Journal of Algebra 407 (2014) 413–433

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On the probability of generating a monolithic group

Eloisa Detomi [a], Andrea Lucchini [a], Colva M. Roney-Dougal [b,*,1]

[a] *Università degli Studi di Padova, Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy*
[b] *University of St Andrews, Mathematical Institute, St Andrews, Fife KY16 9SS, Scotland, United Kingdom*

ARTICLE INFO

Article history:
Received 20 September 2013
Available online 18 April 2014
Communicated by E.I. Khukhro

Keywords:
Finite group theory
Random generation of finite groups
Finite simple groups
Crown-based power

ABSTRACT

A group L is *primitive monolithic* if L has a unique minimal normal subgroup, N, and trivial Frattini subgroup. By $P_{L,N}(k)$ we denote the conditional probability that k randomly chosen elements of L generate L, given that they project onto generators for L/N. In this article we show that $P_{L,N}(k)$ is controlled by $P_{Y,S}(2)$, where $N \cong S^r$ and Y is a 2-generated almost simple group with socle S that is contained in the normalizer in L of the first direct factor of N. Information about $P_{L,N}(k)$ for L primitive monolithic yields various types of information about the generation of arbitrary finite and profinite groups.

1. Introduction

A group L is *primitive monolithic* if L has a unique minimal normal subgroup N, and trivial Frattini subgroup. By $P_{L,N}(k)$ we denote the conditional probability that k randomly chosen elements of L generate L, given that they project onto generators for L/N, and by $d(L)$ we denote the cardinality of the smallest generating set for L.

* Corresponding author.
[1] Colva Roney-Dougal acknowledges the support of EPSRC grant EP/I03582X/1.

http://dx.doi.org/10.1016/j.jalgebra.2014.03.010

Bounds on $P_{L,N}(k)$ were studied in [6]. The results presented there depend on a detailed analysis of the behavior of $P_{L,N}(d(L))$ when L is almost simple [14]. Although these bounds were strong enough to solve a series of open problems on the generation of finite groups, an interesting question arises from [14] and [6]: is it true that if $k \geqslant d(L)$ then $P_{L,N}(k)$ is bounded below by the conditional probability $P_{Y,S}(2)$? Here Y is a 2-generated group such that $S \trianglelefteqslant Y \leqslant N_L(S_1)/C_L(S_1) \leqslant \operatorname{Aut} S$, with $N \cong S_1 \times \cdots \times S_r \cong S^r$. By [14], $P_{Y,S}(2) \geqslant 53/90$ and indeed $P_{Y,S}(2) \geqslant 0.9$ apart from very few exceptions, so a lower bound $P_{L,N}(k) \geqslant P_{Y,S}(2)$ can be considered quite satisfactory. In any case, a positive solution would allow a neater and more efficient formulation of the results in [6].

In fact, the only remaining case to prove is when $k = r = 2$, which needs a deeper insight into the structure of almost simple groups. By [3], if X is almost simple with socle S, then $d(X) = \max(2, d(X/S)) \leqslant 3$. In Section 4 of [6] it is shown that in order to settle our conjecture, it would suffice to prove that every almost simple group X satisfies the following property $\mathcal{P}$: *there exists a 2-generated subgroup Y, with $S = \operatorname{soc} X \leqslant Y \leqslant X$ and*

$$P_{X,S}(3) - P_{Y,S}(2) \geqslant \frac{|\operatorname{Out} S|}{|S|}. \tag{1}$$

In the present paper we prove that indeed all the finite almost simple groups have this property:

Proposition 1.1. *Every finite almost simple group has property $\mathcal{P}$.*

This immediately allows us to settle the conjecture and give a positive answer to our question.

Theorem 1.2. *Let L be a primitive monolithic group with non-abelian socle $N \cong S_1 \times \cdots \times S_r$, and identify S with S_1. If $k \geqslant d(L)$ then there exists a 2-generated group Y with $S \trianglelefteqslant Y \leqslant N_L(S_1)/C_L(S_1) \leqslant \operatorname{Aut} S$ such that $P_{L,N}(k) \geqslant P_{Y,S}(2)$.*

Let G be a finite group, and let L be monolithic with socle N. We define the *crown-based power* of L of *size* t to be

$$L_t = \big\{(l_1, \ldots, l_t) \in L^t \;\big|\; l_1 N = \cdots = l_t N\big\}.$$

In [4] it was proved that there exist a primitive monolithic group L and a positive integer t such that the crown-based power L of size t is an epimorphic image of G, and $d(G) = d(L_t)$. Clearly, $d(L_t)$ increases with t, hence for each $k \geqslant d(L)$ there exists a largest positive integer $f_L(k)$ such that $d(L_{f_L(k)}) \leqslant k$. Information about the behavior of $f_L(k)$ is of relevance to several problems in the generation of finite and profinite groups: see, for example, [6].

Theorem 2.7 in [4] gives a formula for $f_L(k)$:

$$f_L(k) = \begin{cases} \frac{P_{L,N}(k)|N|^k}{|C_{\mathrm{Aut}_N(L/N)}|} & \text{if } N' = N \\ \log_q\left(\frac{|N|^{k-1}}{|H^1(L/N,N)|}\right) & \text{if } N' = 1, \text{ where } q = |\mathrm{End}_{L/N}N|. \end{cases}$$

Notice that when N is abelian, we can readily compute $f_L(k)$, but when $N \cong S^r$ is a direct product of non-abelian simple groups S, the value of $f_L(k)$ depends on $P_{L,N}(k)$.

We therefore get the following corollary to Theorem 1.2. Note that throughout, all logarithms are to base 2 unless otherwise specified.

Corollary 1.3. *Let L be a monolithic primitive group with non-abelian socle $N = S^r$ and let $d = d(L)$. Then there exists a 2-generated almost simple group Y with socle S, with the property that*

$$f_L(d) \geqslant f_Y(2)\frac{|N|^{d-1}}{r|S|}.$$

In particular,

$$f_L(d) \geqslant \alpha\frac{|N|^{d-1}}{r\log|S|}$$

where $\alpha = \frac{121}{1680}\log 20\,160 > 1.029$.

In Section 2 we prove Proposition 1.1 when $d(X) = 2$. In Section 3 we collect some background material for the proof of Proposition 1.1 in the cases where $d(X) \neq 2$: in particular we show that if $d(X) = 3$, then S is either a linear or an orthogonal group. In Section 4 we prove Proposition 1.1 when $S = \mathrm{L}_n(q)$ and $d(X) = 3$, then in Section 5 we prove the result when $S = \mathrm{O}_n^+(q)$ and $d(X) = 3$. In the last section we prove Corollary 1.3.

2. The 2-generator case

In this section we prove Proposition 1.1 for the case $d(X) = 2$. Given a non-abelian simple group S and a prime divisor u of $|S|$, we define the number c_u as follows: $c_u = 2u$ if u^2 does not divide $|S|$, otherwise $c_u = u^2$. Then we set

$$\alpha_u = \max\Big\{c_u, \min_{t\in S,|t|=u}\big\{\big|C_S(t)\big|\big\}\Big\}.$$

Proposition 2.1. *Let X be a 2-generated almost simple group with socle S. If*

$$\alpha_u \geqslant |\operatorname{Out} S|/P_{X,S}(2)$$

for every prime divisor u of $|S|$, then X satisfies property $\mathcal{P}$.

Proof. Say $X = \langle g_1, g_2 \rangle$ and set

$$\begin{aligned} \Phi &= \big\{(s_1, s_2, s_3) \in S^3 \;\big|\; \langle g_1 s_1, g_2 s_2, s_3 \rangle = X\big\} \\ &= \big\{(s_1, s_2, s_3) \in S^3 \;\big|\; \langle g_1 s_1, g_2 s_2, s_3 \rangle \geqslant S\big\}. \end{aligned}$$

Note that, by Gaschütz [8], $P_{X,S}(3) = |\Phi|/|S|^3$.

This set Φ contains the set

$$\Phi_1 = \big\{(s_1, s_2, s_3) \in S^3 \;\big|\; \langle g_2 s_2, s_3 \rangle \geqslant S\big\}$$

whose cardinality is $P_{Y,S}(2)|S^2| \cdot |S| = P_{Y,S}(2)|S|^3$ for $Y = \langle g_2, S \rangle$ (the first component is free).

Moreover, Φ contains the set

$$\Phi_2 = \big\{(s_1, s_2, s_3) \in S^3 \;\big|\; \langle g_1 s_1, g_2 s_2 \rangle \geqslant S \text{ and } \langle g_2 s_2, s_3 \rangle \not\geqslant S\big\}$$

where the second condition ensures that $\Phi_1 \cap \Phi_2 = \emptyset$. Say

$$\alpha = \min_{s_2 \in S} \big|\big\{s_3 \in S \;\big|\; \langle g_2 s_2, s_3 \rangle \not\geqslant S\big\}\big|,$$

then $|\Phi_2| \geqslant P_{X,S}(2)|S^2| \cdot \alpha$. Therefore

$$\begin{aligned} P_{X,S}(3) = \frac{|\Phi|}{|S|^3} &\geqslant \frac{|\Phi_1|}{|S|^3} + \frac{|\Phi_2|}{|S|^3} \\ &\geqslant P_{Y,S}(2) + \frac{P_{X,S}(2)\alpha}{|S|} \end{aligned}$$

so we are left to prove that $\frac{P_{X,S}(2)\alpha}{|S|} \geqslant \frac{|\operatorname{Out} S|}{|S|}$, that is,

$$P_{X,S}(2)\alpha \geqslant |\operatorname{Out} S|.$$

Given $s_2 \in S$, we know that $C_S(g_2 s_2) \neq \{1\}$, since by [15] a simple group cannot have a fixed-point-free automorphism. Therefore, there exists a non-trivial element $t \in S$ such that $g_2 s_2 \in C_X(t)$, and we can assume t to be of prime order, say u, by taking suitable powers, if necessary.

