Rend. Lincei Mat. Appl. 36 (2025), 445–483
DOI 10.4171/RLM/1078

Algebra, Number Theory, and Group Theory. – *Non-congruence presentations of finite simple groups*, by William Y. Chen, Alexander Lubotzky and Pham Huu Tiep, accepted on 1 July 2025.

Dedicated to Enrico Bombieri on the occasion of his 85th birthday.

Abstract. – We prove two results on some special generators of finite simple groups and use them to prove that every non-abelian finite simple group S admits a non-congruence presentation (as conjectured by Chen, Lubotzky, and Tiep (2024)), and that if S has a non-trivial Schur multiplier, then it admits a smooth cover (as conjectured by Chen, Fan, Li, and Zhu (2024)).

Keywords. – finite simple groups, generators, presentations, congruence subgroups.

Mathematics Subject Classification 2020. – 20D05 (primary); 20F05 (secondary).

1. Introduction

In this paper, we prove two theorems about some special generators of finite simple groups.

Theorem A. *Let S be any finite non-abelian simple group. Then, S is generated by two elements u and v such that the integers $|u|$, $|v|$, and $|uv|$ are pairwise coprime.*

Theorem B. *Let S be any finite non-abelian simple group with non-trivial Schur multiplier. Then, S admits a* smooth covering *in the sense of* [8]*; i.e., there exist a finite quasisimple group G with $S \cong G/\mathbf{Z}(G)$, $\mathbf{Z}(G) \neq 1$, and two elements $x, y \in G$ such that $G = \langle x, y\rangle$, and each of the elements x, y, xy has the same orders in G and in $G/\mathbf{Z}(G)$.*

These results are of some interest for their own sake, but our interest arose from their applications. Theorem B proves Conjecture 1.10 of [8], and Theorem A proves Conjecture 6.3 of [11]. To explain this latter conjecture, we will need the notion of a *non-congruence* presentation.

We begin with some generalities. Let H be a group and $N \leq H$ a finite-index normal subgroup. Let $A := \mathrm{Aut}(H)$, and let

$$A_N := \{\gamma \in A \mid \gamma(N) = N \text{ and } \gamma \text{ induces the identity on } H/N\}.$$

The group A_N is the (principal) H-congruence subgroup of A associated with N. A subgroup of A is H-congruence if it contains A_N for some normal finite-index subgroup $N \leq H$. Similarly, we say that a subgroup of $\mathrm{Out}(H) := \mathrm{Aut}(H)/\mathrm{Inn}(H)$ is H-congruence if it contains the image of some A_N. We should mention H in the notion of "congruence" since the same abstract group can be the outer automorphism group of different groups H.

The examples most relevant to us are the cases of $H = H_1 := \mathbb{Z}^2$ and $H = H_2 := F_2$, the free group of rank 2. In both cases, $\mathrm{Out}(H) \cong \mathrm{GL}_2(\mathbb{Z})$, the isomorphism being given as follows: there is a natural map

$$\mathrm{Aut}(F_2) \to \mathrm{Aut}(F_2/F_2') = \mathrm{Aut}(\mathbb{Z}^2),$$

which by a classical result of Nielsen induces an isomorphism

$$\mathrm{Out}(F_2) \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z}).$$

In this case, to be consistent with the number-theoretic literature, we will instead work inside the index 2 subgroup $\mathrm{Aut}^+(F_2) \leq \mathrm{Aut}(F_2)$ consisting of automorphisms which act with determinant $+1$ on $\mathbb{Z}^2$, and its image $\mathrm{Out}^+(F_2) \cong \mathrm{SL}_2(\mathbb{Z})$ inside $\mathrm{Out}(F_2) \cong \mathrm{GL}_2(\mathbb{Z})$. Accordingly, for a finite-index normal subgroup $N \leq F_2$, we define the principal F_2-congruence subgroups $\Gamma_N \leq \mathrm{Out}^+(F_2)$ by

$$\Gamma_N := \big\{\gamma \in \mathrm{Aut}^+(F_2) \mid \gamma(N) = N \text{ and } \gamma \text{ induces an inner automorphism of } F_2/N\big\}/\mathrm{Inn}(F_2). \tag{1.1}$$

As in the general case, we say that a subgroup of $\mathrm{Out}^+(F_2)$ is F_2-congruence if it contains Γ_N for some N.

The $\mathbb{Z}^2$-congruence subgroups of $\mathrm{Out}^+(F_2) \cong \mathrm{SL}_2(\mathbb{Z})$, defined analogously, are the classical congruence subgroups, which are classically defined as the subgroups containing, for some integer $n \geq 1$, the principal level n congruence subgroup

$$\Gamma(n) := \mathrm{Ker}\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n)\big).$$

Henceforth, a *congruence* subgroup of $\mathrm{SL}_2(\mathbb{Z})$ will refer to a classical (i.e., $\mathbb{Z}^2$-) congruence subgroup. While the classical ($\mathbb{Z}^2$-)congruence subgroups have attained a legendary status in number theory via its connections to elliptic curves and modular forms, the well-known failure of the *congruence subgroup property* for $\mathrm{SL}_2(\mathbb{Z})$ states that $\mathrm{SL}_2(\mathbb{Z})$ also admits finite-index subgroups which are not ($\mathbb{Z}^2$-)congruence. Such subgroups, typically called "non-congruence", are far less well understood. Despite its name, a breakthrough result of Asada [1] using algebraic geometry, later translated into group theory in [3,7], asserts that *every* finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is F_2-congruence. In particular, every non-congruence subgroup is F_2-congruence.

Asada's result led the first author to give moduli interpretations to non-congruence modular curves [9] in terms of "non-abelian level structures" and suggests the following fundamental question:

(1.2) Given an epimorphism $\varphi : F_2 \to G$ with G finite,
when is $\Gamma_\varphi := \Gamma_{\ker\varphi}$ a classical congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$?

In what follows, an epimorphism $\varphi : F_2 \to G$ will also be called a (2-generator) presentation of G. We say that φ is a *congruence* (resp. *non-congruence*) presentation of G if $\Gamma_\varphi = \Gamma_{\ker\varphi}$ is a classical ($\mathbb{Z}^2$-)congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ or not.

It is easy to see that for abelian G, every (2-generator) presentation of an abelian group is congruence. A more subtle result, independently discovered by the first author in a joint work with Deligne [10], and in a different language by Ben-Ezra [2], is that the same also holds for any metabelian G; i.e., all presentations of finite 2-generated metabelian groups are congruence.

Computations done in [9] show that amongst 2-generated groups G of order ≤ 255, all presentations of solvable length 4 groups are non-congruence, and solvable length 3 groups only sometimes admit non-congruence presentations. Moreover, among non-abelian finite simple groups of order $\leq |\mathrm{J}_1| = 175560$, where J_1 is the Janko group, the overwhelming majority of presentations are non-congruence.[1] These results suggest the philosophy that the existence of non-congruence presentations is a measure of "non-abelianness". In accordance with this philosophy, we will use Theorem A to show the following.

COROLLARY C (cf. [11, Conjecture 6.3]). *Every non-abelian finite simple group admits a* totally *non-congruence presentation.*

Here, a presentation $\varphi : F_2 \to G$ is *totally non-congruence* if it is non-congruence and the smallest congruence subgroup containing Γ_φ is $\mathrm{SL}_2(\mathbb{Z})$ (see Section 3). Corollary C strengthens and generalizes the results of [9, Section 4.4], which showed that the groups A_n ($n \geq 5$) and $\mathrm{PSL}_2(p)$ ($p \geq 5$ prime) admit non-congruence presentations.

Note that a single group can admit both congruence and non-congruence presentations. This can even happen for a non-abelian finite simple group, the smallest examples being that of $G = \mathrm{PSU}_3(\mathbb{F}_4), \mathrm{PSU}_3(\mathbb{F}_5)$. In both cases, G admits a single $\mathrm{Aut}(G)$-orbit of congruence presentations, every other presentation being non-congruence.[2]

(1) Data for all 2-generated groups of order ≤ 255, as well as the finite simple groups of order $\leq |\mathrm{Sz}(8)| = 29120$ can be found in the appendix of [9].

(2) These groups have order 62400 and 126000, respectively, and are the only non-abelian simple groups of order $\leq |\mathrm{J}_1|$ to admit congruence presentations. The total number of presentations is approximately $|G|^2$; see [30, 32].

In particular, these exceptional congruence presentations are *characteristic*, in the sense that their kernels are characteristic subgroups of F_2. In our recent paper [11], we showed that these examples belong to an infinite family, containing characteristic presentations of the groups $\mathrm{PSL}_3(\mathbb{F}_q)$ and $\mathrm{PSU}_3(\mathbb{F}_q)$ for all $q \geq 7$, constructed using appropriate specializations of the Burau representation of the braid group B_4.

Despite the infinitude of such examples, we expect that they are rare. Indeed, a congruence presentation of a non-abelian simple group would correspond to a functorial method of constructing, from an isogeny of elliptic curves $E_1 \to E_2$, a non-abelian finite simple cover of E_2, only ramified above the origin [9]. Accordingly, we suggest the following.

CONJECTURE D. *Almost all presentations of a non-abelian finite simple group S are non-congruence, in the following sense:*

$$\lim_{|S|\to\infty} \frac{\#\textit{non-congruence presentations}}{\#\textit{all presentations}} = 1.$$

Here, a presentation is understood to be an epimorphism $F_2 \to S$.

Note that since almost every pair of elements of S generate S [30, 32], the denominator is approximately $|S|^2$.

Organization of the paper. In Section 2, we will phrase the discussion above in the language of profinite "congruence" topologies on $\mathrm{SL}_2(\mathbb{Z})$, which leads to a number of interesting questions. In Section 3, we will show how Corollary C follows from Theorem A. Finally, in the remaining sections, we will prove Theorems A and B.

Dedication. This paper, which combines number theory and finite simple groups, is dedicated to E. Bombieri, who has made fundamental contributions to both subjects.

2. CONGRUENCE TOPOLOGIES AND FURTHER RESEARCH DIRECTIONS

The notions and results described in the introduction can be viewed from the more general perspective of profinite topologies on $\mathrm{SL}_2(\mathbb{Z})$, suggesting further questions. Let $\mathfrak{F}$ be a formation of finite groups, i.e., a class of finite groups closed under homomorphic images and subdirect product [39, Section 2.1]. Important examples are

- $\mathfrak{F}_{\mathrm{all}}$ – the class of all finite groups,
- $\mathfrak{S}_\ell$ – the finite solvable groups of derived length $\leq \ell$, so $\mathfrak{S}_1 = \mathfrak{A}$ is the class of abelian groups and $\mathfrak{S}_2$ the class of metabelian groups,
- $\mathfrak{F}_p$ – the class of finite p-groups, when p is a prime.

The formation $\mathfrak{F}$ defines a topology $T(\mathfrak{F})$ on the free group F_2, by taking the normal subgroups $N \leq F_2$ for which $F_2/N \in \mathfrak{F}$ as basis of open neighborhoods of the identity.

This topology is preserved by $\mathrm{Aut}(F_2)$ and defines a topology on $\mathrm{Out}^+(F_2) \cong \mathrm{SL}_2(\mathbb{Z})$, called the $\mathfrak{F}$-congruence topology. Specifically, a basis to this topology is given by the groups Γ_N given in (1.1):

$$\Gamma_N := \left\{\gamma \in \mathrm{Aut}^+(F_2) \mid \gamma(N) = N \text{ and } \gamma \text{ induces the identity on } F_2/N\right\}/\mathrm{Inn}(F_2),$$

where now N runs over the finite-index normal subgroups $N \trianglelefteq F_2$ with $F_2/N \in \mathfrak{F}$. We will call this topology the $\mathfrak{F}$-congruence topology of $\mathrm{SL}_2(\mathbb{Z})$. Thus, the classical congruence topology is the $\mathfrak{S}_1 = \mathfrak{A}$-congruence topology, and Asada's theorem [1] asserts that the $\mathfrak{F}_{\mathrm{all}}$-congruence topology is equal to the full profinite topology. Clearly, if $\mathfrak{F}_1 \subset \mathfrak{F}_2$, then the $\mathfrak{F}_2$-congruence topology is stronger than (or equal to) the $\mathfrak{F}_1$-congruence topology.

The results of Chen–Deligne [10] and Ben-Ezra [2] mentioned in the introduction mean that the $\mathfrak{S}_1$-congruence topology is equal to the $\mathfrak{S}_2$-congruence topology. However, the computational results mentioned in the introduction show that the $\mathfrak{S}_3$-congruence topology is strictly stronger.

Another way to define the $\mathfrak{F}$-congruence topology of $\mathrm{SL}_2(\mathbb{Z})$ is the following. Let $F_2^{\mathfrak{F}}$ be the pro-$\mathfrak{F}$ completion of F_2, i.e., the completion of F_2 w.r.t. the $\mathfrak{F}$-topology:

$$F_2^{\mathfrak{F}} := \varprojlim_{N \in \mathfrak{F}} F_2/N.$$

There is a canonical map $F_2 \to F_2^{\mathfrak{F}}$, which is injective if and only if F_2 is residually-$\mathfrak{F}$, i.e., if and only if $\bigcap_{N\in\mathfrak{F}} N = 1$. Since $\mathrm{Aut}(F_2)$ preserves the $\mathfrak{F}$-topology, this induces a map $\mathrm{Aut}(F_2) \to \mathrm{Aut}(F_2^{\mathfrak{F}})$, and hence also a map $\mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{Out}^+(F_2) \to \mathrm{Out}(F_2^{\mathfrak{F}})$. The $\mathfrak{F}$-congruence topology of $\mathrm{SL}_2(\mathbb{Z})$ is also the topology induced on $\mathrm{SL}_2(\mathbb{Z})$ from the profinite group $\mathrm{Out}(F_2^{\mathfrak{F}})$.[3]

This suggests a few interesting problems:

(i) In the sequence of the $\mathfrak{S}_\ell$-congruence topologies, are there infinitely many jumps? We do not even know if the $\mathfrak{S}_4$-congruence topology is strictly stronger than the $\mathfrak{S}_3$-congruence topology or if they are equal.

(ii) Let $\mathfrak{S} = \bigcup_{\ell=1}^{\infty} \mathfrak{S}_\ell$. Is the $\mathfrak{S}$-congruence topology strictly weaker than the $\mathfrak{F}_{\mathrm{all}}$-congruence topology (= the full profinite topology) of $\mathrm{SL}_2(\mathbb{Z})$?

(iii) It is easy to see that the $\mathfrak{F}_p$-congruence topology of $\mathrm{SL}_2(\mathbb{Z})$ is stronger than (or equal to) the topology induced from $\mathrm{SL}_2(\mathbb{Z}) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}_p)$. At the same time, it is weaker than (or equal to) the topology of $\mathrm{SL}_2(\mathbb{Z})$ induced on it from the full

[3] The map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Out}(F_2^{\mathfrak{F}})$ is not always injective, in which case the $\mathfrak{F}$-congruence topology of $\mathrm{SL}_2(\mathbb{Z})$ would not be Hausdorff, but it is so for all the interesting cases. In particular, it is true for all the examples we will discuss.

pro-p topology on the congruence subgroup

$$\Gamma(p) := \mathrm{Ker}\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p)\big).$$

Is it equal to the latter one? A positive answer would be a "local p" version of Asada's theorem.

Added in proof. After the paper has been accepted, we have found an article of Hoshi and Iijima [28] which gives a positive answer to question (iii) for $p = 2$, and a negative answer for $p \geq 11$. Also see [4] for results on the pro-$\mathfrak{F}$ analogs of question (iii).

3. Theorem A implies Corollary C

In this section, we recall (and give a cleaner proof of) the non-congruence criterion of [9, Theorem 4.4.10] and [45], which shows that coprime generation in the sense of Theorem A implies that the associated presentation is totally non-congruence, thereby proving Corollary C.

For a finite-index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, its *congruence closure*, denoted by Γ^c, is the smallest (classical) congruence subgroup containing Γ. The discussion in the previous section implies that the (classical) congruence topology on $\mathrm{SL}_2(\mathbb{Z})$ is induced by the topology on $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. Moreover, if $\overline{\Gamma}$ denotes the closure of Γ inside $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, then we have

$$\overline{\Gamma} \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma^c.$$

It follows that Γ is congruence if and only if $\Gamma = \Gamma^c$. In the antipodal case, where Γ is non-congruence and $\Gamma^c = \mathrm{SL}_2(\mathbb{Z})$, we will further say that Γ is *totally non-congruence*. Thus, a finite-index $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is totally non-congruence if it is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which is dense in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

Corollary C immediately follows from the following non-congruence criterion.

Theorem 3.1 (Coprime generation implies totally non-congruence). *Let F_2 be a free group of rank 2, with generators a, b. Let G be a non-trivial finite group generated by x, y, z satisfying $xyz = 1$. Suppose the orders $|x|, |y|, |z|$ satisfy the following property:*

$(*)$ *The integers $|x|, |y|, |z|$ are pairwise coprime.*

Then, the $\mathrm{SL}_2(\mathbb{Z})$-stabilizer $\Gamma_{\varphi_{x,y}} := \Gamma_{\ker\varphi}$ of the surjection $\varphi_{x,y} : F_2 \to G$ sending $a, b \mapsto x, y$ is totally non-congruence.

Before giving the proof, we make some remarks:

- The coprimality condition $(*)$ is equivalent to the statement that the gcd δ of the set $\{|x||y|, |x||z|, |y||z|\}$ is 1. If G is abelian, then all three pairwise least common

multiples of $|x|, |y|, |z|$ are equal to the exponent $e(G)$, and hence the gcd δ would be divisible by $e(G)$ in this case. Thus, δ can be viewed as a measure of non-abelianness of G relative to the generating triple (x, y, z), and the theorem links this non-abelianness to the non-congruenceness of the stabilizer $\Gamma_{\varphi_{x,y}}$.

