

1 ON THE MAXIMUM ORDERS OF ELEMENTS OF FINITE ALMOST
2 SIMPLE GROUPS AND PRIMITIVE PERMUTATION GROUPS

3 SIMON GUEST, JOY MORRIS, CHERYL E. PRAEGER, AND PABLO SPIGA

ABSTRACT. We determine upper bounds for the maximum order of an element of a finite almost simple group with socle T in terms of the minimum index $m(T)$ of a maximal subgroup of T : for T not an alternating group we prove that, with finitely many exceptions, the maximum element order is at most $m(T)$. Moreover, apart from an explicit list of groups, the bound can be reduced to $m(T)/4$. These results are applied to determine all primitive permutation groups on a set of size n that contain permutations of order greater than or equal to $n/4$.

4 1. INTRODUCTION

5 In 1903, Edmund Landau [25, 26] proved that the maximum order of an element of
6 the symmetric group $\text{Sym}(n)$ or alternating group $\text{Alt}(n)$ of degree n is $e^{(1+o(1))(n \log n)^{1/2}}$,
7 though it is now known from work of Erdős and Turan [13, 14] that most elements have
8 far smaller orders, namely at most $n^{(1/2+o(1)) \log n}$ (see also [3, 4]). Both of these bounds
9 compare the element orders with the parameter n , which is the least degree of a faithful
10 permutation representation of $\text{Sym}(n)$ or $\text{Alt}(n)$. Here we investigate this problem for all
11 finite almost simple groups:

12 *Find upper bounds for the maximum element order of an almost simple group with socle*
13 *T in terms of the minimum degree $m(T)$ of a faithful permutation representation of T .*

14 We discover that the alternating and symmetric groups are exceptional with regard to
15 this element order comparison. We also study maximal element orders for many natural
16 classes of subgroups of $\text{Sym}(n)$, in particular for many families of primitive subgroups. Our
17 most general result for almost simple groups is Theorem 1.1. For a group G we denote
18 by $\text{meo}(G)$ the maximum order of an element of G . We note that the value of $\text{meo}(T)$
19 for T a simple classical group of odd characteristic was determined in [22] and its relation
20 to $m(T)$ can be deduced. If G is almost simple, say $T \leq G \leq \text{Aut}(T)$ with its socle T a
21 non-abelian simple group, then naturally $\text{meo}(G) \leq \text{meo}(\text{Aut}(T))$.

22 **Theorem 1.1.** *Let G be a finite almost simple group with socle T , such that $T \neq \text{Alt}(m)$*
23 *for any $m \geq 5$. Then with finitely many exceptions, $\text{meo}(G) \leq m(T)$; and indeed either*
24 *$T = \text{PSL}_d(q)$ for some d, q , or $\text{meo}(G) \leq m(T)^{3/4}$. Moreover, given positive $\epsilon, A > 0$, there*
25 *exists $Q = Q(\epsilon, A)$ such that, if $T = \text{PSU}_4(q)$ with $q > Q$, then $\text{meo}(G) > A m(T)^{3/4-\epsilon}$.*

26 We note again that this result gives upper bounds for $\text{meo}(\text{Aut}(T))$ in terms of $m(T)$,
27 and for $\text{meo}(G)$ in terms of $m(G)$ (since $m(T) \leq m(G)$). Moreover equality in the up-
28 per bound $\text{meo}(\text{Aut}(T)) \leq m(T)$ holds when $T = \text{PSL}_d(q)$ for all but two pairs (d, q) ,
29 see Table 3 and Theorem 2.16. (Theorem 2.16 and Table 3 provide good estimates for

2000 *Mathematics Subject Classification.* 20B15, 20H30.

Key words and phrases. primitive permutation groups; conjugacy classes; cycle structure.

Address correspondence to P. Spiga, E-mail: pablo.spiga@unimib.it

The second author is supported in part by the National Science and Engineering Research Council of Canada. The research is supported in part by the Australian Research Council grants FF0776186, and DP130100106.

30 $\text{meo}(\text{Aut}(T))$ for all finite classical simple groups T in terms of the field size and dimen-
 31 sion.) We are particularly interested in linear upper bounds for $\text{meo}(\text{Aut}(T))$ of the form
 32 $cm(T)$ with a constant $c < 1$. It turns out that, after excluding the groups $\text{Alt}(m)$ and
 33 $\text{PSL}_d(q)$, such an upper bound holds with the constant $c = 1/4$ for all but 12 simple groups
 34 T .

35 **Theorem 1.2.** *For a finite non-abelian simple group T , either $\text{meo}(\text{Aut}(T)) < m(T)/4$,
 36 or T is listed in Table 1.*

M_{11}	M_{23}	$\text{Alt}(m)$	$\text{PSL}_d(q)$	$\text{PSU}_3(3)$	$\text{PSp}_6(2)$
M_{12}	M_{24}			$\text{PSU}_3(5)$	$\text{PSp}_8(2)$
M_{22}	HS			$\text{PSU}_4(3)$	$\text{PSp}_4(3)$

TABLE 1. Exceptions in Theorem 1.2

37 Clearly, Theorems 1.1 and 1.2 do not provide the last word on this type of result. One
 38 might wonder, if minded so, “What is the slowest growing function of $m(T)$ with the
 39 property that Theorem 1.2 is still valid?” (possibly allowing a *finite* extension of the list
 40 in Table 1). We do not investigate this here. Instead we turn our attention to $\text{meo}(G)$ for a
 41 wider family of primitive permutation groups G than the almost simple primitive groups.
 42 For such groups of degree n , it also turns out that $\text{meo}(G) < n/4$, apart from a number
 43 of explicitly determined families and individual primitive groups. We refer to [19] for the
 44 affine case in which G has an abelian socle, since the proof in that case is very delicate and
 45 quite different from the arguments in this paper, which are based on properties of finite
 46 simple groups.

47 **Theorem 1.3.** *Let G be a finite primitive permutation group of degree n such that $\text{meo}(G)$
 48 is at least $n/4$. Then the socle $N \cong T^\ell$ of G is isomorphic to one of the following (where
 49 $k, \ell \geq 1$):*

- 50 (1) $\text{Alt}(m)^\ell$ in its natural action on ℓ -tuples of k -subsets from $\{1, \dots, m\}$;
- 51 (2) $\text{PSL}_d(q)^\ell$ in either of its natural actions on ℓ -tuples of points, or ℓ -tuples of hyper-
 52 planes, of the projective space $\text{PG}_{d-1}(q)$;
- 53 (3) an elementary abelian group C_p^ℓ and G is described in [19]; or to
- 54 (4) one of the groups in Table 2.

55 Moreover, there exists a positive integer ℓ_T , depending only on T , such that $\ell \leq \ell_T$.

56 **Remark 1.4.** The possibilities for the degree n of G in Theorem 1.3(4) are, in fact,
 57 quite restricted. In column 2 of Table 6, we list the possibilities for the degree m of the
 58 permutation representation of the socle factor T of a primitive group G of PA type of
 59 degree $n = m^\ell$. The integer ℓ can be as small as 1, in which case G is of AS type, and has
 60 maximum value ℓ_T , which is also listed in column 2. If G is of HS or SD type (with socle
 61 $\text{Alt}(5)^2$) then we simply have $n = 60$.

62 Our choice of $n/4$ in Theorems 1.2 and 1.3 is in some sense arbitrary. However it yields
 63 a list of exceptions that is not too cumbersome to obtain and to use, and yet is sufficient
 64 to provide useful information on the normal covering number of $\text{Sym}(m)$, an application
 65 described in [20]. (The normal covering number of a non-cyclic group G is the smallest
 66 number of conjugacy classes of proper subgroups of G such that the union of the subgroups
 67 in all of these conjugacy classes is equal to G , that is to say the classes ‘cover’ G .) In [20]
 68 we use Theorem 1.3 to study primitive permutation groups containing elements with at
 69 most four cycles, and our results about such groups yield critical information on normal
 70 covers of $\text{Sym}(n)$, and a consequent number theoretic application. The primitive groups
 71 containing at most two cycles have been classified by Müller [34], also for applications in
 72 number theory. Moreover, many of our methods and results, both here and in [20], were
 73 inspired by, and are quite similar to, the methods and results in [34].

AS type						HS or SD type	PA type
Alt(5)	M_{11}	PSL ₂ (7)	PSL ₂ (49)	PSU ₃ (3)	PSP ₆ (2)	Alt(5) ²	T^ℓ where T is one of the groups in the AS type part of this table
Alt(6)	M_{12}	PSL ₂ (8)	PSL ₃ (3)	PSU ₃ (5)	PSP ₈ (2)		
Alt(7)	M_{22}	PSL ₂ (11)	PSL ₃ (4)	PSU ₄ (3)	PSP ₄ (3)		
Alt(8)	M_{23}	PSL ₂ (16)	PSL ₄ (3)				
Alt(9)	M_{24}	PSL ₂ (19)					
	HS	PSL ₂ (25)					

TABLE 2. The socles for the exceptions G in Theorem 1.3 (4)

74 **1.1. Comments on the proof of Theorem 1.3.** Our proof of Theorem 1.3 uses the
 75 bounds of Theorem 1.2, and proceeds according to the structure of G and its socle as
 76 specified by the “O’Nan–Scott type” of G . This is one of the most effective modern
 77 methods for analysing finite primitive permutation groups. The *socle* N of G is the
 78 subgroup generated by the minimal normal subgroups of G . For an arbitrary finite group
 79 the socle is isomorphic to a direct product of simple groups, and, for finite primitive
 80 groups these simple groups are pairwise isomorphic. The O’Nan–Scott theorem describes
 81 in detail the embedding of N in G and provides some useful information on the action of
 82 N , identifying a small number of pairwise disjoint possibilities. The subdivision we use in
 83 our proofs is described in [36] where eight types of primitive groups are defined (depending
 84 on the structure and on the action of the socle), namely HA (*Holomorphic Abelian*), AS
 85 (*Almost Simple*), SD (*Simple Diagonal*), CD (*Compound Diagonal*), HS (*Holomorphic*
 86 *Simple*), HC (*Holomorphic Compound*), TW (*Twisted wreath*), PA (*Product Action*), and
 87 it follows from the O’Nan–Scott Theorem (see [29] or [12, Chapter 4]) that every primitive
 88 group is of exactly one of these types.

89 In the light of this subdivision, Theorem 1.3 asserts that a finite primitive group con-
 90 taining elements of large order relative to the degree is either of AS or PA type (with a
 91 well-understood socle), or of HA type, or it has bounded order. The proof of Theorem 1.3
 92 for primitive groups of HA type is in our companion paper [19], where we obtain an explicit
 93 description of the permutations $g \in G$ with order $|g| \geq n/4$ together with detailed infor-
 94 mation on the structure of G . We refer the interested reader to [19] for more information
 95 on this case.

96 **1.2. Structure of the paper.** In Section 2 we determine tight upper bounds on the
 97 maximum element orders for the almost simple groups and we give in Table 3 some valuable
 98 information on the maximum element order of $\text{Aut}(T)$ when T is a simple group of Lie
 99 type. In Section 3, we collect some well-established results on the minimal degree of a
 100 permutation representation for the non-abelian simple groups. (These include corrections
 101 noticed by Mazurov and Vasil’ev [33] to [24, Table 5.2.A].) We then prove Theorem 1.2 in
 102 Section 4. The proof of Theorem 1.3, which relies on Theorem 1.2, is given in Section 5.
 103 We provide some information on the positive integers ℓ_T (defined in Theorem 1.2) in
 104 Remark 5.11 and in Table 6. Finally, Section 6 contains the proof of Theorem 1.1.

105 **2. MAXIMUM ELEMENT ORDERS FOR SIMPLE GROUPS**

106 For a finite group G , we write $\text{exp}(G)$ for the *exponent* of G ; that is, the minimum
 107 positive integer k for which $g^k = 1$ for all $g \in G$. We denote the *order* of the element
 108 $g \in G$ by $|g|$ and we write $\text{meo}(G)$ for the *maximum element order* of G ; that is, $\text{meo}(G) =$
 109 $\max\{|g| \mid g \in G\}$. Clearly, $\text{meo}(G)$ divides $\text{exp}(G)$.

110 In this section we study $\text{meo}(G)$ where G is an almost simple group. We start by
 111 considering the symmetric groups. It is well-known that

$$\text{meo}(\text{Sym}(m)) = \max\{\text{lcm}(n_1, \dots, n_N) \mid m = n_1 + \dots + n_N\}.$$

112 The expression $\text{meo}(\text{Sym}(m))$ is often referred to as *Landau's function* (and is usually
 113 denoted by $g(m)$), in honour of Landau's theorem in [25]. We record the main results
 114 from [25] and [32] on $\text{meo}(\text{Sym}(m))$, to which we will refer in the sequel. As usual $\log(m)$
 115 denotes the logarithm of m to the base e .

116 **Theorem 2.1** ([25] and [32, Theorem 2]). *For all $m \geq 3$, we have*

$$\sqrt{m \log(m)/4} \leq \log(\text{meo}(\text{Sym}(m))) \leq \sqrt{m \log m} \left(1 + \frac{\log(\log(m)) - a}{2 \log(m)}\right)$$

117 *with $a = 0.975$.*

118 *Proof.* The lower bound is proved in [25] and the upper bound is proved in [32]. \square

119 Since $\text{Aut}(\text{Alt}(m)) \cong \text{Sym}(m)$ unless $m \in \{2, 6\}$, Theorem 2.1 gives good estimates of
 120 the maximum element order of $\text{Aut}(\text{Alt}(m))$. And since the minimal degree of a permuta-
 121 tion representation of $\text{Alt}(m)$ is m , for $m \neq 6$, we find that $\text{Alt}(m)$ is one of the exceptional
 122 groups in Theorem 1.2 listed in Table 1.

123 For the groups of Lie type, the following three lemmas will be used frequently in the
 124 proof of Theorem 1.2. Here $\log_p(x)$ denotes the logarithm of x to the base p and $\lceil x \rceil$
 125 denotes the least integer k satisfying $x \leq k$. We denote by J_d the *cyclic unipotent element*
 126 of $\text{GL}_d(q)$ that sends the canonical basis element e_i to $e_i + e_{i+1}$ for $i < d$ and fixes e_d ; that
 127 is, J_d is a $d \times d$ unipotent Jordan block. Also, we denote the identity matrix in $\text{GL}_d(q)$ by
 128 I_d .

129 **Lemma 2.2.** *Let u be a unipotent element of $\text{GL}_d(p^f)$ where p is prime. Then $|u| \leq$
 130 $p^{\lceil \log_p(d) \rceil}$ and equality holds if and only if the Jordan decomposition of u has a block of size
 131 b such that $\lceil \log_p(d) \rceil = \lceil \log_p(b) \rceil$.*

132 *Proof.* Let b be the dimension of the largest Jordan block of u . Let $B = J_b - I_b$, a $b \times b$
 133 matrix over \mathbb{F}_{p^f} . Then since J_b is unipotent, it follows that B is nilpotent and $B^b = 0$.
 134 Now fix a positive integer k . Using the binomial theorem, we have

$$J_b^{p^k} = (I_b + B)^{p^k} = \sum_{i=0}^{p^k} \binom{p^k}{i} B^i.$$

135 Since $\binom{p^k}{i}$ is divisible by p for every $i \in \{1, \dots, p^k - 1\}$, we have $J_b^{p^k} = I_b + B^{p^k}$. In
 136 particular, $J_b^{p^k} = I_b$ if and only if $B^{p^k} = 0$. Since J_b is a cyclic unipotent element, b is the
 137 least positive integer such that $B^b = 0$; therefore $r = \lceil \log_p(b) \rceil$ is the least nonnegative
 138 integer such that $B^{p^r} = 0$. Thus $|J_b| = p^{\lceil \log_p(b) \rceil}$.

139 Suppose that the maximum size of a Jordan block of u is b . Then by the previous
 140 paragraph, $|u| = |J_b| = p^{\lceil \log_p(b) \rceil}$. Since $b \leq d$, this implies that $|u| \leq p^{\lceil \log_p(d) \rceil}$ and that
 141 equality holds if and only if $\lceil \log_p(d) \rceil = \lceil \log_p(b) \rceil$. \square

142 The following elementary lemma, on the direct product of cyclic groups, will be applied
 143 to the maximal tori of groups of Lie type.

144 **Lemma 2.3.** *Let k be a positive integer, and for each $i \in \{1, \dots, t\}$, let k_i be a multiple of
 145 k and let $C_i = \langle x_i \rangle$ be a cyclic group of order k_i . Let C be the subgroup of $G := C_1 \times \dots \times C_t$
 146 of order k generated by $x_1^{k_1/k} \dots x_t^{k_t/k}$. Then the exponent of the quotient group G/C is
 147 k_1/k if $t = 1$ and $\text{lcm}\{k_1, \dots, k_t\}$ if $t \geq 2$.*

148 *Proof.* If $t = 1$, then the exponent of $\langle x_1 \rangle / \langle x_1^{k_1/k} \rangle$ is clearly k_1/k . So suppose that $t \geq 2$.
 149 Set $r = \text{lcm}\{k_1, \dots, k_t\}$ and $r' = \exp(G/C)$. The group G has exponent r and so $r' =$
 150 $\exp(G/C) \leq r$. Conversely, for each $i \in \{1, \dots, t\}$, we have $x_i^{r'} \in C$. Since $t \geq 2$, we have
 151 $C_i \cap C = 1$ because the non-trivial elements of C all have the form $x_1^{j k_1/k} \cdots x_t^{j k_t/k}$ with
 152 $1 \leq j < k$, and so do not lie in C_i . Thus $x_i^{r'} = 1$. This shows that, for each $i \in \{1, \dots, t\}$,
 153 the integer k_i divides r' . Therefore $r \leq r'$, and so $r' = r$. \square

154 The following technical lemma will be applied repeatedly to estimate the maximum
 155 element order of a group of Lie type.