If $s_3 \in N_S(\langle t \rangle)$, then $\langle g_2 s_2, s_3 \rangle \not\geqslant S$, because $\langle t \rangle$ is centralized by $g_2 s_2$ and normalized by s_3, and hence is normal in $\langle g_2 s_2, s_3 \rangle$.

Thus

$$\alpha \geqslant \min_{t \in P} \big|N_S\big(\langle t \rangle\big)\big| \geqslant \min_{t \in P} \big|C_S(t)\big|$$

where P is a Sylow u-subgroup. If u^2 divides $|S|$, then $|N_P(\langle t\rangle)| \geqslant u^2$ so u^2 divides $|N_S(\langle t\rangle)|$. Otherwise, $P = \langle t\rangle$ is abelian and by Burnside's normal p-complement theorem, P is not self-normalizing, hence $|N_S(\langle t\rangle)| \geqslant 2u$. □

By [14], $P_{X,S}(2) \geqslant 1/2$, and actually $P_{X,S}(2) \geqslant 0.9$ for all but a finite set $\mathcal{S}$ of exceptions. The exceptions have socle one of: A_n (with $5 \leqslant n \leqslant 11$), $\mathrm{L}_2(q)$ (with $7 \leqslant q \leqslant 11$), $\mathrm{L}_3(q)$ (with $3 \leqslant q \leqslant 4$), $\mathrm{S}_4(3)$, M_{11} or M_{12}.

Lemma 2.2. *Let X be a 2-generated almost simple group with socle S. If there exists a 2-generator almost simple group H with socle S such that $P_{H,S}(2) < 0.9$, or if $|\operatorname{Out} S| \leqslant 4$, then X satisfies property $\mathcal{P}$.*

Proof. The probabilities $P_{H,S}(2)$ for $H \in \mathcal{S}$ are listed in [14]. Furthermore, [14, Corollary 1.2] proves that $P_{X,S}(3) \geqslant 139/150$ for all almost simple groups X. Thus it is straightforward to check that if X contains a 2-generator almost simple group H with socle S such that $P_{H,S}(2) < 0.9$, then X satisfies property $\mathcal{P}$.

Now assume that $|\operatorname{Out} S| \leqslant 4$ and X has no 2-generated subgroup with socle S that belongs to $\mathcal{S}$; in particular, $P_{X,S}(2) \geqslant 0.9$. By Corollary 4 in [10], all finite non-abelian simple groups containing an element t such that $|C_S(t)| < 5$ lie in $\mathcal{S}$. Therefore $|C_S(t)| \geqslant 5$ for every $t \in S$. Then $|C_S(t)| \geqslant 5 \geqslant 10|\operatorname{Out} S|/9 \geqslant |\operatorname{Out} S|/P_{X,S}(2)$ for every $t \in S$, hence by Proposition 2.1 the group X satisfies property $\mathcal{P}$. □

Lemma 2.3. *Let S be simple, with $|\operatorname{Out} S| > 4$. Then $\alpha_2 \geqslant \frac{10}{9}|\operatorname{Out} S|$.*

Proof. Since $|\operatorname{Out} S| > 4$ we deduce that $|S| \geqslant |\mathrm{L}_2(27)| = 9828$. In [1, Remark 2] it is stated that for every non-abelian simple group S and any involution t we can bound $|S| \leqslant |C_S(t)|^3$. Since $|\operatorname{Out} S| \leqslant \frac{6}{7}\log|S|$ (see [14]), it follows that $|C_S(t)| \geqslant |S|^{1/3} \geqslant \frac{10}{9}\frac{6}{7}\log|S| \geqslant \frac{10}{9}|\operatorname{Out} S|$ for every involution t. □

Fix a type of simple algebraic group X of rank r over the algebraic closure of a finite field. Let σ be an endomorphism of X with fixed point group X_σ of finite order. We will write $X(q) = X_\sigma$ if q is the absolute value of the eigenvalues of σ on the character group of the maximal torus T of X.

Lemma 2.4. *(See [7, Lemma 3.4].) Let C be the centralizer of an element in $X(q)$, then $|C| \geqslant (q-1)^r$.*

In the remainder of this section we consider the families of simple groups S with the property that $|\operatorname{Out} S| > 4$ for at least one group in the family. In the majority of cases, it suffices to use Lemma 2.4 to bound the order of an element centralizer in the simple group, and hence to show that the conditions of Proposition 2.1 are satisfied; however for a small number of groups we must calculate various values of α_u explicitly.

Lemma 2.5. *Let X be a 2-generated almost simple group with socle $S = \mathrm{L}_n(q)$. Then X satisfies property $\mathcal{P}$.*

Proof. Recall that $|\operatorname{Out} S| = 2dh$ for $n \geqslant 3$, and $|\operatorname{Out} S| = dh$ when $n = 2$, where $q = p^h$ and $d = (n, q-1)$. By Lemma 2.2, we can assume that $dh \geqslant 2$, and that $P_{X,S}(2) \geqslant 0.9$. In particular, the case $S = L_n(2)$ follows.

Let $t \in S = \mathrm{L}_n(q)$. We apply the previous lemma, with $r = n-1$ and dividing by d to pass from $X(q)$ to the associated simple group, to deduce that $|C_S(t)| \geqslant \frac{(q-1)^{n-1}}{d}$. By Proposition 2.1 it suffices to prove that

$$\begin{aligned} (q-1)^{n-1} &\geqslant \frac{20}{9} d^2 h \quad \text{if } n \geqslant 3 \\ q-1 &\geqslant \frac{10}{9} d^2 h \quad \text{if } n = 2. \end{aligned} \tag{2}$$

Suppose first that $n = 2$. If $q = 2^h$ then $d = 1$, and the result follows. Otherwise, if $q - 1 < 10d^2h/9$ then $q \in \{5, 9\}$ and $P_{X,\mathrm{L}_2(q)}(2) < 0.9$, contrary to assumption.

Now let $n = 3$, so that $d \leqslant 3$. Our assumption on $P_{X,S}(2)$ implies that $q \geqslant 5$. If $(q-1)^2 < 20h$ then $q \in \{5, 8\}$, but $d = 1$ for both of these q, so it suffices to verify that $(q-1)^2 \geqslant 20h/9$, which is clear.

Let $n \geqslant 4$. We use the fact that $d \leqslant q-1$, hence $(q-1)^{n-1}/d^2 \geqslant q-1$. For $p = 2$, if $2^h - 1 < 20h/9$ then $h < 3$. Hence $q = 2^2$, and so $(q-1)^{n-1} > 40d^2/9$ for $n \geqslant 4$ (if $n = 4$ then $d = 1$). If $p = 3$ then $3^h - 1 \geqslant 20h/9$ whenever $h \geqslant 2$; if $h = 1$, then $|\operatorname{Out} S| \leqslant 4$, contrary to assumption. If $p \geqslant 5$ then $q - 1 \geqslant 5^h - 1 \geqslant 20h/9$ for every h. □

Lemma 2.6. *Let X be an almost simple group with socle $S = \mathrm{U}_n(q)$, $n \geqslant 3$. Then X satisfies property $\mathcal{P}$.*

Proof. Let $t \in S = \mathrm{U}_n(q)$. Applying Lemma 2.4 with $r = n-1$ and dividing by $d = (n, q+1)$ to pass to the associated simple group, we get $|C_S(t)| \geqslant \frac{(q-1)^{n-1}}{d}$. Since $|\operatorname{Out} S| = 2dh$, with $q = p^h$, by Proposition 2.1 and Lemma 2.2 it suffices to prove that

$$(q-1)^{n-1} \geqslant \frac{20}{9} d^2 h \tag{3}$$

for groups S with $dh > 2$ and $P_{X,S} \geqslant 0.9$.

Now $d \leqslant n$, hence if $q > 2$ then $(q-1)^{n-1}/d^2 \geqslant (q-1)^{n-1}/n^2 \geqslant (q-1)^{3-1}/3^2$. Then $(q-1)^{3-1}/3^2 \geqslant \frac{20}{9}h$ for $q = 7$ or $q \geqslant 9$.

We now study the cases $q = 2, 4, 8, 3, 5$. Let $q = 2$. As $h = 1$, we can assume that 3 divides n (and $n \neq 3$, as $\mathrm{U}_3(2)$ is not simple). Then 3^2 divides $|S| = \frac{1}{d} 2^{n(n-1)/2}(2^2 - 1)(2^3 + 1)(2^4 - 1) \prod_{i=5}^{n} (2^i - (-1)^i)$, hence $\alpha_3 \geqslant 9 \geqslant (10/9)6 = (10/9)|\operatorname{Out} S|$. The same holds for the other odd prime divisors u of $|S|$, since $2u \geqslant 9$, and we conclude from Proposition 2.1 and Lemma 2.3.

Let $q = 4$. As $h = 2$, we can assume that $5 \mid n$. If $S = \mathrm{U}_5(4)$, then $|\operatorname{Out} S| = 20$ and we can use GAP to check that $\alpha_u \geqslant (10/9)20$ for every odd prime divisor of S, and as before we conclude from Proposition 2.1 and Lemma 2.3. If $n \geqslant 10$, then (3) holds.