- As will be evident from the proof, the theorem has some room for flexibility. If the pairwise gcd's in $(*)$ are not too large compared to the index of $\Gamma_{\varphi_{x,y}}$, then we can still show that $\Gamma_{\varphi_{x,y}}$ is non-congruence, though maybe not totally non-congruence.

Proof. Define $\varphi_{z,x}$ and $\varphi_{y,z}$ analogously to $\varphi_{x,y}$. We note that $\varphi_{x,y}, \varphi_{z,x}, \varphi_{y,z}$ lie in the same $\mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{Out}^+(F_2)$-orbit, and hence their stabilizers $\Gamma_{\varphi_{x,y}}, \Gamma_{\varphi_{z,x}}, \Gamma_{\varphi_{y,z}}$ are conjugate. Further observe that

$$\text{(3.1)}\quad \begin{bmatrix} 1 & |x| \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ |y| & 1 \end{bmatrix} \in \Gamma_{\varphi_{x,y}}, \quad \begin{bmatrix} 1 & |z| \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ |x| & 1 \end{bmatrix} \in \Gamma_{\varphi_{z,x}}, \quad \begin{bmatrix} 1 & |y| \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ |z| & 1 \end{bmatrix} \in \Gamma_{\varphi_{y,z}}.$$

For ease of notation, let $\Gamma_1, \Gamma_2, \Gamma_3$ be these three subgroups. Since G is non-trivial, condition $(*)$ implies that x, y, z are not all conjugate to each other, and hence the Γ_i's are proper subgroups of $\mathrm{SL}_2(\mathbb{Z})$. It remains to show that each Γ_i is dense in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$. For this, fix an integer n with prime factorization $n = \prod_j p_j^{r_j}$, and consider the direct product decomposition

$$\text{(3.2)}\qquad \mathrm{SL}_2(\mathbb{Z}/n) \cong \prod_j \mathrm{SL}_2(\mathbb{Z}/p_j^{r_j}).$$

The coprimality assumption $(*)$ implies that for each j, at least two of $|x|, |y|, |z|$ are coprime to p_j, and hence at least one of $\Gamma_1, \Gamma_2, \Gamma_3$ projects onto $\mathrm{SL}_2(\mathbb{Z}/p_j^{r_j})$. Since the Γ_i's are conjugate, each Γ_i projects onto $\mathrm{SL}_2(\mathbb{Z}/p_j^{r_j})$ for every j, so the image of each Γ_i in the product (3.2) is a subdirect product. Since the direct factors have no non-trivial common quotients, this subdirect product is the entirety of $\mathrm{SL}_2(\mathbb{Z}/n)$, and hence each Γ_i surjects onto $\mathrm{SL}_2(\mathbb{Z}/n)$. Since n was arbitrary, this shows that each Γ_i is dense in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$, as desired. ∎

4. Coprime generation of finite simple groups

In this section, we first outline our strategy to prove Theorems A and B. In fact, for many of the groups S we will show that the elements u, v desired in Theorem A can be chosen so that $|u|, |v|, |uv|$ are (pairwise) coprime. Also, to prove Theorem A for a given S, it suffices to prove that the conclusion of Theorem A holds for some quasisimple group G with $G/\mathbf{Z}(G) \cong S$. In most of the cases, we will show that $G = \langle x, y \rangle$ so that $u = x\mathbf{Z}(G)$ and $v = y\mathbf{Z}(G)$ satisfy the conclusion of Theorem A; moreover, the orders of x, y, and xy are all coprime to $|\mathbf{Z}(G)|$, and hence x and y satisfy the conclusion of Theorem B.

We will employ a case-by-case approach to prove Theorems A and B, relying on the Classification of Finite Simple Groups [23]. We work with some quasisimple cover G of S, with $\mathbf{Z}(G) \neq 1$ if $\mathrm{Mult}(S) \neq 1$, and aim to find two elements $x, y \in G$ such that

(A) $r = |x|$ *and* $s = |y|$ are *coprime* (in fact primes if possible). This condition ensures that the elements

$$u := x\mathbf{Z}(G) \quad \text{and} \quad v := y\mathbf{Z}(G) \tag{4.1}$$

of $S = G/\mathbf{Z}(G)$ have coprime orders.

(B) $x^G \cdot y^G$ *contains every non-central element of* G. This condition implies that $u^S \cdot v^S$ contains every non-trivial element of S. To ensure this condition, by Frobenius' character formula, it suffices to show that

$$\left| \sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)} \right| < 1 \tag{4.2}$$

for any $z \in G \setminus \mathbf{Z}(G)$. Now, if r and s are primes, then by Burnside's $p^a q^b$-theorem, S contains an element w of prime order $t \neq r, s$, and without loss of generality, we may assume that $w = uv$. In general, we aim to show that *we can find some prime divisor* $t \nmid rs|\mathbf{Z}(G)|$ *of* $|S|$, and hence an element $z \in G$ of order t for which we may again assume that $z = xy$.

(C) *No maximal subgroup of* S *can have order divisible by* $D := \mathrm{lcm}(|u|, |v|, t)$. By our construction of u, v in (A) and (B), this implies that $S = \langle u, v \rangle$, as desired in Theorem A. In the cases where this requirement cannot be fulfilled, we will show instead that no maximal subgroup of S can simultaneously contain elements of order $|u|$, $|v|$, and $|w|$.

Recall [46] that if $a, d \in \mathbb{Z}_{\geq 2}$, then $a^d - 1$ admits a *primitive prime divisor* ℓ, i.e., a prime ℓ that divides $a^d - 1$ but not $\prod_{i=1}^{d-1}(a^i - 1)$, unless $(a, d) = (2, 6)$ or $d = 2$ and $a + 1$ is a 2-power. Any such prime divisor ℓ satisfies $\ell \geq d + 1$. Among all primitive prime divisors for the given pair (a, d), we will write $\ell = \mathrm{ppd}(a, d)$ to denote the largest one among them.

The main bulk of the work is to prove Theorem A for $S = \mathsf{A}_n$ or $S = G/\mathbf{Z}(G)$, G a quasisimple group of Lie type defined over a field $\mathbb{F}_q$ in characteristic p, so $q = p^f$ with $f \geq 1$. With q fixed, we will denote by $\Phi_m = \Phi_m(q)$ the value of the mth cyclotomic polynomial evaluated at q.

Most of the times, we will choose $x, y \in G$ to be suitable regular semisimple elements and use (4.2) if necessary to show that (B) holds. To prove (C), in particular for classical groups, first we make use of [5] to rule out all maximal subgroups of S if S has low rank. For the remaining classical groups, we will use results of [25] to

narrow down the list of maximal subgroups of S that may have order divisible by D. For exceptional groups of Lie type, we will use results of [33] and the following lemma.

LEMMA 4.1. *Suppose that the simple group S is a Hurwitz group, i.e.,*

$$S = \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle.$$

Then, Theorem A holds for S. In particular, Theorem A holds for A_n with $n \geq 168$ and for the following simple groups of Lie type:

(i) ${}^2G_2(q)$, $q = 3^{2a+1} \geq 27$.

(ii) $G_2(q)$, $q \geq 5$.

(iii) ${}^3D_4(q)$, *where* $q = p^f \neq 4$ *and* $p \neq 3$.

PROOF. The first statement is obvious. The alternating case follows from [13, Corollary]. Next, cases (i) and (ii) follow from the main result of [34], and (iii) follows from [36]. ∎

There are further results in literature showing that certain finite groups of Lie type are Hurwitz. However, these results usually assume the simple, say classical, group in question has very large rank, or specific fields of definition. Since we aim to prove Theorem A for *all* simple classical groups as well as a variation of Theorem A in the case S has non-trivial Schur multiplier, we will follow our main outline instead. More precisely, we will follow the outline above to prove Theorems A and B for all but a finite number of exceptional cases. These remaining cases will be individually verified using [21] via randomized search over generating pairs, or deduced as a corollary of existing results. Due to the complexity and variety of the groups involved, we will for the most part limit our exposition to general remarks and will avoid writing down explicit generators.

5. PROOF OF THEOREMS A AND B: ALTERNATING GROUPS

Suppose $S = \mathsf{A}_n$ with $2 \nmid n \geq 5$. Then, we choose $u \in S$ to be an n-cycle and $v \in S$ to be an $(n-2)$-cycle. Say v fixes 1 and 2 while acting on $\Omega = \{1, 2, \ldots, n\}$. By [27, Theorem 7], $u^{\mathsf{S}_n} v^{\mathsf{S}_n} = S \setminus \{1\}$. Hence, conjugating u and v in S_n suitably, we may assume that uv is a double transposition when $n = 5$, and an $(n-4)$-cycle when $n \geq 7$. We claim that $H := \langle u, v \rangle$ equals S. Indeed, when $n = 5$, $H \leq \mathsf{A}_5$ has order divisible by 30, and so $H = \mathsf{A}_5$. Suppose $n \geq 7$. Then, $H \ni u$ is transitive on $\Omega := \{1, 2, \ldots, n\}$. Since H contains the $(n-2)$-cycle v and $2 \nmid n$, H is primitive. But H contains the $(n-4)$-cycle uv, so $H = \mathsf{A}_n$ by [29, Corollary 1.3].

This proves Theorem A for $S = \mathsf{A}_n$ with $2 \nmid n \geq 5$. To prove Theorem B for $2 \nmid n \geq 19$, we will work with $G = 2\mathsf{S}_n$, and consider $x \in G$ an inverse image of odd order of an n-cycle and $y \in G$ an inverse image of odd order of an $(n-2)$-cycle. Taking

$z \in G$ an inverse image of odd order of an $(n-4)$-cycle, we claim that $z \in x^G y^G$. We will use (4.2), but dividing the sum into characters of G which are non-faithful, respectively, faithful. Note that for any $g \in G$ we have

$$\sum_{\chi \in \mathrm{Irr}(G/\mathbf{Z}(G))} |\chi(g)|^2 = |\mathbf{C}_{G/\mathbf{Z}(G)}(g\mathbf{Z}(G))|,$$
$$\sum_{\chi \in \mathrm{Irr}(G) \smallsetminus \mathrm{Irr}(G/\mathbf{Z}(G))} |\chi(g)|^2 = |\mathbf{C}_G(g)| - |\mathbf{C}_{G/\mathbf{Z}(G)}(g\mathbf{Z}(G))|.$$

By [31, Corrollary 3.1.2], there are exactly n characters $\chi \in \mathrm{Irr}(G/\mathbf{Z}(G))$ which are non-trivial at x, namely, the ones labeled by hook partitions, all taking values ± 1 at x. Furthermore, among these characters, the two labeled by $(n-1,1) \vdash n$ and $(2,1^{n-2}) \vdash n$ vanish at z, and all other ones have degree 1 or $\geq (n-1)(n-2)/2$. It follows from the Cauchy–Schwarz inequality that

$$\left| \sum_{\chi \in \mathrm{Irr}(G/\mathbf{Z}(G)), \chi(1)>1} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| \leq \frac{2\sqrt{48(n-2)(n-4)}}{(n-1)(n-2)}.$$

For the faithful, i.e., spin, characters, we have $|\chi(x)| \leq \sqrt{n}$ and $|\chi(1)| \geq 2^{(n-1)/2}$, so again by Cauchy–Schwarz,

$$\left| \sum_{\chi \in \mathrm{Irr}(G) \smallsetminus \mathrm{Irr}(G/\mathbf{Z}(G))} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| \leq \frac{\sqrt{48n(n-2)(n-4)}}{2^{(n-1)/2}}.$$

Taking $n \geq 19$, we have

$$\left| \sum_{\chi \in \mathrm{Irr}(G), \chi(1)>1} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| < 2.$$

It follows from (4.2) that $z \in x^G y^G$. Conjugating x and y suitably, we may assume $z = xy$. Since we have shown above that $S = \langle x\mathbf{Z}(G), y\mathbf{Z}(G) \rangle$, we are done.

Suppose $S = \mathsf{A}_n$ with $2 \mid n \geq 6$. Then, we choose $u \in S$ to be an $(n-1)$-cycle and $v \in S$ to be an $(n-3)$-cycle. By [27, Theorem 7], $u^{\mathsf{S}_n} v^{\mathsf{S}_n} = S \smallsetminus \{1\}$. Hence, conjugating u and v in S_n suitably, we may assume that uv is a disjoint product

(i) of a 5-cycle and an $(n-5)$-cycle when $n \equiv 2, 4 \pmod 5$ (this ensures that 5 is coprime to $(n-1)(n-3)(n-5)$, and so $|u|$, $|v|$, $|uv|$ are pairwise coprime), and

(ii) of a 2-cycle and an $(n-2)$-cycle when $n \equiv 0, 1, 3 \pmod 5$ (clearly, $|u|$, $|v|$, $|uv|$ are pairwise coprime by this choice).

We claim that $H := \langle u, v \rangle$ equals S. Indeed, if $H \ni u$ is intransitive on $\Omega = \{1, 2, \ldots, n\}$, then H has to fix the only fixed point, say 1 of u. But $uv \in H$ has no fixed point, a contradiction. So H is transitive and contains the $(n-1)$-cycle u, and so it is doubly

transitive; in particular, it is primitive. As H contains the $(n-3)$-cycle v, $H = \mathsf{A}_n$ by [29, Corollary 1.3].

This proves Theorem A for $S = \mathsf{A}_n$ with $2 \mid n \geq 6$. To prove Theorem B for $2 \mid n \geq 20$, we will again work with $G = 2\mathsf{S}_n$, and consider $x \in G$ an inverse image of odd order of an $(n-1)$-cycle and $y \in G$ an inverse image of odd order of an $(n-3)$-cycle. Taking $z \in G$ an inverse image of odd order of the disjoint product of a 5-cycle and an $(n-5)$-cycle, we claim that $z \in x^G y^G$. As in the odd-n case, we will use (4.2), but dividing the sum into characters of G which are non-faithful, respectively, faithful. By [31, Corrollary 3.1.2], there are exactly $n-1$ characters $\chi \in \mathrm{Irr}(G/\mathbf{Z}(G))$ which are non-trivial at x, all taking values ± 1 at x and having degree 1 or $\geq n(n-3)/2$. It follows from the Cauchy–Schwarz inequality that

$$\left| \sum_{\chi \in \mathrm{Irr}(G/\mathbf{Z}(G)), \chi(1)>1} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| \leq \frac{2\sqrt{30(n-3)(n-5)}}{n(n-3)}.$$

For the faithful, i.e., spin, characters, we have $|\chi(x)| \leq \sqrt{n-1}$ and $|\chi(1)| \geq 2^{(n-2)/2}$, so again by Cauchy–Schwarz,

$$\left| \sum_{\chi \in \mathrm{Irr}(G) \smallsetminus \mathrm{Irr}(G/\mathbf{Z}(G))} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| \leq \frac{\sqrt{30(n-1)(n-3)(n-5)}}{2^{(n-2)/2}}.$$

Taking $n \geq 20$, we have

$$\left| \sum_{\chi \in \mathrm{Irr}(G), \chi(1)>1} \frac{\chi(x)\chi(y)\overline{\chi(z)}}{\chi(1)} \right| < 2.$$

It follows from (4.2) that $z \in x^G y^G$. Conjugating x and y suitably, we may assume $z = xy$. Since we have shown above that $S = \langle x\mathbf{Z}(G), y\mathbf{Z}(G) \rangle$, we are done.

Thus, we have proved Theorem A for A_n with $n \geq 5$, and Theorem B for A_n with $n \geq 19$.

Finally, we check Theorem B for the cases A_n with $5 \leq n \leq 18$. For all such n, we checked using [21] that the perfect central double cover of A_n admits a generating pair x, y such that $|x|, |y|, |xy|$ are all odd. To help the reader reproduce such a pair for $n \neq 6$, we remark that these pairs are Nielsen equivalent[4] to the pair given by the [21] command

(5.1) `GeneratorsOfGroup(DoubleCoverOfAlternatingGroup(n));`

(4) Recall that two generating pairs $(x, y), (x', y')$ are *Nielsen equivalent* if (x', y') can be produced from (x, y) via a sequence of moves of the form $(x, y) \mapsto (x, xy)$, $(x, y) \mapsto (xy, y)$, and $(x, y) \mapsto (x, y^{-1})$.

where one should replace `n` with the appropriate degree. The reader can efficiently find the desired pair via a random walk on the product replacement graph centered at the pair given by (5.1). For $n = 6$, the claimed generating pair is Nielsen equivalent to the pair given by

```
GeneratorsOfGroup(AtlasGroup("2.A6"));.
```

6. Proof of Theorems A and B: Exceptional groups of Lie type

We begin with the case $G = S = {}^2B_2(q)$, $q = 2^{2a+1} \geq 8$. Then, we choose $|x| = q + \sqrt{2q} + 1$ and $|y| = q - 1$. Checking the character table of G [6], one sees that the only non-trivial irreducible character of G that is non-vanishing at both x and y is the Steinberg character St, of degree q^2. Since $|\mathsf{St}(x)| = |\mathsf{St}(y)| = 1$ but $|\mathsf{St}(z)| < \mathsf{St}(1)$ for any $1 \neq z \in G$, (4.2) holds. We can now choose $|w| = q - \sqrt{2q} + 1$ to fulfill (B). Now $D = (q^2 + 1)(q - 1)$, and so (C) holds by [5, Table 8.16].