156 **Lemma 2.4.** *Suppose that m, k, f, p are positive integers where p is prime and $q = p^f$.
 157 Then*

- 158 (i) $q^k - 1$ divides $q^{km} - 1$ and $(q^{km} - 1)/(q^k - 1) \geq p^{\lceil \log_p(m) \rceil}$;
 159 (ii) if m is odd, then $q^k + 1$ divides $q^{km} + 1$; furthermore, if $(p, k, m, f) \neq (2, 1, 3, 1)$,
 160 then $(q^{km} + 1)/(q^k + 1) \geq p^{\lceil \log_p(m) \rceil}$;
 161 (iii) if m is even, then $q^k + 1$ divides $q^{km} - 1$; furthermore, if $(k, m, f) \neq (1, 2, 1)$, then
 162 $(q^{km} - 1)/(q^k + 1) \geq p^{\lceil \log_p(m) \rceil}$.

163 *Proof.* The divisibility assertions in (i), (ii) and (iii) are obvious. For Part (i), note that
 164 $(q^{km} - 1)/(q^k - 1) = q^{k(m-1)} + q^{k(m-2)} + \cdots + q^k + 1 \geq q^{k(m-1)}$. Furthermore, $q^{k(m-1)} \geq$
 165 $q^{m-1} \geq p^{m-1} \geq m$ and so $m - 1 \geq \log_p(m)$. However $m - 1$ is an integer, so $m - 1 \geq$
 166 $\lceil \log_p(m) \rceil$ and $(q^{km} - 1)/(q^k - 1) \geq p^{m-1} \geq p^{\lceil \log_p(m) \rceil}$.

167 Assume that m is odd. The assertions hold if $m = 1$, so assume that $m \geq 3$. Then
 168 $(q^{km} + 1)/(q^k + 1) \geq q^{k(m-2)} = p^{fk(m-2)} \geq m$ (where the last inequality holds for $m \geq 3$
 169 provided $(p, k, m, f) \neq (2, 1, 3, 1)$). So, arguing as in the previous paragraph, we have
 170 $(q^{km} + 1)/(q^k + 1) \geq p^{\lceil \log_p(m) \rceil}$ for $(p, k, m, f) \neq (2, 1, 3, 1)$, which gives Part (ii).

171 Next, suppose that m is even. The assertions all hold for $m = 2$ unless $(k, m, f) =$
 172 $(1, 2, 1)$. So assume that $m \geq 4$. Then $(q^{km} - 1)/(q^k + 1) \geq q^{k(m-2)} = p^{fk(m-2)} \geq m$. Now
 173 arguing as in the first paragraph we have $(q^{km} - 1)/(q^k + 1) \geq p^{\lceil \log_p(m) \rceil}$, which proves
 174 Part (iii). \square

175 Before proceeding and obtaining some tight bounds on the maximum element order
 176 for the groups of Lie type, we need to prove some results on centralizers of semisimple
 177 elements in $\text{PGL}_d(q)$ and related classical groups. In order to do so, we introduce some
 178 notation.

179 **Notation 2.5.** Let $\delta = 1$ unless we deal with a unitary group in which case let $\delta = 2$.
 180 Let s be a semisimple element of $\text{PGL}_d(q^\delta)$ and let \bar{s} be a semisimple element of $\text{GL}_d(q^\delta)$
 181 projecting to s in $\text{PGL}_d(q^\delta)$. The action of the matrix \bar{s} on the d -dimensional vector space
 182 $V = \mathbb{F}_{q^\delta}^d$ naturally defines the structure of an $\mathbb{F}_{q^\delta}\langle \bar{s} \rangle$ -module on V . Since \bar{s} is semisimple,
 183 V decomposes, by Maschke's theorem, as a direct sum of irreducible $\mathbb{F}_{q^\delta}\langle \bar{s} \rangle$ -modules, that
 184 is, $V = V_1 \oplus \cdots \oplus V_l$, with V_i an irreducible $\mathbb{F}_{q^\delta}\langle \bar{s} \rangle$ -module. Relabelling the index set
 185 $\{1, \dots, l\}$ if necessary, we may assume that the first t submodules V_1, \dots, V_t are pairwise
 186 non-isomorphic (for some $t \in \{1, \dots, l\}$) and that for $j \in \{t+1, \dots, l\}$, V_j is isomorphic
 187 to some V_i with $i \in \{1, \dots, t\}$. Now, for $i \in \{1, \dots, t\}$, let $\mathcal{W}_i = \{W \leq V \mid W \cong V_i\}$,
 188 the set of $\mathbb{F}_{q^\delta}\langle \bar{s} \rangle$ -submodules of V isomorphic to V_i and write $W_i = \sum_{W \in \mathcal{W}_i} W$. The
 189 module W_i is usually referred to as the *homogeneous* component of V corresponding to
 190 the simple submodule V_i . We have $V = W_1 \oplus \cdots \oplus W_t$. Set $a_i = \dim_{\mathbb{F}_{q^\delta}}(W_i)$. Since
 191 V is completely reducible, we have $W_i = V_{i,1} \oplus \cdots \oplus V_{i,m_i}$ for some $m_i \geq 1$, where
 192 $V_{i,j} \cong V_i$, for each $j \in \{1, \dots, m_i\}$. Thus we have $a_i = d_i m_i$, where $d_i = \dim_{\mathbb{F}_{q^\delta}} V_i$, and
 193 $\sum_{i=1}^t d_i m_i = d$. For $i \in \{1, \dots, t\}$, we let x_i (respectively $y_{i,j}$) denote the element in
 194 $\text{GL}(W_i)$ (respectively $\text{GL}(V_{i,j})$) induced by the action of \bar{s} on W_i (respectively $V_{i,j}$). In

195 particular, $x_i = y_{i,1} \cdots y_{i,m_i}$ and $\bar{s} = x_1 \cdots x_t$. We note further that

$$p(s) = \underbrace{(d_1, \dots, d_1)}_{m_1 \text{ times}} \underbrace{(d_2, \dots, d_2)}_{m_2 \text{ times}} \cdots \underbrace{(d_t, \dots, d_t)}_{m_t \text{ times}}$$

196 is a partition of n .

197 Now let $c \in \mathbf{C}_{\mathrm{GL}_d(q^\delta)}(\bar{s})$. Given $i \in \{1, \dots, t\}$ and $W \in \mathcal{W}_i$, we see that W^c is an
198 $\mathbb{F}_{q^\delta}\langle \bar{s} \rangle$ -submodule of V isomorphic to W (because c commutes with \bar{s}). Thus $W^c \in \mathcal{W}_i$.
199 This shows that W_i is $\mathbf{C}_{\mathrm{GL}_d(q^\delta)}(\bar{s})$ -invariant. It follows that

$$\mathbf{C}_{\mathrm{GL}_d(q^\delta)}(\bar{s}) = \mathbf{C}_{\mathrm{GL}(W_1)}(x_1) \times \cdots \times \mathbf{C}_{\mathrm{GL}(W_t)}(x_t)$$

200 and every unipotent element of $\mathbf{C}_{\mathrm{GL}_d(q^\delta)}(\bar{s})$ is of the form $u = u_1 \cdots u_t$ with $u_i \in \mathbf{C}_{\mathrm{GL}(W_i)}(x_i)$
201 unipotent in $\mathrm{GL}(W_i)$, for each i .

202 Since \bar{s} is semisimple and $V_{i,j}$ is irreducible, Schur's lemma implies that $V_{i,j} \cong \mathbb{F}_{q^{\delta d_i}}$ and
203 that the action of $y_{i,j}$ on $V_{i,j}$ is equivalent to the scalar multiplication action on $\mathbb{F}_{q^{\delta d_i}}$ by a
204 field generator $\lambda_{i,j}$ of $\mathbb{F}_{q^{\delta d_i}}$. As $V_{i,j_1} \cong V_{i,j_2}$, we have $\lambda_{i,j_1} = \lambda_{i,j_2}$, for $j_1, j_2 \in \{1, \dots, m_i\}$
205 and we write $\lambda_i = \lambda_{i,1}$. Under this identification, replacing x_i by a suitable conjugate
206 in $\mathrm{GL}_{a_i}(q^\delta)$ if necessary, we have $x_i = \lambda_i I_{m_i} \in \mathrm{GL}_{m_i}(q^{\delta d_i}) < \mathrm{GL}_{a_i}(q^\delta)$. Now a direct
207 computation shows that $\mathbf{C}_{\mathrm{GL}(W_i)}(x_i) \cong \mathrm{GL}_{m_i}(q^{\delta d_i})$.

208 **Proposition 2.6.** *Let s be as in Notation 2.5. A unipotent element u of $\mathrm{PGL}_d(q)$ cen-*
209 *tralizing s has order at most $\max\{p^{\lceil \log_p(m_1) \rceil}, \dots, p^{\lceil \log_p(m_t) \rceil}\}$.*

210 *Proof.* We use the notation established in Notation 2.5. Let u be a unipotent element
211 of $\mathrm{PGL}_d(q)$ and let \bar{u} be the unique unipotent element of $\mathrm{GL}_d(q)$ projecting to u . Since
212 u centralizes s , \bar{u} commutes with \bar{s} modulo $\mathbf{Z}(\mathrm{GL}_d(q))$. Thus $\bar{u}\bar{s} = (\bar{s}\bar{u})c$, for some
213 scalar matrix c of $\mathrm{GL}_d(q)$. Arguing by induction, we see that, for each $k \geq 1$, we have
214 $\bar{u}^k \bar{s} = \bar{s} \bar{u}^k c^k$. In particular, for $k = q-1$, since $c^{q-1} = 1$, it follows that \bar{u}^{q-1} centralizes \bar{s} .
215 Since the order of \bar{u} is a p -power, we find that \bar{u} centralizes \bar{s} . Thus $|u|$ is bounded above
216 by the maximum order a unipotent element in $\mathbf{C}_{\mathrm{GL}_d(q)}(\bar{s}) \cong \mathrm{GL}_{m_1}(q^{d_1}) \times \cdots \times \mathrm{GL}_{m_t}(q^{d_t})$.
217 The result now follows from Lemma 2.2. \square

218 The following corollary is well-known and somehow not surprising.

219 **Corollary 2.7.** $\mathrm{meo}(\mathrm{PGL}_d(q)) = (q^d - 1)/(q - 1)$.

220 *Proof.* A Singer cycle of $\mathrm{PGL}_d(q)$ has order $(q^d - 1)/(q - 1)$ and so $\mathrm{meo}(\mathrm{PGL}_d(q)) \geq$
221 $(q^d - 1)/(q - 1)$. Let $g \in \mathrm{PGL}_d(q)$. Then g has a unique expression as $g = su = us$ with s
222 semisimple and u unipotent. We use Notation 2.5 for the element s . By Lemma 2.3 and
223 the proof of Proposition 2.6, we see that if $t = 1$, so that $d = m_1 d_1$, then

$$|g| \leq \frac{q^{d_1} - 1}{q - 1} p^{\lceil \log_p(m_1) \rceil} \leq \frac{q^d - 1}{q - 1}$$

224 (using Lemma 2.4(i)). If $t \geq 2$, then

$$|g| \leq \mathrm{lcm}\{(q^{d_i} - 1)p^{\lceil \log_p(m_i) \rceil} \mid i = 1, \dots, t\} \leq \frac{1}{(q - 1)^{t-1}} \prod_{i=1}^t (q^{d_i} - 1)p^{\lceil \log_p(m_i) \rceil},$$

225 which by Lemma 2.4 (i) is at most

$$\frac{1}{(q - 1)^{t-1}} \prod_{i=1}^t (q^{d_i m_i} - 1) \leq \frac{q^d - 1}{(q - 1)^{t-1}} \leq \frac{q^d - 1}{q - 1}.$$

226 \square

227 **Remark 2.8.** As one might expect, sometimes we have $\text{meo}(\text{Aut}(\text{PSL}_d(q))) > (q^d - 1)/(q - 1)$.
 228 For example, $\text{PGL}_2(4) = \text{PSL}_2(4) \cong \text{Alt}(5)$ and $\text{meo}(\text{PSL}_2(4)) = 5$, but $\text{Aut}(\text{Alt}(5)) =$
 229 $\text{Sym}(5)$ and $\text{meo}(\text{Sym}(5)) = 6$. Similarly, $\text{meo}(\text{PSL}_3(2)) = 7$ but $\text{meo}(\text{Aut}(\text{PSL}_3(2))) = 8$.
 230 Later, in Theorem 2.16 (using an application of Lang's theorem) we will prove that, in
 231 fact, $\text{meo}(\text{Aut}(\text{PSL}_d(q))) = (q^d - 1)/(q - 1)$ in all other cases.

232 Before studying other classical groups we need the following number-theoretic lemma
 233 which will be crucial in studying the asymptotic value of $\text{meo}(\text{PSP}_{2m}(q))$ as m tends to
 234 infinity (see Corollary 2.10 and Remark 2.11). In the proof of Lemma 2.9, we denote by
 235 $(a)_2$ the largest power of 2 dividing the positive integer a .

236 **Lemma 2.9.** *Let (a_1, \dots, a_t) be a partition of d , let q be a prime power and, for each*
 237 *$i \in \{1, \dots, t\}$, let $\varepsilon_i \in \{-1, 1\}$. Then $\text{lcm}_{i=1}^t \{q^{a_i} - \varepsilon_i\} \leq q^{d+1}/(q - 1)$ if q is even or $t = 1$,*
 238 *and $\text{lcm}_{i=1}^t \{q^{a_i} - \varepsilon_i\} \leq q^{d+1}/2(q - 1)$ if q is odd and $t \geq 2$.*

239 *Proof.* Set $L := \text{lcm}_{i=1}^t \{q^{a_i} - \varepsilon_i\}$. If $t = 1$, then $L = q^d - \varepsilon_1 \leq q^d + 1 = q^d(1 + 1/q^d) \leq$
 240 $q^{d+1}/(q - 1)$ and the lemma is proved. Thus we may assume that $t > 1$. We argue by
 241 induction on d . Write $I = \{i \in \{1, \dots, t\} \mid \varepsilon_i = -1\}$. If $a_i = a_j$ for distinct elements
 242 $i, j \in I$ then, replacing d by $d - a_j$ and replacing the partition (a_1, \dots, a_t) by the same
 243 partition with the part a_j removed, it follows by induction that $L \leq q^{d-a_j+1}/(q - 1) \leq$
 244 $q^{d+1}/2(q - 1)$. Therefore, we may assume further that the set $\{a_i\}_{i \in I}$ consists of pairwise
 245 distinct elements. Let α and β be distinct elements of $\{1, \dots, t\}$ and write $r = \gcd(q^{\alpha} -$
 246 $\varepsilon_\alpha, q^{\alpha\beta} - \varepsilon_\beta)$ and $s = (\gcd(q - 1, 2))^{t-1}$. Now

$$(1) \quad \begin{aligned} L = \text{lcm}_{i=1}^t \{q^{a_i} - \varepsilon_i\} &\leq \frac{1}{rs} \prod_{i \in I} (q^{a_i} + 1) \prod_{i \notin I} (q^{a_i} - 1) \leq \frac{1}{rs} \prod_{i \in I} q^{a_i} \prod_{i \in I} \left(1 + \frac{1}{q^{a_i}}\right) \prod_{i \notin I} q^{a_i} \\ &= \frac{q^d}{rs} \prod_{i \in I} \left(1 + \frac{1}{q^{a_i}}\right) \leq \frac{q^d}{rs} \prod_{k \in \mathbb{N}} \left(1 + \frac{1}{q^k}\right). \end{aligned}$$

247 Since $\log(1 + x) \leq x$ for $x \geq 0$, we have

$$\log \left(\prod_{k \in \mathbb{N}} \left(1 + \frac{1}{q^k}\right) \right) = \sum_{k \in \mathbb{N}} \log \left(1 + \frac{1}{q^k}\right) \leq \sum_{k \in \mathbb{N}} \frac{1}{q^k} = \frac{1}{q - 1}.$$

248 Thus $L \leq (q^d/rs) \exp(1/(q - 1))$. If $r \geq 2$, then

$$\frac{\exp(1/(q - 1))}{r} \leq \frac{\exp(1/(q - 1))}{2} \leq \frac{1}{2} + \frac{1}{q - 1} < 1 + \frac{1}{q - 1} = \frac{q}{q - 1}$$

249 (the second inequality follows from the inequality $\exp(y) \leq 1 + 2y$, which is valid for
 250 $0 \leq y \leq 1$), and hence $L \leq q^{d+1}/s(q - 1)$ and the result follows.

