^{\pm}(n,q)$ and $\widetilde{m}_2^{\pm}(n,q)$ for $n=5\cdot 2^t+1$, $t\geqslant 3$

	$\widetilde{m}_1^{+}(n,q), \widetilde{m}_1^{-}(n,q), \widetilde{m}_2^{-}(n,q)$
	$(q+1)(q^{5\cdot 2^t+1}+1)$, $(q+1)(q^{2^t}+1)(q^{2^{t+2}}+1)$, $(q+1)(q^{3\cdot 2^t}+1)(q^{2^{t+1}}+1)$
	$\widetilde{m}_2^{+}(n,q)$
t odd	$(q^3+1)(q^2+1)\dots(q^{2^{t-2}}+1)(q^{2^{t-1}}+1)(q^{2^{t+2}}+1)$
t even	$(q^3+1)(q^2+1)\dots(q^{2^{t-2}}+1)(q^{3\cdot 2^{t-1}}+1)(q^{2^t}+1)(q^{2^{t+1}+1}+1)$

Since $(n-5)_{2'}=3\cdot 2^{t-2}-1=5\cdot 2^{t-3}+2^{t-4}+\dots+1$, it follows that

$$\widetilde{m}_1^{\varepsilon}((n-5)_{2'},q^4)=(q^4+1)\dots(q^{2^{t-2}}+1)\widetilde{m}_1^{(-1)^{t-1}\varepsilon}(5,q^{2^{t-1}}). \tag{3.12}$$

It remains to take the values of $\widetilde{m}_1^{\pm}(3,q^{2^{t-1}})$ and $\widetilde{m}_1^{\pm}(5,q^{2^{t-1}})$ from Table 3 and substitute them into (3.11) and (3.12).

Similarly, if $n=5\cdot 2^t+1$, where $t\geqslant 3$, then

$$\widetilde{m}_i(n,q)=(q+1)\widetilde{m}_i(5,q^{2^t})$$

for $i=1,2,3$ and thus we determine $\widetilde{m}_1^{\pm}(n,q)$ and $\widetilde{m}_2^{-}(n,q)$. Also

$$\widetilde{m}_2^{+}(n,q)=(q^2+1)(q^3+1)\widetilde{m}_1^{+}((n-5)_{2'},q^4).$$

Since $(n-5)_{2'} = 5 \cdot 2^{t-2} - 1 = 9 \cdot 2^{t-3} + 2^{t-4} + \cdots + 1$, it follows that

$$\widetilde{m}_1^+((n-5)_{2'}, q^4) = (q^4+1)\dots(q^{2^{t-2}}+1)\widetilde{m}_1^{(-1)^{t-1}}(9, q^{2^{t-1}}),$$

and substituting the relevant values form Table 3 completes the proof. □

Lemma 9. *Let $n \geqslant 7$ be odd, $n = n_1 + \cdots + n_s$ be a binary expansion of n with $n_s > \cdots > n_1 = 1$ and $\tau = (-1)^s$. Then $\widetilde{m}_i^\varepsilon(n,q)$, where $\varepsilon \in \{+,-\}$ and $i \in \{1,2\}$, is as follows.*

(i) *If $n_s = 2^t n_{s-1}$, where $t \geqslant 3$, then*

$$\widetilde{m}_i^\varepsilon(n,q) = (q^{n_1}+1)\dots(q^{n_{s-2}}+1)\widetilde{m}_i^{\varepsilon\tau}(2^t+1, q^{n_{s-1}}).$$

(ii) *If $n_s = 2n_{s-1}$ and $n_{s-1} = 2^t n_{s-2}$, then*

$$\widetilde{m}_i^\varepsilon(n,q) = (q^{n_1}+1)\dots(q^{n_{s-3}}+1)\widetilde{m}_i^{-\varepsilon\tau}(3 \cdot 2^t+1, q^{n_{s-2}}).$$

(iii) *If $n_s = 4n_{s-1}$ and $n_{s-1} = 2^t n_{s-2}$, then*

$$\widetilde{m}_i^\varepsilon(n,q) = (q^{n_1}+1)\dots(q^{n_{s-3}}+1)\widetilde{m}_i^{-\varepsilon\tau}(5 \cdot 2^t+1, q^{n_{s-2}}).$$

In particular, $\widetilde{m}_2^\pm(n,q) \geqslant (q^3+1)(q^2+1)(q^{n-5}+1)$ for $n > 21$.