Next we complete the case $G = S = G_2(q)$ with $q > 2$. Suppose $q = 3$. Using (4.2) and [14] one can check that $u^S v^S = S \smallsetminus \{1\}$ for $u \in S$ of order 7 and $v \in S$ of order 8. In particular, we may assume that $w = uv$ has order 13. None of the maximal subgroups of S can contain elements for all of the orders 7, 8, and 13 [14], whence $S = \langle u, v\rangle$. Suppose $q = 4$. Using (4.2) and [14] one can check that $u^S v^S = S \smallsetminus \{1\}$ for $u \in S$ of order 13 and $v \in S$ of order 15. In particular, we may assume that $w = uv$ has order 7. None of the maximal subgroups of S can have order divisible by $7 \cdot 13 \cdot 15$ [14], whence $S = \langle u, v\rangle$. The case $q \geq 5$ is already done in Lemma 4.1 (ii).

Suppose $G = S = {}^3D_4(q)$. By Lemma 4.1 (iii), it suffices to consider the case $p > 2$ or $q = 4$. Then, we choose $x \in G$ an element of order Φ_{12} (belonging to class s_{14} in the notation of [17]), and $y \in G$ of order $\Phi_1\Phi_2\Phi_6$. Among the irreducible characters of G, whose degrees are listed in [17, Table 4.4], only five are not of ℓ_1-defect 0, where $\ell_1 = \mathrm{ppd}(p, 12f)$. So only these five characters can be non-vanishing at x, and two of them are 1_G and the Steinberg character St. Two of the three remaining ones have ℓ_2-defect 0, where $\ell_2 = \mathrm{ppd}(p, 6f)$, and hence vanish at y. The fifth one, ${}^3D_4[-1]$, whose values are listed in [42, Table 2], also vanishes at y. It follows that (4.2) holds for any $1 \neq z \in G$, and hence $x^G y^G \supseteq G \smallsetminus \{1\}$. Thus, (B) holds, and hence we can choose x and y in such a way that $|xy| = p$; in particular, $|\langle x, y\rangle|$ has order divisible by $p\Phi_1\Phi_2\Phi_6\Phi_{12}$. Inspecting the list of maximal subgroups of G [5, Table 8.51], we see that $G = \langle x, y\rangle$.

Suppose $G = S = {}^2F_4(q)$ with $q > 2$. By [26, Lemma 2.13], G admits elements x of order $\mathrm{ppd}(p, 12f)$ and y of order $\mathrm{ppd}(p, 6f)$ such that $x^G y^G = G \smallsetminus \{1\}$. In particular, we may assume that $|xy| = \mathrm{ppd}(p, 4f)$. Checking the list of maximal subgroups of G [35], we conclude that $G = \langle x, y\rangle$. Next suppose that $S = {}^2F_4(2)'$.

Using (4.2) and [14] one can check that $u^S v^S = S \smallsetminus \{1\}$ for $u \in S$ of order 13 and $v \in S$ of order 10. In particular, we may assume that $w = uv$ has order 3. None of the maximal subgroups of S can contain elements for all of the orders 13, 10, and 3 [14], whence $S = \langle u, v\rangle$.

Suppose $G = S = F_4(q)$ with $q > 2$. Then, the proof of [33, Theorem 3.1] shows that $G = \langle x, y\rangle$ for some x of order Φ_{12} and y of order 2, with $|xy| = 3$. In the case $G = 2 \cdot F_4(2)$, we can choose $x \in G$ of class $17a$ and $y \in G$ of class $13a$, and $z \in G$ of class $15a$, in the notation of [21]. Then, we can check using [21] that $z \in x^G y^G$, and so, conjugating x and y suitably, we may assume $z = xy$. According to [14], no maximal subgroup of $S = G/\mathbf{Z}(G)$ can have order divisible by $13 \cdot 17$, whence $G = \langle x, y\rangle$, and thus we have proved Theorems A and B for $S = F_4(2)$.

Let $G = E_6^\varepsilon(q)_{\mathrm{sc}}$ denote $E_6(q)_{\mathrm{sc}}$ when $\varepsilon = +1$, and ${}^2E_6(q)_{\mathrm{sc}}$ when $\varepsilon = -1$. Then, $S = G/\mathbf{Z}(G)$ is simple and $|\mathbf{Z}(G) = \gcd(3, q - \varepsilon)$. Then, the proof of [33, Theorem 4.1] when $\varepsilon = +1$, and of [33, Theorem 5.1] when $\varepsilon = -1$, shows that $G = \langle x, y\rangle$ for some x of order $q^6 + \varepsilon q^3 + 1$ and y of order 2, with $|xy| = 3$. Now if $3 \nmid (q - \varepsilon)$, then $\gcd(6, q^6 + \varepsilon q^3 + 1) = 1$, and so we are done. Suppose $3|(q - \varepsilon)$. Note that $T := \langle x\rangle$ is a cyclic maximal torus of G, so $T > \mathbf{Z}(G) \cong C_3$. It follows that $u = x\mathbf{Z}(G)$ has order $(q^6 + \varepsilon q^3 + 1)/3$ which is coprime to 6, and hence we have proved Theorem A in this case.

Using the recent result of Craven [15], we can give an alternate argument, which also proves the conclusion of Theorem B for $G = E_6^\varepsilon(q)_{\mathrm{sc}}$. As mentioned in [26, Section 2.2.5], G contains regular semisimple elements x of order $\ell_1 = \mathrm{ppd}(p, 8f)$, and y of order ℓ_2, where $\ell_2 = \mathrm{ppd}(p, 9f)$ if $\varepsilon = +1$ and $\ell_2 = \mathrm{ppd}(p, 18f)$ otherwise, such that $x^G y^G = G \smallsetminus \mathbf{Z}(G)$. Conjugating x and y suitably, we may assume that $|xy| = \ell_3 = \mathrm{ppd}(p, 12f)$. Note that $\ell_1 \geq 17$ and $\ell_2 \geq 19$. Assume the contrary that $\langle u, v\rangle \leq M$ for some maximal subgroup M of S. Using the list of (possible) maximal subgroups of S as given in [15, Theorem 1.1] and the fact that $|M|$ is divisible by $\ell_1\ell_2\ell_3$, we see that $M = \mathbf{N}_S(R)$, where R is some non-abelian simple group with either $\ell_1 \nmid |\mathrm{Aut}(R)|$ or $\ell_2 \nmid |\mathrm{Aut}(R)|$, unless

$$(G, R, \ell_1, \ell_2) = \big(E_6(4)_{\mathrm{sc}}, J_3, 17, 19\big).$$

Note that in fact the latter case cannot occur since we have $\ell_1 = 257$ when $q = 4$. In the former case, either x or y centralizes R. In other words, there is some element $a \in \{x, y\}$ such that $R \leq \mathbf{C}_S(a)$, which is impossible since $\mathbf{C}_G(a)$ is a torus.

Next we consider the case $G = E_7(q)_{\mathrm{sc}}$, so that $S = G/\mathbf{Z}(G)$ with $|\mathbf{Z}(G) = \gcd(2, q - 1)$. As mentioned in [26, Section 2.2.5], G contains regular semisimple elements x of order $\ell_1 = \mathrm{ppd}(p, 18f)$ and y of order $\ell_2 = \mathrm{ppd}(p, 7f)$ such that $x^G y^G = G \smallsetminus \{1\}$. Conjugating x and y suitably, we may assume that $|xy| = \ell_3 = \mathrm{ppd}(p, 14f)$. Note that $\ell_2 \geq 19$ and $\max(\ell_1, \ell_3) \geq 43$. Assume the contrary that

$\langle u, v\rangle \leq M$ for some maximal subgroup M of S. Using the list of (possible) maximal subgroups of S as given in [16, Theorem 1.1] and the fact that $|M|$ is divisible by $\ell_1\ell_2\ell_3$, we see that $M = \mathbf{N}_S(R)$, where $R = \mathrm{PSL}_2(t)$ with $t \in \{7, 8, 9, 13\}$ or $R = \mathrm{PGL}_3(q), \mathrm{PGU}_3(q)$. In particular, $\ell_1 \nmid |\mathrm{Aut}(R)|$, and so x centralizes R. In other words, $R \leq \mathbf{C}_S(x)$, which is impossible since $\mathbf{C}_G(x)$ is a torus.

Suppose $G = S = E_8(q)$. Then, the proof of [33, Proposition 8.1, Theorem 8.2] when $p = 3$, and the proof of [33, Theorem 9.1] when $p \neq 3$, shows that $G = \langle x, y\rangle$ for some x of order Φ_{30} and y of order 2, with $|xy| = 3$. Note that $\gcd(6, \Phi_{30}) = 1$, so we are done.

Finally, we use [21] to check Theorem B for the remaining cases $G_2(3)$, $G_2(4)$, and ${}^2B_2(8)$. The Schur multiplier of $G_2(3)$ has order 3, and the Schur cover admits a generating pair x, y with $|x| = |y| = |xy| = 13$, and which is Nielsen equivalent to the generating pair given by

```
GeneratorOfGroup(AtlasGroup("3.G2(3)"));.
```

The group $G_2(4)$ has a Schur multiplier of order 2, and the Schur cover admits a generating pair x, y with $|x| = |y| = 13$, $|xy| = 5$, and which is Nielsen equivalent to the pair

```
GeneratorOfGroup(AtlasGroup("2.G2(4)"));.
```

The group ${}^2B_2(8)$ has Schur multiplier isomorphic to $C_2 \times C_2$, and the Schur cover admits a generating pair x, y with $|x| = |y| = 7$, $|xy| = 5$, and which is Nielsen equivalent to the pair

```
GeneratorOfGroup(AtlasGroup("2^2.Sz(8)"));.
```

7. Proof of Theorems A and B: Linear and unitary groups

In this section, we prove Theorem A for $S = \mathrm{PSL}_n(q), \mathrm{PSU}_n(q)$, with $q = p^f$.

7.1. Low-rank groups

We begin with the case $G = \mathrm{SL}_2(q)$, $q \geq 4$. Then, we choose $|x| = (q+1)_{2'}$ and $|y| = (q-1)_{2'}$ if none of $q \pm 1$ is a 2-power, and $|x| = q+1$ and $|y| = q-1$ otherwise. Checking the character table [18, Theorems 38.1, 38.2], we see that the only non-trivial irreducible character χ of G with $\chi(x)\chi(y) \neq 0$ is the Steinberg character St, of degree q. Since $|\mathsf{St}(x)| = |\mathsf{St}(y)| = 1$ but $|\mathsf{St}(z)| < |\mathsf{St}(1)$ for any $z \in G \smallsetminus \mathbf{Z}(G)$, (4.2) holds. By our choice, the elements u and v in (4.1) have coprime orders. We can now choose $|xy| = p$ to fulfill (B). If both $q \pm 1$ are not 2-powers, then we also have $(|x|, |y|, |xy|) = (|u|, |v|, |uv|)$. Since none of the maximal subgroups of $\mathrm{SL}_2(q)$

[5, Table 8.1, 8.2] can contain elements of every order $|x|$, $|y|$, and p, we conclude that $G = \langle x, y\rangle$.

If $q = 9$, we can take $x = \left(\begin{smallmatrix} 1 & \alpha^4 \\ 0 & 1 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 1 & 0 \\ \alpha^5 & 1 \end{smallmatrix}\right)$, where α is a generator of $\mathbb{F}_9^\times$. Then, $|x| = |y| = 3$ and $|xy| = 5$, thus proving Theorem B for this case. It remains to check Theorem B for $\mathrm{PSL}_2(p)$ where $p \geq 5$ is a prime of the form $2^r \pm 1$. For such p, we wish to find generators $x, y \in G := \mathrm{SL}_2(p)$ such that $|x|, |y|, |xy|$ are all odd. Let ℓ be any odd prime divisor of $(p-1)/2$ when $p \equiv 3 \pmod 4$ and of $(p+1)/2$ otherwise. Again using the character table we can check that one can choose x and y of order p (and non-conjugate in G) such that xy has order ℓ. The latter implies that the subgroup $\langle x, y\rangle$ is irreducible on $\overline{\mathbb{F}_p}^2$, and hence by the classification of maximal subgroups of $\mathrm{SL}_2(p)$ [5, Table 8.1], we deduce that $G = \langle x, y\rangle$.

Now we consider the case $G = \mathrm{SL}_3(q)$, $q \geq 3$ (note that $\mathrm{SL}_3(2) \cong \mathrm{PSL}_2(7)$). Then, we choose $|x| = (q^2+q+1)/\gcd(3, q-1)$, $|y| = q^2 - 1$ if $3 \nmid (q-1)$, and $|y| = (q^2-1)_{3'}$ if $3|(q-1)$. Note that both $|x|$ and $|y|$ are coprime to $|\mathbf{Z}(G)| = d := \gcd(3, q-1)$, and $|u| = |x|$ and $|v| = |y|$ are coprime. Checking the character table of G [41], one sees that the only non-trivial irreducible character χ of G with $\chi(x)\chi(y) \neq 0$ is the Steinberg character St, of degree q^3. Since $|\mathsf{St}(x)| = |\mathsf{St}(y)| = 1$ but $|\mathsf{St}(z)| < |\mathsf{St}(1)$ for any $z \in G \smallsetminus \mathbf{Z}(G)$, (4.2) holds. We can now choose $|xy| = p = |w|$ to fulfill (B). Assuming the contrary that $\langle x, y\rangle \leq M < G$ for a maximal subgroup M of G, we will use [5, Tables 8.3, 8.4] to check possible candidates for M. First, if $q = 4$, then $|u| = 7$ and $|v| = 5$, but no maximal subgroup of $S = \mathrm{PSL}_3(4)$ has order divisible by 35, a contradiction. So we may assume $q \neq 4$, and hence $|u|$ is divisible by $\ell_1 = \mathrm{ppd}(p, 3f)$. Now $|u| = |x| \geq 13$, ruling out the possibilities $M = d \times \mathrm{PSL}_2(7)$ and $M = 3 \cdot \mathsf{A}_6$. If $2|f$, $f \neq 3$ and $|v|$ is divisible by $\ell_2 = \mathrm{ppd}(p, 2f)$, ruling out the possibility $M = \mathrm{SU}_3(\sqrt{q})$. All other possibilities for M are ruled out by the fact that $|M|$ is divisible by $\ell_1 p |y|$.

Next assume that $G = \mathrm{SU}_3(q), q = p^f \geq 3$. Then, we choose $|x| = (q^2 - q + 1)/d$, where $d := \gcd(3, q+1)$, $|y| = q^2 - 1$ if $d = 1$, and $|y| = (q^2-1)_{3'}$ if $d = 3$. Arguing as in the preceding case and using the character table of G, given in [41] and corrected in [22], we can choose $|xy| = p = |w|$ to fulfill (B). Assuming the contrary that $\langle x, y\rangle \leq M < G$ for a maximal subgroup M of G, we will use [5, Tables 8.5, 8.6] to check possible candidates for M. Note that $|u|$ is divisible by

$$\ell_1 = \mathrm{ppd}(p, 6f) \geq 7,$$

ruling out the possibilities $M = 3 \cdot \mathsf{A}_6$ and $3 \cdot \mathsf{A}_6 \cdot 2_3$. Next, $|v| \geq 8$, ruling out the possibility $M = d \times \mathrm{PSL}_2(7)$, and also $M = 3 \cdot \mathsf{A}_7$ when $q = 5$. All other possibilities for M are ruled out by the fact that $|M|$ is divisible by $p|x| \cdot |y|$.

We next record the following facts, established in [26] based on the results of [31, 37].

LEMMA 7.1. *Let $q = p^f$ and $n \geq 4$. Then, the following statements hold.*

(i) [26, Section 2.2.1] *Let $G = \mathrm{SL}_n(q)$ with $(n,q) \neq (6,2), (7,2)$, $T_1 < G$ a cyclic maximal torus of order $(q^n-1)/(q-1)$ and $T_2 < G$ a cyclic maximal torus of order $q^{n-1}-1$. Choose $\ell_1 = \mathrm{ppd}(p, nf)$, and $\ell_2 = \mathrm{ppd}(p,(n-1)f)$ if $(n,q) \neq (4,4)$ and $\ell_2 = 7$ otherwise. Then, for any element $x \in T_1$ of order divisible by ℓ_1 and any $y \in T_2$ of order divisible by ℓ_2, $x^G \cdot y^G \supseteq G \smallsetminus \mathbf{Z}(G)$.*

(ii) [26, Section 2.2.2] *Let $G = \mathrm{SU}_n(q)$ with $(n,q) \neq (4,2)$, $T_1 < G$ a cyclic maximal torus of order $(q^n-(-1)^n)/(q+1)$ and $T_2 < G$ a cyclic maximal torus of order $q^{n-1}-(-1)^{n-1}$. If $2 \nmid n$, choose $\ell_1 = \mathrm{ppd}(p, 2nf)$, and $\ell_2 = \mathrm{ppd}(p,(n-1)f)$ when $n \equiv 1 \pmod 4$, $\ell_2 = \mathrm{ppd}(p,(n-1)f/2)$ if $n \equiv 3 \pmod 4$ and $(n,q) \neq (7,4)$, and $\ell_2 = 7$ if $(n,q) = (7,4)$. If $2|n$, choose $\ell_2 = \mathrm{ppd}(p, 2(n-1)f)$, and $\ell_1 = \mathrm{ppd}(p,nf)$ when $n \equiv 0 \pmod 4$, $\ell_1 = \mathrm{ppd}(p,nf/2)$ if $n \equiv 2 \pmod 4$ and $(n,q) \neq (6,4)$, and $\ell_2 = 7$ if $(n,q) = (6,4)$. Then, for any element $x \in T_1$ of order divisible by ℓ_1 and any $y \in T_2$ of order divisible by ℓ_2, $x^G \cdot y^G \supseteq G \smallsetminus \mathbf{Z}(G)$.*

For $G = \mathrm{SL}_n(q)$ and $\mathrm{SU}_n(q)$ with $4 \leq n \leq 7$, we use Lemma 7.1 to choose x and y of order as indicated in Table I. By Lemma 7.1, $x^G \cdot y^G \supseteq G \smallsetminus \mathbf{Z}(G)$, so we can choose x and y so that xy has the order listed in Table 1. This ensures that (A) and

G	$r = \lvert x\rvert$	$s = \lvert y\rvert$	$\lvert xy\rvert$
$\mathrm{SL}_4(q), q > 2$	ℓ_1	q^2+q+1	p
$\mathrm{SU}_4(q), q > 3$	$(q^2+1)/\gcd(2,q-1)$	q^2-q+1	p
$\mathrm{SU}_4(2)$	5	9	2
$\mathrm{SU}_4(3)$	8	7	9
$\mathrm{SL}_5(q)$	ℓ_1	$(q^2+1)(q+1)$	p
$\mathrm{SU}_5(q), q > 2$	ℓ_1	q^2+1	p
$\mathrm{SU}_5(2)$	11	5	9
$\mathrm{SL}_6(q), q > 2$	ℓ_1	ℓ_2	p
$\mathrm{SL}_6(2)$	63	31	2
$\mathrm{SU}_6(q), q \neq 2,4$	ℓ_1	ℓ_2	p
$\mathrm{SU}_6(4)$	21	41	p
$\mathrm{SU}_6(2)$	7	11	15
$\mathrm{SL}_7(q), q > 2$	ℓ_1	ℓ_2	2
$\mathrm{SL}_7(2)$	127	7	2
$\mathrm{SU}_7(q), q \neq 4$	ℓ_1	ℓ_2	2
$\mathrm{SU}_7(4)$	113	7	2

TABLE 1. Elements x and y in some special linear and unitary groups.

