CHARACTERISTIC COVERING NUMBERS OF FINITE SIMPLE GROUPS

MICHAEL LARSEN, ANER SHALEV, AND PHAM HUU TIEP

Abstract. In the past few decades there has been intense interest in word maps on groups with emphasis on (non-abelian) finite simple groups. Various asymptotic results (holding for sufficiently large groups) have been obtained.

More recently non-asymptotic results (holding for all finite simple groups) emerged, with emphasis on particular words (commutators and certain power words) which are not an identity of any finite simple group. In this paper we initiate a systematic study of *all* words with the above property.

In particular, we show that, if $w_1, \ldots, w_6$ are words which are not an identity of any (non-abelian) finite simple group, then $w_1(G)w_2(G)\cdots w_6(G) = G$ for *all* (non-abelian) finite simple groups G. Consequently, for every word w, either $w(G)^6 = G$ for all finite simple groups, or $w(G) = 1$ for some finite simple group.

These theorems follow from more general results we obtain on *characteristic collections* of finite groups and their covering numbers, which are of independent interest and have additional applications.

1. Introduction

The theory of word maps on groups, and on finite simple groups in particular, dates back to Borel [Bo], and has developed significantly in the past 3 decades; see for instance [MZ], [SW], [LiSh1], [La], [Sh1], [LS1], [LS2], [LOST], [LST1], [GT], [B1], [B2] as well as the monograph [Se] and the survey paper [Sh2].

Most of these works are of asymptotic nature. For example, it is shown in [LST1] (following [LS1, LS2]) that, for every non-identity word w there exists $N(w) \in \mathbb{N}$ such that, if G is a finite simple group of order at least $N(w)$ then $w(G)^2 = G$. Recall that a *word* is an element of a free group F_d of rank d, and it defines a *word map* $w\colon G^d \to G$ for every group G, induced by substitution. The image of this word map is denoted by $w(G)$.

Here and throughout this paper, by a finite simple group we mean a non-abelian finite simple group.

1991 *Mathematics Subject Classification.* Primary 20D06.

ML was partially supported by NSF grant DMS-2001349. AS was partially supported by ISF grant 686/17 and the Vinik Chair of mathematics which he holds. PT was partially supported by NSF grant DMS-1840702, the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton). The authors were also partially supported by BSF grant 2016072.

The authors are grateful to Frank Lübeck for kindly providing us with the character table of the Steinberg group ${}^3D_4(3)$.

Non-asymptotic results on word maps are often very challenging and require more tools. See, for instance, [LOST], [LOST2], [GM], [GT] and [GLOST]. In [LOST] it is shown that the commutator map is surjective on *all* finite simple groups, proving the Ore Conjecture. Using a somewhat similar strategy, it was subsequently proved in [LOST2] that, if $w = x^p$ for a prime $p \neq 3, 5$, then $w(G)^2 = G$ for *all* finite simple groups G. In [GM] a stronger result is established, yielding the same conclusion for $w = x^k$, where k is any prime power or a power of 6.

The above result was further extended in [GLOST]. Consider the power words $w_1 = x^k$ and $w_2 = x^\ell$, where $k = p^a q^b$ for primes p, q and ℓ is an odd integer. By celebrated theorems of Burnside and of Feit and Thompson, finite groups satisfying the identity w_1 or the identity w_2 are solvable. In particular, w_1, w_2 are not identities of any finite simple group. It was proved in [GLOST] that, $w_1(G)^2 = G$ and $w_2(G)^3 = G$ for *all* finite simple groups G.

Our main theorems, stated below, may be regarded as far-reaching extensions of the above mentioned results. In particular, we derive similar conclusions for *every* word w which is not an identity of any finite simple group, sometimes with somewhat larger exponents. Our strategy is to pose and study a more general problem.

Definition 1.1. A collection of non-empty subsets $S(G) \subseteq G$, one for each finite group G, is *characteristic* if for every homomorphism $\varphi\colon G \to H$ we have $\varphi(S(G)) \subseteq S(H)$.

Some comments are in order.