Let $q = 8$. If $S = \mathrm{U}_3(8)$ then $|\operatorname{Out} S| = 18$, and we use GAP to check that $\alpha_u \geqslant 20$ for all odd prime divisors u of $|S|$. If $n \geqslant 4$, then $(8-1)^{n-1}/d^2 \geqslant 7^{n-1}/n^2 \geqslant 7^3/16 \geqslant (20/9)3$ and (3) holds.

Let $q = 3$. As $h = 1$, we can assume that $4 \mid n$. If $S = \mathrm{U}_4(3)$, then $|\operatorname{Out} S| = 8$ and, as 3^2 divides $|S|$, we see that $\alpha_u \geqslant 9 \geqslant (10/9)8$ for every odd prime divisor u of $|S|$. If $n \geqslant 8$, then $2^7 \geqslant (20/9)4^2 \geqslant (10/9)2d^2$ and (3) holds.

Let $q = 5$. As $h = 1$, we can assume that $3 \mid n$. If $S = \mathrm{U}_3(5)$, then $|\operatorname{Out} S| = 6$ and, as 3^2 divides $|S|$, we see that $\alpha_u \geqslant 7 \geqslant (10/9)6$ for every odd prime divisor u of $|S|$. If $n \geqslant 6$, then $4^5 \geqslant (20/9)6^2 \geqslant (10/9)2d^2$ and (3) is satisfied. □

Lemma 2.7. *Let X be an almost simple group with socle $S = \mathrm{S}_{2n}(q)$ $(n \geqslant 2)$ or $S = \mathrm{O}_{2n+1}(q)$ (q odd and $n \geqslant 3$). Then X satisfies property $\mathcal{P}$.*

Proof. Let $t \in S$. Applying Lemma 2.4 and dividing by $d = (2, q-1)$ to pass to the associated simple group, we get $|C_S(t)| \geqslant \frac{(q-1)^n}{d}$. Here $d \leqslant 2$, and by Lemma 2.2 we may assume that $|\operatorname{Out} S| = dh > 4$, so $h \geqslant 3$. It therefore suffices to prove that

$$\begin{aligned} \frac{(q-1)^n}{h} &\geqslant \frac{10}{9}4 \quad \text{if } q \text{ is odd} \\ \frac{(2^h-1)^n}{h} &\geqslant \frac{10}{9} \quad \text{if } q = 2^h > 2^4. \end{aligned} \tag{4}$$

If q is odd, then $(q-1)^n/h \geqslant (q-1)^2/h \geqslant (3^3-1)^2/3 > 40/9$. Otherwise $q = 2^h$ and $(2^h-1)^n/h \geqslant (2^3-1)^2/3 \geqslant 10/9$. Thus (4) is always satisfied. □

Lemma 2.8. *Let X be a 2-generated almost simple group with socle $S = \mathrm{O}^+_{2n}(q)$, $n \geqslant 4$. Then X satisfies property $\mathcal{P}$.*

Proof. Let $t \in S$. Applying Lemma 2.4 and dividing by $d = (4, q^n - 1)$ to pass to the associated simple group, we get $|C_S(t)| \geqslant \frac{(q-1)^n}{d}$. Since $|\operatorname{Out} S| = 2dh$ for $n \geqslant 5$ and $|\operatorname{Out} S| = 6dh$ for $n = 4$, it suffices to prove that

$$\begin{aligned} \frac{(q-1)^n}{d^2h} &\geqslant \frac{10}{9}2 \quad \text{if } n \geqslant 5 \\ \frac{(2^h-1)^n}{d^2h} &\geqslant \frac{10}{9}6 \quad \text{if } n = 4. \end{aligned} \tag{5}$$

Consider first the case $n \geqslant 5$. If q is odd, then $\frac{(q-1)^n}{d^2h} \geqslant \frac{(p^h-1)^5}{4^2h} \geqslant \frac{2^{5h}}{16h} \geqslant \frac{20}{9}$ whenever $h \geqslant 2$; if $h = 1$, then (5) is satisfied for either $p \geqslant 5$ or $p = 3$ and $n \geqslant 6$; finally, for $p = 3$ and $n = 5$ we get $d = (4, 3^5 - 1) = 2$ and thus $2^5 \geqslant \frac{20}{9}2^2$ and (5) is satisfied.

If $n \geqslant 5$ and q is even, then $d = 1$ and $|\operatorname{Out} S| = 2h$, so we can assume $h \geqslant 3$. Then $(2^h - 1)^n/h \geqslant (2^h - 1)^5/h \geqslant (2^3 - 1)^5/3 > 20/9$.

Let $n = 4$. If q is odd and $h \geqslant 2$ then $\frac{(q-1)^4}{d^2 h} \geqslant \frac{(p^h-1)^4}{4^2 h} \geqslant \frac{2^{4h}}{16h} \geqslant \frac{20}{3}$. If $h = 1$, then (5) is satisfied for $p \geqslant 5$. If $S = \mathrm{O}_8^+(3)$, then $P_{X,S}(2) \geqslant 139/150$, by [14, Remark 4.1], so $|\operatorname{Out} S|/P_{X,S}(2) < 26$. A straightforward GAP calculation shows that $N_S(\langle t \rangle) \geqslant 26$ whenever $|t|$ is an odd prime, and the result follows from Lemma 2.3 and Proposition 2.1.

Finally, if $n = 4$ and $q = 2^h$, then $d = 1$ and (5) is satisfied whenever $h \geqslant 2$. If $S = \mathrm{O}_8^+(2)$, then $|S| = 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$ and $(10/9)|\operatorname{Out} S| < 7$; thus $\alpha_u \geqslant (10/9)|\operatorname{Out} S|$ for every odd prime u and we conclude as before. □

Lemma 2.9. *Let X be a 2-generated almost simple group with socle $S = \mathrm{O}_{2n}^-(q)$, with $n \geqslant 4$. Then X satisfies property $\mathcal{P}$.*

Proof. Let $t \in S$. Applying Lemma 2.4 and dividing by $d = (4, q^n + 1)$ to pass to the associated simple group, we get $|C_S(t)| \geqslant \frac{(q-1)^n}{d}$. Since $|\operatorname{Out} S| = 2dh$, it suffices to prove that

$$\frac{(q-1)^n}{d^2 h} \geqslant \frac{10}{9} 2, \tag{6}$$

and by Lemma 2.2 we may assume that $dh > 2$ and $P_{X,S} \geqslant 0.9$.

If q is odd, then $\frac{(q-1)^n}{d^2 h} \geqslant \frac{(p^h-1)^4}{4^2 h} \geqslant \frac{2^{4h}}{16h} \geqslant \frac{20}{9}$ whenever $h \geqslant 2$. If $h = 1$, then (6) is satisfied for either $p \geqslant 5$ or $p = 3$ and $n \geqslant 6$. If $p = 3$ and $n = 4$ then $d = 2$, so $2^4 \geqslant \frac{20}{9} 2^2$ and again (6) is satisfied. If $S = \mathrm{O}_{10}^-(5)$, then $(10/9)|\operatorname{Out} S| < 9$; since 3^2 divides $|S|$ and $2 \cdot 5 > 9$, for every odd prime u we see that $\alpha_u \geqslant 9$ for every odd prime u. The result follows from Proposition 2.1.

Finally, if $q = 2^h$ then $d = 1$, so by assumption $h \geqslant 3$, and (6) holds. □

Lemma 2.10. *Let X be a 2-generated almost simple group with socle S. If S is a simple group of exceptional type, then X satisfies property $\mathcal{P}$.*

Proof. Let $t \in S$. Applying Lemma 2.4 and dividing by d to pass to the associated simple group, we get $|C_S(t)| \geqslant \frac{(q-1)^n}{d}$. By Lemma 2.2 it suffices to prove that

$$\frac{(q-1)^n}{d|\operatorname{Out} S|} \geqslant \frac{10}{9}, \tag{7}$$

and we may assume that $|\operatorname{Out} S| > 4$.

Let $S = \mathrm{G}_2(q)$. Then $d = 1$ and $|\operatorname{Out} S| \leqslant 2h$, so $h \geqslant 3$. Thus $\frac{(q-1)^2}{2h} \geqslant \frac{(2^h-1)^2}{2h} \geqslant (2^3 - 1)^2/6 \geqslant 10/9$ and (7) is satisfied. The same argument holds for $S = \mathrm{F}_4(q)$, since $d = 1$, $|\operatorname{Out} S| \leqslant 2h$ and $n = 4$.

Let $S = {}^2\mathrm{B}_2(q)$. Then $d = 1$ and $|\operatorname{Out} S| = h$, so $h \geqslant 5$. Thus $(q^{1/2} - 1)^2/h \geqslant (2^{h/2} - 1)^2/h \geqslant (2^{5/2} - 1)^2/5 \geqslant 10/9$ and (7) is satisfied. The same argument holds for $S = {}^2\mathrm{G}_2(q)$ and for $S = {}^2\mathrm{F}_4(q)$.

Let $S = {}^3\mathrm{D}_4(q)$. Since $d = 1$ and $|\operatorname{Out} S| \leqslant 3h$, we can assume that $h \geqslant 2$. Then $\frac{(q-1)^4}{3h} \geqslant \frac{(2^h-1)^2}{3h} \geqslant (2^2-1)^2/6 \geqslant 10/9$ and (7) is satisfied.

Let $S = \mathrm{E}_n(q)$, $n = 6, 7, 8$. Since $d \leqslant (q-1)$, $h \leqslant (q-1)$ and $|\operatorname{Out} S| \leqslant 2dh$, if $q \geqslant 3$ then $\frac{(q-1)^n}{2d^2h} \geqslant (q-1)^{6-3}/2 \geqslant (3-1)^3/2 \geqslant 10/9$ and (7) is satisfied. If $q = 2$, then $|\operatorname{Out} S| \leqslant 2$, contradicting our assumptions.