(B) hold. It remains to show that $G = \langle x, y\rangle$ for the chosen x, y. Assume the contrary: $\langle x, y\rangle \leq M$ for a maximal subgroup M of G. We proceed case-by-case, indicating how we rule out all possibilities for M as listed in [5].

Assume $G = \mathrm{SL}_4(q)$ with $q \geq 3$ (note that $\mathrm{SL}_4(2) \cong \mathsf{A}_8$). Note that $|y| = q^2 + q + 1 \geq 13$, ruling out the possibilities A_7, $2 \cdot \mathsf{A}_7$, $\mathrm{PSL}_2(7)$, and $\mathrm{SU}_4(2)$ for M. All other possibilities for M in [5, Tables 8.8, 8.9] are ruled out by the fact that $|M|$ is divisible by rs.

Assume $G = \mathrm{SU}_4(q)$. When $q = 2$, respectively, $q = 3$, this choice of u, v, w shows that $\langle u, v\rangle = S$ since no maximal subgroup of S can have elements for each order 5 and 9, respectively, 7, 8, and 9 [14]. Assume $q > 3$. Then, $|x| = (q^2 + 1)/\gcd(2, q - 1) \geq 13$ and $|v| = q^2 - q + 1 \geq 7$, ruling out the possibilities $d \circ \mathrm{SL}_2(7)$ and $d \circ \mathrm{Sp}_4(3)$ for M, and also $M \ncong d \circ 2 \cdot \mathsf{A}_7$ if $q \geq 5$. All other possibilities for M in [5, Tables 8.10, 8.11] are ruled out by the fact that $|M|$ is divisible by rs.

Assume $G = \mathrm{SL}_5(q)$. Then, $|y| \geq 15$ shows $M \ncong M_{11}$ when $q = 3$, and $|u| = \ell_1 \geq 11$ shows that $M \neq d \times \mathrm{SU}_4(2)$. In fact, we have $|v| = |y| \geq 15$, and this shows $M \neq d \times \mathrm{PSL}_2(11)$. (We freely use the fact that maximal subgroups in class $\mathcal{S}$, such as the ones listed in [5, Table 8.19], act absolutely irreducibly on the natural G-module $\mathbb{F}_q^5$, and hence their centers are contained in $\mathbf{Z}(G)$.) All other possibilities for M in [5, Tables 8.18, 8.19] are ruled out by the fact that $|M|$ is divisible by rs.

Assume $G = \mathrm{SU}_5(q)$. Then, $|u| = \ell_1 \geq 11$ shows that $M \neq d \times \mathrm{SU}_4(2)$. Another candidate from [5, Table 8.21] is $M = d \times \mathrm{PSL}_2(11)$ with $d = \gcd(q + 1, 5)$, and $q = 2$ or $q \geq 7$. However, in such a case M does not contain any element of order 9, contradicting $|w| = 9$ when $q = 2$, and M has no $11'$-element of order > 30, contradicting $|y| = q^2 + 1 \geq 50$ when $q \geq 7$. All other possibilities for M in [5, Tables 8.20, 8.21] are ruled out by the fact that $|M|$ is divisible by rs.

Assume $G = \mathrm{SL}_6(q)$. Setting $\ell_1 = 7$ if $q = 2$, we note for all $q \geq 2$ that $|u|$ is divisible by the prime $\ell_1 \equiv 1 \pmod 6$ and $|v| = \ell_2 \equiv 1 \pmod 5$, and this rules out all possibilities for M listed in [5, Table 8.25]. All other possibilities for M, listed in [5, Table 8.24], are ruled out by the fact that $|M|$ is divisible by rs.

Assume $G = \mathrm{SU}_6(q)$. Note that $|u|$ is divisible by the prime $\ell_1 \equiv 1 \pmod 6$ and $|v| = \ell_2 \equiv 1 \pmod{10}$. This, together with $|uv| = 15$ when $q = 2$, rules out all possibilities for M listed in [5, Table 8.27]. All other possibilities for M, listed in [5, Table 8.26], are ruled out by the fact that $|M|$ is divisible by rs.

This proves Theorem A for all $\mathrm{PSU}_6(q)$, and also Theorem B for all $\mathrm{PSU}_6(q)$ with $q \neq 2$. To verify Theorem B for $S = \mathrm{PSU}_6(2)$, let G be the perfect group $3 \cdot S$. Then, G admits a generating pair x, y with $|x| = |y| = 11$, $|xy| = 7$, and which is Nielsen equivalent to the pair given by the [21] command

```
GeneratorsOfGroup(AtlasGroup("3.U6(2)"));.
```

Assume $G = \mathrm{SL}_7(q)$ or $\mathrm{SU}_7(q)$. Here, when $G = \mathrm{SL}_7(2)$, we choose $y \in G$ in class $7c$ in [21]. According to [5, Tables 8.35–8.38], no maximal subgroup of G can have order divisible by $2rs$.

7.2. *The case* $G = \mathrm{SL}_n(q)$ *with* $n \geq 8$

In the notation of Lemma 7.1, we choose x of order

$$r = \ell_1 = \mathrm{ppd}(p, nf) \geq nf + 1 \geq 11,$$

and y of order

$$s = \ell_2 = \mathrm{ppd}\big(p, (n-1)f\big) \geq (n-1)f + 1 \geq 11.$$

Then, (A) and (B) hold; in particular, we can choose xy of order $\ell_3 = \mathrm{ppd}(p, (n-2)f)$ if $(n, q) \neq (8, 2)$ and order $\ell_3 = 7$ otherwise. We also note that $(|x|, |y|, |xy|) = (|u|, |v|, |uv|)$, and

$$\max(\ell_1, \ell_2) \geq 2n - 1.$$

(Indeed, otherwise we must have that $f = 1$ and $(\ell_1, \ell_2) = (n+1, n)$, which is impossible.)

It remains to show that $S = \langle u, v\rangle$. Assume the contrary: $\langle x, y\rangle$ is contained in a maximal subgroup M of $\mathrm{SL}_n(q)$. By its choice, x has the $\mathrm{ppd}(n, q; e)$-property as defined in [25], with $e = n$. Similarly, y has the $\mathrm{ppd}(n, q; n-1)$-property. Hence, we can apply [25, Main Theorem] to see that M is in one of Examples 2.1–2.9 described therein. In what follows, to indicate that M is as in [25, Example 2.k], $1 \leq k \leq 9$, we will say that

$$M \text{ is in (2.k), or we are in (2.k).}$$

Suppose M is in (2.1). Since $\ell_1 = \mathrm{ppd}(p, nf)$, we must have $q_0 = q$. Furthermore, as $M < \mathrm{SL}_n(q)$, either $2|n$ and $M \leq \mathrm{CSp}_n(q)$ or $M \leq \mathrm{CO}_n^-(q)$, or $2|f, 2 \nmid n$, and $M \leq \mathrm{CU}_n(\sqrt{q})$ (these three groups are conformal groups, i.e., the subgroup of $\mathrm{GL}_n(q)$ that preserves the symplectic, orthogonal, or Hermitian form, up to $\mathbb{F}_q$-scalars). However, none of these conformal groups have order divisible by $\ell_2 = \mathrm{ppd}(p, (n-1)f)$.

Note that x is irreducible on the natural module $\mathbb{F}_q^n$, showing M is not in (2.2). Also, $e = n$ so M is not in (2.3). Suppose M is in (2.4). As $e = n$, we have $M \leq \mathrm{GL}_{n/b}(q^b) \cdot b$ for some divisor $b > 1$ of n. Then, $\ell_2 = \mathrm{ppd}(p, (n-1)f)$ cannot divide $|\mathrm{GL}_{n/b}(q^b)|$, so ℓ_2 must divide b. But $\ell_2 \geq (n-1)f + 1 \geq n$, so $b = n = \ell_2$. In this case, $M \leq \mathrm{GL}_1(q^n) \cdot \ell_2$, a contradiction as ℓ_3 divides $|xy|$.

Suppose M is in (2.5). Then, $n = 2^m$ and $\ell_1 = n + 1$ is a Fermat prime. As $\ell_1 \geq nf + 1$, we have $q = p$. As mentioned above, y has the $\mathrm{ppd}(n, q; n-1)$-property, and $\ell_2 = \mathrm{ppd}(p, n-1) \geq 2n-1$ (as $n = 2^m$). This is impossible for the groups in (2.5).

All the remaining candidates for M are almost quasisimple; in particular, $L := M^{(\infty)}$ is quasisimple. For the groups in (2.6), $\max(\ell_1, \ell_2) \le \max(n+2, 7) < 2n-1$, a contradiction. For the groups in (2.8), e can be equal to n only when $n = 4$, a contradiction.

Suppose we are in (2.7). For a fixed pair (n, L), the only pairs of two distinct primes $\{\ell_1, \ell_2\}$ both larger than 10 that occurs for groups in (2.7) are $\{11, 23\}$ (for $n = 11$, $p = 2$, and $L = M_{23}$ or $L = M_{24}$), $\{17, 19\}$ (with $n = 18$), and $\{11, 13\}$ (with $n = 12$). The latter two pairs cannot be realized in our situations because we would then have $\{\ell_1, \ell_2\} = \{n-1, n+1\}$. So we are in the former case, whence $q = p = 2$ and $L \lhd M \le \mathbf{N}_G(L) = L$, i.e., $M = L$ and $G = \mathrm{SL}_{11}(2)$. However, in this case, we can choose $\ell_1 = \mathrm{ppd}(2, 11)$ to be 89, which does not divide $|M|$, a contradiction.

Finally, suppose M is in (2.9). Then, again $11 \le \ell_1 \in \{n+1, 2n+1\}$ and $11 \le \ell_2 \in \{n, 2n-1\}$. None of the groups in [25, Table 7] can possess such a pair $\{\ell_1, \ell_2\}$. Inspecting possibilities for $\{\ell_1, \ell_2\}$ for a fixed pair (n, L) in [25, Table 8], we see that $L = \mathrm{PSL}_2(s)$, and either $s = 2^c$, $n = s$ or $s+1$, $\{\ell_1, \ell_2\} = \{s-1, s+1\}$, or s is a prime, $n = (s \pm 1)/2$, and $\{\ell_1, \ell_2\} = \{s, (s \pm 1)/2\}$. In the first case, $n \ge 8$ implies that $s = 2^c \ge 8$, so $s-1$ and $s+1$ cannot be primes at the same time. In the second case, the indicated ranges for ℓ_1, ℓ_2 imply that $n = (s-1)/2$, $\ell_1 = 2n+1$, and $\ell_2 = n \ge 8$; in particular, $n \ge 11$. Now we observe that the element xy also has the $\mathrm{ppd}(n, q; n-2)$-property, as it has order divisible by $\ell_3 = \mathrm{ppd}(p, (n-2)f)$. As n is prime, $\ell_3 \ge 2n-3$, and there is no place for the third prime ℓ_3 to occur for M.

REMARK 7.2. In a sense, the discussion in this and the next subsections first analyzes when the subgroup M can be a *generic subgroup* as defined in [38, Definition 3.2 (b)] and hence one can apply [38, Theorem 4.8] to it. The remaining arguments are to rule out the possibilities of M given in [38, Theorem 4.8], as well as the non-generic cases.

7.3. *The case* $G = \mathrm{SU}_n(\sqrt{q})$ *with* $n \ge 8$

We depart from the notation of Section 7.1 and denote $q = p^{2f}$, so that $G = \mathrm{SU}_n(p^f) = \mathrm{SU}(V)$ is a subgroup of $\mathrm{GL}_n(q) = \mathrm{GL}(V)$, where $V = \mathbb{F}_q^n$ is endowed with a non-degenerate Hermitian form $\circ$. In the notation of Lemma 7.1, we choose x of order $r = \ell_1$, and y of order $s = \ell_2$. If $2 \nmid n$, then $\ell_1 = \mathrm{ppd}(p, 2nf) \ge 2n+1 \ge 19$. If $2|n$, then $\ell_2 = \mathrm{ppd}(p, 2(n-1)f) \ge 2n-1 \ge 19$. Then, (A) and (B) hold; in particular, we can choose xy of order

$$\ell_3 = \mathrm{ppd}\big(p, 2(n-2)f\big) \ge 2n-3$$

if $2 \nmid n$, and order

$$\ell_3 = \mathrm{ppd}\big(p, 2(n-3)f\big) \ge 2n-5$$

if $2|n$. Note that $(|x|, |y|, |xy|) = (|u|, |v|, |uv|)$.

It remains to show that $S = \langle u, v\rangle$. Assume the contrary: $\langle x, y\rangle$ is contained in a maximal subgroup M of $\mathrm{SL}_n(q)$. When $2 \nmid n$, x has the $\mathrm{ppd}(n, q; e_1)$-property with $e_1 = n$, and xy has the $\mathrm{ppd}(n, q; e_2)$-property with $e_2 = n - 2$. When $2|n$, y has the $\mathrm{ppd}(n, q; e_1)$-property with $e_1 = n - 1$, and xy has the $\mathrm{ppd}(n, q; e_2)$-property with $e_2 = n - 3$. Hence, we can apply [25, Main Theorem] to see that M is in one of Examples 2.1–2.9 described therein.

Suppose M is in (2.1). Since $e_1 \geq n - 1$, we must have $q_0 = q$. Furthermore, as $M < \mathrm{SU}_n(\sqrt{q})$, $2|e_1$ and either $2|n$ and $M \leq \mathrm{CSp}_n(q)$ or $M \leq \mathrm{CO}^{\varepsilon}_n(q)$. However, our e_1 is always odd, a contradiction.

Suppose M is in (2.2); i.e., M is reducible on $V = \mathbb{F}_q^n$. As x is irreducible on V when $2 \nmid n$, we must have that $2|n$. In this case, y cannot act nontrivially on any subspace of V of dimension less than $n - 1$, so $M < \mathrm{SU}(V)$ preserves an orthogonal decomposition $V = \mathbb{F}_q^{n-1} \oplus \mathbb{F}_q$, showing that

$$M \leq \mathrm{GU}_1(\sqrt{q}) \times \mathrm{GU}_{n-1}(\sqrt{q}).$$

However, the order of such M is not divisible by $\ell_1 = |x|$.

Suppose M is in (2.3). As $e_1 = n$ when $2 \nmid n$, we must have that $2|n$ and $e_1 = n - 1$. But in this case, $\ell_2 = \mathrm{ppd}(p, 2(n-1)f) \geq 2n - 1$, impossible for groups in (2.3).

Suppose M is in (2.4). In [25, Example 2.4 (a)], we have $e_1 = n - 1$, so $2|n$, but then $\ell_2 \geq 2n - 1$, a contradiction. So $M \leq \mathrm{GL}_{n/b}(q^b) \cdot b$ for some divisor $b > 1$ of $\gcd(n, e_1)$. This implies that $e_1 = n$, whence $2 \nmid n$. Using $1 < b|n$ we can check that $\ell_2 \in \{\mathrm{ppd}(p, (n-1)f), \mathrm{ppd}(p, (n-1)f/2)\}$ cannot divide $|\mathrm{GL}_{n/b}(q^b)|$, so ℓ_2 must divide b. But $\ell_2 \geq (n-1)f/2 + 1 > n/2$, so $b = n = \ell_2$. In this case, $M \leq \mathrm{GL}_1(q^n) \cdot \ell_2$, a contradiction as ℓ_3 divides $|xy|$.

Suppose M is in (2.5). Then, $n = 2^m$ and $\max(\ell_1, \ell_2) = n + 1$, a contradiction.

All the remaining candidates for M are almost quasisimple; in particular, $L := M^{(\infty)}$ is quasisimple. For the groups in (2.6), $\max(\ell_1, \ell_2) \leq \max(n + 2, 7) < 2n - 1$, a contradiction. For the groups in (2.8), e_1 can be $\geq n - 1$ only when $n \leq 7$, a contradiction.

Suppose we are in (2.7); in particular, $n \neq 8$, and so $n \geq 9$. If $2 \nmid n$, then we note that $\ell_1, \ell_3 \geq 19$. Similarly, if $2 \nmid n$, then $\ell_2, \ell_3 \geq 19$. However, for a fixed pair (n, L), there are no pairs of two distinct primes both larger than 18 that can occur for groups in (2.7), a contradiction.