1. For any characteristic collection S and for any finite group G, $S(G)$ must be a fully invariant – in particular, a characteristic – subset of G (take $\varphi\colon G \to G$); furthermore, $1 \in S(G)$ (take φ to be the trivial endomorphism of G).
2. For any characteristic collection S, any finite group G, and any subgroup H of G, we have $S(H) \subseteq S(G)$; indeed, $S(H) = \iota(S(H)) \subseteq S(G)$ for the natural embedding $\iota : H \hookrightarrow G$.
3. Trivial examples of characteristic collections are $S(G) = \{1\}$ for all G (the minimal collection) and $S(G) = G$ for all G (the maximal collection).
4. Given characteristic collections S, T, define their union $S \cup T$ and intersection $S \cap T$ by $(S \cup T)(G) := S(G) \cup S(T)$ and $(S \cap T)(G) := S(G) \cap T(G)$. Then $S \cup T$ and $S \cap T$ are characteristic collections.
5. Given characteristic collections S, T, define their product ST by $ST(G) := S(G)T(G)$, which is easily seen to be a characteristic collection. This binary operation is associative with an identity element (the minimal collection). Thus the set of all characteristic collections is a monoid, which is partially ordered by inclusion (where $S \subseteq T$ if $S(G) \subseteq T(G)$ for all G).
6. Let $w \in F_d$ be a word, and consider the word maps it defines on finite groups G. Then the collection $S(G) := w(G)$ is obviously characteristic.
7. Let P_d denote the free profinite group on $x_1, \dots, x_d$ (namely the profinite completion of F_d). For any finite group G and $g = (g_1, \dots, g_d) \in G^d$ there is a unique homomorphism $\psi_g : P_d \to G$ satisfying $\psi_g(x_i) = g_i$ $(i = 1, \dots, d)$. Any element $W \in P_d$ (which may be regarded as a profinite word) gives rise to a function (a profinite word map) $W : G^d \to G$ satisfying $W(g) := \psi_g(W)$. Setting $S(G) := W(G)$, the image of W, we obtain a characteristic collection S.

It is easy to see that different elements $W_1, W_2 \in P_d$ give rise to distinct characteristic collections S_1, S_2. Hence the monoid of characteristic collections has cardinality $2^{\aleph_0}$.

8. Any word w in one variable, i.e. $w = x^k$ for some integer k, defines a word map $w\colon G \to G$ on each finite group G, and the collection of kernels $S(G) := w^{-1}(1) = \{g \in G : g^k = 1\}$ is characteristic.

Definition 1.2. A characteristic collection S is *ample* if $|S(G)| \geq 2$ for all finite simple groups G.

For example, let w be a word, and let S be its associated characteristic collection (i.e. $S(G) = w(G)$). Then the ampleness of w is equivalent to each of the following conditions.

(a) w is not an identity of any finite simple group.
(b) w is not an identity of any minimal finite simple group (these are certain well known groups of type PSL_2 or Suzuki type).
(c) For all finite groups G, $w(G) = 1$ implies that G is solvable.

In general, if S, T are ample characteristic collections, then so is their product ST. Therefore the set of all ample characteristic collections forms a submonoid of the monoid of all characteristic collections.

Definition 1.3. We define the *characteristic covering number* $\mathsf{ccn}(G)$ of a finite group G to be the smallest integer n such that if $S_1, \dots, S_n$ are ample characteristic collections, then $S_1(G) \cdots S_n(G) = G$. If no such n exists, we say $\mathsf{ccn}(G) = \infty$.

The main result of this paper is the following:

Theorem A. If G is a finite simple group, then $\mathsf{ccn}(G) \leq 6$.

Applying this for characteristic collections associated with words, we immediately obtain the following.

Theorem B. If $w_1, \dots, w_6$ are words in disjoint letters, and none of the w_i is an identity on any finite simple group, then the juxtaposition $w_1 \cdots w_6$ is surjective on every finite simple group.

Corollary C. If w is a word which is not an identity on any finite simple group, then $w(G)^6 = G$ for every finite simple group G.

Clearly, Theorem B and Corollary C also follow when w, w_i are replaced by profinite words W, W_i.

Note that the condition that none of the w_i (or w) is an identity on any finite simple group in Theorem B and Corollary C is necessary. As shown in [KaN], [GT], for any integer N, there exist a word w and a finite simple group G such that $w(G) \neq 1$ and $w(G)^N \neq G$.

One can apply Theorem A to other characteristic collections to get upper bounds on their widths as well, and we indicate one of such applications. A theorem of John Thompson states that any finite simple $3'$-group is a Suzuki group and hence contains elements of order 5. Therefore Theorem A applied to $S(G) := \{x \in G \mid |x| = 1, 3, \text{ or } 5\}$ implies

Corollary D. If G is a finite simple group, then any element in G is a product $x_1 \cdots x_6$ with $x_i \in G$ and $|x_i| = 1$, 3, or 5.

For comparison, it is shown in [GT, 3.8], that for odd primes p, the width of finite simple groups of order divisible by p with respect to its elements of pth power order is at most 70. See also Malcolm [Ma2] for the state of the art on the p-width of finite simple groups.