Finally, let $S = {}^2\mathrm{E}_6(q)$. Then $d = (3, q+1)$ and $|\operatorname{Out} S| = 2dh$. As $d \leqslant 3$ and $h \leqslant q-1$, if $q \geqslant 3$ then $\frac{(q-1)^6}{2\cdot d^2h} \geqslant \frac{(q-1)^5}{18} \geqslant (3-1)^5/18 \geqslant 10/9$ and (7) is satisfied. If $S = {}^2\mathrm{E}_6(2)$ then $(10/9)|\operatorname{Out} S| < 7$: since 3^2 divides $|S|$ and $2 \cdot 5 > 7$, for every odd prime u dividing $|S|$ we get $\alpha_u \geqslant 7$. The result follows from Lemma 2.3 and Proposition 2.1. □

3. Background material for the case $d(X) = 3$

In this section we collect some results and prove some elementary lemmas that will be helpful in both of the next two sections.

Theorem 3.1. *(See Häsä [9].) Let G be a finite almost simple classical group, of dimension n over $\mathbb{F}_q$. Let $m(G)$ be the number of conjugacy classes of maximal subgroups of G that do not contain* $\operatorname{soc} G$. *Then*

$$m(G) \leqslant 2n^{5.2} + n \log\log q.$$

Lemma 3.2. *Let $\mathcal{I}$ be a finite set of positive integers, and let $q \geqslant 3$. Then $\prod_{i\in\mathcal{I}}(q^i - 1) > q^{-1+\sum_{i\in\mathcal{I}} i}$.*

Proof. We see that

$$\prod_{i\in\mathcal{I}}(q^i-1) = q^{\sum_{i\in\mathcal{I}} i}\prod_{i\in\mathcal{I}}(1-q^{-i}) > q^{\sum_{i\in\mathcal{I}} i}\prod_{i=1}^{\infty}(1-q^{-i})$$

This product converges to a limit c_q with $1/q < c_q < 1$. □

The following result will be used extensively, without repeated citations, throughout Sections 4 and 5.

Proposition 3.3. *Let $q > 2$.*

(1) *Let $G = \mathrm{SL}_n(q)$. Then $q^{n^2-2} < |G| < q^{n^2-1}$.*
(2) *Let $G = \mathrm{SU}_n(q)$. Then $|G| < q^{n^2-1}$.*
(3) *Let $G = \mathrm{Sp}_n(q)$. Then $|G| < q^{(n^2+n)/2}$.*
(4) *Let $G_+ = \mathrm{SO}^+_n(q)$. Then $q^{n^2/2-n/2-1} < |G_+| < q^{(n^2-n)/2}$.*
(5) *Let $G_- = \mathrm{SO}^-_n(q) n-q$. Then $q^{n^2/2-n/2-1} < |G_-| < 2q^{(n^2-n)/2}$.*
(6) *Let $G_\circ = \mathrm{SO}^\circ_n(q)$. Then $|G_\circ| < q^{(n^2-n)/2}$.*

Proof. (1) We use the expression $|G| = q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-1)$. The upper bound is clear, and the lower bound follows from Lemma 3.2.

(2) We use $|G| = q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-(-1)^i)$. Note that $(q^{2k}-1)(q^{2k+1}+1) < q^{4k+1}$ for all k. Thus if n is odd then $|G| < q^{n(n-1)/2}\prod_{i=1}^{(n-1)/2} q^{4i+1} = q^{(n^2-n)/2+(n^2+n-2)/2}$. The result for n even is similar.

(3) This follows easily from $|G| = q^{n^2/4}\prod_{i=1}^{n/2}(q^{2i}-1)$.

(4) and (5) We use $|G_{\pm}| = q^{n(n-2)/4}(q^{n/2}\mp 1)\prod_{i=1}^{n/2-1}(q^{2i}-1)$. For the upper bound for G_-, note that $q^{n/2}+1 < 2q^{n/2}$. For the lower bound, use Lemma 3.2.

(6) This follows easily from $|G_\circ| = q^{(n-1)^2/4}\prod_{i=1}^{(n-1)/2}(q^{2i}-1)$. □

The following lemma follows straightforwardly from [3].

Lemma 3.4. *Let X be almost simple with socle S a classical group. If $d(X) = 3$, then n is even and at least four, and q is an even power of an odd prime. Furthermore, either $S = \mathrm{L}_n(q)$ and $X \not\leqslant \mathrm{P\Gamma L}_n(q)$, or $n \geqslant 8$ and $S = \mathrm{O}_n^+(q)$.*

Lemma 3.5. *Let X be almost simple with socle S. Let $\mathcal{M}$ be the set of maximal subgroups of X that supplement S, up to X-conjugacy. Then*

$$P_{X,S}(l) \geqslant 1 - \sum_{M\in\mathcal{M}} \frac{1}{|S : M\cap S|^{l-1}}.$$

Furthermore, if $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$ and $\sum_{M\in\mathcal{M}_1}|M| \leqslant m$, then

$$P_{X,S}(l) \geqslant 1 - \frac{m^{l-1}}{|X|^{l-1}} - \sum_{M\in\mathcal{M}_2} \frac{1}{|S : M\cap S|^{l-1}}.$$

Proof. The proof of the first claim is a routine calculation, using the fact that if l elements of X fail to generate X, but do project onto generators for X/S, then they must lie in some maximal subgroup of X that supplements S. For the second, rewrite $1/[S : M\cap S]$ as $|M|/|X|$. □

4. The linear groups X with $d(X) = 3$

In this section we prove that if X is almost simple with socle $S = \mathrm{L}_n(q)$, and $d(X) = 3$ (so that $q \geqslant 9$), then X has property $\mathcal{P}$. We fix this notation and these assumptions throughout this section.

The following is a straightforward calculation.

Lemma 4.1. *The value of $|\operatorname{Out} S|/|S|$ is less than $q^{-(n^2-5)}$.*

Lemma 4.2. *The probability $P_S(2)$ is bounded above by*

$$P_S(2) \leqslant 1 - \frac{(q-1)^2}{(q^n-1)^2} \leqslant 1 - \frac{4}{q^{2n-1}}.$$

Proof. The group S has a permutation action on $(q^n-1)/(q-1)$ points, and hence a maximal subgroup of the same index. For the final inequality, use $(q^{n-1}+\cdots+1)^2 < 2q^{2n-2}$. □

Lemma 4.3. *The group X has at most $n(5+\log n+\log\log q)$ conjugacy classes of geometric maximal subgroups.*

Proof. The group $X \not\leqslant \mathrm{P\Gamma L}_n(q)$, by Lemma 3.4. We use [12, Table 3.5.A] to count the geometric maximal subgroups of X, up to X-conjugacy. There are at most $n-1$ $\mathcal{C}_1$-subgroups, $n/2$ $\mathcal{C}_2$-subgroups, $\log n$ $\mathcal{C}_3$-subgroups, $(\sqrt{n}-1)^2$ $\mathcal{C}_4$-subgroups, $n\log\log q$ $\mathcal{C}_5$-subgroups, no $\mathcal{C}_6$-subgroups (since q is an odd square), $n\log n$ $\mathcal{C}_7$-subgroups, and $5n/2$ $\mathcal{C}_8$-subgroups. Since $n \geqslant 4$ we may simplify using $\log n \leqslant \sqrt{n}$. □

Lemma 4.4. *Assume that $n \geqslant 8$. Then the largest maximal subgroup of X that supplements S is geometric and has index $(q^n-1)(q^{n-1}-1)/(q-1)^2$. Furthermore, the largest non-geometric maximal subgroup of X has index at least q^{n^2-3n-3}.*

Proof. We take the classification of geometric subgroups of X from [12, Table 3.5.A]. We will work in $\mathrm{SL}_n(q)$, since the formulae for the subgroup orders are more straightforward.

Consider first the $\mathcal{C}_1$-subgroups. By Lemma 3.4, the group $X \not\leqslant \mathrm{P\Gamma L}_n(q)$, so the parabolic subgroups P_i are not maximal in X unless $i = n/2$, in which case they have order less than $q^{n^2/4}|\mathrm{SL}_{n/2}(q)|^2(q-1) < q^{3n^2/4-1} < q^{n^2-2n}$. The subgroup of type $P_{k,n-k}$ has order $q^{k(2n-3k)}|\mathrm{SL}_k(q)|^2|\mathrm{SL}_{n-2k}(q)|(q-1)^2$, so the index of $P_{1,n-1}$ follows from Proposition 3.3, and $|P_{k,n-k}| < q^{n^2-2nk+3k^2-1}$. Since $n \geqslant 2k$, $|P_{k,n-k}| \leqslant |P_{1,n-1}|$. The completely reducible subgroup of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_{n-1}(q)$ has order $q^{(n^2-3n+2)/2}\prod_{i=1}^{n-1}(q^i-1) < |P_{1,n-1}|$, whilst for $k \geqslant 2$ the subgroups of type $\mathrm{GL}_k(q) \oplus \mathrm{GL}_{n-k}(q)$ have order $|\mathrm{SL}_k(q)||\mathrm{SL}_{n-k}(q)|(q-1) < q^{n^2-2nk+2k^2-1} < q^{n^2-2n}$.

A $\mathcal{C}_2$-subgroup has order $|\mathrm{SL}_{n/t}(q)|^t(q-1)^{t-1}t! < q^{(n^2/t)-1}t^t$ for some divisor $t > 1$ of n. It suffices to show that $n^2(t-1)/t+1 \geqslant 2n+t\log_q t$. Now $t \geqslant 2$, so $n^2(t-1)/t \geqslant n^2/2$. Furthermore, $t \leqslant n$ and $q \geqslant 9$ so $2n + t\log_q t < n\log_2 n$, whilst $n^2/2+1 > n\log n$ for all $n \geqslant 8$.