251 Thus we may assume that $q^{\alpha} - \varepsilon_\alpha$ and $q^{\alpha\beta} - \varepsilon_\beta$ are coprime, for distinct $\alpha, \beta \in \{1, \dots, t\}$.
 252 In particular, q is even and so $s = 1$. Consider distinct $\alpha, \beta \in I$. A direct computation
 253 shows that $q^{\alpha} + 1$ and $q^{\alpha\beta} + 1$ have a non-trivial common factor if and only if $(a_\alpha)_2 = (a_\beta)_2$.
 254 Thus in particular, for each $k \geq 0$, there is at most one $i \in I$ with $(a_i)_2 = 2^k$. From (1),
 255 we have

$$(2) \quad L \leq q^d \prod_{i \in I} \left(1 + \frac{1}{q^{a_i}}\right) \leq q^d \prod_{k \geq 0} \left(1 + \frac{1}{q^{2^k}}\right)$$

256 (where in the last inequality we use the fact that if $2^k = (a_i)_2$, then $1 + 1/q^{a_i} \leq 1 + 1/q^{2^k}$).
 257 By expanding the infinite product on the right hand side of (2), we see that

$$\prod_{k \geq 0} \left(1 + \frac{1}{q^{2^k}}\right) = \sum_{r \geq 0} \frac{1}{q^r} = \frac{q}{q - 1}$$

258 and the lemma is proved. \square

259 In the remainder of this section the vector space V admits a non-degenerate form or
 260 quadratic form of classical type which is preserved up to a scalar multiple by the preimage
 261 in $\mathrm{GL}_d(q^\delta)$ of the group G . We frequently make use of a theorem of B. Huppert [21, Satz
 262 2], which we apply to semisimple elements $\bar{s} \in G$ that preserve the form. Such elements
 263 generate a subgroup acting completely reducibly on V , and by Huppert's Theorem, V
 264 admits an orthogonal decomposition of the following form which gives finer information
 265 than we had in Notation 2.5:

$$(3) \quad \begin{aligned} V &= V_+ \perp V_- \perp ((V_{1,1} \oplus V'_{1,1}) \perp \cdots \perp (V_{1,m_1} \oplus V'_{1,m_1})) \perp \cdots \\ &\quad \perp ((V_{r,1} \oplus V'_{r,1}) \perp \cdots \perp (V_{r,m_r} \oplus V'_{r,m_r})) \\ &\quad \perp (V_{r+1,1} \perp \cdots \perp V_{r+1,m_{r+1}}) \perp \cdots \perp (V_{t',1} \perp \cdots \perp V_{t',m_{t'}}) \end{aligned}$$

266 where V_+ and V_- are the eigenspaces of \bar{s} for the eigenvalues 1 and -1 , of dimensions
 267 d_+ and d_- , respectively (note V_\pm is non-degenerate if $d_\pm > 0$ and we set $d_- = 0$ if q is
 268 even), and each $V_{i,j}$ is an irreducible $\mathbb{F}_{q^\delta}\langle\bar{s}\rangle$ -submodule. Moreover for $i = r+1, \dots, t'$,
 269 $V_{i,j}$ is non-degenerate of dimension $2d_i/\delta$ and \bar{s} induces an element $y_{i,j}$ of order dividing
 270 $q^{d_i} + 1$ on $V_{i,j}$ (in the unitary case $\delta = 2$ and the dimension d_i is odd). For $i = 1, \dots, r$,
 271 $V_{i,j}$ and $V'_{i,j}$ are totally isotropic of dimension d_i/δ (here d_i is even if $\delta = 2$), $V_{i,j} \oplus V'_{i,j}$
 272 is non-degenerate, and \bar{s} induces an element $y_{i,j}$ of order dividing $q^{d_i} - 1$ on $V_{i,j}$ while
 273 inducing the adjoint representation $(y_{i,j}^{-1})^{tr}$ on $V'_{i,j}$ (where x^{tr} denotes the transpose of the
 274 matrix x). For our claims about the orders of the $y_{i,j}$, we also refer to [7, 22] for some
 275 standard facts on the structure of the maximal tori of the finite classical groups.

276 We denote by $\mathrm{CSp}_{2m}(q)$ the conformal symplectic group, that is, the elements of
 277 $\mathrm{GL}_{2m}(q)$ preserving a given symplectic form up to a scalar multiple. Also $\mathrm{PCSp}_{2m}(q)$
 278 denotes the projection of $\mathrm{CSp}_{2m}(q)$ in $\mathrm{PGL}_{2m}(q)$. From [9, Table 5, page xvi], we have
 279 $|\mathrm{PCSp}_{2m}(q) : \mathrm{PSp}_{2m}(q)| = \gcd(2, q-1)$. In the rest of this section, by abuse of notation,
 280 we write $p^{\lceil \log_p(0) \rceil} = 1$.

281 **Lemma 2.10.** $\mathrm{meo}(\mathrm{PCSp}_{2m}(q)) \leq q^{m+1}/(q-1)$.

282 *Proof.* Using Corollary 2.7 and the fact that $\mathrm{PCSp}_2(q) \cong \mathrm{PGL}_2(q)$, we may assume that
 283 $m \geq 2$. Let g be an element of $\mathrm{PCSp}_{2m}(q)$ and write $g = su = us$ with s semisimple and
 284 u unipotent. We use Notation 2.5 for the element s . First suppose that $g \in \mathrm{PSp}_{2m}(q)$,
 285 and let $\bar{g}, \bar{s}, \bar{u} \in \mathrm{Sp}_{2m}(q)$ correspond to g, s, u , respectively. Consider the orthogonal \bar{s} -
 286 invariant decomposition of V given by (3) (and note that in this case $\delta = 1$). Here V_+
 287 and V_- have even dimension, and we write $2m_+ := \dim V_+$, $2m_- := \dim V_-$. Note that,
 288 for $1 \leq i \leq r$, $V_{i,j}$ and $V'_{i,j}$ are isomorphic $\mathbb{F}_q\langle\bar{s}\rangle$ -modules if and only if $y_{i,j}$ acts as the
 289 multiplication by 1 or -1 on $V_{i,j}$, and by definition of V_\pm this is not the case; thus $V_{i,j}$
 290 and $V'_{i,j}$ are non-isomorphic.

291 Now $m = m_+ + m_- + m_1 d_1 + \cdots + m_{t'} d_{t'}$, and by the information from (3) on the orders
 292 of the $y_{i,j}$, and the result in Proposition 2.6 (using the notation from Notation 2.5) about
 293 the order of \bar{u} , we see that the order of g is at most

$$(4) \quad \prod_{i=1}^r \{q^{d_i} - 1\} \cdot \prod_{i=r+1}^{t'} \{q^{d_i} + 1\} \cdot \max\{p^{\lceil \log_p(2m_\pm) \rceil}, p^{\lceil \log_p(m_i) \rceil} \mid i = 1, \dots, t'\}.$$

294 Using Lemma 2.4, for $i = 1, \dots, r$, we see that by replacing the action of g on $(V_{i,1} \oplus V'_{i,1}) \oplus$
 295 $\cdots \oplus (V_{i,m_i} \oplus V'_{i,m_i})$ with the action given by a semisimple element of order $q^{d_i m_i} - 1$ (and so
 296 having only two totally isotropic irreducible $\mathbb{F}_q\langle\bar{s}\rangle$ -submodules), we obtain an element g'
 297 such that $|g|$ divides $|g'|$ and $m_i = 1$. In particular, replacing g by g' if necessary, we may
 298 assume that $g = g'$. With a similar argument, for those $i \in \{r+1, \dots, t'\}$ with m_i odd and
 299 $(p, d_i, m_i, f) \neq (2, 1, 3, 1)$, we may assume that $m_i = 1$. Also, applying again Lemma 2.4,
 300 for $i \in \{r+1, \dots, t'\}$, we may assume that if m_i is even, then $(d_i, m_i, f) = (1, 2, 1)$.

301 Suppose that, for some $i_0 \in \{r+1, \dots, t'\}$, we have $(p, d_{i_0}, m_{i_0}, f) = (2, 1, 3, 1)$. The ele-
 302 ment g induces on $W := V_{i_0,1} \perp V_{i_0,2} \perp V_{i_0,3}$ an element of order dividing $(q+1)p^{\lceil \log_p(3) \rceil} =$
 303 $2^2 \cdot 3$. Let g' be the element acting as g on W^\perp , inducing an element of order $q+1$ on
 304 $V_{i_0,1}$ and inducing a regular unipotent element on $V_{i_0,2} \perp V_{i_0,3}$. Now, g' induces on W an
 305 element of order $(q+1)p^{\lceil \log_p(4) \rceil} = 2^2 \cdot 3$. Therefore $|g| = |g'|$ and so, we may replace g by
 306 g' (note that in doing so the dimension of V_+ increases by 2 and m_{i_0} decreases from 3 to
 307 1). In particular, we may assume that $m_i = 1$ for each $i \in \{r+1, \dots, t'\}$ with m_i odd.

308 Suppose that, for some $i_0 \in \{r+1, \dots, t'\}$, we have $(d_{i_0}, m_{i_0}, f) = (1, 2, 1)$. The element
 309 g induces on $W = V_{i_0,1} \perp V_{i_0,2}$ an element of order dividing $(p+1)p^{\lceil \log_p(2) \rceil} = (p+1)p$.
 310 Let g' be the element acting as g on W^\perp , inducing an element of order $p+1$ on $V_{i_0,1}$
 311 and inducing an element of order p on $V_{i_0,2}$. Now, g' induces on W an element of order
 312 $(p+1)p$. Therefore $|g| = |g'|$ and so, replacing g by g' if necessary, we may assume that
 313 $m_i = 1$, for each $i \in \{r+1, \dots, t'\}$. Thus $m = m_+ + m_- + d_1 + \dots + d_{t'}$.

314 Now, using Lemma 2.9, we see that the element g has order at most

$$(5) \quad \begin{aligned} & \text{lcm}_{i=1}^r \{q^{d_i} - 1\} \cdot \text{lcm}_{i=r+1}^{t'} \{q^{d_i} + 1\} \cdot \max\{p^{\lceil \log_p(2m_+) \rceil}, p^{\lceil \log_p(2m_-) \rceil}\} \\ & \leq \frac{q^{m_+ + m_- + m_-}}{q-1} \max\{p^{\lceil \log_p(2m_+) \rceil}, p^{\lceil \log_p(2m_-) \rceil}\} \leq \frac{q^{m+1}}{q-1} \end{aligned}$$

315 (where the last inequality follows from an easy computation). This proves the result
 316 for elements $g \in \text{PSP}_{2m}(q)$. If q is even then $\text{PCSp}_{2m}(q) = \text{PSP}_{2m}(q)$, and the proof is
 317 complete. Thus we may assume that q is odd, and in this case, by Lemma 2.9, the upper
 318 bound is reduced to $q^{m+1}/(2(q-1))$ if $t' \geq 2$.

319 We must consider elements $g \in \text{PCSp}_{2m}(q) \setminus \text{PSP}_{2m}(q)$. Now $g^2 \in \text{PSP}_{2m}(q)$ and we
 320 have just shown that $|g^2| \leq q^{m+1}/(2(q-1))$ if the parameter t' for g^2 is at least 2, and
 321 hence in this case $|g| \leq q^{m+1}/(q-1)$. Thus we may assume that $t' \in \{0, 1\}$. If $t' = 0$ then

$$|g^2| \leq \max\{p^{\lceil \log_p(2m_+) \rceil}, p^{\lceil \log_p(2m_-) \rceil}\} \leq p^{\lceil \log_p(2m) \rceil} \leq q^{m+1}/2(q-1),$$

322 where the last inequality holds unless $(m, q) = (2, 3)$ (this follows from a direct computa-
 323 tion). We verify directly the claim of the lemma for $\text{PCSp}_4(3)$. Therefore we may assume
 324 that the parameter $t' = 1$ for g^2 .

325 In this case the parameters for g^2 satisfy $m = m_+ + m_- + d_1$. If $m_+ = m_- = 0$ then
 326 \bar{g}^2 is semisimple with eigenvalues $\lambda, \lambda^{-1}, \lambda^q, \lambda^{-q}, \dots, \lambda^{q^{m-1}}, \lambda^{-q^{m-1}}$, where $\lambda^{q^{m \pm 1}} = 1$.
 327 In particular, $\bar{g}^{q^{m \pm 1}} = \pm I_{2m}$ and so g has order at most $q^m + 1$, which is less than
 328 $q^{m+1}/(q-1)$. Thus we may assume that $m_+ + m_- > 0$. Now (5) gives $|g^2| \leq (q^{d_1} +$
 329 $1) \max\{p^{\lceil \log_p(2m_+) \rceil}, p^{\lceil \log_p(2m_-) \rceil}\}$. To bound the right hand side, we may assume that
 330 $m_- = 0$ and $m = d_1 + m_+$. A direct computation shows that, since q is odd, this bound is
 331 less than $q^{m+1}/2(q-1)$ (and hence $|g| \leq q^{m+1}/(q-1)$) when $m_+ \geq 2$ unless $(q, m_+) = (3, 2)$
 332 and g^2 has order $9(3^{m-2} + 1)$. If $m_+ = 1$ then either \bar{g}^2 is semisimple and has order at
 333 most $q^{m-1} + 1$, which is less than $q^{m+1}/2(q-1)$, or $\bar{g}^2 = J_2 + h$ where h has order dividing
 334 $q^{m-1} \pm 1$. The eigenvalues of \bar{g}^2 are therefore $\lambda_1, \dots, \lambda_{2m-2}$, with each $\lambda_i \neq \pm 1$ and all
 335 distinct, and 1 with algebraic multiplicity 2. The eigenvalues of \bar{g} are therefore $a, a, \nu_1,$
 336 \dots, ν_{2m-2} where $a = \pm 1$ and each $\nu_i^2 = \lambda_i$; and since \bar{g} is not semisimple, the eigenvalue
 337 a must have algebraic multiplicity 2. However \bar{g} is a similarity with respect to the skew-
 338 symmetric form J ; that is $\bar{g}^T J \bar{g} = \mu J$ for some $\mu \in \mathbb{F}_q$ and therefore $J^{-1} \bar{g}^T J = \mu \bar{g}^{-1}$.
 339 In particular, \bar{g} and $\mu \bar{g}^{-1}$ are $\text{GL}_n(q)$ -conjugate and have the same eigenvalues with the
 340 same algebraic multiplicities. So since a is an eigenvalue of \bar{g} with algebraic multiplicity 2,
 341 so is $a\mu$ and we must have $\mu = 1$. But then $g \in \text{PSP}_{2m}(q)$, contradicting our assumption.
 342 Finally suppose that $(q, m_+) = (3, 2)$ and g^2 has order $9(3^{m-2} + 1)$. Then the eigenvalues
 343 of \bar{g}^2 are $1, \lambda_1, \dots, \lambda_{2m-4}$, where 1 has algebraic multiplicity 4, the λ_i are distinct and
 344 $\lambda_i \neq \pm 1$. It follows that the eigenvalues of \bar{g} are $a, \nu_1, \dots, \nu_{2m-4}$, where $a = \pm 1$ has

345 algebraic multiplicity 4, and each $\nu_i^2 = \lambda_i$ (since 9 divides $|g|$). Again, since $\bar{g}^T J \bar{g} = \mu J$,
 346 it follows that $a\mu$ is also an eigenvalue of \bar{g} with algebraic multiplicity 4, and therefore
 347 $\mu = 1$ and $g \in \text{P}\mathbb{S}\text{p}_{2m}(q)$, which is a contradiction. \square

348 **Remark 2.11.** We note that Corollary 2.10 is, for q even, asymptotically the best possible.
 349 Indeed, let q be a 2-power, let k be a positive integer and let s be a semisimple element
 350 of $\text{P}\mathbb{S}\text{p}_{2^{k+1}-2}(q) \cong \text{S}\mathbb{p}_{2^{k+1}-2}(q)$. Suppose that the natural $\mathbb{F}_q\langle \bar{s} \rangle$ -module V decomposes as
 351 $V_1 \perp \cdots \perp V_k$ with $\dim_{\mathbb{F}_q} V_i = 2^i$ and with \bar{s} inducing on V_i an element of order $q^{2^{i-1}} + 1$.
 352 (This is the decomposition of (3) for \bar{s} where we have $V_{\pm} = 0, r = 0, t' = k$ and for each
 353 $i, m_i = 1, d_i = i$.) Now, we have

$$\begin{aligned} |s| &= \text{lcm}\{q+1, q^2+1, q^{2^2}+1, \dots, q^{2^{k-1}}+1\} = (q+1)(q^2+1)\cdots(q^{2^{k-1}}+1) \\ &= q^{2^k-1} \prod_{i=0}^{k-1} \left(1 + \frac{1}{q^{2^i}}\right), \end{aligned}$$

354 which approaches $q^{2^k}/(q-1)$ as k tends to infinity.

355 Moreover, the extra care that we used in handling the subspaces V_+ and V_- in the proof
 356 of Corollary 2.10 may seem ostensibly artificial and unnecessary. However we remark that
 357 the maximum order of an element g of $\text{P}\mathbb{S}\text{p}_{36}(2)$ is $2^3 \cdot (2+1) \cdot (2^2+1) \cdot (2^4+1) \cdot (2^8+1)$ (see [22,
 358 p. 808]). Such an element g can be chosen to be of the form $su = us$ (with u unipotent
 359 and s semisimple), where the element \bar{u} fixes a 30-dimensional subspace pointwise and acts
 360 as a regular unipotent element on a 6-dimensional subspace W , and where the element
 361 \bar{s} acts trivially on W . In particular, this shows that the contribution of V_+ and V_- are
 362 sometimes essential in achieving the maximum element order of $\text{P}\mathbb{S}\text{p}_{2m}(q)$.