Proof. Since $n \geqslant 7$, Lemma 8 implies that $\widetilde{m}_i^\pm(c \cdot 2^t + 1, q)$, with $c = 1, 3, 5$, exist. So the formulas for $\widetilde{m}_i^\varepsilon(n,q)$ follow from (3.8). If $n > 21$, then these formulas and Lemma 8 guarantee that both $\widetilde{m}_2^+(n,q)$ and $\widetilde{m}_2^-(q)$ are divisible by either $q+1$ or $(q^3+1)(q^2+1)$, and hence they are greater than or equal to $(q^3+1)(q^2+1)(q^{n-5}+1)$ (cf. the proof of Lemma 7). □

Now we are ready to determine $o_1(S)$ and $o_2(S)$.

Theorem 1. *Let $S = \Omega_{2n}^\varepsilon(q)$, where $n \geqslant 4$, $q = 2^m \geqslant 4$, $\varepsilon \in \{+,-\}$, and let $i = 1, 2$. If $n \leqslant 9$ or $(n, \varepsilon) = (11,+), (13,+)$, then $o_i(S)$ is as in Tables 7 and 8. Otherwise, $o_i(S) = \widetilde{m}_i^\varepsilon(n,q)$, and so its value is given in Lemmas 6, 8 and 9. In both cases, $o_i(\mathrm{Aut}\, S) = o_i(S)$ provided that $S \neq \Omega_8^+(q)$.*

Proof. Let $n = 4$. By Lemma 1, the set $\omega(S)$ consists of all divisors of the following numbers:

$$q^4-1, q^3 \pm 1, 2(q^2 \pm 1), 4(q \pm 1), 8 \text{ for } \varepsilon = +,$$

$$q^4 \pm 1, (q^3 \pm 1)(q \mp 1), 2(q^2+1)(q \pm 1), 4(q^2-1), 8 \text{ for } \varepsilon = -.$$

It is easily seen that two largest numbers in these lists are $q^4 - 1$, $q^3 + 1$ and $(q^3-1)(q+1)$, q^4+1 respectively. Also it is clear that every proper divisor of $(q^3-1)(q+1)$ is less than q^4+1, and so for $\varepsilon = -$ we are done. Since $q^4 - 1$ is divisible by 3 and $(q^4-1)/3 > q^3+1$, for $\varepsilon = +$ the assertion follows too.

Let $n \geqslant 5$. Then $M^c(n,q) \cap \omega(S)$ consists of at least two numbers greater than q^n. Thus $o_i(S) > q^n$, and so Lemma 5 implies that $o_i(S)$ divides some element of $M^c(n,q)$, say a_i. If $o_i(S) \neq a_i$, then

$$o_i(S) \leqslant \frac{a_i}{3} \leqslant \frac{q^{n+1}}{3(q-1)} < q^n,$$

which is a contradiction. Hence $o_i(S) = a_i$, and it remains to find the two largest elements of $M^c(n,q)$.

For all $n \leqslant 21$, we found these numbers by computation with $q = 4$. It turns out that they are contained in $\widetilde{M}(n,q)$ if $n \geqslant 10$ and $(n, \varepsilon) \neq (11,+), (13,+)$. For other n and ε, they are given in Tables 7 and 8.

TABLE 7. $S = \Omega^+_{2n}(q)$, n small, $q \geqslant 4$ even

	$o_1(S)$	$o_2(S)$
$n = 4$	$q^4 - 1$	$(q^4 - 1)/3$
$n = 5, 7, 9$	$(q + 1)(q^{n-1} + 1)$	$(q^2 + 1)(q^{n-2} + 1)$
$n = 6$	$(q + 1)(q^2 + 1)(q^3 - 1)$	$(q^2 + 1)(q^4 + 1)$
$n = 8$	$(q + 1)(q^2 + 1)(q^5 - 1)$	$(q + 1)(q^4 + 1)(q^3 - 1)$
$n = 11, 13$	$(q + 1)(q^{10} + 1)$	$(q^2 + 1)(q^4 + 1)(q^{n-6} - 1)$