The $\mathcal{C}_3$-subgroups have order at most $|\mathrm{GL}_{n/r}(q^r)|.r < q^{n^2/r+r} < q^{n^2-2n}$, for some prime divisor r of n. The $\mathcal{C}_4$-subgroups have order less than $|\mathrm{GL}_k(q)||\mathrm{GL}_{n/k}(q)| < q^{n^2/k^2+k^2} < q^{n^2/4+n} < q^{n^2-2n}$, since $k \geqslant 2$. The $\mathcal{C}_5$-subgroups have order at most $|\mathrm{SL}_n(q_0)|(q-1) < q^{n^2/2+1} < q^{n^2-2n}$, since $q_0^r = q$ with $r > 1$. Class $\mathcal{C}_6$ is empty as q is a square.

The $\mathcal{C}_7$-subgroups have order less than $|\mathrm{GL}_k(q)|^r r! < q^{rk^2} r^r$. Using $k = n^{1/r}$ and $2 \leqslant r < \sqrt{n}$, it suffices to prove that $rn^{2/r} + r\log_q r \leqslant n^2 - 2n$. Now $r\log_q r < (1/3)r\log_2 r$, so $rn^{2/r} + r\log_q r < n^{3/2} + (1/6)n^{1/2}\log n < 2n^{3/2}$, and the result follows.

In class $\mathcal{C}_8$, the symplectic groups have order less than $q^{n^2/2+n/2+1}$, and are larger than the orthogonal groups. The unitary groups have order at most $|\mathrm{SU}_n(q^{1/2})|(q-1) < q^{n^2-2n}$.

Finally, by [13], if a subgroup H of X is not geometric, then either H has socle A_{n+1} or A_{n+2} (which would imply that H preserves a non-degenerate form, and hence is non-maximal: see for instance [11, Table 2(a)]), or $|H|$ is at most q^{3n}. Since $n \geqslant 8$ this is less than q^{n^2-2n-1}. □

Theorem 4.5. *Let $n \geqslant 8$. Then X satisfies property $\mathcal{P}$.*

Proof. We use Lemma 3.5: group together first the geometric maximal subgroups of S, using Lemma 4.3 and the first part of Lemma 4.4, and then the non-geometric maximal subgroups, using Theorem 3.1 and the second part of Lemma 4.4.

$$\begin{aligned} P_{X,S}(3) &\geqslant 1 - \frac{n(5+\log n+\log\log q)(q-1)^4}{(q^n-1)^2(q^{n-1}-1)^2} - \frac{2n^{5.2}+n\log\log q}{q^{2n^2-6n-6}} \\ &\geqslant 1 - \frac{q^{\log n}(q+\log(q^{\log n})+q)}{(q^{n-1}+\cdots+1)^2(q^{n-2}+\cdots+1)^2} - \frac{2q^{5.2\log_9 n}+q^{\log_9 n+1}}{q^{2n^2-6n-6}} \\ &\geqslant 1 - \frac{q^{2\log n}}{q^{2(2n-3)}} - \frac{2q^{2\log n}}{q^{2n^2-6n-6}} \\ &\geqslant 1 - q^{-2(2n-\log n-3)} - q^{-(2n^2-7n-6)}. \end{aligned}$$

Then by Lemma 4.2,

$$P_{X,S}(3) - P_S(2) \geqslant \frac{4}{q^{2n-1}} - \frac{1}{q^{2(2n-\log n-3)}} - \frac{1}{q^{2n^2-7n-6}} > \frac{1}{q^{n^2-5}}.$$

The result then follows from Lemma 4.1. □

We finish this section by considering the cases not covered by Theorem 4.5.

Proposition 4.6. *Let $n = 4$. Then X satisfies property $\mathcal{P}$.*

Proof. First we show that

$$P_{X,S}(3) \geqslant 1 - \frac{5(q-1)^2}{(q^2+1)^2(q^3-1)^2} \tag{8}$$

By Lemma 3.4, the group $X \not\leqslant \mathrm{P\Gamma L}_4(q)$, and $q \geqslant 9$. We work in $\mathrm{SL}_4(q)$. We shall divide the conjugacy classes of maximal subgroups of X that supplement S into five sets, each

of combined order at most $q^6(q-1)(q^2-1)^2$, and then (8) will follow from Lemma 3.5. We take the list of maximal subgroups of X from [2, Tables 8.8 and 8.9].

There is one conjugacy class of $\mathcal{C}_1$-subgroups of each type. The subgroups of type P_2 have order $q^6(q-1)(q^2-1)^2 > q^{10}$, and hence index $(q^3-1)(q^2+1)/(q-1)$. The subgroups of type $P_{1,3}$ have order less than q^{10}. The subgroups of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_3(q)$ have order less than q^9.

There are two classes of $\mathcal{C}_2$-subgroups, of combined order less than q^8. There is one class of $\mathcal{C}_3$-subgroups, of order less than q^8.

There are at most $4 \log\log q$ classes of $\mathcal{C}_5$-subgroups, of combined order at most $16(\log\log q)q^3(q-1)(q^{3/2}-1)(q^2-1) < q^{10}$.

There are at most two classes of symplectic groups, of combined order at most $4q^4(q^2-1)(q^4-1) < |P_2|$, since $q \geqslant 9$. There are at most four classes of unitary groups, of combined order at most $16(q^{1/2})^{15} < q^9$, by Proposition 3.3. There are at most four classes of orthogonal groups, with total order sum less than $32q^6 < q^8$ by Proposition 3.3. Since q is not prime, there are no further maximal subgroups.

Our first set of subgroups contains only P_2; our second contains $P_{1,3}$; our third contains the subgroup of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_3(q)$, the $\mathcal{C}_2$- and the $\mathcal{C}_3$-subgroups, the unitary and the orthogonal subgroups; our fourth is the $\mathcal{C}_5$-subgroups; and our fifth is the symplectic subgroups. Eq. (8) is now proved.

By Lemma 4.2

$$P_{X,S}(3) - P_S(2) \geqslant \frac{(q-1)^2((q^3-1)^2 - 5(q^2-1)^2)}{(q^3-1)^2(q^4-1)^2} > \frac{(q-1)^2(q^6-q^5)}{q^{14}}.$$

The result now follows from Lemma 4.1. □

Proposition 4.7. *Let $n = 6$. Then X satisfies property $\mathcal{P}$.*

Proof. First we show that

$$P_{X,S}(3) \geqslant 1 - 3q^{-16} \tag{9}$$

We take the lists of maximal subgroups of X from [2, Tables 8.24 and 8.25]. As before, we shall work in $\mathrm{SL}_6(q)$. We shall divide the conjugacy class representatives of the maximal subgroups into three sets, such that the sum of the orders of the subgroups in each set is at most q^{26}. Proposition 3.3 then implies (9).

There is one class of each type of $\mathcal{C}_1$-subgroup. The subgroup P_3 has order less than q^{26}, and forms the first set on its own. The subgroup $P_{1,5}$ has order less than q^{26}, and forms the second set on its own.

The remaining groups all form one set. The subgroup $P_{2,4}$ has order less than q^{23}. The subgroup of type $\mathrm{GL}_1(q) \oplus \mathrm{GL}_5(q)$ has order less than q^{25}. The subgroup of type $\mathrm{GL}_2(q) \oplus \mathrm{GL}_4(q)$ has order less than q^{19}.

Next we consider the $\mathcal{C}_2$-, $\mathcal{C}_3$- and $\mathcal{C}_4$-subgroups, of which there is one class of each type. The $\mathcal{C}_2$-subgroups of types $\mathrm{GL}_1(q) \wr \mathrm{S}_6$, $\mathrm{GL}_2(q) \wr \mathrm{S}_3$ and $\mathrm{GL}_3(q) \wr \mathrm{S}_2$ have order less than q^8, q^{12} and q^{18}, respectively, since $q \geqslant 9$. The $\mathcal{C}_3$-subgroups of types $\mathrm{GL}_3(q^2)$ and $\mathrm{GL}_2(q^3)$ have order less than q^{18} and q^{12}, respectively. The $\mathcal{C}_4$-subgroups have order less than q^{11}.

Now consider the $\mathcal{C}_5$-subgroups. There are at most $6 \log \log q$ classes, each of order at most $6q^{35/2}$. Thus we bound the sum of their orders by q^{20}.

Next we consider the $\mathcal{C}_8$- and $\mathcal{C}_9$-subgroups. There are at most six classes of orthogonal groups, of total order less than q^{17}. There are at most three classes of symplectic groups, of total order at most q^{22}. There are at most six classes of unitary groups, of total order at most q^{20}. Since $d(X) = 3$, the $\mathcal{C}_9$-subgroups have order sum less than $4|\mathrm{SL}_3(4)| < q^{10}$, so (9) now follows.

The result is now immediate from Lemmas 4.1 and 4.2. □

5. The orthogonal groups X with $d(X) = 3$

Throughout this section, we let $S = \Omega_n^+(q)$ for $n \geqslant 8$, and let $\overline{S} = S/Z(S)$ be the corresponding simple group. We let X be almost simple with socle $\overline{S}$, and assume throughout that $d(X) = 3$. Note that this implies that $q \geqslant 9$. We shall show that X has property $\mathcal{P}$. Information about the maximal subgroups of X is taken from [12] and [2, Chapter 2].

The following is a straightforward calculation, using Proposition 3.3.