363 The following result is a consequence of Lemma 2.10 and results in [22].

364 **Corollary 2.12.** *Let $q = p^f$ with p a prime. For $m \geq 3$, we have $\text{meo}(\text{P}\mathbb{G}\mathbb{O}_{2m+1}(q)) \leq$
 365 $q^{m+1}/(q-1)$ (with q odd), and for $m \geq 4$ and $\varepsilon \in \{+, -\}$, we have $\text{meo}(\text{P}\mathbb{G}\mathbb{O}_{2m}^{\varepsilon}(q)) \leq$
 366 $q^{m+1}/(q-1)$.*

367 *Proof.* If q is odd, then the result follows by comparing $q^{m+1}/(q-1)$ with the maximum
 368 element order of the orthogonal groups obtained in [22]. Now, assume that q is even. It
 369 is well-known that orthogonal groups of characteristic 2 are subgroups of the symplectic
 370 groups, that is, $\text{P}\mathbb{G}\mathbb{O}_{2m}^{\varepsilon}(q) \leq \text{P}\mathbb{C}\mathbb{S}\mathbb{p}_{2m}(q)$, for $\varepsilon \in \{+, -\}$ (see [7, Section 5] or [24,
 371 Table 3.5.C]). It follows from Lemma 2.10 that $\text{meo}(\text{P}\mathbb{G}\mathbb{O}_{2m}^{\varepsilon}(q)) \leq q^{m+1}/(q-1)$, for
 372 $\varepsilon \in \{+, -\}$. \square

373 The next two lemmas will be used for computing the maximum element order for unitary
 374 groups.

375 **Lemma 2.13.** *Let (b_1, \dots, b_t) be a partition of d and let q be a prime power. If $t \geq 2$, then
 376 $\text{lcm}_{i=1}^t \{q^{b_i} - (-1)^{b_i}\} \leq q^{d-1} - (-1)^{d-1}$. Moreover $(q^d - (-1)^d)/(q+1) \leq q^{d-1} - (-1)^{d-1}$.*

377 *Proof.* For the first part of the lemma, we argue by induction on t . Note that $q+1$ divides
 378 $q^{b_i} - (-1)^{b_i}$ for each $i \in \{1, \dots, t\}$. If $t = 2$, then

$$\text{lcm}\{q^{b_1} - (-1)^{b_1}, q^{b_2} - (-1)^{b_2}\} \leq \frac{(q^{b_1} - (-1)^{b_1})(q^{b_2} - (-1)^{b_2})}{q+1} \leq q^{d-1} - (-1)^{d-1}$$

379 (where the last inequality follows from a direct computation). Assume that $t \geq 3$. Now,
 380 by induction, $\text{lcm}_{i=1}^{t-1} \{q^{b_i} - (-1)^{b_i}\} \leq q^{d-b_t-1} - (-1)^{d-b_t-1}$. Therefore

$$\begin{aligned} \text{lcm}_{i=1}^t \{q^{b_i} - (-1)^{b_i}\} &\leq \frac{1}{q+1} \left(\text{lcm}_{i=1}^{t-1} \{q^{b_i} - (-1)^{b_i}\} \right) (q^{b_t} - (-1)^{b_t}) \\ &\leq \frac{(q^{d-b_t-1} - (-1)^{d-b_t-1})(q^{b_t} - (-1)^{b_t})}{q+1} \leq q^{d-1} - (-1)^{d-1} \end{aligned}$$

381 (where the last inequality, as before, follows by a direct computation). The last part of
 382 the lemma is immediate. \square

383 **Lemma 2.14.** *Let $d = d_+ + d_- + e$ with $d_+, d_-, e \geq 0$ and $d \geq 3$, and let $q = p^f$ with p a
 384 prime number and $f \geq 1$. Then*

$$(q^{e-1} - (-1)^{e-1}) \max\{p^{\lceil \log_p(d_+) \rceil}, p^{\lceil \log_p(d_-) \rceil}\} \leq \begin{cases} q^{d-1} - 1 & \text{if } d \text{ is odd and } q > p, \\ (p^{d-2} + 1)p & \text{if } d \text{ is odd and } q = p, \\ q^{d-1} + 1 & \text{if } d \text{ is even and } q > 2, \\ 2^2(2^{d-3} + 1) & \text{if } d \text{ is even and } q = 2. \end{cases}$$

385 *Proof.* Note that $p^{\lceil \log_p(m) \rceil} \leq p^{m-1}$, for every integer $m \geq 1$. Interchanging d_- and d_+ if
 386 necessary, we may assume that $d_- \leq d_+$. If $d_- \geq 1$, then

$$(q^{e-1} - (-1)^{e-1}) \max\{p^{\lceil \log_p(d_+) \rceil}, p^{\lceil \log_p(d_-) \rceil}\} \leq (q^{d-d_+-2} - (-1)^{d-d_+-2})p^{\lceil \log_p(d_+) \rceil}$$

387 and the lemma follows with an easy computation (the polynomial in q on the right-hand
 388 side has degree at most $d - 3$). Thus we may assume that $d_- = 0$. Now, the rest of the
 389 proof follows easily by treating separately the four cases listed. \square

390 Let f be a unitary form. We consider Δ/Z , where Δ is the subgroup of $\mathrm{GL}_d(q^2)$
 391 preserving f up to a scalar multiple, and $Z \cong Z_{q^2-1}$ is the centre of $\mathrm{GL}_d(q^2)$. We claim
 392 that $\Delta = \mathrm{GU}_d(q)Z$, where $\mathrm{GU}_d(q)$ is the subgroup of $\mathrm{GL}_d(q^2)$ preserving f . To see
 393 this, note that, if $g \in \mathrm{GL}_d(q^2)$ maps f to af for some $a \in \mathbb{F}_{q^2}^*$, then for all $v, w \in V$,
 394 we have $af(v, w)^q = af(w, v)$ (since f is unitary), which equals $f(wg, vg) = f(vg, wg)^q =$
 395 $a^q f(v, w)^q$, and hence $a^q = a$. Thus $a \in \mathbb{F}_q$, so $a = b^{q+1}$ for some $b \in \mathbb{F}_{q^2}$ and $g = b(b^{-1}g) \in$
 396 $\mathrm{GU}_d(q)Z$. This proves the claim and thus we have $\Delta/Z \cong \mathrm{GU}_d(q)/(\mathrm{GU}_d(q) \cap Z) =$
 397 $\mathrm{PGU}_d(q)$. For the unitary groups $\mathrm{PSU}_d(q)$ to be simple and different from $\mathrm{PSL}_2(q)$, we
 398 require $d \geq 3$ and $(d, q) \neq (3, 2)$.

Lemma 2.15.

$$\mathrm{meo}(\mathrm{PGU}_d(q)) = \begin{cases} q^{d-1} - 1 & \text{if } d \text{ is odd and } q > p, \\ (p^{d-2} + 1)p & \text{if } d \text{ is odd and } q = p, \\ q^{d-1} + 1 & \text{if } d \text{ is even and } q > 2, \\ 4(2^{d-3} + 1) & \text{if } d \text{ is even and } q = 2. \end{cases}$$

Proof. Let g be an element of $\mathrm{PGU}_d(q)$ and write $g = su = us$ with s semisimple and u
 unipotent. If $g = u$ then, by Lemma 2.2, $|g| \leq p^{\lceil \log_p(d) \rceil} \leq p^{d-1}$ and the result follows. Thus
 we may assume that $s \neq 1$. We use Notation 2.5 for the element s and a corresponding
 element $\bar{s} \in \mathrm{GL}_d(q^2)$. From our remarks above, $\bar{s} = a\bar{r}$ for some $a \in \mathbb{F}_{q^2}^*$ and $\bar{r} \in \mathrm{GU}_d(q)$,
 and hence the \bar{r} -invariant orthogonal decomposition described in (3) is also \bar{s} -invariant.
 Recall that, for $1 \leq i \leq r$, $|y_{ij}|$ divides $q^{d_i} - 1$ and d_i is even, while for $r < i \leq t'$, $|y_{ij}|$
 divides $q^{d_i} + 1$ and d_i is odd (and $t' \geq 1$ since $s \neq 1$). Also the order of $\bar{s}|_{V_{\pm}}$ is 1 if q is
 even and at most 2 if q is odd, and the dimension $d = d_+ + d_- + d_1 m_1 + \cdots + d_{t'} m_{t'}$. Thus
 $|s|$ divides $\prod_{i=1}^{t'} (q^{d_i} - (-1)^{d_i})$. Moreover, combining Notation 2.5 and Proposition 2.6
 (together with the description of the maximal tori of $\mathrm{GU}_d(q)$ [7, 22]), we see that the
 order of g is at most

$$\mathrm{lcm}_{i=1}^{t'} \{q^{d_i} - (-1)^{d_i}\} \cdot \max\{p^{\lceil \log_p(d_{\pm}) \rceil}, p^{\lceil \log_p(m_i) \rceil} \mid i = 1, \dots, t'\}.$$

399 if $t' > 1$, and it is at most

$$(q^{d_1} - (-1)^{d_1}) \cdot \max\{p^{\lceil \log_p(d_{\pm}) \rceil}, p^{\lceil \log_p(m_1) \rceil}\}$$

400 if $t' = 1$. Using Lemma 2.4 and arguing exactly as in the proof of Lemma 2.10, we see
 401 that by replacing g if necessary by an element of larger or equal order, we may assume
 402 that $m_i = 1$ for every $i \in \{1, \dots, t'\}$, with the exception of at most two values of i such

403 that $(q, d_i, m_i) = (2, 1, 3)$ and such that g induces an element of order $(q+1)p^{\lceil \log_p(m_i) \rceil} =$
 404 $3 \cdot 2^2 = 12$ on $V_{i,1} \perp V_{i,2} \perp V_{i,3}$. However, in these exceptional cases we have $q = 2$ and the
 405 restriction of the element g to $V_{i,1} \perp V_{i,2} \perp V_{i,3}$ is an element of $\text{PGU}_3(2)$, modulo scalars,
 406 and the maximum order of such elements is 6 rather than 12. Thus in these cases we
 407 have overestimated the order by a factor of 2; we may replace the restriction of g to this
 408 space by an element inducing an element of order 3 on $V_{i,1}$ and an element of order 2 on
 409 $V_{i,2} \perp V_{i,3}$ (thus increasing the dimension of V_+ by 2). In this way, even if the exceptional
 410 cases occur, we obtain an element attaining the maximum order for which $m_i = 1$ for
 411 every $i \in \{1, \dots, t'\}$. Thus we see that

$$|g| \leq \begin{cases} (q^{d-d_+-d_-} - (-1)^{d-d_+-d_-}) \max\{p^{\lceil \log_p(d_{\pm}) \rceil}\} & \text{if } t' = 1; \\ \text{lcm}_{i=1}^{t'} \{q^{d_i} - (-1)^{d_i}\} \max\{p^{\lceil \log_p(d_{\pm}) \rceil}\} & \text{if } t' \geq 2. \end{cases}$$

412 Using Lemma 2.13, it follows that in both cases

$$|g| \leq (q^{d-d_+-d_- - 1} - (-1)^{d-d_+-d_- - 1}) \max\{p^{\lceil \log_p(d_{\pm}) \rceil}\}$$

413 and the proof follows in these cases from Lemma 2.14.

414 From the description of the semisimple elements given above it is easy to see that
 415 $\text{PGU}_d(q)$ contains an element g with $|g|$ achieving the stated value of $\text{meo}(\text{PGU}_d(q))$. For
 416 example, when d is odd and $q > p$, it suffices to take g a semisimple element of order
 417 $q^{d-1} - 1$ in the maximal torus of order $(q+1)(q^{d-1} - 1)$. Similarly, when d is even and
 418 $q = 2$, it suffices to fix a 3-dimensional non-degenerate subspace W and take $g = su = us$,
 419 with s a semisimple element of order $p^{d-3} + 1$ on W^\perp and u an element of order 4 on W .
 420 The other two cases are similar. \square

421 Finally, combining all the results we have obtained for the non-abelian simple classical
 422 groups and Lang's theorem, we are ready to give a proof of Theorem 2.16.

Simple Group T	$\text{meo}(\text{Aut}(T))$	Remark
$\text{PSL}_d(q)$	$(q^d - 1)/(q - 1)$ 6 8	$(d, q) \neq (2, 4), (3, 2)$ $(d, q) = (2, 4)$ $(d, q) = (3, 2)$
$\text{PSU}_d(q)$	$q^{d-1} - 1$ 16 $(p^{d-2} + 1)p$ 24 $q^{d-1} + 1$ $4(2^{d-3} + 1)$	d odd, $q > p$ and $(d, q) \neq (3, 4)$ $(d, q) = (3, 4)$ d odd, $q = p$ and $(d, q) \neq (5, 2)$ $(d, q) = (5, 2)$ d even and $q > 2$ d even and $q = 2$
$\text{PSp}_{2m}(q)$	$\leq q^{m+1}/(q - 1)$	$(m, q) \neq (2, 2)$
$\text{PSp}_4(2)$	10	$(m, q) = (2, 2)$
$\text{P}\Omega_{2m+1}(q)$	$\leq q^{m+1}/(q - 1)$	
$\text{P}\Omega_{2m}^+(q)$	$\leq q^{m+1}/(q - 1)$	
$\text{P}\Omega_{2m}^-(q)$	$\leq q^{m+1}/(q - 1)$	

TABLE 3. Maximum element order of $\text{Aut}(T)$ for T a non-abelian simple classical group

423 **Theorem 2.16.** *For a classical simple group T as in column 1 of Table 3, the value of*
 424 *$\text{meo}(\text{Aut}(T))$ is as in column 2 of Table 3.*

425 *Proof.* As usual, we write $q = p^f$ for some prime p . For each of the classical groups
 426 $\text{PGL}_d(q)$, $\text{PCSp}_{2m}(q)$, $\text{PGO}_{2m+1}(q)$ and $\text{PGO}_{2m}^+(q)$, let X be the corresponding algebraic
 427 group over the algebraic closure of the finite field \mathbb{F}_q . Let $F : X \rightarrow X$ be a Lang–Steinberg

map for X . We denote the group of fixed points of F by $X^F(q)$. In particular, $X^F(q)$ is one of the following groups: $\mathrm{PGL}_d(q)$ or $\mathrm{PGU}_d(q)$ (when X is of type A_{d-1}), $\mathrm{PGO}_{2m+1}(q)$ (when X is of type B_m), $\mathrm{PCSp}_{2m}(q)$ (when X is of type C_m), a subgroup of index two of $\mathrm{PGO}_{2m}^+(q)$ or $\mathrm{PGO}_{2m}^-(q)$ (when X is of type D_m ; namely $(\mathrm{GO}_{2m}^\pm(q)^\circ)/Z(\mathrm{GO}_{2m}^\pm(q)^\circ)$ where $\mathrm{GO}_{2m}^\pm(q)^\circ$ is the subgroup of $\mathrm{GO}_{2m}^\pm(q)$ that stabilizes each of the two $\mathrm{SO}_{2m}^\pm(q)$ -orbits of m -dimensional totally singular subspaces; see [8, p. 39-41]). Write $Y = \mathrm{PGO}_{2m}^+(q)$ or $\mathrm{PGO}_{2m}^-(q)$, as appropriate, in these last cases, and in all other cases write $Y = X^F(q)$.

Let T be the socle of $X^F(q)$. From [9, Table 5, page xvi], the automorphism group A of T is $(Y \rtimes \langle \phi \rangle) \cdot \Gamma$ where ϕ is a generator of the group of field automorphisms and Γ is the group of graph automorphisms of the corresponding Dynkin diagram. In particular, $|\Gamma| \in \{1, 2, 6\}$ and in fact $|\Gamma| = 6$ if and only if $T = \mathrm{P}\Omega_8^+(q)$. Moreover, $|\Gamma| = 2$ if and only if $T = \mathrm{PSL}_d(q)$ with $d \geq 3$, $T = \mathrm{P}\Omega_{2m}^+(q)$ with $m \geq 5$, or $T = \mathrm{PSp}_4(2^f)$.

First suppose that $g \in Y \rtimes \langle \phi \rangle$. Then $g = x\psi^{-1}$ with $x \in Y$, where ψ is an element of order e in $\langle \phi \rangle$. We have $|\langle \phi \rangle| = 2f$ if and only if $Y = \mathrm{PGU}_d(q)$ or $Y = \mathrm{PGO}_{2m}^-(q)$, and $|\langle \phi \rangle| = f$ otherwise (see [9, Table 5, page xvi] for example).

If $\psi = 1$, then $g \in Y$ and $|g|$ is at most the bound in Table 3, by the results in Corollaries 2.7 and 2.12, and Lemmas 2.10 and 2.15. So suppose that $\psi \neq 1$; that is $e \geq 2$. Observe that when $X^F(q)$ is untwisted, ψ is the restriction to $X^F(q)$ of the Lang–Steinberg map σ_{q_0} (where $q_0^e = q$), which by abuse of notation, we also denote by ψ . When $X^F = \mathrm{PGU}_d(q)$ or $P(\mathrm{GO}_{2m}^-(q)^\circ)$, then $F = \sigma_q \tau$, where τ is a graph automorphism of X induced from the order 2 symmetry of the Dynkin diagram, and ψ is the restriction to $X^F(q)$ of the Lang–Steinberg map $\sigma_{q_0} \tau$ when e is odd (and where $q_0^e = q$) and σ_{q_0} when $e = 2k$ is even, (and where $q_0^k = q$). As in the untwisted case, by abuse of notation we also denote these maps by ψ .