Finally, suppose M is in (2.9). None of the groups in [25, Table 7] can admit a prime $\ell_i > 13$. Inspecting possibilities for $\{\ell_1, \ell_3\}$ when $2 \nmid n$, and $\{\ell_2, \ell_3\}$ when $2|n$ for a fixed pair (n, L) in [25, Table 8], we see that $L = \mathrm{PSL}_2(s)$, and either $s = 2^c$ and $n = s$ or $s + 1$, with the pair of primes being $\{s - 1, s + 1\}$, or s is a prime and $n = (s \pm 1)/2$, with the pair of primes being $\{s, (s \pm 1)/2\}$. In particular, at least one of the occurring primes is $\leq n + 1$, whereas both of our primes in consideration are at least $n + 3$, a contradiction.

8. Proof of Theorems A and B: Symplectic and odd-dimensional orthogonal groups

8.1. *Some low-rank groups*

First, assume that $G = \mathrm{Sp}_6(2)$. Let H be its unique double cover. Using [21], we can check that there exist generators $x, y \in H$ such that $|x| = 5$, $|y| = 7$, $|xy| = 9$. This pair is Nielsen equivalent to the pair given by the [21] command

```
GeneratorsOfGroup(AtlasGroup("2.S6(2)"));.
```

This proves Theorems A and B for $\mathrm{Sp}_6(2)$.

Assume $G = \mathrm{Sp}_8(3)$, respectively, $\mathrm{Spin}_9(3)$. As shown in the proof of Lemma 2.12 in [26], we can choose $x \in G$ of order $\ell_1 = 41$, and y of order $s = 10$, respectively, $s = 39$, such that $x^G y^G = G \setminus \{1\}$. In particular, we can choose x and y so that $|xy| = 13$, respectively, $|xy| = 5$. Checking [5, Tables 8.48, 8.49, 8.58, and 8.59], we see that no maximal subgroup of G can simultaneously contain elements of order $|x|$, $|y|$, and $|xy|$. Hence, $G = \langle x, y\rangle$. Note that $v = y\mathbf{Z}(G)$ also has the same order in S as of y in S. Thus, we have proved Theorems A and B for $S = \mathrm{PSp}_8(3)$ and $S = \Omega_9(3)$.

Next we handle the case $S = \mathrm{PSp}_4(q)'$. We may assume that $q \geq 4$ since $\mathrm{Sp}_4(2)' \cong \mathsf{A}_6$ and $\mathrm{PSp}_4(3) \cong \mathrm{SU}_4(2)$ have already been handled. First, we consider the case $2 \nmid q \geq 5$. The proof of [26, Lemma 2.11] shows that we can find a regular semisimple element $x \in G$ of odd order $r = (q^2+1)/2 \geq 13$, and a regular semisimple element $y \in G$ of order $s|(q^2-1)/2$ such that $x^G y^G \supseteq G \setminus \mathbf{Z}(G)$. In fact, unless $q = 5, 7$, y can be chosen so that s is odd: this was done in the proof of [26, Lemma 2.11] if both $q \pm 1$ are not 2-powers or $q = 9$. If $q \geq 17$ is a Fermat prime, we choose y from class $B_4(2,4)$ of order $(q+1)/2$ in the notation of [43], and if $q \geq 31$ is a Mersenne prime, we choose y from class $B_3(2,4)$ of order $(q-1)/2$. Hence, we can conjugate x and y so that xy is a transvection (of order p); furthermore, $(|x|, |y|, |xy|) = (|u|, |v|, |uv|)$ if $q \geq 9$. Now suppose that $\langle x, y\rangle \leq M$ for some maximal subgroup M of G. Note that $r = |x|$ is odd and divisible by $\mathrm{ppd}(p, 4f)$. So using [5, Tables 8.12, 8.13], we get that $M = \mathrm{Sp}_2(q^2) \rtimes 2$, an extension field subgroup of G. As $|xy| = p$ is odd, $xy \in \mathrm{Sp}_2(q^2)$. But any element of order p in $\mathrm{Sp}_2(q^2)$ while acting on $\mathbb{F}_{q^2}^2$ is a fixed point subspace of dimension 1 over $\mathbb{F}_{p^2}$, i.e., 2-dimensional fixed point subspace on $\mathbb{F}_q^4$, and thus cannot be a transvection. Hence, $G = \langle x, y\rangle$, as desired. We now check Theorem B for $q = 5, 7$. For $\mathrm{PSp}_4(5)$, we check using [21] that its unique double cover admits a generating pair x, y such that $|x| = 5$, $|y| = 13$, $|xy| = 15$ and which is Nielsen equivalent to the pair

```
GeneratorsOfGroup(AtlasGroup("2.S4(5)"));.
```

For $q = 7$, its unique double cover admits a generating pair x, y with $|x| = |y| = |xy| = 25$, and which is Nielsen equivalent to the pair

```
GeneratorsOfGroup(AtlasGroup("2.S4(7)"));.
```

Suppose now that $q = 2^f \geq 4$. Then, we choose a regular semisimple element x of order $r = q^2 + 1$, in class $B_5(i)$ in the notation of [19], and a regular semisimple element y of order $s = q + 1$, in class $B_4(i, j)$ and with centralizer of order $(q + 1)^2$. Using the character table of G [19], we can check that only three characters: 1_G, the Steinberg character St, and another (θ_8 in [19], of degree $q(q-1)^2/2$) can be non-vanishing at x and at y. This allows us to verify (4.2), and thus $x^G y^G \supseteq G \setminus \{1\}$. As in the previous case, we may choose x and y so that xy is a transvection (of order 2); by our choice $(|x|, |y|, |xy|) = (|u|, |v|, |uv|)$. Now suppose that $\langle x, y\rangle \leq M$ for some maximal subgroup M of G. Note that $r = |x|$ is divisible by $\mathrm{ppd}(2, 4f)$. So using [5, Table 8.14], we get that $M \cong \mathrm{Sp}_2(q^2) \rtimes 2$. In either case, as y has odd order (dividing $q^2 - 1$), $y \in \mathrm{Sp}_2(q^2)$ and hence its centralizer in M has order divisible by $q^2 - 1$, contradicting the fact that $|\mathbf{C}_G(y)| = (q + 1)^2$. Hence, $G = \langle x, y\rangle$, as desired.

8.2. The general case

We will need the following result which is essentially recorded in [26, Section 2.2.3], whose proof relies on [37, Theorem 2.3].

LEMMA 8.1. *Let $q = p^f$, $n \geq 2$, $(n, q) \neq (2, 2), (2, 3), (3, 2), (4, 3)$. Let $G = \mathrm{Spin}_{2n+1}(q)$ with $2 \nmid q$, or $G = \mathrm{Sp}_{2n}(q)$, and let $T_1 < G$ be a maximal torus of order $q^n + 1$, $T_2 < G$ a cyclic maximal torus of order $q^n - 1$. Let $\ell_1 = \mathrm{ppd}(p, 2nf)$.*

(i) *Suppose $2 \nmid n$. Choose $\ell_2 = \mathrm{ppd}(p, nf)$ if $(n, q) \neq (3, 4)$ and $\ell_2 = 7$ otherwise. Then, for any elements $x \in T_1$ of order divisible by ℓ_1 and $y \in T_2$ of order divisible by ℓ_2, we have $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

(ii) *Suppose $2|n \geq 4$. Choose $s_1 = \ell_2 = \mathrm{ppd}(p, nf)$ if $(n, q) \neq (6, 2)$ and $s_1 = 3$ otherwise. Furthermore, if $n \geq 6$, choose $s_2 = \mathrm{ppd}(p, nf/2)$ if $(n, q) \neq (12, 2)$ and $s_2 = 7$ otherwise. If $n = 4$, choose $s_2 = \mathrm{ppd}(p, nf/2)$ if q is not a Mersenne prime, and $s_2 = 3$ if $q \geq 7$ is a Mersenne prime. Then, for any elements $x \in T_1$ of order divisible by ℓ_1 and $y \in T_2$ of order divisible by $s_1 s_2$, we have $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

First, we consider the case where $G = \mathrm{Spin}_7(q)$ with $2 \nmid q$, or $G = \mathrm{Sp}_6(q)$ with $q > 2$. Then, for the elements $x, y \in G$ constructed in Lemma 8.1 (i), we have

$$x^G y^G \supseteq G \setminus \mathbf{Z}(G).$$

In particular, we can choose x and y so that xy has order $(q^2+1)/\gcd(2,q-1)$ (indeed, $G/\mathbf{Z}(G)$ contains a subgroup that projects onto $\mathrm{PSp}_4(q) > \mathrm{PSp}_2(q^2)$). Assuming the contrary that $\langle x, y\rangle \leq M < G$ for a maximal subgroup M of G, we will use [5, Tables 8.39, 8.40], respectively [5, Tables 8.28, 8.29], to check possible candidates for M. Note that $|xy|$ is odd and ≥ 25 if $q \geq 7$, $|xy| = 5$ if $q = 3$, and $\ell_2 = 31$ if $q = 5$. This allows us to show $M \ncong \mathrm{SL}_2(13)$ when $2 \nmid q$. All other candidates for M are ruled out by considering the orders of x, y, and xy, using in particular that $\max(\ell_1, \ell_2) \geq 13$.

Now we assume $n \geq 4$, $(n,q) \neq (4,3)$, and handle the cases where $G = \Omega_{2n+1}(q)$ with $2 \nmid q$, or $G = \mathrm{Sp}_{2n}(q)$. We will construct the elements x and y using Lemma 8.1 (but working in $\Omega_{2n+1}(q)$ instead of $\mathrm{Spin}_{2n+1}(q)$ in the former case). If $2 \nmid n$, then we choose $x \in T_1$ of order $r = \ell_1$ and $y \in T_2$ of order $s = \ell_2$ as in Lemma 8.1 (i). If $2|n$, then we choose $x \in T_1$ of order r the part of $q^n + 1$ that is coprime to $2n$ (so divisible by ℓ_1 and coprime to $2n(q-1)$), and $y \in T_2$ of order $s = s_1 s_2$ as in Lemma 8.1 (ii). By our construction,

$$
\begin{aligned}
&\ell_1 = \mathrm{ppd}(p, 2nf) \geq 2nf + 1 \geq 11,\\
&\ell_2 = \mathrm{ppd}(p, nf) \geq nf + 1 \quad \text{if } (n,q) \neq (6,2),\\
&\max(\ell_1, \ell_2) \geq 4n + 1 \geq 23 \quad \text{if } 2 \nmid n,\\
&r \geq 4n + 1 \geq 17 \quad \text{unless } (n,q) = (9,2).
\end{aligned} \tag{8.1}
$$

(Indeed, the first two claims are given by the choice of ℓ_i. For the third claim, note that, since $2nf\,|(\ell_1 - 1)$, either $\ell_1 \geq 4n + 1 \geq 17$, in which case we are done, or $\ell_1 = 2n + 1$. Consider the latter case. If $2 \nmid n$, then $n|(\ell_2 - 1)$ but $\ell_2 \neq n + 1, 3n + 1$ (by parity) and $\ell_2 \neq \ell_1$, so $\ell_2 \geq 4n + 1$. Also, by [20], we have $r \geq 4n + 1$, unless $(n, f) = (5,2)$, $(6,2)$, and $(9,2)$, in which cases we have $r = 33$, 65, and 19, respectively.)

Let $V = \mathbb{F}_q^d$ with $d = 2n + 1$, respectively, $d = 2n$, be the natural module for G, considered with the corresponding bilinear form $(\cdot,\cdot)$. As $x^G y^G \supseteq G \smallsetminus \mathbf{Z}(G)$, we can choose x and y such that xy is a regular unipotent element, so that it acts with a single Jordan block of size d and a one-dimensional fixed point subspace $\langle v_1\rangle_{\mathbb{F}_q}$ on V; in particular, $(v_1, v_1) = 0$.

It remains to show that $S = \langle u, v\rangle$. Assume the contrary: $H := \langle x, y\rangle$ is contained in a maximal subgroup M of $G = \Omega_d(q)$, respectively, $\mathrm{Sp}_d(q)$. By its choice, x has the $\mathrm{ppd}(d, q; e)$-property, with $e = d$, respectively, $e = d - 1$. Hence, we can apply [25, Main Theorem] to see that M is in one of Examples 2.1–2.9 described therein.

Suppose M is in (2.1). Since $\ell_1 = \mathrm{ppd}(p, ef)$, we must have $q_0 = q$. Certainly, M cannot contain $\mathrm{SL}_d(q)$. If $M \rhd \mathrm{Sp}_d(q)$, then $G = \mathrm{Sp}_d(q)$ and hence $M = G$, a contradiction. Suppose $M \rhd \Omega_d^\varepsilon(q)$. Then, since $M < G$, we must have that $G = \mathrm{Sp}_d(q)$ with $d = 2n$, $2|q$, and $M = \mathrm{O}_d^-(q) = \Omega_d^-(q) \cdot 2$. Note that both x and y have

odd orders, so $H = \mathbf{O}^2(H) \leq \mathbf{O}^2(M) = \Omega_d^-(q)$. But in this case, the element xy, which is a regular unipotent element of $\mathrm{Sp}_d(q)$ and hence acts on $\mathbb{F}_q^d$ with a single Jordan block, has quasi-determinant -1 (see [14, p. xi]) and so cannot lie inside $\Omega_d^-(q)$, again a contradiction. The remaining possibility is that $\mathrm{SU}_d(\sqrt{q}) \lhd M \leq \mathrm{CU}_d(\sqrt{q})$ if $2|f$. However, if $2 \nmid d$, then $d = 2n+1$, and $\mathrm{ppd}(p, (2n+1)f)$ divides $|\mathrm{SU}_d(\sqrt{q})|$ but not $|G|$. If $2 \mid d$, then $d = 2n$, and $\ell_1 = \mathrm{ppd}(p, 2nf)$ divides $|M|$ but not $|\mathrm{CU}_d(\sqrt{q})|$.

Suppose M is in (2.2); i.e., M is reducible on V. If $d = 2n$, then x is irreducible on V. Hence, $d = 2n+1$, in which case the $\langle x\rangle$-module V is an orthogonal sum of two irreducible submodules: a non-degenerate subspace $\langle v_2\rangle_{\mathbb{F}_q}$ and its $2n$-dimensional orthogonal complement. It follows that M fixes $\langle v_2\rangle_{\mathbb{F}_q}$, and hence xy fixes v_2. But this is a contradiction since the fixed point subspace for xy is spanned by the singular vector e_1.

Suppose M is in (2.3). Then, $\ell_1 = e+1 \leq d$, whence $d = 2n+1 = \ell_1$, $2 \nmid q$, and $M \leq \mathrm{GL}_1(q) \wr \mathsf{S}_d$. Now if $2 \nmid n$, then $\ell_2 > d$ by (8.1) and $\ell_2 \nmid (q-1)$, and so $\ell_2 \nmid |M|$, a contradiction. Suppose $2|n$, whence $n \geq 6$ (as $\ell_1 = 2n+1$). Now $d = \ell_1$ is prime, and the only element order divisible by ℓ_1 in S_d is ℓ_1, so $x^{\ell_1} \in \mathrm{GL}_1(q)^d$ and thus $x^{\ell_1(q-1)} = 1$. But $|x| = r$ is coprime to $q-1$, so $x^{\ell_1} = 1$ and thus $r = \ell_1 = 2n+1$, contrary to (8.1).

Suppose M is in (2.4), so that $M \leq \mathrm{GL}_{d/b}(q^b) \cdot b$ for some $1 < b|d$. Here, the first possibility is that $\ell_1 = d = b = e+1$, whence $d = 2n+1$, $2 \nmid q$, and $M \leq \mathrm{GL}_1(q^d) \cdot d$. On the other hand, $s = |y|$ has a prime divisor $\ell_2 \neq \ell_1$ that divides $q^n - 1$ and so coprime to $q^d - 1$, a contradiction. Hence, we are in the second possibility: $b > 1$ divides $\gcd(e, d)$. As $d - 1 \leq e \leq d$, this implies that $e = d = 2n$. We claim that in this case

$$xy \in \mathrm{GL}_{d/b}(q^b). \tag{8.2}$$

This is certainly the case if $|x|$ and $|y|$ are both coprime to b, as this ensures that $H \leq \mathrm{GL}_{d/b}(q^b)$. Now, by our choice, $|x| = r$ is coprime to d. If $2 \nmid n$, then $|y| = \ell_2 > n$ is again coprime to d. If $2|n$, then the only case that $|y| = s$ is not coprime to d is when $(n, q, s) = (6, 2, 21)$. In this exception, using [5, Table 8.80], we can check that $M = \mathrm{Sp}_6(4) \cdot 2$ (in which case $H = \mathbf{O}^2(H) \leq \mathrm{Sp}_6(4) < \mathrm{GL}_{d/b}(q^b)$), or $M = \mathrm{Sp}_4(8) \cdot 3$ (in which case the 2-element xy belongs to $\mathrm{Sp}_4(8) < \mathrm{GL}_{d/b}(q^b)$). We have therefore proved (8.2), which implies that the p-element xy acts on $V = \mathbb{F}_q^d$ with every Jordan block repeating b times. But this is a contradiction since xy is regular unipotent.

Suppose M is in (2.5). Then, $2n = d = 2^{m+1}$ with $m \geq 2$. Furthermore, $p > 2$, and $\ell_1 = d+1$ is a Fermat prime, which implies that $m \geq 3$ is odd, whence $d - 1 = (2^{(m+1)/2} - 1)(2^{(m+1)/2} + 1)$ and $3|(2^m + 1)$. The structure of M then shows that any odd prime divisor of $|M|$ is either ℓ_1, a divisor of $q-1$, or at most $2^m - 1 = n - 1$. On the other hand, $|y|$ has a prime divisor $\ell_2 = \mathrm{ppd}(p, nf) \geq n+1$, a contradiction.