Lemma 5.1. *The value of* $|\operatorname{Out} \overline{S}|/|\overline{S}|$ *is less than* $q^{-(n^2/2-n/2-3)}$.

Lemma 5.2. *The probability* $P_{\overline{S}}(2)$ *is bounded above by*

$$P_{\overline{S}}(2) \leqslant 1 - \frac{2(q-1)^2}{(q^{n-1} + q^{n/2} - q^{n/2-1} - 1)^2} + \frac{1}{q^{4n-10}}.$$

Proof. The group S has a permutation action on $(q^{n/2} - 1)(q^{n/2-1} + 1)/(q-1)$ points, on the cosets of the parabolic P_1. Here P_1 is the stabilizer of a totally singular 1-space $\langle v_1 \rangle$, and has shape $[q^{n-2}].(\frac{q-1}{2} \times \Omega_{n-2}^+(q)).2$.

Let $g \in S$ send v_1 to $v_2 \in \langle v_1 \rangle^\perp \setminus \langle v_1 \rangle$. Then $K := P_1 \cap P_1^g$ has shape $[q^{1+2(n-4)}].(((q-1)/2)^2 \times \Omega_{n-4}^+(q)).2^2$. Thus

$$[S : K] = q\big(q^{n/2} - 1\big)\big(q^{(n-4)/2} + 1\big)\big(q^{n-2} - 1\big)/(q-1)^2 \geqslant q^{2n-5},$$

since $n \geqslant 8$ and $q \geqslant 9$. If two elements of S both lie in P_1, or in P_1^g, then they do not generate S. Thus $P_{\overline{S}}(2) \leqslant 1 - [S : P_1]^{-2} - [S : P_1^g]^{-2} + [S : K]^{-2}$, and the result follows. □

In Lemmas 5.3 to 5.9 we find upper bounds for the sum of the orders of the preimages in S of the intersection of various classes of maximal subgroups of X with $\overline{S}$, up to X-conjugacy. We describe this as their 'contribution to the subgroup order sum'.

Lemma 5.3. *The contribution to the subgroup order sum of the maximal subgroups $P_2, P_3, \ldots, P_{n/2}$ is at most $(1/2)q^{n^2/2-39n/16+7}$ when $n \geqslant 14$, and at most q^{51} when $n = 12$.*

Proof. There is one class of each P_k except when $k \geqslant n/2 - 1$. When $k = n/2$ there are two or no classes, depending on $X/\overline{S}$, and when $k = n/2 - 1$ there are no classes or one class, with the same conditions on $X/\overline{S}$.

If $k < n/2$, then

$$|P_k| = q^{k(n-\frac{1+3k}{2})}\big|\mathrm{GL}_k(q)\big|\big|\Omega^+_{n-2k}(q)\big| < 1/2q^{(n^2-n-2nk+k+3k^2)/2}, \tag{10}$$

whilst $|P_{n/2}|$ is half of this.

For $n = 12$ the result now follows from (10) and a routine calculation, so assume for the rest of the proof that $n \geqslant 14$. There are at most $n/2 - 1$ classes, and we claim that each group has order less than $(1/2)q^{n^2/2-5n/2+7}$. Since $n/2 - 1 < q^{n/16}$ for these n and q, the result will follow.

For $k = 2$ the claim follows from (10). For other k, it suffices to show

$$\big(n^2 - 5n + 14\big) - \big(n^2 - n - 2nk + k + 3k^2\big) = -3k^2 + k(2n-1) - 4n + 14 \geqslant 0.$$

The left hand side is a quadratic in k with negative k^2 coefficient, which is positive when $k = 3$, and non-negative when $k = n/2$, so it must be positive for all values of k in between. □

Lemma 5.4. *Let $\mathcal{K}$ be the groups of type $\mathrm{GO}^\epsilon_m(q) \perp \mathrm{GO}^\epsilon_{n-m}(q)$, with $m \geqslant 2$. The contribution of $\mathcal{K}$ to the subgroup order sum is at most $q^{n^2/2-9n/4+4}$.*

Proof. If m is odd then there are up to two conjugacy classes, whilst if m is even then there is one class with $\epsilon = +$ and one with $\epsilon = -$.

Each group has size at most $|\mathrm{SO}^\epsilon_m(q)||\mathrm{SO}^\epsilon_{n-m}(q)| \leqslant 4q^{\frac{1}{2}(n^2+2m^2-n(2m+1))}$. Substituting $m+1$ in place of m, and using $2m \leqslant n-2$, shows that this decreases with increasing m, so is bounded above by $4q^{\frac{1}{2}(n^2-5n+8)}$. Bounding $4(n-4)$ by $q^{n/4}$ gives the result. □

Lemma 5.5. *The contribution of the $\mathcal{C}_2$-subgroups to the subgroup order sum is less than $q^{8n^2/25+n+1}$ when $n \geqslant 14$, and less than q^{37} when $n = 12$.*

Proof. The result for $n = 12$ is a straightforward calculation, using [2, Table 8.82], so assume $n \geqslant 14$.

Since $d(X) = 3$, there are no groups of type $\mathrm{GO}_1(p) \wr \mathrm{S}_n$ or $\mathrm{GO}_{n/2}(q)^2$. There are at most two classes of type $\mathrm{GL}_{n/2}(q)$, each of order at most $2q^{n^2/4}$.

This leaves only type $\mathrm{GO}^\epsilon_m(q) \wr \mathrm{S}_t$, where $n = mt$ with $m > 1$. For each m there are at most two classes, and the group order is bounded above by

$$\begin{aligned}\left|\mathrm{SO}^\epsilon_m(q)\right|^t 2^{2(t-2)} t! &< q^{n(m-1)/2} 2^{2(t-2)} t! \\ &< q^{n(n/t-1)/2} t^{2t} = q^{n(n/t-1)/2 + 2t\log_q t} \\ &< q^{n(n/4-1/2+2\log_9 n)} < q^{n(8n/25+15/16)}.\end{aligned}$$

The number of choices for t is at most $n/2 - 1 \leqslant q^{n/16}$. Thus the total contribution of these groups is $2q^{8n^2/25+n}$. The result follows. □

Lemma 5.6. *The contribution of the $\mathcal{C}_3$-subgroups to the subgroup order sum is less than $q^{n^2/4+1}$.*

Proof. If $n \equiv 0 \bmod 4$, then there are up to two classes of groups of order at most $(q+1)|\mathrm{SU}_{n/2}(q)| < 2q^{n^2/4}$. Conversely, if $n \equiv 2 \bmod 4$, then there are up to two classes of groups of order at most $2|\mathrm{SO}^\circ_{n/2}(q^2)| < 2q^{n^2/4-n/2}$. Thus these two types contribute at most $4q^{n^2/4}$ between them.

The remaining type is $\mathrm{GO}^+_{n/s}(q^s)$. For $s = 2$ there are up to two classes, of order at most $2|\mathrm{SO}^+_{n/2}(q^2)| < 2q^{n^2/4-n/2}$. For odd s there are $\log n < \frac{2}{3}q^{n/2}$ classes, each of order at most $3|\Omega^+_{n/3}(q^3)| < \frac{3}{2}q^{n^2/6-n/2}$. So for s odd the order sum is at most $q^{n^2/6}$. Thus the $\mathcal{C}_3$-groups contribute less than $5q^{n^2/4} + q^{n^2/6}$, as required. □

Lemma 5.7. *The contribution of the $\mathcal{C}_4 \cup \mathcal{C}_7$-subgroups to the subgroup order sum is at most $q^{n^2/8+n/2+3}$.*

Proof. We work our way through the types of $\mathcal{C}_4$- and $\mathcal{C}_7$-subgroups. Consider first type $\mathrm{Sp}_m(q) \otimes \mathrm{Sp}_{n/m}(q)$. When these groups are maximal, there are two classes. Since both m and n/m are even, and $m < \sqrt{n}$, there are at most $n/8$ possible m. Each group has order at most $|\mathrm{Sp}_m(q)||\mathrm{Sp}_{n/m}(q)| < q^{\frac{1}{2}(m^2+m+n^2/m^2+n/m)}$. Substitute $m+2$ for m, and use $m(m+2) \leqslant n$, to see that this is non-increasing with m, and so is maximal when $m = 2$. Thus the sum of the group orders is less than $(n/4)q^{n^2/8+n/4+3} < (1/2)q^{n^2/8+n/2+3}$.

Consider next type $\mathrm{GO}^{\epsilon_1}_{n_1}(q) \otimes \mathrm{GO}^{\epsilon_2}_{n_2}(q)$. Here $n_1 \geqslant 4$ with n_1 even, $n_2 \geqslant 3$ and $n_1 n_2 = n$. If n_2 is odd then $\epsilon_1 = +$ and there is a unique conjugacy class, so there are at most $n/4$ groups. Otherwise (ϵ_1, ϵ_2) is $(+,+)$, $(+,-)$ or $(-,-)$. If $\epsilon_1 = \epsilon_2$ then without loss of generality $n_1 < \sqrt{n}$, and since $n \geqslant 24$ for this type to exist we deduce $n_1 < n/4$. For each such n_1 we get up to two classes of each type. If $(\epsilon_1, \epsilon_2) = (+,-)$ then n_1 and n_2 are even, so there are at most $n/4$ possible n_1, and for each n_1 we get up to two classes. So we have found at most $7n/4$ classes of groups. Each group has order at most $2|\mathrm{SO}^{\epsilon_1}_m(q)||\mathrm{SO}^{\epsilon_2}_{n/m}(q)| < 8q^{m^2/2-m/2+n^2/2m^2-n/2m}$. Substituting $m+1$ for m gives

a non-increasing function for $m < \sqrt{n}$, so the maximum of this bound is when $m = 3$. Thus we bound the sum of the group orders by $7n/4 \cdot 8q^{n^2/18-n/6+3} < q^{n^2/18+n/6+3}$.