By Lang’s theorem, there exists a in the algebraic group X such that $aa^{-\psi} = x$. Observe that $(x\psi^{-1})^e = xx^\psi \cdots x^{\psi^{e-2}} x^{\psi^{e-1}}$ and write $z = a^{-1}(x\psi^{-1})^e a$. Now observe further that

$$\begin{aligned} (6) \quad z^\psi &= a^{-\psi}(x^\psi x^{\psi^2} \cdots x^{\psi^{e-1}} x^{\psi^e}) a^\psi = a^{-\psi}(x^\psi x^{\psi^2} \cdots x^{\psi^{e-1}} x) a^\psi \\ &= (a^{-\psi} x^{-1})(xx^\psi \cdots x^{\psi^{e-1}})(xa^\psi) = a^{-1}(xx^\psi \cdots x^{\psi^{e-1}}) a = a^{-1}(x\psi^{-1})^e a = z \end{aligned}$$

and so z is invariant under the Lang–Steinberg map ψ . It follows that in the untwisted cases $z \in Y(q^{1/e})$, where $Y(q^{1/e}) = \mathrm{PGL}_d(q^{1/e})$, $\mathrm{PGO}_{2m+1}(q^{1/e})$, $\mathrm{PCSp}_{2m}(q^{1/e})$, $\mathrm{GO}_{2m}^+(q^{1/e})^\circ/Z(\mathrm{GO}_{2m}^+(q^{1/e})^\circ)$. If Y is twisted and e is odd then $z \in Y(q^{1/e})$ where $Y(q^{1/e}) = \mathrm{PGU}_d(q^{1/e})$, $\mathrm{GO}_{2m}^-(q^{1/e})^\circ/Z(\mathrm{GO}_{2m}^-(q^{1/e})^\circ)$. So unless Y is twisted and e is even we have

$$|g| = |x\psi^{-1}| \leq e|(x\psi^{-1})^e| = e|z| \leq e \operatorname{meo}(Y(q^{1/e})).$$

Using the bounds obtained in Corollaries 2.7 and 2.12, and Lemmas 2.10 and 2.15 for $\operatorname{meo}(Y(q^{1/e}))$ and $\operatorname{meo}(Y)$, we can show (by a straightforward calculation) that the quantity $e \operatorname{meo}(Y(q^{1/e})) \leq \operatorname{meo}(Y)$ unless $Y = X^F(q) = \mathrm{PGL}_2(4)$, and in this case $|g| \leq 6$ (see line 2 of Table 3). If Y is twisted and $e = 2k$ is even, then $z \in \mathrm{PGL}_d(q^{1/k})$ or $\mathrm{GO}_{2m}^+(q^{1/k})^\circ/Z(\mathrm{GO}_{2m}^+(q^{1/k})^\circ)$ and similar arguments eliminate these cases unless $e = 2$ (and ψ induces a graph involution in the terminology of [17]). But in this case, we appeal to the element order preserving bijection between $\langle \mathrm{PGL}_n(q), \tau \rangle$ conjugacy classes in the coset $\mathrm{PGL}_n(q)\tau$ and $\langle \mathrm{PGU}_n(q), \tau \rangle$ conjugacy classes in the coset $\mathrm{PGU}_n(q)\tau$. See [18, Lemmas 2.1–2.3] for details. Thus the case of $e = 2$ and $Y = \mathrm{PGU}_d(q)$ can be covered by the case of $g = x\tau$ and $Y = \mathrm{PGL}_d(q)$ below. Similarly, by [18, Lemmas 2.1–2.3] the case $e = 2$ and $Y = \mathrm{PGO}_{2m}^-(q)$ is covered by the case of $g = x\tau$, $Y = \mathrm{PGO}_{2m}^+(q)$ below.

Thus we assume that $g \notin Y \rtimes \langle \phi \rangle$ from now on. In particular, T is either $\mathrm{PSL}_d(q)$ (with $d \geq 3$), $\mathrm{PSp}_4(2^f)$, or $\mathrm{P}\Omega_{2m}^+(q)$ (that is, T is a simple classical group admitting a non-trivial graph automorphism). We deal with each of these three cases separately.

CASE $Y = X^F(q) = \mathrm{PGL}_d(q)$.

474 We may assume that $g = x\psi^{-1}\tau$, with $x \in X^F(q)$, ψ an element of order e in $\langle\phi\rangle$ and τ
 475 the inverse-transpose automorphism. In particular, $d \geq 3$.

476 First suppose that $\psi = 1$ and set $y = g^2 = xx^{-tr}$, where x^{tr} denotes the transpose of
 477 the matrix x . The possibilities for y are described explicitly in [16, Theorem 4.2]:

- 478 (1) if $\theta(t)^k$ is an elementary divisor of y , then so is $\bar{\theta}(t)^k$ (and with the same multi-
 479 plicity), where $\bar{\theta}(t) = t^{\deg\theta}\theta(1/t)/\theta(0)$;
- 480 (2) the elementary divisors $(t-1)^{2k}$ occur with even multiplicity for $k = 1, 2, \dots$;
- 481 (3) if q is odd, the elementary divisors $(t+1)^{2k+1}$ occur with even multiplicity for
 482 $k = 1, 2, \dots$

483 Now $\mathrm{Sp}_{2n}(q)$ contains elements z with elementary divisors satisfying the following prop-
 484 erties (see [15, p. 210] and [16, Corollary 5.3]):

- 485 (1) if $\theta(t)^k$ is an elementary divisor of z , then so is $\bar{\theta}(t)^k$ (with the same multiplicity);
- 486 (2) the elementary divisors $(t-1)^{2k+1}$ occur with even multiplicity for $k = 1, 2, \dots$;
- 487 (3) the elementary divisors $(t+1)^{2k+1}$ occur with even multiplicity for $k = 1, 2, \dots$

488 Thus, either (i) y is conjugate to an element of $\mathrm{Sp}_d(q)$ (and d is even), or (ii) an elementary
 489 divisor $(t-1)^{2k+1}$ occurs with odd multiplicity. In case (i), $|g| \leq 2q^{d/2+1}/(q-1)$ by
 490 Lemma 2.10, which is at most $(q^d-1)/(q-1)$ unless $(d, q) = (4, 2)$. If (ii) holds then
 491 y is conjugate to $u + y'$ for $u = J_{2k_1+1} + \dots + J_{2k_i+1} \in \mathrm{GL}_{d'}(q)$ and $y' \in \mathrm{Sp}_{d-d'}(q)$; in
 492 particular,

$$|g| \leq 2 \max_i \{p^{\lceil \log_p(2k_i+1) \rceil}\} \mathrm{meo}(\mathrm{Sp}_{d-d'}(q)).$$

493 Clearly, to bound the right hand side, it suffices to bound $p^{\lceil \log_p(2k+1) \rceil} \mathrm{meo}(\mathrm{Sp}_{d-2k-1}(q))$.
 494 For $d = 3$, either $k = 1$ and $|g| = 2|J_3|$ or $k = 0$ and $|g| \leq 2 \mathrm{meo}(\mathrm{Sp}_2(q)) = 2q + 2$; thus
 495 $|g| \leq (q^3-1)/(q-1)$ unless $q = 2$. If $d \geq 4$, then by Lemma 2.10 we have (in case (ii))

$$|g| \leq 2p^{\lceil \log_p(2k+1) \rceil} q^{(d-2k+1)/2}$$

496 which we can check is at most $(q^d-1)/(q-1)$ unless $(d, q) = (4, 2), (5, 2)$. The exceptional
 497 cases $(d, q) = (3, 2), (4, 2), (5, 2)$ from (i) and (ii) can be dealt with by direct computation,
 498 and we note that the first case appears in line 3 of Table 3.

499 Next, suppose that ψ is a non-trivial element of even order e . By Lang's theorem, there
 500 exists a in the algebraic group X with $aa^{-\psi\tau} = x$. Note that since ψ and τ commute,
 501 the element $\psi\tau$ has order e . Now the same argument as in (6) shows that $z = a^{-1}g^e a$ is
 502 fixed by $\psi\tau$. Therefore g^e is X -conjugate to an element in $X^\sigma(q^{1/e}) = \mathrm{PGU}_d(q^{1/e})$ where
 503 $\sigma = \tau F^{1/e}$ and so $|g| \leq e \mathrm{meo}(\mathrm{PGU}_d(q^{1/e}))$. Lemma 2.15 implies that the right hand side
 504 is less than $(q^d-1)/(q-1)$ for $d \geq 3$.

505 It remains to consider the case where $\psi \in \langle\phi\rangle$ has odd order $e \geq 3$. In this case,
 506 $g^2 \in \mathrm{P}\Gamma\mathrm{L}_d(q)$ and the argument for field automorphisms applied to g^2 shows that $|g| \leq$
 507 $2e(q^{d/e}-1)/(q^{1/e}-1)$, and the right hand side is less than $(q^d-1)/(q-1)$ for $e \geq 3$.

508 CASE $T = \mathrm{PSp}_4(q)$ WITH $q = 2^f$.

509 The cases where $f = 1, 2$ can be treated by a direct calculation (or with the invaluable
 510 help of `magma` [6]). Thus we may assume that $f \geq 3$. We have $g \notin X^F(q) \rtimes \langle\phi\rangle$, and we
 511 note that $g^2 \in X^F(q) \rtimes \langle\phi\rangle$.

512 First suppose that $g^2 \notin X^F(q)$. Then $g^2 = x'\psi'$, for some $x' \in X^F(q)$ and for some field
 513 automorphism ψ' of order $e \geq 2$. The same argument as in the previous case shows that
 514 $|g| = 2|g^2| \leq 2e \mathrm{meo}(X^F(q^{1/e}))$. Applying Lemma 2.10 implies that $|g| \leq 2eq^{3/e}/(q^{1/e}-1)$,
 515 which is bounded above by $q^3/(q-1)$ as required.

516 So we may assume that $g^2 \in X^F(q)$. Since $g \notin X^F(q)$, the element g projects to an
 517 element of order 2 in $\mathrm{Out}(T)$. Now $\mathrm{Out}(T)$ is cyclic of order $2f$ and is generated by the
 518 extraordinary ‘‘graph automorphism’’. In particular, if f were even, then g^2 would not lie
 519 in $X^F(q)$. Hence f is odd. We note that g^2 cannot have order q^2-1 or q^2+1 , as in these

520 cases $g^2 \in \mathbf{C}_{\mathrm{PSP}_4(q)}(g^{|g^2|})$ and $g^{|g^2|}$ is an outer involution whose centralizer in $\mathrm{PSP}_4(q)$ is
 521 isomorphic to ${}^2\mathrm{B}_2(q)$ by [2, (19.5)]. This is not possible since the Suzuki groups do not
 522 contain elements of order $q^2 \pm 1$. It now follows from an analysis of the element orders in
 523 $\mathrm{PSP}_4(q)$ that $|g^2| \leq (q^2 + 1)/2 \leq q^3/(2(q - 1))$ (see (4)). Hence $|g| \leq q^3/(q - 1)$.

524 CASE $T = \mathrm{P}\Omega_{2m}^+(q)$.

525 We may assume that $g = x\psi^{-1}\tau$, where $x \in \mathrm{PGO}_{2m}^+(q)$, $\psi \in \langle \phi \rangle$ (the group of field auto-
 526 morphisms) and ψ has order $e \geq 1$, and in this case we let τ denote a graph automorphism
 527 of order 2 or 3. If $e = 1$ and τ has order 2 then $g \in \mathrm{PGO}_{2m}^+(q)$ and Corollary 2.12 applies.

528 If τ has order 2 and $e \geq 2$ then we consider three cases: If $e \geq 4$ and e is even, then
 529 $g^2 \in Y.\langle \phi \rangle$ is in the Y -coset of a field automorphism of order $e/2$. Arguing as above we
 530 find that g^e is X -conjugate to an element in $X^{F^{2/e}}(q^{2/e}) = P(\mathrm{GO}_{2m}^{\epsilon'}(q^{2/e})^\circ)$ [8, p. 40]
 531 and $|g| \leq eq^{2(m+1)/e}/(q^{2/e} - 1)$ by Corollary 2.12. If $e \geq 3$ and e is odd then g^2 is in
 532 the Y -coset of a field automorphism of order e and so g^{2e} is X -conjugate to an element
 533 in $X^{F^{1/e}}(q^{1/e}) = P(\mathrm{GO}_{2m}^{\epsilon'}(q^{1/e})^\circ)$; therefore $|g| \leq 2eq^{(m+1)/e}/(q^{1/e} - 1)$. If $e = 2$ then,
 534 picking $a \in X$ such that $x = aa^{-\psi\tau}$, we can show that $a^{-1}g^2a$ is fixed by $\tau\psi$ (in the same
 535 way as in (6)); thus g^2 is conjugate to an element of $P(\mathrm{GO}_{2m}^-(q^{1/2})^\circ)$ [17, 4.9.1(a),(b)] and
 536 $|g| \leq 2q^{(m+1)/2}/(q^{1/2} - 1)$. In all three cases, a direct calculation shows that the upper
 537 bounds we have found are less than $q^{m+1}/(q - 1)$ for all q and all $m \geq 4$.

538 Now suppose that τ has order 3 so that $m = 4$. If $e = 1$ then $g \in \mathrm{P}\Omega_8^+(q).\mathrm{Sym}(3)$ if
 539 q is even, and $g \in \mathrm{P}\Omega_8^+(q).\mathrm{Sym}(4) = \mathrm{PGO}_8^+(q).3$ if q is odd (see [?, p. 75] for example).
 540 Since $(2, q - 1)^2.\mathrm{P}\Omega_8^+(q).\mathrm{Sym}(3)$ is a subgroup of $\mathrm{F}_4(q)$ (see [31, Table 5.1]), it follows
 541 that $|g| \leq \mathrm{meo}(\mathrm{F}_4(q))$ and the bound $|g| \leq q^5/(q - 1)$ follows from [22] when q is odd and
 542 from [37] when q is even.

543 Finally, if τ has order 3 and $e \geq 2$, then $g^3 \in Y \rtimes \langle \phi \rangle$. If $e \neq 3$ then g^3 is in the Y -coset of
 544 a field automorphism of order e' say, where $e' \geq 2$. Therefore $|g| \leq 3e'q^{(m+1)/e'}/(q^{1/e'} - 1)$
 545 for some $e' \geq 2$. If $e = 3$ then, picking a in the algebraic group X such that $x = aa^{-\psi\tau}$,
 546 we can show that $a^{-1}g^3a$ is fixed by $\tau\psi$; thus $a^{-1}g^3a$ is an element of ${}^3\mathrm{D}_4(q^{1/3})$ [17,
 547 4.9.1(a),(b)]. It follows that $|g| \leq 3\mathrm{meo}({}^3\mathrm{D}_4(q^{1/3}))$, which is at most $3(q - 1)(q^{1/3} + 1)$
 548 by [22] for q odd, and by [11, Tables 1.1 and 2.2a] for q even, unless $q^{1/3} = 2$. For $q^{1/3} = 2$,
 549 we have $\mathrm{meo}({}^3\mathrm{D}_4(2)) = 28$ using [9]. In all three cases, a direct computation shows that
 550 our upper bounds are at most $q^{m+1}/(q - 1)$ for all $m \geq 4$, as required. \square

551

3. PERMUTATION REPRESENTATIONS OF NON-ABELIAN SIMPLE GROUPS

552 In this section we collect in Table 4 some results from the literature describing the
 553 minimal degree of a permutation representation of each simple group of Lie type. For the
 554 simple classical groups this information is obtained from [24, Table 5.2.A] (which in turn
 555 came from [10]) and for the exceptional groups of Lie type it is obtained from [40], [41,
 556 Theorems 1, 2 and 3], and [42, Theorems 1, 2, 3 and 4]. We note that the rows correspond-
 557 ing to the classical groups $\mathrm{P}\Omega_{2m}^+(q)$ and $\mathrm{PSU}_{2m}(2)$ in [24, Table 5.2.A] are incorrect and
 558 our Table 4 takes into account the corrections that were brilliantly spotted by Mazurov
 559 and Vasil'ev [33] in 1994.

Group	Degree of Min. Perm. Repres.	Condition
$\mathrm{PSL}_d(q)$ $\mathrm{PSL}_2(q), \mathrm{PSL}_4(2)$	$\frac{q^d - 1}{q - 1}$ 5, 7, 6, 11, 8	$(q, d) \neq (2, 5), (2, 7),$ $(2, 9), (2, 11), (4, 2)$ $q = 5, 7, 9, 11$
$\mathrm{PSp}_{2m}(q)$ $\mathrm{PSp}_{2m}(2)$ $\mathrm{PSp}_4(2)', \mathrm{PSp}_4(3)$	$\frac{q^{2m} - 1}{q - 1}$ $2^{m-1}(2^m - 1)$ 6, 27	$m \geq 2, q > 2, (m, q) \neq (2, 3)$ $m \geq 3$
$\mathrm{P}\Omega_{2m+1}(q)$ $\mathrm{P}\Omega_{2m+1}(3)$	$\frac{q^{2m} - 1}{q - 1}$ $3^m(3^m - 1)/2$	$m \geq 3, q \geq 5$ $m \geq 3$
$\mathrm{P}\Omega_{2m}^+(q)$ $\mathrm{P}\Omega_{2m}^+(3)$ $\mathrm{P}\Omega_{2m}^+(2)$	$\frac{(q^m - 1)(q^{m-1} + 1)}{q - 1}$ $3^{m-1}(3^m - 1)/2$ $2^{m-1}(2^m - 1)$	$m \geq 4, q \geq 4$ $m \geq 4$ $m \geq 4$
$\mathrm{P}\Omega_{2m}^-(q)$	$\frac{(q^m + 1)(q^{m-1} - 1)}{q - 1}$	$m \geq 4$
$\mathrm{PSU}_3(q)$ $\mathrm{PSU}_3(5)$ $\mathrm{PSU}_4(q)$ $\mathrm{PSU}_d(q)$ $\mathrm{PSU}_{2m}(2)$	$q^3 + 1$ 50 $\frac{(q + 1)(q^3 + 1)}{q^2 - 1}$ $\frac{(q^d - (-1)^d)(q^{d-1} - (-1)^{d-1})}{q^2 - 1}$ $2^{2m-1}(2^{2m} - 1)/3$	$q \neq 5$ $d \geq 5, d$ odd or, d even and $q \neq 2$ $m \geq 3$
$\mathrm{G}_2(q)$ $\mathrm{G}_2(3)$ $\mathrm{G}_2(4)$ $\mathrm{F}_4(q)$ $\mathrm{E}_6(q)$ $\mathrm{E}_7(q)$ $\mathrm{E}_8(q)$	$\frac{q^6 - 1}{q - 1}$ 351 416 $\frac{(q^{12} - 1)(q^4 + 1)}{q - 1}$ $\frac{(q^9 - 1)(q^8 + q^4 + 1)}{q - 1}$ $\frac{(q^{14} - 1)(q^9 + 1)(q^5 - 1)}{q - 1}$ $\frac{(q^{30} - 1)(q^{12} + 1)(q^{10} + 1)(q^6 + 1)}{q - 1}$	$q > 4$
${}^2\mathrm{B}_2(q)$ ${}^2\mathrm{G}_2(q)$ ${}^3\mathrm{D}_4(q)$ ${}^2\mathrm{E}_6(q)$ ${}^2\mathrm{F}_4(q)$	$q^2 + 1$ $q^3 + 1$ $\frac{(q^8 + q^4 + 1)(q + 1)}{(q^{12} - 1)(q^6 - q^3 + 1)(q^4 + 1)}$ $\frac{q - 1}{(q^6 + 1)(q^3 + 1)(q + 1)}$	$q = 2^f, f$ odd $q = 3^f, f$ odd $q = 2^f$

TABLE 4. Degree of the minimal permutation representations

561 In this section, we prove Theorem 1.2 by determining the finite non-abelian simple
562 groups T for which $\mathrm{meo}(\mathrm{Aut}(T)) \geq m(T)/4$.