All the remaining candidates for M are almost quasisimple; in particular, $L := M^{(\infty)}$ is quasisimple acting absolutely irreducibly on V. Suppose M is in (2.6). Since $\ell_1 \geq 11$ by (8.1), we have that $L = \mathsf{A}_m$ acting on V via its deleted permutation module and $M \leq (C_{q-1} \times L) \cdot 2$. Here, $d \in \{m-2, m-1\}$ and all prime divisors of M that are coprime to $q-1$ are at most m. In particular, $\ell_1 \leq m \leq d+2 \leq 2n+3$. Using (8.1), we deduce that $\ell_1 = 2n+1$ and $f = 1$; in particular, $n > 4$. Now, if $2 \nmid n$, then $\ell_2 \geq 4n+1$ by (8.1) and hence cannot divide $|M|$. Hence, $2|n \geq 6$. Note that the only element order divisible by ℓ_1 in S_m is ℓ_1. It follows that $x^{\ell_1} \in C_{q-1}$, and hence $x^{\ell_1(q-1)} = 1$. But $(r, q-1) = 1$, so $x^{\ell_1} = 1$ and hence $r = \ell_1 = 2n+1$, which contradicts (8.1).

Suppose M is in (2.7). Since $d - 1 \leq e = 2n \geq 8$, from [25, Table 5], we see that $(e, d, \ell_1) = (10, 10, 11)$, $(10, 11, 11)$, $(12, 12, 13)$, $(18, 18, 19)$, $(22, 22, 23)$, $(22, 23, 23)$, or $(28, 28, 29)$. For $e = 10$, i.e., $n = 5$, we have $\ell_2 \geq 21$ and $5|(\ell_2 - 1)$ by (8.1), so $\ell_2 \geq 31$. For $e = 18$, i.e., $n = 9$, we have $\ell_2 \geq 37$ by (8.1). For $e = 22$, i.e., $n = 11$, we have $\ell_2 \geq 45$ and $11|(\ell_2 - 1)$ by (8.1), so $\ell_2 \geq 67$. In all these three cases, $\ell_2 \nmid (q-1)$ by its definition, and we can then check that ℓ_2 does not divide $|M|$ for any of the groups in [25, Table 5]. So $d = e = 12$ or 28. If moreover $e = 28$, i.e., $n = 14$, then as $14|(\ell_2 - 1)$ and $\ell_2 \neq 29$, we have $\ell_2 \geq 43$ and hence cannot divide $|M|$. In the case $d = e = 12$, we have $L = 6 \cdot \mathrm{Suz}$ and $p > 2$, so $|y| = s = s_1 s_2$ with $s_1 = \mathrm{ppd}(p, 6f) \geq 7$ and $s_2 = \mathrm{ppd}(p, 3f) \geq 7$, both different from $\ell_1 = \mathrm{ppd}(p, 12f)$. It follows that at least one of s_1, s_2 is ≥ 19 and hence does not divide $|M$, again a contradiction.

Suppose we are in (2.8). Since $e = 2n \geq d - 1$, we see from [25, Table 6] that $e \leq 6$, which is impossible since $n \geq 4$.

Finally, suppose M is in (2.9). Since $d - 1 \leq e = 2n \geq 8$, for the groups in [25, Table 7], we see that $(e, d, \ell_1) = (12, 12, 13)$, $p > 2$, and $L = 2 \cdot G_2(4)$. As in the previous case, we now see that at least one of s_1, s_2 is ≥ 19 and hence does not divide $|M$, a contradiction.

Next we consider the possibilities for L listed in [25, Table 8]. We will use the upper bounds for $\mathsf{meo}(L)$, the maximum order of elements $h \in \mathrm{Aut}(L)$, listed in [24, Table 3]. The construction of our elements x and y ensures that their order is the same order in $\mathrm{PGL}(V)$, and hence in $\mathrm{Aut}(L)$ as L acts absolutely irreducibly on V. The first case is $L/\mathbf{Z}(L) = \mathrm{PSL}_m(t)$ with $m \geq 3$ a prime and $e + 1 = \ell_1 = (t^m - 1)/(t - 1)$. Here, $\mathsf{meo}(L) = \ell_1 = 2n + 1$, so by (8.1) we must have $r = \ell_1$, and hence $(n, q) = (9, 2)$ and $(t^m - t)/(t - 1) = 18$, which is impossible.

The second case is $L/\mathbf{Z}(L) = \mathrm{PSU}_m(t)$ with $m \geq 3$ a prime and $e + 1 = \ell_1 = (t^m + 1)/(t + 1)$. Note that $e = (t^m - t)/(t + 1) \neq 18$. Now, if $L \neq \mathrm{SU}_5(2)$, then $\mathsf{meo}(L) < 2\ell_1$ by [24], and so $r = \ell_1$, contrary to (8.1). If $L = \mathrm{SU}_5(2)$, then $n = 5$ and $|y| = \ell_2 = \mathrm{ppd}(p, 5f)$ is ≥ 31 (as $\ell_2 \neq \ell_1 = 11$), and so $\ell_2 \nmid |M|$, again a contradiction.

The third family is $L/\mathbf{Z}(L) = \mathrm{PSp}_{2m}(t)$, where either $\ell_1 = (t^m + 1)/2$ and $2 \nmid t$ or $\ell_1 = (3^m - 1)/2$, $t = 3$, and m is a prime. It is easy to see that $t = t_0^{2^a}$ for a prime t_0 in the first case. As $H = \mathbf{O}^2(H)$, in either case we have $H \leq \mathbf{O}^2(M) \leq \mathbf{Z}(M)L$ (as $\mathrm{Out}(L)$ is a 2-group). Now we can check that the element x of order ℓ_1 generates a maximal torus in $L/\mathbf{Z}(L)$, and hence $r = \ell_1 = e + 1 = 2n + 1$, which implies $(n, q) = (9, 2)$ by (8.1). As $18 = 2n = e = \ell_1 - 1$, this cannot happen for the indicated $\ell_1 = (t^m \pm 1)/2$.

In the remaining families, we have $L/\mathbf{Z}(L) = \mathrm{PSL}_2(t)$ with $t \geq 7$. Since $\ell_1 \geq 11$, by (8.1), in fact we have $t \geq 11$, and $\mathsf{meo}(L) = t + 1$ by [24]. If $d \in \{t, t \pm 1\}$, then $\mathsf{meo}(L) \leq d + 2 \leq 2n + 3$, whereas when $2 \nmid n$, some $\ell_i \geq 4n + 1$ by (8.1), a contradiction. If $2|n$, then $r \geq 4n + 1$ by (8.1), a contradiction as well. Thus, $d = (t \pm 1)/2$, and so $\mathsf{meo}(L) = t + 1 \leq 2d + 2 \leq 4n + 4$. If $(n, q) = (9, 2)$ in addition, then we can choose $\ell_2 = 73$ which then does not divide $|M|$. So $(n, q) \neq (9, 2)$, whence $r \geq 4n + 1$ by (8.1). As $e = 2n$ and r is an odd multiple of ℓ_1 which is $2n + 1, 4n + 1$ or $\geq 6n + 1$, it follows that $r = \ell_1 = 4n + 1 = 2e + 1$. Applying [44, Theorem 3.2.2], we see that (q, n) is one of $(2, 4)$, $(2, 5)$, $(2, 6)$, $(2, 9)$ (which is already excluded), $(2, 10)$, or $(3, 9)$. However, by our choice r is 33, respectively, 65, and 4921, if $(q, n) = (2, 5)$, $(2, 6)$, or $(3, 9)$, respectively. If $(n, q) = (2, 10)$, then $s = 351$ by our construction. The only remaining case is $(n, q) = (4, 2)$, i.e., $G = \mathrm{Sp}_8(2)$, $r = \ell_1 = 17$, $s = 15$, and $|xy| = 8$. Checking the maximal subgroups with socle $\mathrm{PSL}_2(t)$ of G [21], we see that $M = \mathrm{PSL}_2(17)$ whose order is however coprime to 5, the final contradiction.

9. Proof of Theorems A and B: Even-dimensional orthogonal groups

9.1. *The rank* 4 *groups*

Assume $G = \mathrm{Spin}_8^+(q)$ with $q \geq 4$. By [26, Lemma 2.4], we can choose x of prime order $r = \ell_1 = \mathrm{ppd}(p, 6f)$, and y of prime order $s = \ell_2 = \mathrm{ppd}(q, 3)$ such that $x^G y^G = G \smallsetminus \mathbf{Z}(G)$. In particular, we can choose x and y so that xy has order $(q^4 - 1)_{2'}$ if both $q \pm 1$ are not 2-powers, and $(q^4 - 1)/\gcd(2, q - 1)$ otherwise (indeed, $\mathrm{SO}_8^+(q) > \mathrm{SO}_2^+(q^4) \cong C_{q^4-1}$, and $\Omega_8^+(q)$ has index $\gcd(2, q - 1)$ in $\mathrm{SO}_8^+(q)$). Assuming the contrary that $\langle u, v\rangle \leq M < S = G/\mathbf{Z}(G)$ for a maximal subgroup M of S, we will use [5, Table 8.50] to check possible candidates for M. Note that $\max(\ell_1, \ell_2) \geq 13$, in fact, $\ell_2 \geq 31$ if $q = 5$, and this rules out all possibilities of M with composition factor $\mathsf{A}_{8,9,10}$, $\Omega_8^+(2)$, or ${}^2B_2(8)$. Using the fact that $|M|$ is divisible by $\ell_1\ell_2$, we can rule out all other possibilities for M, except for $M \cong \Omega_7(q)$ if $2 \nmid q$, and $M \cong \mathrm{Sp}_6(q)$ or $G_2(q)$ when $2|q$. However, none of these two groups can contain elements of order equal to $|uv|$ (because $|uv| \geq (q^4 - 1)/\gcd(2, q - 1)^2 > (q^2 + 1)(q + 1)/\gcd(2, q - 1)$), a contradiction.

This proves Theorem A for $S = P\Omega_8^+(q)$ for $q \geq 4$, and also Theorem B if in addition none of $q \pm 1$ is a 2-power. To prove Theorem B for the remaining values of $q \geq 5$, we work with $L = \Omega_8^+(q) = \Omega(V)$ where $V = \mathbb{F}_q^8$. We again choose $x \in L$ of order $r = \ell_1 = \mathrm{ppd}(p, 6f)$ as before, but for y we choose a regular semisimple element of order $s = (q^2+1)/2 \geq 13$ in the torus T_2 considered in [37, Section 2.5]; in particular, y has no non-zero fixed point on V (such a y exists since $q \geq 5$). As shown in the proof of [37, Theorem 2.7], there are only three characters of L that are non-vanishing at both x and y: 1_L, St_L of degree q^{12}, and another one, γ, of degree $q^3(q^3-1)(q-1)^3/2$. They all take values ± 1 at x and y, except that $|\gamma(y)| = 2$. Now we choose $z \in L$ of order $(q^2+1)/2$ which has a 4-dimensional fixed point subspace on V, so that $|\mathbf{C}_L(y)|$ divides $q^2(q^2+1)(q^4-1)$, which implies $|\gamma(z)| < q^2(q^2+1)$ and $|\mathsf{St}_L(z)| = q^2$. It follows from (4.2) that $z \in x^L y^L$, so without loss of generality, we may assume that $z = xy$. Again using [5, Table 8.50], we can check that any maximal subgroup of L that contains elements of both orders r and s contains a unique conjugacy class of cyclic subgroups of order s. However, $\langle y \rangle$ and $\langle xy \rangle$ are not conjugate in L. It follows that $L = \langle x, y \rangle$. Since $S = L/\mathbf{Z}(L)$ with $|\mathbf{Z}(L)| = 2$, this proves Theorem B for S.

Assume $G = 2 \cdot \Omega_8^+(2)$. Choosing x from class $7a$ (number 51) of order $r = 7$, and y from class $12e$ (number 66), and z from class $5b$ (number 29) in the notation [21], we can check that $z \in x^G y^G$. Conjugating x and y suitably, we may assume that $z = xy$. We also note that only three characters of $S = G/\mathbf{Z}(G)$ (of degree 1, 50, 300) can be non-vanishing at both x and y, and the sum in (4.2) has absolute value at most $18/50 + 60/300 < 1$. Hence, $u^S v^S = S \smallsetminus \{1\}$ for $u = x\mathbf{Z}(G)$ and $v = y\mathbf{Z}(G)$. As elements of S, u belongs to class $7a$, v belongs to class $12a$, and uv belongs to class $5b$ in the notation of [21] (so $|uv| = 5$). Assume the contrary that $\langle u, v \rangle \leq M < S$ for a maximal subgroup M of S. As M contains u of order 7 and v from class $12a$, M is conjugate to one of three maximal subgroups of type $2^6 \rtimes \mathsf{A}_8$. However, none of these three subgroups can intersect both classes $12a$ and $5b$ at the same time, as can be seen using [21]. Hence, $S = \langle u, v \rangle$, and we have proved Theorems A and B for S.

Assume $S = P\Omega_8^+(3)$. Choosing u of order $r = 13$ from class $13a$ in the notation of [21], and v of order $s = 5$ from class $5a$ (number 24) in the notation [21], we can check that only three characters (of degree 1, 24192, 3^{12}) can be non-vanishing at both u and v, and the sum in (4.2) has absolute value at most $1/81 + 2/7 < 1$. Hence, $u^S v^S = S \smallsetminus \{1\}$. In particular, we can choose u and v so that uv belongs to class $18b$ (number 107) in the notation of [21] (so $|uv| = 18$). Assume the contrary that $\langle u, v \rangle \leq M < S$ for a maximal subgroup M of G. As M contains u of order 13 and uv of order 18, M is conjugate to one of six maximal subgroups of type $\Omega_7(3)$. However, none of these six subgroups can intersect both classes $5a$ and $18b$ at the same time, as can be seen using [21]. Thus, we have proved Theorem A for $S = P\Omega_8^+(3)$. To

prove Theorem B for S, we work inside $L = \Omega_8^+(3)$, and choose $x \in L$ from class $13a$ (number 159) and $y \in L$ from class $5a$ (number 41) in the notation of [21], so that $u' = x\mathbf{Z}(L)$ and $v' = y\mathbf{Z}(L)$ are conjugate in S to the aforementioned elements u, v of $S = L/\mathbf{Z}(L)$. Now choosing $z \in L$ from class $5b$ (number 43) and using [21], we can check that $z \in x'^L y^L$, whence we may assume $z = xy$. We can also check using [14] that if $M < S$ is a maximal subgroup that contains elements of both orders 13 and 5, then M has a unique conjugacy class of Sylow 5-subgroups (of order 5). However, by our choice, $\langle y\mathbf{Z}(L)\rangle$ and $\langle xy\mathbf{Z}(L)\rangle$ are not conjugate in S. It follows that $L = \langle x, y\rangle$, and hence we have proved Theorem B for S.

Assume $G = \Omega_8^-(2)$. Choosing x of order $\ell_1 = 17$, and y of order $\ell_2 = 7$ and using [21], we can check that $x^G y^G = G \setminus \{1\}$. In particular, we can choose x and y so that $|xy| = 2$. Since no maximal subgroup of G has order divisible by $17 \cdot 7$ [14], $G = \langle x, y\rangle$.

Assume $G = \mathrm{Spin}_8^-(q)$ with $q \geq 3$. By [26, Section 2.2.4], we can choose x of prime order $r = \ell_1 = \mathrm{ppd}(p, 8f)$, and y of prime order $s = \ell_2 = \mathrm{ppd}(p, 6f)$ such that $x^G y^G = G \setminus \mathbf{Z}(G)$. In particular, we can choose x and y so that xy has order $\ell_3 = \mathrm{ppd}(q, 3)$. According to [5, Tables 8.52, 8.53], no maximal subgroup of $S = G/\mathbf{Z}(G)$ can have order divisible by $\ell_1\ell_2\ell_3$. Hence, $G = \langle x, y\rangle$.

9.2. The general case

We will need the following result recorded in [26].