Consider next the $\mathcal{C}_7$-subgroups, which are only maximal when $t \leqslant 3$. For type $\mathrm{Sp}_m(q) \wr \mathrm{S}_t$, we require $t = 2$ for maximality, so we find one class, of order at most $|\mathrm{Sp}_{\sqrt{n}}(q)|^2 < q^{n+\sqrt{n}}$. For type $\mathrm{GO}^+_m(q) \wr \mathrm{S}_t$, when $t = 2$ there is one class, of order $|\mathrm{SO}^+_{\sqrt{n}}(q)|^2 \cdot 2 < 2q^{n-\sqrt{n}}$, and when $t = 3$ there are two classes, of total order at most $96|\mathrm{SO}^+_{n^{1/3}}(q)|^3 < q^{3/2n^{2/3}-3/2n^{1/3}+2}$. For type $\mathrm{GO}^-_m(q) \wr \mathrm{S}_t$, when $t = 2$ there are at most two classes, of total order at most $8|\mathrm{SO}^-_{\sqrt{n}}(q)|^2 < q^{n-\sqrt{n}+2}$, and when $t = 3$ there are at most two classes, of total order at most $96|\mathrm{SO}^-_{n^{1/3}}(q)|^3 < q^{3/2n^{2/3}-3/2n^{1/3}+4}$. The order sum of the non-symplectic groups is less than $\frac{1}{2}q^{n+\sqrt{n}}$, so the total contribution from $\mathcal{C}_7$-subgroups is less than $q^{n+\sqrt{n}+1}$. The result follows. □

Lemma 5.8. *The contribution of the $\mathcal{C}_5$-subgroups of X to the subgroup order sum is at most $q^{n^2/4-n/4+2}$.*

Proof. There are at most two classes of types $\mathrm{GO}^-_n(q^{1/2})$ and $\mathrm{GO}^+_n(q^{1/2})$, and $\log\log q$ of type $\mathrm{GO}^+_n(q^{1/r})$. Groups of type $\mathrm{GO}^-_n(q^{1/2})$ have order at most $2|\mathrm{SO}^-_n(q^{1/2})| < 4q^{n^2/4-n/4}$, whilst groups of type $\mathrm{GO}^+_n(q^{1/2})$ have order at most $2|\mathrm{SO}^+_n(q^{1/2})| < 2q^{n^2/4-n/4}$. Type $\mathrm{GO}^+_n(q^{1/r})$ has group order at most $q^{n^2/6-n/6}$, since $r \geqslant 3$. Thus we bound the sum by $12q^{n^2/4-n/4} + (\log\log q)q^{n^2/6-n/6} \leqslant q^{n^2/4-n/4+3/2} + q^{n^2/6-n/6+1}$. □

Lemma 5.9. *The contribution of the $\mathcal{C}_2 \cup \cdots \cup \mathcal{C}_9$-subgroups to the subgroup order sum is at most $2q^{8n^2/25+n+1}$ when $n \geqslant 14$, and at most $2q^{44}$ when $n = 12$.*

Proof. We first consider $n \neq 12$. By Lemma 5.5 the sum of the orders of the maximal $\mathcal{C}_2$-subgroups is at most $N := q^{8n^2/25+n+1}$. We divide the remaining maximal subgroups under consideration into four sets, which in total sum to N.

The first is the maximal $\mathcal{C}_3$-subgroups, which by Lemma 5.5 have order summing to $q^{n^2/4+1}$. The second is the maximal $\mathcal{C}_4 \cup \mathcal{C}_7$-subgroups, which by Lemma 5.7 have order summing to $q^{n^2/8+n/2+3}$. The fourth is the maximal $\mathcal{C}_5$-subgroups, which by Lemma 5.8 have order summing to $q^{n^2/4-n/4+2}$.

The final set is the maximal $\mathcal{C}_9$-subgroups. By [13] any such subgroup of X either has order at most q^{3n} (in X) or is almost simple, with socle A_{n+1} or A_{n+2}. The groups with socle A_{n+1} or A_{n+2} arise only over prime fields. By Theorem 3.1 there are at most $2n^{5/2} + n\log\log q$ classes of subgroups, and $2n^{5/2} + n\log\log q < q^{2n/3}/2$ since $n \geqslant 12$ and $q \geqslant 9$. So the sum of the orders of the maximal $\mathcal{C}_9$-subgroups is at most $q^{3n+2n/3}$.

Classes $\mathcal{C}_6$ and $\mathcal{C}_8$ are empty, so the result for $n \geqslant 14$ follows. For $n = 12$ we perform a similar calculation, but using the more precise value in Lemma 5.5, and noting that the largest contribution is from Class $\mathcal{C}_9$. □

Theorem 5.10. *Let $n \geqslant 12$. Then X satisfies property $\mathcal{P}$.*

Proof. To bound $P_{X,\overline{S}}(3)$ we consider two individual conjugacy classes of groups, namely the groups of type P_1 and $\mathrm{GO}_1(q) \perp \mathrm{GO}_{n-1}(q)$, and three sets of groups, namely the remaining parabolic subgroups, the remaining completely reducible subgroups, and all other maximal subgroups.

If $n \geqslant 18$, then $2q^{8n^2/25+n+1}+\frac{1}{2}q^{n^2/2-39n/16+7} < q^{n^2/2-9n/4+4}$, so we use Lemmas 5.3, 5.4 and 5.9 to bound the sum of the three sets of groups by $2q^{n^2/2-9n/4+4}$. If $n \in \{12, 14, 16\}$ then we bound the sum of the orders of these groups by $2q^{51}$, $3q^{78}/2$ and q^{99}, respectively.

The parabolic group P_1 has order $q^{n-2}(q-1)|\Omega^+_{n-2}(q)|$, and there are two classes of groups of type $\mathrm{GO}_1(q) \perp \mathrm{GO}_{n-1}(q)$ each of order $|\mathrm{SO}_{n-1}(q)|$.

Thus, using Proposition 3.3, for $n \geqslant 18$ we calculate

$$\begin{aligned} P_{X,S}(3) &\geqslant 1 - \left(\frac{q^{n-2}(q-1)|\Omega^+_{n-2}(q)|}{|\Omega^+_n(q)|}\right)^2 - 2\left(\frac{|\mathrm{SO}_{n-1}(q)|}{|\Omega^+_n(q)|}\right)^2 - \left(\frac{2q^{n^2/2-9n/4+4}}{\frac{1}{2}q^{n^2/2-n/2-1}}\right)^2 \\ &\geqslant 1 - \frac{(q-1)^2}{(q^{n-1}+q^{n/2}-q^{n/2-1}-1)^2} - \frac{8}{q^{n-2}(q^n-2q^{n/2}+1)} - \frac{16}{q^{7n/2-10}}. \end{aligned}$$

The result then follows from Lemmas 5.1 and 5.2. For $n \in \{12, 14, 16\}$ we carry out a similar calculation. □

Proposition 5.11. *Let $n = 10$. Then X satisfies property $\mathcal{P}$.*

Proof. We use [2, Tables 8.66 and 8.67]. Consider first the parabolic subgroups, of which there is one class of each. The group P_1 has order less than $\frac{1}{2}q^{37}$, whilst the orders of P_2, P_3 and P_4 are less than $\frac{1}{2}q^{32}$, $\frac{1}{2}q^{30}$, and $\frac{1}{2}q^{31}$, respectively. The group P_5 is non-maximal, since $d(X) = 3$.

Consider next the completely reducible subgroups. We shall multiply the order of the stabilizers of odd-dimensional subspaces by 2, since there are at most two classes. Thus the sum of the orders of the groups of type $\mathrm{GO}_1(q) \perp \mathrm{GO}_9(q)$, $\mathrm{GO}^{\pm}_2(q) \perp \mathrm{GO}^{\pm}_8(q)$, $\mathrm{GO}_3(q) \perp \mathrm{GO}_7(q)$ and $\mathrm{GO}^{\pm}_4(q) \perp \mathrm{GO}^{\pm}_6(q)$ are less than $2|\mathrm{SO}_9(q)|$, $5q^{29}$, $2q^{24}$ and $5q^{21}$, respectively. We bound the sum of the last three of these by q^{30}.

Moving on to the $\mathcal{C}_2$-subgroups, type $\mathrm{GO}^+_2(q) \wr \mathrm{S}_5$ contributes less than $960|\mathrm{SO}^+_2(q)|^5 < q^9$. The order sum for types $\mathrm{GO}_5(q) \wr \mathrm{S}_2$ and $\mathrm{GO}_5(q)^2$ is less than $4|\mathrm{SO}_5(q)|^2 < 4q^{20}$. There is one class of groups of type $\mathrm{GL}_5(q).2$, of order at most q^{25}. There are at most two classes of $\mathcal{C}_3$-subgroups, of combined order less than $4q^{20}$. There are at most $\log\log q$ classes of $\mathcal{C}_5$-subgroups of type $\Omega^+_{10}(q_0)$, of combined order at most q^{16}. There are two classes of groups of each of the types $\mathrm{SO}^{\pm}_{10}(q^{1/2})$, of combined order at most $2q^{45/2} < q^{23}$.

These complete the maximal subgroups of X. Thus the sum of the $\mathcal{C}_2$-, $\mathcal{C}_3$- and $\mathcal{C}_5$-subgroups of X is at most $2q^{25}$, and so the sum of the orders of all maximal subgroups of X, up to X-conjugacy, is $|P_1|+2|\mathrm{SO}_9(q)|+q^{32}$. The result now follows from Lemmas 5.1 and 5.2. □

We finish with $n = 8$. Detailed maximal subgroup information is taken from [2, Table 8.50], and it may help the reader to consult this table.