563 *Proof of Theorem 1.2.* Let T be a finite non-abelian simple group and write $o(T) =$
 564 $\text{meo}(\text{Aut}(T))$ and $m(T)$ for the minimal degree of a faithful permutation representation
 565 of T . First, we quickly deal with the cases where T is an alternating group or a sporadic
 566 group. Then we may assume that T is a simple group of Lie type, where the situation
 567 is more complex. If $T = \text{Alt}(m)$ (and $m \geq 5$), then the minimal degree of a permuta-
 568 tion representation of T is m . Since $\text{Aut}(T)$ contains an element of order m , we have
 569 $\text{meo}(\text{Aut}(T)) \geq m$ and so T is one of the exceptions in the statement of the theorem. Sim-
 570 ilarly, if T is a sporadic simple group (including the Tits group), then the proof follows
 571 from a case-by-case analysis using [9].

572 If T is a classical group, then the theorem follows by comparing Table 3 with Table 4.
 573 We find that if $o(T) \geq m(T)/4$, then either $T = \text{PSL}_d(q)$ or T belongs to a short list of
 574 exceptions. These exceptions are then analysed using `magma`.

575 Now suppose that T is a finite exceptional group. As one might expect, we consider the
 576 possibilities for the Lie type of T on a case-by-case basis. Complete information on $m(T)$
 577 is listed in Table 4. We shall use repeatedly the inequalities

$$(7) \quad o(T) \leq \text{meo}(\text{Out}(T)) \text{meo}(T) \leq |\text{Out}(T)| \text{meo}(T).$$

578 Detailed information on $|\text{Out}(T)|$ and on the group-structure of $\text{Out}(T)$ can be found
 579 in [9, Table 5, page xvi].

580 When T has odd characteristic, we use the explicit formula for $\text{meo}(T)$ (see [22]) together
 581 with (7) to obtain upper bounds on $o(T)$. These bounds suffice to show that $o(T) <$
 582 $m(T)/4$ when $T = \text{E}_6(q)$, ${}^2\text{E}_6(q)$, $\text{E}_7(q)$, $\text{E}_8(q)$, $\text{F}_4(q)$, $\text{G}_2(q)$, ${}^3\text{D}_4(q)$ or ${}^2\text{G}_2(3^f)$.

583 Now suppose that T has even characteristic; in this case there is no known formula for
 584 $\text{meo}(T)$. In some cases we therefore use *ad hoc* arguments.

585 First suppose that $T = {}^2\text{B}_2(2^{2k+1})$ with $k \geq 1$. From [9, Table 5, page xvi], we see that
 586 $|\text{Out}(T)| = 2k + 1$. It follows from [38] that $\text{meo}(T) = 2^{2k+1} + 2^{k+1} + 1$. In particular,
 587 $o(T) \leq (2k + 1)(2^{2k+1} + 2^{k+1} + 1)$ and $(2k + 1)(2^{2k+1} + 2^{k+1} + 1) < m(T)/4$ in all cases.

588 For the other exceptional groups we observe that every element $g \in T$ can be written
 589 uniquely as $g = su = us$, with s semisimple and u unipotent. In particular,

$$|g| = |s||u| \leq |s_{\max}||u_{\max}|$$

590 where s_{\max} is a semisimple element in T of maximum order and u_{\max} is a unipotent
 591 element in T of maximum order. Suppose that $T = \text{E}_6(2^f)$. By [9, Table 5, page xvi],
 592 we have $|\text{Out}(T)| = 2f(3, 2^f - 1)$. The description of the maximal tori of T in [23,
 593 Section 2.7] implies that the maximum order of a semisimple element of T is at most
 594 $\alpha = (q + 1)(q^5 - 1)/(3, q - 1)$. From [27, Table 5] we see that the maximum order of a
 595 unipotent element in $\text{E}_6(q)$ is $16 = |u_{\max}|$ when q is even. Summing up, we have

$$(8) \quad o(T) \leq \alpha |u_{\max}| |\text{Out}(T)|,$$

596 and the right hand side in our case is $32f(2^f + 1)(2^{5f} - 1)$. A direct computation shows
 597 that the inequality $32f(2^f + 1)(2^{5f} - 1) < m(T)/4$ holds for all $f \geq 1$.

598 This argument works for nearly all of the other exceptional groups in even characteristic.
 599 We list these cases in Table 4. For the reader's convenience we list the formulas for
 600 $|\text{Out}(T)|$ in column 4 of Table 4 for all q (not necessarily of the form $q = 2^f$). For nearly
 601 all values of $q = 2^f$, we have

$$(9) \quad m(T)/4 > \alpha |u_{\max}| |\text{Out}(T)|;$$

602 Column 5 of Table 4 lists the only values of $q = 2^f$ for which the inequality in (9) fails.

603 In view of Column 5 of Table 4, it remains to consider $T = \text{G}_2(4)$ and ${}^3\text{D}_4(2)$. In the
 604 first case we see from [9, page 97] that the maximum element order of $\text{Aut}(\text{G}_2(4))$ is 24
 605 and so $24 = o(T) < m(T)/4 = 104$. In the second case we see from [9, page 89] that the
 606 maximum element order of $\text{Aut}({}^3\text{D}_4(2))$ is 24 and so $24 = o(T) < m(T)/4 = 819/4$. \square

T	α where $ s_{\max} \leq \alpha$	$ u_{\max} $	$ \text{Out}(T) $	2^f where (9) fails
$E_6(2^f)$	$(2^f + 1)(2^{5f} - 1)/(3, q - 1)$	16	$2f(3, q - 1)$	—
$E_7(2^f)$	$(q + 1)(q^2 + 1)(q^4 + 1)$	32	$f(2, q - 1)$	—
$E_8(2^f)$	$(q + 1)(q^2 + q + 1)(q^5 - 1)$	32	f	—
$F_4(2^f)$	$(q + 1)(q^3 - 1)$	16	$f(2, p)$	—
$G_2(2^f)$ ($f \geq 2$)	$q^2 + q + 1$	8	$f(3, p)$	4
${}^3D_4(2^f)$	$q^4 + q^3 - q - 1$	8	$3f$	2
${}^2E_6(2^f)$	$(q + 1)(q^2 + 1)(q^3 - 1)/(3, q + 1)$	16	$2f(3, q + 1)$	—
${}^2F_4(2^f)$ ($f \geq 3$)	$q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$	16	f	—

TABLE 5. Calculations in proof of Theorem 1.2

607

5. PROOF OF THEOREM 1.3

608 In this section, we classify the primitive permutation groups of degree n that contain
609 an element of order at least $n/4$. Our proof proceeds according to the O’Nan–Scott type
610 of the primitive permutation group G , and we use the notation for these types discussed
611 in Subsection 1.1. We treat the almost simple AS and the simple diagonal SD types in
612 separate subsections, and then consider the other types to complete the proof.

613 **5.1. Proof of Theorem 1.3 for almost simple groups.** In this subsection we prove
614 Theorem 1.3 for primitive groups of AS type. We start with a series of very technical
615 lemmas concerning $\text{GL}_d(q)$ and the affine general linear group $\text{AGL}_d(q)$.

616 **Lemma 5.1.** *Let $d \geq 2$ and let K be the subgroup of $\text{GL}_d(q)$ containing $\text{SL}_d(q)$ that*
617 *satisfies $|\text{GL}_d(q) : K| = \gcd(d + 1, q - 1)$. Assume that there exists $H \leq K$ with $|K : H| \leq$*
618 *8. Then either $d = 2$ and $q \in \{2, 3, 4, 5, 7\}$, or $d \in \{3, 4\}$ and $q = 2$, or $\text{SL}_d(q) \leq H$.*

619 *Proof.* Write $G = \text{GL}_d(q)$, $S = \text{SL}_d(q)$ and let $Z = Z(S)$. Now either $(H \cap S)Z/Z$ equals
620 S/Z or $(H \cap S)Z/Z$ is a proper subgroup of the simple group $S/Z \cong \text{PSL}_d(q)$ of index at
621 most 8. In the former case, since S is a perfect group, we find that $S = S' = ((H \cap S)Z)' =$
622 $(H \cap S)' \leq H \cap S \leq H$. Checking Table 4, we see that in the latter case we must have $d = 2$
623 and $q \in \{2, 3, 4, 5, 7, 9\}$, or $d \in \{3, 4\}$ and $q = 2$. If $d = 2$ and $q = 9$ then $K = \text{GL}_2(9)$ and
624 we check using [9] that if H is a subgroup of index at most 8 in K , then $S \leq H$. \square

625 **Lemma 5.2.** *Let $d \geq 2$ and let K be the subgroup of $\text{AGL}_d(q)$ containing $\text{ASL}_d(q)$ that*
626 *satisfies $|\text{AGL}_d(q) : K| = \gcd(d + 1, q - 1)$. Suppose that $H \leq K$ satisfies $|K : H| \leq 8$*
627 *and $H = \mathbf{N}_K(H)$. Then either $K = H$, or $d = 2$ and $q \in \{2, 3, 4, 5, 7\}$, or $d \in \{3, 4\}$ and*
628 *$q = 2$.*

629 *Proof.* Write $G = \text{AGL}_d(q)$ and $S = \text{SL}_d(q)$, and assume that $K > H$. Let V be the
630 socle of G . Now $|K/V : HV/V| \leq 8$ and K/V is isomorphic to the subgroup of $\text{GL}_d(q)$
631 containing $\text{SL}_d(q)$ of index $\gcd(d + 1, q - 1)$. By Lemma 5.1, we see that either $d = 2$ and
632 $q \in \{2, 3, 4, 5, 7\}$, or $d \in \{3, 4\}$ and $q = 2$, or $SV \subseteq HV$. Suppose that $SV \subseteq HV$. Then
633 the group HV acts by conjugation on V as a linear group containing $\text{SL}_d(q)$. Therefore
634 either $V \cap H = 1$ or $V \cap H = V$. In the former case, $8 \geq |K : H| \geq |HV : H| = |V :$
635 $(V \cap H)| = q^d$ and so $(q, d) = (2, 2)$ or $(2, 3)$. In the latter case, $V \subseteq H$ and hence $VS \leq H$
636 and $H \trianglelefteq G$. Since $H = \mathbf{N}_K(H)$, we have $K = H$, contradicting the fact that $K > H$. \square

637 **Lemma 5.3.** *Let K be the subgroup of $\text{AGL}_1(q)$ of index $\gcd(2, q - 1)$. Suppose that*
638 *$H \leq K$ satisfies $|K : H| \leq 4$ and $H = \mathbf{N}_K(H)$. Then either $K = H$ or $q = 4$.*

639 *Proof.* Write $G = \text{AGL}_1(q)$ and assume that $K > H$. Let V be the subgroup of G of
640 order q . Since $|K : H| \leq 4$ and $H = \mathbf{N}_K(H)$, it follows that $|K : H| = 3$ or 4 and H is a

641 maximal subgroup of K . If $HV = H$, then $V \leq H$ and $H \trianglelefteq G$, which is a contradiction
 642 since $H = \mathbf{N}_K(H)$. Thus $H < HV \leq K$ and hence $K = HV$.

643 Since V is abelian, we have $V \cap H \trianglelefteq HV = K$. Further, since $V \cap H \leq V$ and K acts as
 644 a cyclic group of order $(q-1)/\gcd(2, q-1)$ on V , it follows that $V \cap H = 1$ or $V \cap H = V$.
 645 In the latter case, $V \leq H$ and $H \trianglelefteq K$, which contradicts the fact that $H = \mathbf{N}_K(H)$. So
 646 $V \cap H = 1$. Thus $|K : H| = |HV : H| = |V : (V \cap H)| = |V| = q$, so $q \in \{3, 4\}$. Finally, it
 647 is an easy computation to see that if $q = 3$, then $K = V$ and H must be K . \square

648 **Lemma 5.4.** *Let H be a proper subgroup of $T = \mathrm{PSL}_d(q)$ such that $H = \mathbf{N}_T(H)$ and
 649 $|T : H|/4 \leq \mathrm{meo}(\mathrm{Aut}(T))$. Then one of the following holds:*

- 650 (i) H is conjugate to the stabilizer of a point or a hyperplane of the projective space
 651 $\mathrm{PG}_{d-1}(q)$;
 652 (ii) $d = 2$ and $q \in \{4, 5, 7, 8, 9, 11, 16, 19, 25, 49\}$, or $d = 3$ and $q \in \{2, 3, 4, 5, 7\}$, or
 653 $d = 4$ and $q \in \{2, 3\}$, or $d = 5$ and $q = 2$.

654 *Proof.* Set $q = p^f$, with p a prime and $f \geq 1$. Let K be a maximal subgroup of T with
 655 $H \leq K$. Clearly, $|T : H| \geq |T : K|$ and hence

$$(10) \quad |K| \geq \frac{|T|}{4 \mathrm{meo}(\mathrm{Aut}(T))}.$$

656 In the first part of the proof, we assume that (i) does not hold for the group K and show
 657 that (d, q) must be as in (ii).

658 First we consider separately the case that $d = 2$. We refer to the description of the
 659 lattice of subgroups of T given in [39, Theorem 6.25, 6.26]. Every subgroup H of T is either
 660 a subgroup of a dihedral group of order $2(q+1)/\gcd(2, q-1)$ or $2(q-1)/\gcd(2, q-1)$
 661 (if H is as in [39, Theorem 6.25(a)]), or a subgroup of a Borel subgroup of order $(q-1)q/\gcd(2, q-1)$
 662 (if H is as in [39, Theorem 6.25(b)]), or isomorphic to $\mathrm{Alt}(4)$, $\mathrm{Sym}(4)$
 663 or $\mathrm{Alt}(5)$ (if H is as in [39, Theorem 6.25(c)]), or isomorphic to $\mathrm{PSL}_2(q_0)$ or to $\mathrm{PGL}_2(q_0)$
 664 (if H is as in [39, Theorem 6.25(d)], where q_0 is a power of p and $q_0^e = q$ for some integer
 665 e dividing f). Theorem 6.26 in [39] describes in detail the conditions when each of these
 666 cases can arise. For each of the three cases (b), (c), (d), it can be verified with a tedious
 667 computation (using Table 3) that the inequality $|T : K|/4 \leq \mathrm{meo}(\mathrm{Aut}(T))$ is only satisfied
 668 if $q \in \{4, 5, 7, 8, 9, 11, 16, 19, 25, 49\}$.

669 We now suppose that $d \geq 3$. Let \bar{K} be the preimage of K in $\mathrm{SL}_d(q)$ and let M be a
 670 maximal subgroup of $\mathrm{GL}_d(q)$ containing $\bar{K}Z$, where Z is the centre of $\mathrm{GL}_d(q)$. We have
 671 $|M| \geq |\bar{K}Z| = (q-1)|K|$. Assume that $|M| < |\mathrm{GL}_d(q)|^{1/3}$. Then (10) implies that

$$(11) \quad |\mathrm{GL}_d(q)|^{1/3} > |M| \geq (q-1)|K| \geq \frac{(q-1)|T|}{4 \mathrm{meo}(\mathrm{Aut}(T))}.$$

672 A direct computation shows that (11) is satisfied only if $(d, q) = (3, 2)$, which is one
 673 of the values in (ii). Therefore we may assume that $|\mathrm{GL}_d(q)|^{1/3} \leq |M|$. Furthermore,
 674 for the rest of the proof we assume that $(d, q) \neq (3, 2)$ and so, according to Table 3,
 675 $\mathrm{meo}(\mathrm{Aut}(T)) = (q^d - 1)/(q - 1)$.