TABLE 8. $S = \Omega^-_{2n}(q)$, n small, $q \geqslant 4$ even

	$o_1(S)$	$o_2(S)$
$n = 4, 6$	$(q + 1)(q^{n-1} - 1)$	$q^n + 1$
$n = 5$	$(q^2 + 1)(q^3 - 1)$	$q^5 + 1$
$n = 7, 9$	$(q^2 + 1)(q^4 + 1)(q^{n-6} + 1)$	$(q^2 + 1)(q^{n-2} - 1)$
$n = 8$	$(q + 1)(q^7 - 1)$	$(q^2 + 1)(q^6 - 1)$

Suppose that $n > 21$. By Lemmas 5, 6 and 9, there is a number b such that $\widetilde{m}^{\varepsilon}_2(n, q) \geqslant b$, while all elements of $M^c(n, q) \setminus \widetilde{M}(n, q)$ are less than b. Thus $o_i(S) = \widetilde{m}^{\varepsilon}_i(n, q)$.

Now assume that $S \neq \Omega^+_8(q)$. Then $\operatorname{Aut} S = S \rtimes \langle\varphi, \gamma\rangle$, where φ and γ are defined before Lemma 4. Let $S_1 = S \rtimes \langle\gamma\rangle$. It is clear that $\omega_{2'}(S_1) = \omega_{2'}(S)$. Furthermore, S_1 is isomorphic to the general orthogonal group $O^{\varepsilon}_{2n}(q)$ and $O^{\varepsilon}_{2n}(q) \leqslant Sp_{2n}(q)$. So arguing as in the proof of Lemma 5, we see that the even elements of $\omega(S_1)$ are less than q^n. Thus $o_i(S_1) = o_i(S)$.

Let $g \in \operatorname{Aut} S \setminus S_1$. Then $g \in S\alpha$, where $\langle\alpha\rangle$ is equal to $\langle\varphi^{m/k}\rangle$ or $\langle\varphi^{m/k}\gamma\rangle$, where $k > 1$ divides m. Writing $q_0 = q^{1/k}$, we deduce from Lemma 4 that $\omega(S\alpha) = k \cdot \omega(S_0)$, where S_0 is one of $\Omega^{\pm}_{2n}(q_0)$ and $\Omega^{\pm}_{2n}(q_0)\gamma$. Thus $|g| \leqslant k \cdot q_0^{n+1}/(q_0 - 1)$, and so

$$|g| \leqslant kq_0^{n+1} \leqslant q_0^{kn} = q^n < o_i(S).$$

The proof is complete. □

We are grateful to the referee for thorough and helpful comments.

REFERENCES

[1] W. M. Kantor and Á. Seress, *Large element orders and the characteristic of Lie-type simple groups*, J. Algebra **322**:3 (2009), 802–832. MR2531224

[2] A. V. Vasil'ev, M. A. Grechkoseeva, and V. D. Mazurov, *Characterization of the finite simple groups by spectrum and order*, Algebra Logic **48**:6 (2009), 385–409. MR2640961

[3] S. Guest, J. Morris, C. E. Praeger, and P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc. **367** (2015), 7665–7694. MR3391897

[4] D. V. Lytkin, *Large element orders and the characteristic of finite simple symplectic groups*, Siberian Math. J. **54**:1 (2013), 78–95. MR3089331

[5] P. Spiga, *The maximum order of the elements of a finite symplectic group of even characteristic*, Comm. Algebra **43**:4 (2015), 1417–1434. MR3314621

[6] A. A. Buturlakin, *Spectra of finite symplectic and orthogonal groups*, Siberian Adv. Math. **21** (2011), no. 3, 176–210.

[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] M. A. Grechkoseeva, *On orders of elements of finite almost simple groups with linear or unitary socle*, Preprint (2016), arXiv:1609.00518[math.GR].

Maria Aleksandrovna Grechkoseeva
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
Novosibirsk State University,
ul. Pirogova, 1,
630090, Novosibirsk, Russia
E-mail address: grechkoseeva@gmail.com

Daniil Vsevolodovich Lytkin
Novosibirsk State University,
ul. Pirogova, 1,
630090, Novosibirsk, Russia
E-mail address: dan.lytkin@gmail.com