LEMMA 9.1 ([26, Section 2.2.4 and Theorem 2.7]). *Let $q = p^f$ and $n \geq 5$.*

(i) *Suppose $2 \nmid n$. Let $G = \mathrm{Spin}_{2n}^+(q)$, $T_1 < G$ a maximal torus of order $(q^{n-1} + 1)(q + 1)$, and $T_2 < G$ a maximal torus of order $q^n - 1$. Then, for any elements $x \in T_1$ of order divisible by $\ell_1 = \mathrm{ppd}(p, 2(n-1)f)$ and $y \in T_2$ of order divisible by $\ell_2 = \mathrm{ppd}(p, nf)$, we have $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

(ii) *Suppose $2 \mid n$. Let $G = \mathrm{Spin}_{2n}^+(q)$, $T_1 < G$ a maximal torus of order $(q^{n-1} + 1)(q + 1)$, and $T_2 < G$ a maximal torus of order $(q^{n-1} - 1)(q - 1)$. Then, for any elements $x \in T_1$ of order divisible by $\ell_1 = \mathrm{ppd}(p, 2(n-1)f)$ and $y \in T_2$ of order divisible by $\ell_2 = \mathrm{ppd}(p, (n-1)f)$ if $(n, q) \neq (4, 4)$ and $\ell_2 = 7$ otherwise, we have $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

(iii) *Let $G = \mathrm{Spin}_{2n}^-(q)$, $T_1 < G$ a maximal torus of order $q^n + 1$, and $T_2 < G$ a maximal torus of order $(q^{n-1} + 1)(q - 1)$. Then, for any elements $x \in T_1$ of order divisible by $\ell_1 = \mathrm{ppd}(p, 2nf)$ and $y \in T_2$ of order divisible by $\ell_2 = \mathrm{ppd}(p, 2(n-1)f)$, we have $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

Now we assume

$$n \geq 5,$$

and complete the proof for

$$G = \Omega(V) = \Omega^{\varepsilon}_{2n}(q),$$

where $V = \mathbb{F}_q^{2n}$ is endowed with a G-invariant non-degenerate quadratic form Q of type $\varepsilon = \pm$. We will construct the elements $x, y \in G$ using Lemma 9.1 but working in $\Omega^{\varepsilon}_{2n}(q)$ instead of $\mathrm{Spin}^{\varepsilon}_{2n}(q)$. If $2|q, \varepsilon = +$, and $2|n$, we choose x of order $r = q^{n-1} + 1$ (so divisible by ℓ_1), and y of order $s = \ell_2$. If $q = 2$, $\varepsilon = -$, and $n = 6$, we choose x of order $r = q^n + 1 = 65$ (so divisible by $\ell_1 = 13$), and y of order $s = \ell_2$. In all other cases, we choose x of order r, the (full) ℓ_1-part of $q^n + 1$ when $\varepsilon = -$ and of $q^{n-1} + 1$ when $\varepsilon = +$, and y of order $s = \ell_2$. By our construction,

$$\ell_1 \geq 2nf + 1 \geq 11 \text{ if } \varepsilon = -, \quad \ell_1 \geq (2n-2)f + 1 \geq 11 \text{ if } \varepsilon = +. \tag{9.1}$$

Moreover,

$$\begin{array}{lll} \text{if } \varepsilon = +, \quad \text{then } r \geq 6(n-1)+1, & \text{unless } q = 2 \text{ and } n = 5, 7, 11, \\ & \text{or } (q, n) = (3, 10), \\ \text{if } \varepsilon = -, \quad \text{then } r \geq 6n + 1, & \text{unless } q = 2 \text{ and } n = 5, 9, 10, \\ & \text{or } (q, n) = (3, 9). \end{array} \tag{9.2}$$

Indeed, in the case $\varepsilon = +$, since $n \geq 5$, by [44, Theorem 3.2.2], we have

$$r \geq (q^{2n-2} - 1)_{\ell_1} \geq 6(n-1) + 1,$$

unless $q = 2$ and $2n - 2 \in \{8, 10, 12, 18, 20\}$, or $(q, 2n-2) = (3, 18)$. Also, when $(q, n) = (2, 6), (2, 10)$, by our choice, we have $r = 33, 513$. Similarly, in the case $\varepsilon = -$, by [44, Theorem 3.2.2], we have $r = (q^{2n} - 1)_{\ell_1} \geq 6n + 1$, unless $q = 2$ and $2n \in \{10, 12, 18, 20\}$, or $(q, 2n) = (3, 18)$. Furthermore, $r = 65$ when $(q, n) = (2, 6)$ by our construction.

Since $x^G y^G \supseteq G \smallsetminus \mathbf{Z}(G)$, we can choose x and y such that xy is a p-element that acts on V with two Jordan blocks, of size $2n - 3$ and 3 if $2 \nmid q$, and of size $2n - 2$ and 2 if $2|q$.

It remains to show that $S = \langle u, v \rangle$. Assume the contrary: $H := \langle x, y \rangle$ is contained in a maximal subgroup M of $G = \Omega^{\varepsilon}_{2n}(q)$. By its choice, x has the $\mathrm{ppd}(2n, q; e)$-property, with $e = 2n - 2$ if $\varepsilon = +$ and $e = 2n$ if $\varepsilon = -$. Hence, we can apply [25, Main Theorem] to see that M is in one of Examples 2.1–2.9 described therein.

Suppose M is in (2.1). Since $\ell_1 = \mathrm{ppd}(p, ef)$, we must have $q_0 = q$. Certainly, M cannot contain $\mathrm{SL}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$, or $\Omega^{\pm}_{2n}(q)$. The remaining possibility is that $\mathrm{SU}_{2n}(\sqrt{q}) \lhd M \leq \mathrm{CU}_{2n}(\sqrt{q})$ if $2|f$. But then $\mathrm{ppd}(p, (2n-1)f)$ divides $|M|$ but not $|G|$, a contradiction.

Suppose M is in (2.2); i.e., M is reducible on V, say with a non-zero submodule $A \neq V$. If $\varepsilon = -$, then x is irreducible on V. Hence, $\varepsilon = +$, in which case the $\langle x \rangle$-module V is an orthogonal sum of submodules: a non-degenerate subspace $U = \mathbb{F}_q^2$ of type $-$ (with respect to Q) and its $(2n-2)$-dimensional orthogonal complement $U^\perp$ which is irreducible over $\langle x \rangle$. Replacing A by $A^\perp$ if necessary, we may assume that $A^\perp \supseteq U^\perp$, and hence $A \subseteq U$. If $2 \nmid q$, then, as U is of type $-$, A contains no (non-zero) singular vector, and so $A \cap A^\perp = 0$ and $V = A \oplus A^\perp$. In this case, xy has a Jordan block of size $\dim(A) \leq 2$, contrary to the choice of x and y. Hence, $2|q$, in which case x acts irreducibly on U and so $A = U$. But then y fixes $U = \mathbb{F}_q^2$ of type $-$, which is impossible by the choice of y: if $2 \nmid n$, then $V|_{\langle y \rangle}$ is the sum of two irreducible submodules of dimension n, and if $2 \mid n$, then $V|_{\langle y \rangle}$ is the sum of two irreducible submodules of dimension $n-1$ and a 2-dimensional submodule which is of type $+$.

Suppose M is in (2.3). Then, $\ell_1 = e + 1 \leq 2n$, whence $\varepsilon = +$, $\ell_1 = 2n - 1$, $f = 1$, and $M \leq \mathrm{GL}_1(q) \wr \mathsf{S}_{2n}$. Now if $2 \nmid n$, then $\ell_2 = \mathrm{ppd}(p, nf) \geq 2n + 1$ and $\ell_2 \nmid (q-1)$, and so $\ell_2 \nmid |M|$, a contradiction. Suppose $2|n$, whence $n \geq 6$. Then, $\ell_2 = \mathrm{ppd}(p, n-1)$ is congruent to 1 module $n-1$ and different from n and $3n-2$ (by parity), and from $2n - 1 = \ell_1$. Thus, $\ell_2 \geq 4n - 3$ and coprime to $q - 1$, so it does not divide $|M|$, again a contradiction.

Suppose M is in (2.4), so that $M \leq \mathrm{GL}_{2n/b}(q^b) \cdot b$ for some $1 < b | 2n$. Here, the first possibility is that $\ell_1 = 2n = b = e + 1$, which is absurd. Hence, we are in the second possibility: $b > 1$ divides $\gcd(e, 2n)$. Note that

$$xy \in \mathrm{GL}_{2n/b}(q^b). \tag{9.3}$$

(Indeed, this is certainly the case if $|x|$ and $|y|$ are both coprime to b, as this ensures that $H \leq \mathrm{GL}_{2n/b}(q^b)$. Now, if $\varepsilon = +$, then $e = 2n - 2$ and hence $b = 2$, whereas by our choice, $|x|$ and $|y|$ are odd. If $\varepsilon = -$, then $\ell_1 > 2n$ and $\ell_2 \geq 2n - 1$, whereas $b = 2n$ or $b \leq n$.) Now (9.3) implies that the p-element xy acts on $V = \mathbb{F}_q^{2n}$ with every Jordan block repeating b times. But this contradicts the choice of xy.

Suppose M is in (2.5). Then, $2n = 2^{m+1}$ with $m \geq 3$. Furthermore, $p > 2$, and either $\ell_1 = 2n + 1$ is a Fermat prime and $\varepsilon = -$, or $\ell_1 = 2n - 1$ is a Mersenne prime and $\varepsilon = +$. In the first case, $m \geq 3$ is odd, so $2n - 1 = (2^{(m+1)/2} - 1)(2^{(m+1)/2} + 1)$. The structure of M then shows that any odd prime divisor of $|M|$ is either ℓ_1, a divisor of $q - 1$, or at most $2^m + 1 = n + 1$. On the other hand, $|y| = \ell_2 = \mathrm{ppd}(p, 2(n-1)f) \geq 2n - 1$, a contradiction. In the second case, $f = 1$ and m is even, so $3|(2n + 1)$. The structure of M then shows that any odd prime divisor of $|M|$ is either ℓ_1, a divisor of $q - 1$, or at most $2^m + 1 = n + 1$. On the other hand, as $n > 4$, $\ell_2 = \mathrm{ppd}(p, n-1) \geq 2n - 1$, again a contradiction.

All the remaining candidates for M are almost quasisimple; in particular, $L := M^{(\infty)}$ is quasisimple acting absolutely irreducibly on V. Suppose M is in (2.6). Since $\ell_1 \geq 11$ by (8.1), we have that $L = \mathsf{A}_m$ acting on V via its deleted permutation module and $M \leq (C_{q-1} \times L) \cdot 2$. Here, $2n \in \{m-2, m-1\}$ and hence all prime divisors of M that are coprime to $q-1$ are at most m. In particular, $\ell_1 \leq m \leq 2n+2$. Using (9.1), we deduce that $\ell_1 = 2n \pm 1$ and $f = 1$. Note that the only element order divisible by ℓ_1 in S_m is ℓ_1. If $\varepsilon = +$, then by (9.2), we either have $\ell_2 > 2n+2$ (and coprime to $q-1$) and hence y cannot be contained in M, or $r > 2n+2 \geq m$. In the latter case $x^{\ell_1(q-1)} = 1$, but $|x| = r$ is coprime to $q-1$, whence $x^{\ell_1} = 1$, which is impossible. If $\varepsilon = -$, then by (9.2), we have $\max(r, \ell_2) > 2n+2$ with $\gcd(q-1, r\ell_2) = 1$, and so we reach a contradiction as in the previous case.

Suppose M is in (2.7). Since $2|e \geq 2n-2 \geq 8$, from [25, Table 5], we see that

$$(e, 2n, \ell_1) = (10,10,11), (10,12,11), (12,12,13), (18,18,19), (18,20,19), (22,22,23), (22,24,23), \text{ or } (28,28,29).$$

In the three cases with $e = 2n-2$: $(10,12,11)$, $(18,20,19)$, and $(22,24,23)$, we have $\varepsilon = +$, $2|n$, $\ell_2 \equiv 1 \pmod{n-1}$ and $\ell_2 \neq \ell_1 = 2n-1$, which together imply $\ell_2 \geq 31$ and so ℓ_2 does not divide $|M|$, a contradiction. In the following three cases with $e = 2n$ (so $\varepsilon = -$): $(10,10,11)$, $(22,22,23)$, and $(28,28,29)$, we have $\ell_2 \geq 17$, 41, 53, respectively, and so ℓ_2 does not divide $|M|$, again a contradiction. In the case of $(12,12,13)$, i.e., $L = 6 \cdot \mathrm{Suz}$, we have $p > 2$, so by (9.1), the power r of $\ell_1 = 13$ satisfies $r \geq 37$, i.e., $r \geq \ell_1^2$. In the case of $(18,18,19)$, i.e., $L = 3 \cdot \mathrm{J}_3$, we have $p > 3$, so by (9.1), the power r of $\ell_1 = 19$ satisfies $r \geq 55$, i.e., $r \geq \ell_1^2$. In both of these two cases, $r = |x|$ is coprime to $q-1$, and hence M cannot have any element of such order $r \geq \ell_1^2$, a contradiction.

Suppose we are in (2.8). Since $n \geq 5$, we have no example from [25, Table 6].

Finally, suppose M is in (2.9). Since $n \geq 5$, for the groups in [25, Table 7], we see that $(2n, e, \ell_1, L)$ is one of $(12,12,13, 2 \cdot G_2(4))$, $(14,12,13, {}^2B_2(8)$ or $G_2(3))$, and $(18,16,17, \mathrm{Sp}_4(4))$. In the first two cases, $\ell_2 = \mathrm{ppd}(p, 5f) \geq 11$ cannot divide $|M|$. In the third case, $\ell_2 = \mathrm{ppd}(p, 8f) \neq 17$, so $\ell_2 \geq 41$ cannot divide $|M|$.

Next we consider the possibilities for L listed in [25, Table 8]. We will again use the upper bounds for $\mathsf{meo}(L)$ listed in [24, Table 3]. The construction of our elements x and y ensures that their order is the same order in $\mathrm{PGL}(V)$, and hence in $\mathrm{Aut}(L)$ as L acts absolutely irreducibly on V. The first case is $L/\mathbf{Z}(L) = \mathrm{PSL}_m(t)$ with $m \geq 3$ a prime and

$$2n+1 \geq e+1 = \ell_1 = (t^m - 1)/(t-1) \geq 2n,$$

so in fact $\ell_1 = 2n+1$, $e = 2n$, and $\varepsilon = -$. Here, $\mathsf{meo}(L) = \ell_1 \leq 2n+1$, so by (9.1), we must have $r = \ell_1$, and hence we are in one of the exceptions of (9.2). Thus, $2n = (t^m - t)/(t-1) \in \{10, 18\}$ (as $\ell_1 = 2n+1 \neq 21$), which is impossible.

The second case is $L/\mathbf{Z}(L) = \mathrm{PSU}_m(t)$ with $m \geq 3$ a prime and $2n+1 \geq e+1 = \ell_1 = (t^m+1)/(t+1) \geq 2n$, so in fact $\ell_1 = 2n+1$, $e = 2n$, and $\varepsilon = -$. Here, $\mathsf{meo}(L) \leq 2\ell_1 + 2 < 3\ell_1$, so by (9.1), we must have $r = \ell_1$, and hence we are in one of the exceptions of (9.2). Thus, $2n = (t^m - t)/(t+1) \in \{10, 18\}$ (as $\ell_1 = 2n+1 \neq 21$), which is possible only when $2n = 10$ and $L = \mathrm{SU}_5(2)$. But in this case, $|y| = \ell_2 = \mathrm{ppd}(p, 8f) \geq 17$, and so $\ell_2 \nmid |M|$, again a contradiction.

The third family is $L/\mathbf{Z}(L) = \mathrm{PSp}_{2m}(t)$, where either $\ell_1 = (t^m+1)/2$ and $2 \nmid t$, or $\ell_1 = (3^m-1)/2$, $t = 3$, and m is a prime. It is easy to see that $t = t_0^{2^a}$ for a prime t_0 in the first case. As $H = \mathbf{O}^2(H)$, in either case, we have $H \leq \mathbf{O}^2(M) \leq \mathbf{Z}(M)L$ (as $\mathrm{Out}(L)$ is a 2-group). Now we can check that the element x of order ℓ_1 generates a maximal torus in $L/\mathbf{Z}(L)$, and hence $r = \ell_1 = e+1 = 2n+1$, which implies $n \in \{5, 7, 9, 10, 11\}$ by (9.2). As $2n = e = \ell_1 - 1$, this cannot happen for the indicated $\ell_1 = (t^m \pm 1)/2$.

In the remaining families, we have $L/\mathbf{Z}(L) = \mathrm{PSL}_2(t)$ with $t \geq 7$. Since $\max(\ell_1, \ell_2) \geq 11$ by (9.1), in fact, we have $t \geq 11$, and $\mathsf{meo}(L) = t+1$ by [24]. Here, $(t-1)/2 \leq 2n$, so $r \leq t+1 \leq 4n+2 < 6n-5$. Hence, we must be in one of the exceptions listed in (9.2), and thus $n \in \{5, 7, 9, 10, 11\}$. In the case $t = 2^c$, we have $2n \in \{t, t \pm 1\}$, and none fits in the indicated range. So $2 \nmid t$. We will now take into account the value of q listed in these exceptions. When $\varepsilon = +$, we have $q = 2$ and $n = 5, 7, 11$, or $(q, n) = (3, 10)$, in which cases we can take $\ell_2 = 31$, 127, 89, or 257, respectively, which all exceed $\mathsf{meo}(L) \leq 4n+2$. When $\varepsilon = -$, we have $q = 2$ and $n = 5, 9, 10$, or $(q, n) = (3, 9)$, in which cases we can take $\ell_2 = 17$, 257, 19, or 193, respectively. Since $\mathsf{meo}(L) \leq 4n+2$, we are left with the two cases $(q, n) = (2, 5)$, $(2, 10)$. If $(q, n) = (2, 5)$, then $t = 9$, 11, or 19, and so $\ell_2 = 17$ does not divide $|\mathrm{Aut}(L)|$. If $(q, n) = (2, 10)$, then $t = 19$, or 41. Since $\ell_1 = 41$ divides $|\mathrm{Aut}(L)|$, we get $t = 41$. But in this case, $\ell_2 = 19$ again does not divide $|\mathrm{Aut}(L)|$, the final contradiction.

This completes the proof of Theorems A and B unless S is a sporadic simple group.

10. Proof of Theorems A and B: The sporadic groups

Here we record some data describing our verification of Theorems A and B for the sporadic simple groups. Typically, we will begin each entry with the name of the group S, followed by its order N, the isomorphism type of its Schur multiplier $H_2(S, \mathbb{Z})$, and the [21] command for constructing a certain perfect central extension of the group. This central extension will be denoted by G, the simple group being $S = G/Z(G)$. If the center of the central extension is not specified, then the extension will be the Schur cover. The end of each entry will be a statement which implies that Theorems A and B hold for the simple group S. Unless otherwise mentioned, our methods employ a random search via the product replacement algorithm using [21].

The default generators of this central extension will refer to the generating pair which can be obtained via the [21] command

`GeneratorsOfGroup(<group>);`.

For a triple of integers $r, s, t \in \mathbb{Z}_{\geq 1}$, an (r, s, t)-pair of a group G is a pair $x, y \in G$ satisfying $|x| = r, |y| = s, |xy| = t$.