676 Alavi [1, Theorem 9.1.1] classified the maximal subgroups M of $\mathrm{GL}_d(q)$ not contain-
 677 ing $\mathrm{SL}_d(q)$ with $|\mathrm{GL}_d(q)| \leq |M|^3$, listing the possible subgroups according to their ‘‘Aschbacher class’’: a detailed description for each class is given. Using the inequality
 678 $|M| \geq (q-1)|K|$, another (rather tedious) computation shows that, for each of the sub-
 679 groups listed in [1, Theorem 9.1.1] that are not contained in the Aschbacher class \mathcal{C}_9 , the
 680 inequality $|T : K|/4 \leq (q^d - 1)/(q - 1)$ is satisfied only in the case that K is conjugate
 681 to the stabilizer of a point or a hyperplane of $\mathrm{PG}_{d-1}(q)$, or (d, q) is as in (ii). It remains
 682 to consider the case that M is contained in the Aschbacher class \mathcal{C}_9 . In this case, Alavi’s
 683 classification implies that $d \leq 9$.
 684

685 For the rest of the proof of our claim we use Liebeck's result [28, Theorem 4.1]: if
 686 H is a maximal subgroup of T in the Aschbacher class \mathcal{C}_9 , then either $|H| < q^{3d}$, or
 687 $H = \text{Alt}(m)$ or $\text{Sym}(m)$ with $m = d + 1$ or $d + 2$. A straightforward calculation shows
 688 that $|\text{PSL}_d(q)|/(4(d+2)!) \leq (q^d - 1)/(q - 1)$ if and only if $d \in \{3, 4\}$ and $q = 2$ or
 689 $(d, q) = (3, 3)$. However since $|\text{PSL}_3(3)|$ is not divisible by $d + 2 = 5$, the case $(d, q) =$
 690 $(3, 3)$ does not actually occur. In particular, we may assume that $|H| < q^{3d}$. Since
 691 $|T : H|/4 \leq (q^d - 1)/(q - 1)$, we have

$$|T| \leq \frac{4(q^d - 1)}{q - 1} |H| < \frac{4(q^d - 1)}{q - 1} q^{3d},$$

692 which implies that $d \leq 4$. In particular, we may assume that $d = 3$ or $d = 4$. The complete
 693 list of the subgroups of $\text{PSL}_3(q)$ and $\text{PSL}_4(q)$ in the Aschbacher class \mathcal{C}_9 is contained in
 694 Sections 5.1.2 and 5.1.3 of [30] and in [5, Theorem 1.1] (for $d = 3$ and q odd). A case-by-
 695 case analysis now shows that $|T : K|/4 > (q^d - 1)/(q - 1)$. We have now found all of the
 696 values of (d, q) for which (i) does not hold for the group K .

697 Therefore, to conclude the proof we may assume that K is the stabilizer of either a
 698 point or a hyperplane of $\text{PG}_{d-1}(q)$, and that $H < K$. Now K is isomorphic to a subgroup
 699 of $\text{AGL}_{d-1}(q)$, namely the subgroup \tilde{K} of $\text{AGL}_{d-1}(q)$ containing $\text{ASL}_{d-1}(q)$ that satisfies
 700 $|\text{AGL}_{d-1}(q) : \tilde{K}| = \gcd(d, q - 1)$. Since $H \leq T$ and $H = \mathbf{N}_T(H)$, we have $H = \mathbf{N}_K(H)$.
 701 Applying Lemma 5.2 (for $d \geq 3$) and Lemma 5.3 (for $d = 2$) implies that $(d, q) = (2, 4)$,
 702 $d = 3$ and $q \in \{2, 3, 4, 5, 7\}$, or $d \in \{4, 5\}$ and $q = 2$. \square

703 The next proposition is the main ingredient in our proof of Theorem 1.3 for projective
 704 special linear groups.

705 **Proposition 5.5.** *Let G be a primitive group on Ω of degree n with socle $\text{PSL}_d(q)$. Assume*
 706 *that the action of G on Ω is not permutation isomorphic to the action on the points or*
 707 *on the hyperplanes of the projective space $\text{PG}_{d-1}(q)$, and that $n/4 \leq \text{meo}(\text{Aut}(\text{PSL}_d(q)))$.*
 708 *Then $d = 2$ and $q \in \{4, 5, 7, 8, 9, 11, 16, 19, 25, 49\}$, or $d = 3$ and $q \in \{2, 3, 4\}$, or $d = 4$*
 709 *and $q \in \{2, 3\}$.*

710 *Proof.* From Table 3 and Lemma 5.4, we see that we may assume that $d = 2$ and $q \in$
 711 $\{4, 5, 7, 8, 9, 11, 16, 19, 25, 49\}$, or $d = 3$ and $q \in \{2, 3, 4, 5, 7\}$, or $d = 4$ and $q \in \{2, 3\}$, or
 712 $d = 5$ and $q = 2$. Now a direct inspection with magma [6], on all the almost simple groups
 713 G with socle T and on all maximal subgroups of G , shows that only the cases listed in the
 714 proposition actually arise. \square

715 For the alternating groups, we will use the following bound in the proof of Theorem 5.7.
 716 This lemma is a modification of [34, Lemma 3.23] and we thank an anonymous referee for
 717 bringing this proof to our attention.

718 **Lemma 5.6.** *Let a, b be positive integers, let $m = ab$ and suppose that $a \geq 2$, $b \geq 2$ and*
 719 *$m \geq 17$. Then*

$$\frac{m!}{(a!)^b b!} \geq 3^{m/2}.$$

720 *Proof.* Let

$$S(a, b) := \frac{(ab)!}{(a!)^b b! 3^{ab/2}}.$$

721 It suffices to show that $S(a, b) \geq 1$ for all integers $a, b \geq 2$ such that $ab \geq 17$. First observe
 722 that

$$\frac{S(a, b+1)}{S(a, b)} = \frac{1}{(b+1)3^{a/2}} \prod_{k=1}^a \left(\frac{ab}{k} + 1 \right) \geq \frac{(b+1)^a}{(b+1)3^{a/2}} \geq \frac{3^{a-1}}{3^{a/2}} \geq 1.$$

723 So if $S(a, b) \geq 1$, then $S(a, b+1) \geq 1$ as well. Clearly any integers $a, b \geq 2$ such that
 724 $ab \geq 17$ satisfy one of the following conditions:

- 725 (i) $a = 2$ and $b \geq 9$;
- 726 (ii) $a \in \{3, 4, 5, 6, 7, 8\}$ and $b \geq 3$;
- 727 (iii) $a \geq 9$ and $b \geq 2$.

728 It is straightforward to check that $S(2, 4) \geq 1$, thus $S(2, b)$ for all $b \geq 4$ and this deals
 729 with case (i). Similarly we check that $S(a, b) \geq 1$ for $b = 3$ and $a \in \{3, 4, 5, 6, 7, 8\}$, which
 730 eliminates case (ii). So we may assume that (iii) holds. Now observe that $\binom{2a}{a}$ is the largest
 731 term in the binomial expansion of $(1+1)^{2a}$. Therefore we have $\binom{2a}{a} \geq 2^{2a}/(2a+1) > 2 \cdot 3^a$
 732 for all $a \geq 9$, which proves that $S(a, 2) = \binom{2a}{a}/(2 \cdot 3^a) \geq 1$ for $a \geq 9$. Therefore $S(a, b) \geq 1$
 733 in case (iii) as well. \square

734 **Theorem 5.7.** *Let G be a finite primitive group on Ω of degree n of AS type. If G
 735 contains a permutation g with $|g| \geq n/4$, then the socle T of G is either $\text{Alt}(m)$ in its
 736 action on the k -subsets of $\{1, \dots, m\}$, for some k , or $\text{PSL}_d(q)$ in its natural action on the
 737 points or on the hyperplanes of the projective space $\text{PG}_{d-1}(q)$, or T is one the groups in
 738 Table 2.*

739 *Proof.* Since all the groups in Table 1 are contained in Table 2, using Theorem 1.2, we
 740 may assume that T is either an alternating group or a projective special linear group. For
 741 $T \cong \text{PSL}_d(q)$, the theorem follows from Proposition 5.5.

742 So we may assume that $T \cong \text{Alt}(m)$ for some $m \geq 5$. Since $\text{Alt}(m)$ is contained in
 743 Table 2 for $m = 5, \dots, 9$, we may assume that $m \geq 10$. Now, for $\omega \in \Omega$, the stabilizer
 744 G_ω is either intransitive, imprimitive, or primitive in its action on $\{1, \dots, m\}$. If it is
 745 intransitive, then the action of T is permutation equivalent to the action on the k -subsets
 746 of $\{1, \dots, m\}$ (for some $1 \leq k < m/2$). If G_ω is imprimitive in its action on $\{1, \dots, m\}$,
 747 then we can identify the elements of Ω with the partitions of a set of cardinality m into
 748 b parts of cardinality a , where $m = ab$ and $a, b \geq 2$. Using Lemma 5.6, if $m \geq 17$,
 749 then we have $n = |\Omega| = m!/(a!^b b!) \geq 3^{m/2}$. Using this bound and the upper bound for
 750 $\text{meo}(\text{Sym}(m))$ in Theorem 2.1, we see that the inequality

$$|\Omega|/4 \leq \text{meo}(\text{Sym}(m))$$

751 is never satisfied. For the remaining cases ($m = 11, \dots, 16$) a computation in magma shows
 752 that no examples arise.

753 Finally, suppose that G_ω is primitive in its action on $\{1, \dots, m\}$. In this case, by [35],
 754 we have $|G_\omega| \leq 4^m$ and $n = |\Omega| \geq m!/4^m$. Again, using the upper bound in Theorem 2.1,
 755 we see that the inequality $|\Omega|/4 \leq \text{meo}(\text{Sym}(m))$ is only satisfied for $m \leq 15$. For the
 756 remaining cases ($m = 11, \dots, 14$) a computation in magma shows that no examples arise.
 757 \square

758 **5.2. Proof of Theorem 1.3 for primitive groups of SD type.**

759 **Lemma 5.8.** *Let T be a finite non-abelian simple group. Then $4|\text{Out}(T)| < |T|^{2/3}$.*

760 *Proof.* The proof follows from a case-by-case analysis (detailed information on $|T|$ and
 761 $|\text{Out}(T)|$ can be found in [9]). \square

762 **Theorem 5.9.** *Let G be a finite primitive group on Ω of degree n of SD type. If G contains
 763 a permutation g with $|g| \geq n/4$, then the socle of G is $\text{Alt}(5)^2$ and $|g| = n/4 = 15$.*

764 *Proof.* By the description of the O’Nan–Scott types in [36], there exists a non-abelian
 765 simple group T such that the socle N of G is isomorphic to $T_1 \times \dots \times T_\ell$ with $T_i \cong T$
 766 for each $i \in \{1, \dots, \ell\}$. The set Ω can be identified with $T_1 \times \dots \times T_{\ell-1}$ and, for the
 767 point $\omega \in \Omega$ that is identified with $(1, \dots, 1)$, the stabilizer N_ω is the diagonal subgroup
 768 $\{(t, \dots, t) \mid t \in T\}$ of N . That is to say, the action of N_ω on Ω is permutation isomorphic
 769 to the action of T on $T^{\ell-1}$ by “diagonal” component-wise conjugation: the image of the
 770 point $(x_1, \dots, x_{\ell-1})$ under the permutation corresponding to $t \in T$ is

$$(x_1^t, \dots, x_{\ell-1}^t).$$

771 The group G_ω is isomorphic to a subgroup of $\text{Aut}(T) \times \text{Sym}(\ell)$ and G is isomorphic to a
 772 subgroup of $T^\ell \cdot (\text{Out}(T) \times \text{Sym}(\ell))$. First suppose that $\ell \geq 3$. Using Lemma 5.8, we have

$$\begin{aligned} \text{meo}(G) &\leq \text{meo}(\text{Out}(T) \times \text{Sym}(\ell)) \text{meo}(T^\ell) \leq |\text{Out}(T)| \text{meo}(\text{Sym}(\ell)) \text{meo}(T^\ell) \\ &\leq |\text{Out}(T)| \text{meo}(\text{Sym}(\ell)) |T| < \text{meo}(\text{Sym}(\ell)) (|T|^{5/3}/4). \end{aligned}$$

773 Furthermore, with a direct computation, using Theorem 2.1 and the fact that $|T| \geq 60$,
 774 we can show that $|T|^{\ell-8/3} \geq \text{meo}(\text{Sym}(\ell))$. Thus

$$\text{meo}(G) < |T|^{\ell-8/3} \frac{|T|^{5/3}}{4} = \frac{|T|^{\ell-1}}{4} = \frac{|\Omega|}{4}.$$

775 Suppose that $\ell = 2$. We claim that $\text{meo}(G) \leq \text{meo}(\text{Aut}(T))^2$. Let x be an element
 776 of G . Now, $x = (g_1, g_2)(1, 2)^i$ for some $i \in \{0, 1\}$ where $g_1, g_2 \in \text{Aut}(T)$ and $g_1 \equiv g_2$
 777 mod $\text{Inn}(T)$. If $i = 0$, then $x = (g_1, g_2)$ and $|x| \leq |g_1||g_2| \leq \text{meo}(\text{Aut}(T))^2$. If $i = 1$, then

$$x^2 = (g_1, g_2)(1, 2)(g_1, g_2)(1, 2) = (g_1g_2, g_2g_1).$$

778 Now $(g_1g_2)^{g_2^{-1}} = g_2g_1$ and so $|x^2| = |g_1g_2| \leq \text{meo}(\text{Aut}(T))$. Thus $|x| \leq 2 \text{meo}(\text{Aut}(T)) \leq$
 779 $\text{meo}(\text{Aut}(T))^2$ and our claim is proved.

780 Now assume that $T = \text{Alt}(m)$, for some $m \geq 5$. Using Theorem 2.1, we see that
 781 $\text{meo}(\text{Aut}(T))^2 < |T|/4$ for every $m \geq 7$. In particular, $\text{meo}(G) < |\Omega|/4$, for $m \geq 7$. If
 782 $m = 6$, then an easy computation shows that $\text{meo}(\text{Alt}(6))^2 \cdot (\text{Out}(\text{Alt}(6)) \times \text{Sym}(2)) = 40$
 783 and $|\Omega| = |\text{Alt}(6)|/4 = 360/4 = 90 > 40$. On the other hand if $m = 5$, then $|\Omega|/4 =$
 784 $|\text{Alt}(5)|/4 = 60/4 = 15$ is the order of $(g_1, g_2) \in G$ with $|g_1| = 3, |g_2| = 5$, and this case is
 785 in the statement of the theorem.

786 Next, suppose that $T = \text{PSL}_d(q)$ for some $m \geq 2$ and $q = p^f$. We may assume that
 787 $(m, q) \neq (2, 4), (2, 5), (2, 9)$ and $(4, 2)$. Using Table 3, we find that $\text{meo}(\text{Aut}(T))^2 < |T|/4$,
 788 for $(m, q) \neq (2, 7), (2, 8)$ and $(3, 2)$. In particular, $\text{meo}(G) < |\Omega|/4$ for $(m, q) \neq (2, 7), (2, 8)$
 789 and $(3, 2)$. Recall that $\text{PSL}_2(7) \cong \text{PSL}_3(2)$. If $(m, q) = (2, 7)$, then an easy computation
 790 shows that $\text{meo}(\text{PSL}_2(7))^2 \cdot (\text{Out}(\text{PSL}_2(7)) \times \text{Sym}(2)) = 28$ and $|\Omega| = |\text{PSL}_2(7)|/4 =$
 791 $168/4 = 42 > 28$. Similarly, if $(m, q) = (2, 8)$, then $\text{meo}(\text{PSL}_2(8))^2 \cdot (\text{Out}(\text{PSL}_2(8)) \times$
 792 $\text{Sym}(2)) = 63$ and $|\Omega| = |\text{PSL}_2(8)|/4 = 504/4 = 126 > 63$.

793 Finally suppose that T is not isomorphic to $\text{Alt}(m)$ or to $\text{PSL}_d(q)$. By Theorem 1.2,
 794 it follows that either $\text{meo}(\text{Aut}(T)) < m(T)/4$ or that T is one of the groups in Table 1.
 795 In the first case, $\text{meo}(\text{Aut}(T))^2 < m(T)^2/16 \leq |T|/4 = |\Omega|/4$ (where the last inequality
 796 follows from a direct inspection of Table 4). It remains to suppose that T is one of the
 797 groups in Table 1. Now a case-by-case analysis using [9] shows that $\text{meo}(\text{Aut}(T))^2 < |T|/4$
 798 in each of the remaining cases. \square

799 **5.3. Proof of Theorem 1.3: the end.** We are finally ready to prove Theorem 1.3.
 800 However first we need some more notation.

801 **Notation 5.10.** Let G be a primitive group of PA or CD type acting on Ω . When G is
 802 of PA type, the socle $\text{soc}(G) = T_1 \times \cdots \times T_\ell$ is isomorphic to T^ℓ , where T is a non-abelian
 803 simple group, and $\ell \geq 2$. When G is of CD type,

$$\text{soc}(G) = (T_{1,1} \times \cdots \times T_{1,r}) \times \cdots \times (T_{\ell,1} \times \cdots \times T_{\ell,r})$$

804 is isomorphic to $T^{\ell r}$, where T is a non-abelian simple group and $\ell, r \geq 2$.

805 In both cases, the action of G on Ω is permutation isomorphic to the product action of
 806 G on a set Δ^ℓ . By identifying Ω with Δ^ℓ we have $G \leq W = H \text{ wr } \text{Sym}(\ell)$, $H \leq \text{Sym}(\Delta)$ is
 807 primitive on Δ , $\text{soc}(G)$ is the socle of W , and W acts on Ω as in the product action. When
 808 G is of PA type, H is primitive of AS type and $\text{soc}(H) = T$. When G is of CD type, H is
 809 primitive of SD type and $\text{soc}(H) = T^r$ (in particular $|\Delta| = |T|^{r-1}$ and $|\Omega| = |T|^{\ell(r-1)}$).