Lemma 5.12. *Let $n = 8$. Then*

$$P_{\overline{S}}(2) \leqslant 1 - \frac{4(q-1)^2}{(q^3+1)^2(q^4+1)^2} + \frac{6}{q^{22}}$$

Proof. Let the basis of the natural vector space be $e_1, \dots, e_4, f_4, \dots, f_1$, so that the bilinear form has antidiagonal matrix with all nonzero entries 1. The group S has a permutation action on $(q^3+1)(q^4-1)/(q-1)$ points, on the cosets of $H_1 = S_{\langle e_1 \rangle}$, of shape $[q^6].(\frac{q-1}{2} \times \Omega_6^+(q)).2$. For $i \in \{2,3,4\}$, let H_i be the conjugate of H that stabilizes $\langle e_i \rangle$.

If $i \neq j$ then $H_{ij} := H_i \cap H_j$ has shape

$$\big[q^9\big].\big(\big((q-1)/2\big)^2 \times \Omega_4^+(q)\big).2^2.$$

Thus $[S : H_{ij}] = q(q^2+1)(q^3+q^2+q+1)(q^5+\cdots+1) > q^{11}$. Furthermore, if i, j, k are distinct then $H_{ijk} := H_i \cap H_j \cap H_k$ has shape

$$\big[q^9\big].\big(\big((q-1)/2\big)^3 \times \Omega_2^+(q)\big).2^3$$

and so has index $q^3(q+1)(q^3+q^2+q+1)^2(q^5+\cdots+1) < q^{16}$ in S. The group $H_{1234} = H_{123} \cap H_4$ has shape $[q^6].((q-1)/2)^4.2^3$ and so has index $q^6(q+1)(q^3+q^2+q+1)^2(q^5+\cdots+1) > q^{18}$ in S.

Hence

$$\begin{aligned} P_{\overline{S}}(2) &\leqslant 1 - 4[S:H_1]^{-2} + 6[S:H_{12}]^{-2} - 4[S:H_{123}]^{-2} + [S:H_{1234}]^{-2} \\ &\leqslant 1 - 4(q-1)^2\big(q^3+1\big)^{-2}\big(q^4-1\big)^{-2} + 6q^{-22} - 4q^{-32} + q^{-36} \\ &\leqslant 1 - 4(q-1)^2\big(q^3+1\big)^{-2}\big(q^4-1\big)^{-2} + 6q^{-22} \end{aligned}$$

and the result follows. □

Proposition 5.13. *Let $n = 8$. Then X satisfies property $\mathcal{P}$.*

Proof. We shall work through the 42 rows of [2, Table 9.50], and divide the maximal subgroups of X that complement $\overline{S}$ into three families: the groups that are $\mathrm{Aut}\,\overline{S}$-conjugate to P_1, the groups that are $\mathrm{Aut}\,\overline{S}$-conjugate to the $\mathcal{C}_1$-subgroups of type $\mathrm{GO}_1(q) \oplus \mathrm{GO}_7(q)$, and the rest. The result will then follow from Lemmas 3.5, 5.1 and 5.12.

Rows 3, 9, 10, 11, 14, 17, 20 to 24, 30, 32, and from 35 onwards, do not occur for $d(X) = 3$, so can be excluded from our calculations.

Rows 1 and 2 describe the groups that are $\mathrm{Aut}\,\overline{S}$-conjugate to P_1. The sum of the squares of the reciprocals of their indices is $3(q-1)^2/((q^3+1)^2(q^4-1)^2)$.

Rows 7 and 8 describe the groups of type $\mathrm{GO}_1(q) \oplus \mathrm{GO}_7(q)$. The sum of the squares of the reciprocals of their indices is less than $24/(q^6(q^4-1)^2)$.

Rows 4 to 6 describe $\mathcal{C}_1$-subgroups, of total order less than $2q^{19}$. Rows 12 and 13 describe $\mathcal{C}_1$-subgroups, of total order less than $3(q-1)q^{15}$. Rows 15 and 16 describe $\mathcal{C}_1$-subgroups, of total order less than $3(q+1)q^{15}$. These four rows describe groups of total order less than $6q^{16}$. Rows 18 and 19 describe $\mathcal{C}_1$-subgroups, of total order less than $6q^{13}$.

Rows 25 and 26 describe $\mathcal{C}_2$-subgroups of total order less than $1732q^4 < q^8$. Rows 27 to 29 describe $\mathcal{C}_2$-subgroups of total order less than $8q^{12} < q^{13}$.

Row 31 is $\mathcal{C}_5$-subgroups, of total order less than $\log\log q(q^{1/3})^{28}/2 < q^{10}$. Rows 33 and 34 describe $\mathcal{C}_5$-subgroups, of total order less than $12q^{14}$.

We bound the sum of the orders of the class representatives of all of the maximal subgroups of X that supplement $\overline{S}$, other than those that are $\operatorname{Aut}\overline{S}$-conjugate to groups of type P_1 or $\mathrm{GO}_1(q) \oplus \mathrm{GO}_7(q)$, by $3q^{19}$. Thus the sum of the squares of the reciprocals of their indices is at most $36/q^{16}$, and the result follows. □

6. Proof of Corollary 1.3

Proof of Corollary 1.3. Let $N = S_1 \times \cdots \times S_r$, set $X = N_L(S_1)/C_L(S_1)$, and identify S with $\operatorname{soc}(X)$. By [4, Theorem 2.7] we know that $f_L(d) = \frac{P_{L,N}(d)|N|^d}{|C_{\operatorname{Aut}_N(L/N)}|}$, where $d = d(L)$. By Proposition 1.1, there exists a 2-generated group Y with $S \trianglelefteq Y \leqslant X$ such that $P_{L,N}(d) \geqslant P_{Y,S}(2)$. In [5, proof of Lemma 1] it is shown that

$$\left|C_{\operatorname{Aut}_N}(L/N)\right| \leqslant r|S|^{r-1}\left|C_{\operatorname{Aut}_S}(X/S)\right|.$$

Thus $|C_{\operatorname{Aut}_N}(L/N)| \leqslant r|S|^{r-1}|C_{\operatorname{Aut}_S}(Y/S)|$ and

$$f_L(d) = \frac{P_{L,N}(d)|N|^d}{|C_{\operatorname{Aut}_N}(L/N)|} \geqslant \frac{P_{Y,S}(2)|N|^d}{r|S|^{r-1}|C_{\operatorname{Aut}_S}(Y/S)|}. \tag{11}$$

Now $f_Y(2) = \frac{P_{Y,S}(2)|S|^2}{|C_{\operatorname{Aut}_S}(Y/S)|}$ by [4, Theorem 2.7], so that (11) becomes

$$f_L(d) \geqslant f_Y(2)\frac{|N|^{d-1}}{r|S|}$$

and the first part of the corollary is proved.

The second part of the corollary follows from (11), an explicit calculation using [14, Table 1] of $P_{Y,S}(2)/|\operatorname{Out} S|$ for those groups Y with $P_{Y,S}(2) \leqslant 0.9$, and the bound $|\operatorname{Out} S| \leqslant 6/7\log|S|$ given in [14, Lemma 2.1] for the general case. □

References

[1] B. Amberg, L. Kazarin, Large subgroups of a finite group of even order, Proc. Amer. Math. Soc. 140 (1) (2012) 65–68.

[2] John N. Bray, Derek F. Holt, Colva M. Roney-Dougal, The Maximal Subgroups of the Low Dimensional Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 407, Cambridge University Press, Cambridge, 2013.
[3] F. Dalla Volta, A. Lucchini, Generation of almost simple groups, J. Algebra 178 (1) (1995) 194–223.
[4] F. Dalla Volta, A. Lucchini, Finite groups that need more generators than any proper quotient, J. Aust. Math. Soc. A 64 (1) (1998) 82–91.
[5] F. Dalla Volta, A. Lucchini, The smallest group with non-zero presentation rank, J. Group Theory 2 (2) (1999) 147–155.
[6] E. Detomi, A. Lucchini, Probabilistic generation of finite groups with a unique minimal normal subgroup, J. Lond. Math. Soc. 87 (3) (2013) 689–706.
[7] J. Fulman, R. Guralnick, Derangements in simple and primitive groups, in: A. Ivanov, et al. (Eds.), Groups, Combinatorics, and Geometry, Durham, 2001, World Sci. Publ., River Edge, NJ, 2003, pp. 99–121.
[8] W. Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, Illinois J. Math. 3 (1959) 469–476.
[9] Jokke Häsä, Growth of cross-characteristic representations of finite quasisimple groups of Lie type, arXiv:1112.3941v1, 2011.
[10] M. Herzog, On centralizers of involutions, Proc. Amer. Math. Soc. 22 (1969) 170–174.
[11] Gerhard Hiss, Gunter Malle, Low-dimensional representations of quasi-simple groups, LMS J. Comput. Math. 4 (2001) 22–63.
[12] Peter Kleidman, Martin Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, Cambridge, 1990.
[13] Martin W. Liebeck, On the orders of maximal subgroups of the finite classical groups, Proc. Lond. Math. Soc. (3) 50 (1985) 426–446.
[14] Nina E. Menezes, Martyn Quick, Colva M. Roney-Dougal, The probability of generating a finite simple group, Israel J. Math. 198 (1) (2013) 371–392.
[15] P. Rowley, Finite groups admitting a fixed-point-free automorphism group, J. Algebra 174 (2) (1995) 724–727.