10.1. Mathieu groups

- M_{11}, $N = 7920$, $H_2(S, \mathbb{Z}) = 0$, `AtlasGroup("M11");`
  G admits a $(3, 8, 11)$-generating pair Nielsen equivalent to the default generators.
- M_{12}, $N = 95040$, $H_2(S, \mathbb{Z}) = C_2$, `AtlasGroup("2.M12");`
  G admits a $(3, 5, 11)$-generating pair Nielsen equivalent to the default generators.
- M_{22}, $N = 443520$, $H_2(S, \mathbb{Z}) = C_{12}$, `AtlasGroup("4.M22");`, $Z(G) \cong C_4$.
  G admits a $(3, 5, 11)$-generating pair Nielsen equivalent to the default generators.
- M_{23}, $N = 10200960$, $H_2(S, \mathbb{Z}) = 0$, `AtlasGroup("M23");`
  G admits a $(7, 8, 15)$-generating pair Nielsen equivalent to the default generators.
- M_{24}, $N = 244823040$, $H_2(S, \mathbb{Z}) = 0$, `AtlasGroup("M24");`

The default generator of G is a $(2, 3, 23)$-pair.

10.2. Janko groups

- J_1, $N = 175560$, $H_2(S, \mathbb{Z}) = 0$, `AtlasGroup("J1");`
  The default generator of G is a $(2, 3, 7)$-pair. Thus, J_1 is a Hurwitz group; see [12].
- J_2, $N = 604800$, $H_2(S, \mathbb{Z}) = C_2$, `AtlasGroup("2.J2");`
  J_2 is a Hurwitz group; see [12]; in fact, the default generator of `AtlasGroup("J2");` is a $(2, 3, 7)$-pair. The Schur cover G admits a $(7, 7, 3)$-generating pair which is Nielsen equivalent to its default generators.
- J_3, $N = 50232960$, $H_2(S, \mathbb{Z}) = C_3$, `AtlasGroup("3.J3");`
  G admits a $(8, 17, 19)$-generating pair Nielsen equivalent to the default generators.
- J_4, $N = 86775571046077562880$, $H_2(S, \mathbb{Z}) = 0$, `AtlasGroup("J4");`
  J_4 is a Hurwitz group [12] and thus admits a $(2, 3, 7)$-generating pair.

10.3. Conway groups

- Co_1, $N = 4157776806543360000$, $H_2(S, \mathbb{Z}) = C_2$, `AtlasGroup("2.Co1");`
  G admits both a $(15, 15, 23)$-generating pair and a $(13, 20, 21)$-generating pair.

- Co_2, $N = 42305421312000$, $H_2(S,\mathbb{Z}) = 0$, `AtlasGroup("Co2");`
  G admits a $(5, 9, 28)$-generating pair Nielsen equivalent to the default generators.
- Co_3, $N = 495766656000$, $H_2(S,\mathbb{Z}) = 0$, `AtlasGroup("Co3");`
  Co_3 is a Hurwitz group [12] and thus admits a $(2, 3, 7)$-generating pair.

10.4. Fischer groups

- Fi_{22}, $N = 64561751654400$, $H_2(S,\mathbb{Z}) = C_6$, `AtlasGroup("3.Fi22");`,
  $Z(G) \cong C_3$.
  G admits a $(7, 11, 13)$-generating pair Nielsen equivalent to the default generators.
- Fi_{23}, $N = 4089470473293004800$, $H_2(S,\mathbb{Z}) = 0$, `AtlasGroup("Fi23");`
  G admits a $(11, 12, 35)$-generating pair Nielsen equivalent to the default generators.
- Fi'_{24}, $N = 1255205709190661721292800$, $H_2(S,\mathbb{Z}) = C_3$,
  `AtlasGroup("3.Fi24'");`
  G admits a $(13, 17, 20)$-generating pair Nielsen equivalent to the default generators.

10.5. Other sporadic groups

- Higman–Sims group HS, $N = 44352000$, $H_2(S,\mathbb{Z}) \cong C_2$, `AtlasGroup("2.HS");`
  G admits a $(5, 7, 11)$-generating pair Nielsen equivalent to the default generators.
- McLaughlin group McL, $N := 898128000$, $H_2(S,\mathbb{Z}) \cong C_3$,
  `AtlasGroup("3.McL");`
  G admits a $(5, 7, 11)$-generating pair Nielsen equivalent to the default generators.
- Held group He, $N = 4030387200$, $H_2(S,\mathbb{Z}) = 0$, `AtlasGroup("He");`
  This is a Hurwitz group [12] and thus admits a $(2, 3, 7)$-generating pair.
- Rudvalis group Ru, $N = 145926144000$, $H_2(S,\mathbb{Z}) \cong C_2$, `AtlasGroup("2.Ru");`
  G admits a $(5, 13, 29)$-generating pair Nielsen equivalent to the default generators.
- Suzuki sporadic group Suz, $N = 448345497600$, $H_2(S,\mathbb{Z}) \cong C_6$,
  `AtlasGroup("2.Suz");`, $Z(G) \cong C_2$.
  G admits a $(5, 13, 21)$-generating pair Nielsen equivalent to the default generators.
- O'Nan group O'N, $N = 460815505920$, $H_2(S,\mathbb{Z}) \cong C_3$, `AtlasGroup("3.ON");`
  G admits a $(19, 20, 31)$-generating pair Nielsen equivalent to the default generators.
- Harada–Norton group HN, $N = 273030912000000$, $H_2(S,\mathbb{Z}) = 0$,
  `AtlasGroup("HN");`
  HN is a Hurwitz group [12] and hence admits a $(2, 3, 7)$-generating pair.
- Lyons group Ly, $N = 51765179004000000$, $H_2(S,\mathbb{Z}) = 0$, `AtlasGroup("Ly");`
  Ly is a Hurwitz group [12] and hence admits a $(2, 3, 7)$-generating pair.

- Thompson group Th, $N = 90745943887872000$, $H_2(S,\mathbb{Z}) = 0$,
  `AtlasGroup("Th");`
  Th is a Hurwitz group [12] and hence admits a $(2,3,7)$-generating pair.
- Baby Monster group B, $N = 4154781481226426191177580544000000$,
  $H_2(S,\mathbb{Z}) \cong C_2$.
  The Baby Monster can be constructed in [21] as `AtlasGroup("B");`, but its Schur double cover cannot. Nonetheless, one can access the character table of the double cover. The following [21] transcript shows that the Schur cover of the Baby Monster admits a $(3,5,47)$-pair:

```
gap> tbl := CharacterTable("2.B");
CharacterTable("2.B")
gap> irr := Irr(tbl);;
gap> OrdersClassRepresentatives(tbl){[8,23,228]};
[3, 5, 47]
gap> Sum(List(irr,ch -> ch[8]*ch[23]*ch[228]/ch[1]));
34626119/41013248
```

  Here, the fourth and fifth lines show that 8th, 23rd, and 228th conjugacy classes (in the table `tbl`) consist of elements of orders 3, 5, 47, respectively. Lines 6–7 then show that if x, y, z are representatives of such conjugacy classes, then

$$\sum_{\chi\,\mathrm{irr}} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)} > 0.$$

  This implies that the Schur cover of the Baby Monster admits a $(3,5,47)$-pair [40, Theorem 7.2.1]. Finally, from the list of the maximal subgroups of the Baby Monster [14], we find that up to conjugation, the only maximal subgroup which contains an element of order 47 has order $23 \cdot 47$. It follows that any $(3,5,47)$-pair is generating.
- Monster group M,
  $N = 808017424794512875886459904961710757005754368 \cdot 10^9$.
  The monster M has a trivial Schur multiplier, so it suffices to note that it is a Hurwitz group [12] and hence admits a $(2,3,7)$-generating pair.

ACKNOWLEDGMENTS. – The authors are grateful to the referees for careful reading and a number of insightful comments that helped improve the exposition of the paper.

FUNDING. – The second author is grateful for the support of the ERC grant 882751, and by a research grant from the Center for New Scientists at the Weizmann Institute of Science. The third author gratefully acknowledges the support of the NSF (grant DMS-2200850), the Simons Foundation, and the Joshua Barlaz Chair in Mathematics.

References

[1] M. Asada, The faithfulness of the monodromy representations associated with certain families of algebraic curves. *J. Pure Appl. Algebra* **159** (2001), no. 2–3, 123–147. Zbl 1045.14013 MR 1828935

[2] D. E.-C. Ben-Ezra, The congruence subgroup problem for the free metabelian group on two generators. *Groups Geom. Dyn.* **10** (2016), no. 2, 583–599. Zbl 1353.20013 MR 3513109

[3] D. E.-C. Ben-Ezra – A. Lubotzky, The congruence subgroup problem for low rank free and free metabelian groups. *J. Algebra* **500** (2018), 171–192. Zbl 1386.20027 MR 3765452

[4] M. Boggi, Congruence topologies on the mapping class group. *J. Algebra* **546** (2020), 518–552. Zbl 1436.32054 MR 4035001

[5] J. N. Bray – D. F. Holt – C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups. With a foreword by Martin Liebeck*. London Math. Soc. Lecture Note Ser. 407, Cambridge University Press, Cambridge, 2013. Zbl 1303.20053 MR 3098485

[6] R. Burkhardt, Über die Zerlegungszahlen der Suzukigruppen $\mathrm{Sz}(q)$. *J. Algebra* **59** (1979), no. 2, 421–433. Zbl 0413.20008 MR 0543261

[7] K.-U. Bux – M. V. Ershov – A. S. Rapinchuk, The congruence subgroup property for Aut F_2: a group-theoretic proof of Asada's theorem. *Groups Geom. Dyn.* **5** (2011), no. 2, 327–353. Zbl 1251.20035 MR 2782176

[8] J. Chen – W. Fan – C. H. Li – Y. Z. Zhu, Coverings of groups, regular dessins, and surfaces. 2024, arXiv:2409.01979v1.

[9] W. Y. Chen, Moduli interpretations for noncongruence modular curves. *Math. Ann.* **371** (2018), no. 1–2, 41–126. Zbl 1454.11110 MR 3788845

[10] W. Y. Chen – P. Deligne, Arithmetic monodromy actions on pro-metabelian fundamental groups of once-punctured elliptic curves. 2017, arXiv:1710.05532v1.

[11] W. Y. Chen – A. Lubotzky – P. H. Tiep, Finite simple characteristic quotients of the free group of rank 2. *Comment. Math. Helv.* (2025), DOI 10.4171/CMH/600.

[12] M. Conder, Hurwitz groups: a brief survey. *Bull. Amer. Math. Soc. (N.S.)* **23** (1990), no. 2, 359–370. Zbl 0716.20015 MR 1041434

[13] M. D. E. Conder, Generators for alternating and symmetric groups. *J. London Math. Soc. (2)* **22** (1980), no. 1, 75–86. Zbl 0427.20023 MR 0579811

[14] J. H. Conway – R. T. Curtis – S. P. Norton – R. A. Parker – R. A. Wilson, ATLAS *of finite groups. Maximal subgroups and ordinary characters for simple groups*. Oxford University Press, Oxford, 1985. Zbl 0568.20001 MR 0827219

[15] D. A. Craven, The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups. *Invent. Math.* **234** (2023), no. 2, 637–719. Zbl 1523.20051 MR 4651009

[16] D. A. Craven, On the maximal subgroups of $E_7(q)$ and related almost simple groups. [v1] 2022, [v2] 2025, arXiv:2201.07081v2.

[17] D. I. Deriziotis – G. O. Michler, Character table and blocks of finite simple triality groups ${}^3D_4(q)$. *Trans. Amer. Math. Soc.* **303** (1987), no. 1, 39–70. Zbl 0628.20014 MR 0896007

[18] L. Dornhoff, *Group representation theory. Part B: Modular representation theory*. Pure Appl. Math. 7, Marcel Dekker, New York, 1972. Zbl 0236.20004 MR 0347960

[19] H. Enomoto, The characters of the finite symplectic group $\mathrm{Sp}(4, q)$, $q = 2^f$. *Osaka Math. J.* **9** (1972), 75–94. Zbl 0254.20005 MR 0302750

[20] W. Feit, On large Zsigmondy primes. *Proc. Amer. Math. Soc.* **102** (1988), no. 1, 29–36. Zbl 0639.10007 MR 0915710

[21] GAP – Groups, Algorithms, and Programming, Version 4.13.0, https://www.gap-system.org/ visited on 2 February 2026.

[22] M. Geck, Irreducible Brauer characters of the 3-dimensional special unitary groups in nondefining characteristic. *Comm. Algebra* **18** (1990), no. 2, 563–584. Zbl 0696.20011 MR 1047328

[23] D. Gorenstein – R. Lyons – R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups*. Math. Surveys Monogr. 40, American Mathematical Society, Providence, RI, 1998. Zbl 0890.20012 MR 1490581

[24] S. Guest – J. Morris – C. E. Praeger – P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.* **367** (2015), no. 11, 7665–7694. Zbl 1330.20002 MR 3391897

[25] R. Guralnick – T. Penttila – C. E. Praeger – J. Saxl, Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc. (3)* **78** (1999), no. 1, 167–214. Zbl 1041.20035 MR 1658168

[26] R. M. Guralnick – P. H. Tiep, Effective results on the Waring problem for finite simple groups. *Amer. J. Math.* **137** (2015), no. 5, 1401–1430. Zbl 1338.20009 MR 3405871

[27] M. Herzog – G. Kaplan – A. Lev, Representation of permutations as products of two cycles. *Discrete Math.* **285** (2004), no. 1–3, 323–327. Zbl 1044.05004 MR 2062857

[28] Y. Hoshi – Y. Iijima, A pro-l version of the congruence subgroup problem for mapping class groups of genus one. *J. Algebra* **520** (2019), 1–31. Zbl 1454.14081 MR 3880862

[29] G. A. Jones, Primitive permutation groups containing a cycle. *Bull. Aust. Math. Soc.* **89** (2014), no. 1, 159–165. Zbl 1297.20003 MR 3163014

[30] W. M. Kantor – A. Lubotzky, The probability of generating a finite classical group. *Geom. Dedicata* **36** (1990), no. 1, 67–87. Zbl 0718.20011 MR 1065213

[31] M. Larsen – A. Shalev – P. H. Tiep, The Waring problem for finite simple groups. *Ann. of Math. (2)* **174** (2011), no. 3, 1885–1950. Zbl 1283.20008 MR 2846493

[32] M. W. Liebeck – A. Shalev, The probability of generating a finite simple group. *Geom. Dedicata* **56** (1995), no. 1, 103–113. Zbl 0836.20068 MR 1338320

[33] F. Lübeck – G. Malle, $(2,3)$-generation of exceptional groups. *J. London Math. Soc. (2)* **59** (1999), no. 1, 109–122. Zbl 0935.20021 MR 1688493

[34] G. Malle, Hurwitz groups and $G_2(q)$. *Canad. Math. Bull.* **33** (1990), no. 3, 349–357. Zbl 0734.20013 MR 1077110

[35] G. Malle, The maximal subgroups of ${}^2F_4(q^2)$. *J. Algebra* **139** (1991), no. 1, 52–69. Zbl 0725.20014 MR 1106340

[36] G. Malle, Small rank exceptional Hurwitz groups. In *Groups of Lie type and their geometries (Como, 1993)*, pp. 173–183, London Math. Soc. Lecture Note Ser. 207, Cambridge University Press, Cambridge, 1995. Zbl 0861.20017 MR 1320522

[37] G. Malle – J. Saxl – T. Weigel, Generation of classical groups. *Geom. Dedicata* **49** (1994), no. 1, 85–116. Zbl 0832.20029 MR 1261575

[38] A. C. Niemeyer – C. E. Praeger, A recognition algorithm for classical groups over finite fields. *Proc. London Math. Soc. (3)* **77** (1998), no. 1, 117–169. Zbl 0893.20035 MR 1625479

[39] L. Ribes – P. Zalesskii, *Profinite groups*. Ergeb. Math. Grenzgeb. (3) 40, Springer, Berlin, 2000. Zbl 0949.20017 MR 1775104

[40] J.-P. Serre, *Topics in Galois theory*. 2nd edn., CRC Press, New York, 2016.

[41] W. A. Simpson – J. S. Frame, The character tables for SL(3, q), SU(3, q^2), PSL(3, q), PSU(3, q^2). *Canadian J. Math.* **25** (1973), 486–494. Zbl 0264.20010 MR 0335618

[42] N. Spaltenstein, Caractères unipotents de ${}^3D_4(\mathbf{F}_q)$. *Comment. Math. Helv.* **57** (1982), no. 4, 676–691. Zbl 0536.20025 MR 0694610

[43] B. Srinivasan, The characters of the finite symplectic group Sp(4, q). *Trans. Amer. Math. Soc.* **131** (1968), 488–525. Zbl 0213.30401 MR 0220845

[44] S. J. Trefethen, *Non-abelian composition factors of m-rational groups*. Ph.D. thesis, The University of Arizona, 2016.

[45] G. Weitze-Schmithüsen, The deficiency of being a congruence group for Veech groups of origamis. *Int. Math. Res. Not. IMRN* **2015** (2015), no. 6, 1613–1637. Zbl 1318.30065 MR 3340368

[46] K. Zsigmondy, Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284. Zbl 24.0176.02 MR 1546236

Received 11 July 2024,
and in revised form 27 April 2025

William Y. Chen
Department of Mathematics, University of Illinois at Urbana-Champaign
Urbana, IL 61801, USA
oxeimon@gmail.com

Alexander Lubotzky
Faculty of Mathematics and Computer Science, The Weizmann Institute of Science
7610001 Rehovot, Israel
alex.lubotzky@mail.huji.ac.il

Pham Huu Tiep
Department of Mathematics, Rutgers University
Piscataway, NJ 08854, USA
tiep@math.rutgers.edu