810 *Proof of Theorem 1.3.* Recall that, according to [36], the finite primitive permutation
 811 groups are partitioned into eight families: AS, HA, SD, HS, HC, CD, TW and PA. If
 812 G is of AS or SD type, then the proof follows from Theorems 5.7 and 5.9. If G is of HA
 813 type, then the proof follows from [19].

814 Suppose that G is of HS type. Then G is contained in a primitive group M of SD type
 815 (one might choose M to be $N_{\text{Sym}(n)}(G)$, see [36]). If G contains an element of order at
 816 least $n/4$, then Theorem 5.9 implies that the socle of G is $\text{Alt}(5)^2$, which is one of the
 817 exceptions listed in Table 2.

818 Next, we recall that every primitive group of TW type is contained in a primitive group
 819 of HC type (see [12, Section 4.7]), and also every primitive group of HC type is contained
 820 in a primitive group of CD type (see [36]). Therefore we will assume from now on that G
 821 is of CD or PA type and we will use Notation 5.10. There are two cases to consider: (i) H
 822 contains a permutation h with $|h| > |\Delta|/4$ and (ii) $\text{meo}(H) \leq |\Delta|/4$. Note that Case (ii)
 823 is always satisfied if G is of CD type since, in this case, H is of SD type and Theorem 5.9
 824 applies. Moreover in Case (ii) we have

$$\begin{aligned} \text{meo}(G) &\leq \text{meo}(H^\ell) \text{meo}(\text{Sym}(\ell)) < (\text{meo}(H))^\ell \text{meo}(\text{Sym}(\ell)) \\ &\leq \frac{|\Delta|^\ell}{4^\ell} \text{meo}(\text{Sym}(\ell)) = |\Omega| \frac{\text{meo}(\text{Sym}(\ell))}{4^\ell} \leq \frac{|\Omega|}{4}, \end{aligned}$$

825 where the second inequality follows since $\ell \geq 2$ and the last inequality follows from Theo-
 826 rem 2.1. Now suppose that Case (i) holds; in particular, H is of AS type. By Theorem 5.7,
 827 $T = \text{soc}(H)$ is $\text{Alt}(m)$ (in its natural action on k -sets) or $\text{PSL}_d(q)$ (in its natural action
 828 on $\text{PG}_{d-1}(q)$), or T is one of the simple groups in Table 2.

829 It remains to show that there exists a positive integer ℓ_T depending only on T with
 830 $\ell \leq \ell_T$. Arguing as above, we have

$$\begin{aligned} \text{meo}(G) &\leq \text{meo}(\text{Aut}(T)^\ell) \text{meo}(\text{Sym}(\ell)) \\ &\leq |\text{Aut}(T)| \text{meo}(\text{Sym}(\ell)) \leq |\text{Aut}(T)| e^{2\sqrt{\ell \log \ell}} \end{aligned}$$

831 where the last inequality follows from Theorem 2.1. Since $|\Omega| \geq m(T)^\ell \geq 5^\ell$, it is easy to
 832 see that $\text{meo}(G) < |\Omega|/4$ for all sufficiently large ℓ . \square

833 **Remark 5.11.** In general, the smallest value of ℓ_T seems hard to obtain without a careful
 834 analysis of the element orders of $\text{Aut}(T)$. Nevertheless, for some groups T in Table 2 the
 835 number ℓ_T can be obtained using some elementary arguments. Consider for example the
 836 group $T = \text{Alt}(7)$. The element orders of $\text{Aut}(T) \cong \text{Sym}(7)$ are 1, 2, 3, 4, 5, 6, 7, 10 and
 837 12. So the maximum element order of $\text{Sym}(7)^2$ is $7 \cdot 12 = 84$ and it is not hard to see
 838 that the maximum element order of $\text{Sym}(7)^\ell$ is $\text{lcm}(7, 10, 12) = 420$ for each integer $\ell \geq 3$.
 839 In particular, $\text{meo}(\text{Sym}(7) \text{ wr } \text{Sym}(\ell)) \leq 420 \text{meo}(\text{Sym}(\ell))$. Now observe that the minimal
 840 degree of a permutation representation of $\text{Alt}(7)$ is 7 and $420 \text{meo}(\text{Sym}(\ell)) < 7^\ell/4$ for
 841 every $\ell \geq 5$. Thus $\ell_T \leq 4$. To obtain the precise value of ℓ_T , one has to embark on a
 842 careful analysis of the possible element orders of $\text{Sym}(7) \text{ wr } \text{Sym}(\ell)$ for $\ell \in \{2, 3, 4\}$. In
 843 this case, it is easy to see that $\ell_T = 4$.

844 A similar argument can be used for the Higman–Sims group $T = HS$ for example.
 845 Remarkably, it turns out that $\ell_T = 1$ here, which can be seen using [9].

846 In Table 6 we give the values of ℓ_T for each of the simple groups in Table 2 (these values
 847 were obtained with the help of a computer). The number m in the table is the degree of
 848 the permutation representation of the socle factor T of a primitive group G of PA type
 849 admitting a permutation $g \in G$ with $|g| \geq m^\ell/4$.

T	(m, ℓ_T) where $n = m^\ell$ and $1 \leq \ell \leq \ell_T$
Alt(5)	(5, 3), (6, 3), (10, 2)
Alt(6)	(6, 3), (10, 2), (15, 1)
Alt(7)	(7, 4), (15, 1), (21, 1), (35, 1)
Alt(8)	(8, 4), (15, 2), (28, 1), (35, 1), (56, 1)
Alt(9)	(9, 4), (36, 1)
M_{11}	(11, 3), (12, 3)
M_{12}	(12, 3)
M_{22}	(22, 2)
M_{23}	(23, 3)
M_{24}	(24, 3)
HS	(100, 1)
$\text{PSL}_2(7)$	(7, 2), (8, 3), (21, 1), (28, 1)
$\text{PSL}_2(8)$	(9, 2), (28, 1), (36, 1)
$\text{PSL}_2(11)$	(11, 2), (12, 3)
$\text{PSL}_2(16)$	(17, 3), (68, 1)
$\text{PSL}_2(19)$	(20, 3), (57, 1)
$\text{PSL}_2(25)$	(26, 2)
$\text{PSL}_2(49)$	(50, 2)
$\text{PSL}_3(3)$	(13, 2), (52, 1)
$\text{PSL}_3(4)$	(21, 2), (56, 1)
$\text{PSL}_4(3)$	(40, 2), (130, 1)
$\text{PSU}_3(3)$	(28, 1), (36, 1)
$\text{PSU}_3(5)$	(50, 1)
$\text{PSU}_4(3)$	(112, 1)
$\text{PSp}_6(2)$	(28, 1), (36, 1)
$\text{PSp}_8(2)$	(120, 1)
$\text{PSp}_4(3)$	(27, 1), (36, 1), (40, 1), (45, 1)

TABLE 6. List of degrees $n = m^\ell$ for which there exists a primitive permutation group G of degree n as in Theorem 1.3(4)

850

6. PROOF OF THEOREM 1.1

851 *Proof of Theorem 1.1.* The first part follows using the values of $m(T)$ in Table 4 and
 852 the upper bounds on $\text{meo}(\text{Aut}(T))$ in Table 3 in the same way as in the proof of Theo-
 853 rem 1.2. We only give full details in the case $T = \text{PSU}_d(q)$, with $q \geq 4$. If $d \geq 5$, then
 854 $\text{meo}(\text{Aut}(T)) \leq q^{d-1} + q^2$. So

$$m(T)^{3/4} = \left(\frac{(q^d - (-1)^d)(q^{d-1} - (-1)^{d-1})}{q^2 - 1} \right)^{3/4} \geq (q^{2d-3})^{3/4},$$

855 which is greater than $q^{d-1} + q^2$. If $d = 3$, then $m(T)^{3/4} = (q^3 + 1)^{3/4} > q^2$ and
 856 $\text{meo}(\text{Aut}(T)) = q^2 - 1$ when $q \neq 4$ and so the bound in the statement of Theorem 1.1
 857 holds with possibly one exception. If $d = 4$, then $m(T)^{3/4} = (q^4 + q^3 + q + 1)^{3/4}$ and
 858 $\text{meo}(\text{Aut}(T)) = q^3 + 1$ when $q \neq 2$ and so the bound in the statement of Theorem 1.1
 859 holds with possibly one exception. Similar calculations show that, apart from a finite
 860 number of exceptions, (i) holds for all finite simple groups T satisfying $T \neq \text{Alt}(m)$ and
 861 $T \neq \text{PSL}_d(q)$.

862 To prove the second part of Theorem 1.1, we let $\epsilon, A > 0$, $g_\epsilon(x) = Ax^{3/4-\epsilon}$ and let
 863 $T = \text{PSU}_4(q)$ with q odd. Then $\text{meo}(\text{Aut}(T)) = q^3 + 1$ and $m(T) = (q^3 + 1)(q + 1) \leq 2q^4$.
 864 Thus $g_\epsilon(m(T)) \leq 2^{3/4} Aq^{3-4\epsilon}$, which is strictly less than $q^3 + 1$ for all sufficiently large
 865 q . □

866

ACKNOWLEDGEMENTS

867 The authors are grateful to an anonymous referee for various suggestions which they
 868 feel have improved the paper and, in particular, for providing a much cleaner proof of
 869 Lemma 5.6.

870

REFERENCES

- 871 [1] S. H. Alavi, *Triple factorisations of general linear groups*, PhD thesis at University of Western Aus-
 872 tralia, 2010.
- 873 [2] M. Aschbacher, G. M. Seitz, Involutions in Chevalley groups over fields of even order, *Nagoya Math.*
 874 *J.* **63** (1976), 1–91.
- 875 [3] A. D. Barbour, S. Tavaré, A rate for the Erdős–Turán law, *Combin. Probab. Comput.* **3** (1994), 16–176.
- 876 [4] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, Á. Seress, Permutations with re-
 877 stricted cycle structure and an algorithmic application, *Combin. Probab. Comput.* **11** (2002), 447–464.
- 878 [5] D. M. Bloom, The subgroups of $\mathrm{PSL}(3, q)$ for odd q , *Trans. Amer. Math. Soc.* **127** (1967), 150–178.
- 879 [6] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic*
 880 *Comput.* **24** (1997), 235–265.
- 881 [7] A. A. Buturlakin, M. A. Grechkoseeva, The cyclic structure of maximal tori in finite classical groups,
 882 *Algebra and Logic* **46** (2007), 73–89.
- 883 [8] R. W. Carter, *Finite groups of Lie type*, Wiley Classics Library. John Wiley & Sons Ltd., Chichester,
 884 1993. Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience
 885 Publication.
- 886 [9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups*, Clarendon
 887 Press, Oxford, 1985.
- 888 [10] B. N. Cooperstein, Minimal degree for a permutation representation of a classical group, *Israel J.*
 889 *Math.* **30** (1978), 213–235.
- 890 [11] D. I. Deriziotis, G. O. Michler, Character table and blocks of finite simple triality groups ${}^3D_4(q)$,
 891 *Trans. Amer. Math. Soc.* **303** (1987), 39–70.
- 892 [12] J. Dixon, B. Mortimer, *Permutation groups*, Springer-Verlag, New York, 1996.
- 893 [13] P. Erdős, P. Turán, On some problems of a statistical group-theory, I, *Z. Wahrscheinlichkeitstheorie*
 894 *Verw. Gebiete* **4** (1965), 175–186.
- 895 [14] P. Erdős, P. Turán, On some problems of a statistical group-theory, III, *Acta Math. Acad. Sci. Hungar.*
 896 **18** (1967), 309–320.
- 897 [15] J. Fulman, A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal
 898 groups, *J. Algebra* **234** (2000), 207–224.
- 899 [16] J. Fulman, R. M. Guralnick, Conjugacy class properties of the extension of $\mathrm{GL}_n(q)$ generated by the
 900 inverse transpose involution, *J. Algebra* **275** (2004), 356–396.
- 901 [17] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups. number 3. part I.*
 902 *chapter A*, **40** (1998), xvi+419.
- 903 [18] R. Gow, C. R. Vinroot, Extending real-valued characters of finite general linear and unitary groups
 904 on elements related to regular unipotents, *J. Group Theory* **11** (2008), 299–331.
- 905 [19] S. Guest, J. Morris, C. E. Praeger, P. Spiga, Affine transformations of finite vector spaces with large
 906 orders or few cycles, submitted, arXiv:1306.1368 [math.GR]
- 907 [20] S. Guest, J. Morris, C. E. Praeger, P. Spiga, Finite primitive permutation groups containing a per-
 908 mutation with at most four cycles, submitted, arXiv:1307.6881 [math.GR]
- 909 [21] B. Huppert, Singer-Zylken in klassischen Gruppen, *Math. Z.* **117** (1970), 141–150.
- 910 [22] W. M. Kantor, Á. Seress, Large element orders and the characteristic of Lie-type simple groups, *J.*
 911 *Algebra* **322** (2009), 802–832.
- 912 [23] W. M. Kantor, Á. Seress, Prime power graphs for groups of Lie type, *J. Algebra* **247** (2002), 370–434.
- 913 [24] P. Kleidman, M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Mathemat-
 914 ical Society Lecture Notes Series **129**, Cambridge University Press, Cambridge.
- 915 [25] E. Landau, Über die Maximalordnung der Permutationen gegebenen Grades, *Arch. Math. Phys.* **5**
 916 (1903), 92–103.
- 917 [26] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig, 1909.
- 918 [27] R. Lawther, Jordan block sizes of unipotent elements in exceptional algebraic groups, *Comm. Algebra*
 919 **23** (1995), 4125–4156.
- 920 [28] M. W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math.*
 921 *Soc.* (3) **50** (1985), 426–446.
- 922 [29] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O’Nan–Scott theorem for finite primitive permutation
 923 groups, *J. Austral. Math. Soc. Ser. A* **44** (1988), 389–396.

- 924 [30] M. W. Liebeck, C. E. Praeger, J. Saxl, *The maximal factorizations of the finite simple groups and*
 925 *their automorphism groups*, Memoirs of the American Mathematical Society, Volume **86**, Nr **432**,
 926 Providence, Rhode Island, USA, 1990.
- 927 [31] M. W. Liebeck, J. Saxl, G. M. Seitz, Subgroups of maximal rank in finite exceptional groups of lie
 928 type, *Proc. London Math. Soc.* **65** (1992), 297–325.
- 929 [32] J. P. Massias, J. L. Nicolas, G. Robin, Effective Bounds for the Maximal Order of an Element in the
 930 Symmetric Group, *Mathematics of Computation* **53** (1989), 665–678.
- 931 [33] V. D. Mazurov, A. V. Vasil'ev, Minimal permutation representations of finite simple orthogonal
 932 groups. (Russian) *Algebra i Logika* 33 (1994), no. 6, 603–627, 716; translation in *Algebra and Logic*
 933 33 (1994), no. 6, 337350
- 934 [34] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent
 935 polynomials, *Ann. Scuola Norm. Sup. Pisa* **12** (2013), 369–438
- 936 [35] Cheryl E. Praeger, J. Saxl, On the orders of primitive permutation groups, *Bull. London Math. Soc.*
 937 **12** (1980), 303–307.
- 938 [36] Cheryl E. Praeger, Finite quasiprimitive graphs, in *Surveys in combinatorics*, *London Mathematical*
 939 *Society Lecture Note Series*, vol. 24 (1997), 65–85.
- 940 [37] K. Shinoda, The conjugacy classes of Chevalley groups of type F_4 over finite fields of characteristic 2,
 941 *J. Fac. Sci. Univ. Tokyo Sect. I A Math.* **21** (1974), 133–159.
- 942 [38] M. Suzuki, A new type of simple groups of finite order, *Proc. Nat. Acad. Sci. U.S.A.* **46** (1960),
 943 868–870.
- 944 [39] M. Suzuki, *Group Theory I*, Grundlehren der mathematischen Wissenschaften **247**, Springer-Verlag,
 945 New York, 1981.
- 946 [40] A. V. Vasil'ev, Minimal permutation representations of finite simple exceptional groups of types G_2
 947 and F_4 , *Algebra and Logic* **35** (1996), 371–383.
- 948 [41] A. V. Vasil'ev, Minimal permutation representations of finite simple exceptional groups of types E_6 ,
 949 E_7 and E_8 , *Algebra and Logic* **36** (1997), 302–310.
- 950 [42] A. V. Vasil'ev, Minimal permutation representations of finite simple exceptional twisted groups, *Al-*
 951 *gebra and Logic* **37** (1998), 9–20.

952 SIMON GUEST, CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATH-
 953 EMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, CRAWLEY, WA 6009, AUS-
 954 TRALIA
 955 CURRENT ADDRESS: MATHEMATICS, UNIVERSITY OF SOUTHAMPTON, HIGHFIELD, SO17 1BJ,
 956 UNITED KINGDOM
 957 *E-mail address:* `s.d.guest@soton.ac.uk`

958 JOY MORRIS, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETH-
 959 BRIDGE, LETHBRIDGE, AB. T1K 3M4. CANADA
 960 *E-mail address:* `joy@cs.uleth.ca`

961 CHERYL E. PRAEGER, CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF
 962 MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, CRAWLEY, WA 6009,
 963 AUSTRALIA
 964 ALSO AFFILIATED WITH KING ABDULAZZIZ UNIVERSITY, JEDDAH, SAUDI ARABIA
 965 *E-mail address:* `Cheryl.Praeger@uwa.edu.au`

966 PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA,
 967 VIA COZZI 53, 20125 MILANO, ITALY
 968 *E-mail address:* `pablo.spiga@unimib.it`