As for lower bounds, it follows from [GLOST, 8.9] that $\mathsf{ccn}(G) \geq 3$ for some finite simple groups G; indeed, there are odd integers ℓ and finite simple groups G such that $w(G)^2 \neq G$ for $w = x^\ell$. This can be improved as follows. In the special case that $w = x^2$, the collection $S(G) = w^{-1}(1)$ is ample by Feit-Thompson. The minimal n such that $S(G)^n = G$ is the *involution width* of G, denoted $\mathsf{iw}(G)$. This invariant has been investigated by several mathematicians (see [Ma] and the references therein). In particular, Knüppel and Nielsen showed [KnN, 16] that $\mathsf{iw}(\mathrm{SL}_n(q)) \geq 4$ if $n \geq 5$ and $q \geq 7$. When, in addition, $\gcd(n, q-1) = 1$, we have $\mathrm{SL}_n(q) = \mathrm{PSL}_n(q)$, and this gives a lower bound of 4 for the characteristic covering number of infinitely many finite simple groups.

It would be interesting to know whether our upper bound of 6 for ccn can be improved. Malcolm showed [Ma] that $\mathsf{iw}(G) \leq 4$ for all finite simple groups, and it seems quite possible that this is the optimal bound for ccn as well. For most finite simple groups we can prove an upper bound of 4 or less. Indeed we have

Theorem E. Let G be a finite simple group. Then $\mathsf{ccn}(G) \leq 4$ unless G is a group of Lie type $X_r(q)$ where $q \leq f(r)$ for a suitable function f.

Consequently, excluding these possible exceptions, we have $w_1(G) \cdots w_4(G) = G$ for all words $w_1, \ldots, w_4$ which are not an identity of any finite simple group.

Treating the remaining groups seems very challenging.

As $\mathsf{ccn}(G)$ reflects information on all simple subgroups of G, it cannot easily be determined from the character table of G, as $\mathsf{iw}(G)$ and similar invariants such as the covering number and extended covering number of G can be. We were able to determine it in a few cases, of which the following results are representative.

Proposition 1.4. *If $p \geq 5$ is a prime, then*

$$\mathsf{ccn}(\mathrm{PSL}_2(p)) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 4, \\ 3 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proposition 1.5. *For all sufficiently large n, $\mathsf{ccn}(\mathsf{A}_n) = 3$.*

Proposition 1.6. *If $n \geq 5$ and $q - 1$ is sufficiently large and relatively prime to n, then $\mathsf{ccn}(\mathrm{PSL}_n(q)) = 4$.*

It would be interesting to find an example where $\mathsf{ccn}(G) > \mathsf{iw}(G)$; at present, we do not know of any.

2. Preliminaries

In this section we obtain various preliminary results, which will be used in proving our main results in subsequent sections.

Lemma 2.1. *Let G be a finite group. Then $\mathsf{ccn}(G) < \infty$ if and only if $S(G)$ generates G for every ample characteristic collection S.*

Proof. Suppose $\mathsf{ccn}(G) < \infty$, and let S be an ample characteristic collection. Then $S(G)^n = G$ for $n = \mathsf{ccn}(G)$, hence $S(G)$ generates G.

To prove the other direction, suppose $S(G)$ generates G for every ample characteristic collection S. Since G has only finitely many, say $s = s(G) \in \mathbb{N}$, distinct characteristic subsets and $S(G) \ni 1$, we may assume that there exists $n_0 = n_0(G) \in \mathbb{N}$ such that $S(G)^{n_0} = G$ for all such S. We have to show that there exists some $n = n(G) \in \mathbb{N}$ such that, given ample characteristic collections S_i, $1 \leq i \leq n$, we have $S_1(G) \cdots S_n(G) = G$. Choosing $n = (n_0 - 1)s + 1$, we see by the pigeon-hole principle that at least n_0 of $S_i(G)$ are all equal to some $C = S_{i_0}(G)$. Since $1 \in S_j(G)$ for all j and $C^{n_0} = G$, we conclude that $S_1(G) \cdots S_n(G) \supseteq C^{n_0} = G$. $\square$

Set

$$\mathcal{G} = \{G : G \text{ is a finite group satisfying } \mathsf{ccn}(G) < \infty\}.$$

Then $\mathcal{G}$ is closed under taking quotients; indeed, it is easy to see that, if $N \lhd G$ then $\mathsf{ccn}(G/N) \leq \mathsf{ccn}(G)$. However, the inequality $\mathsf{ccn}(N) \leq \mathsf{ccn}(G)$ for $N \lhd G$ does not hold in general; moreover, the set $\mathcal{G}$ is not closed under passing to normal subgroups. Indeed we have the following observations:

Proposition 2.2. (i) *Let G be a finite group. If $\mathsf{ccn}(G) < \infty$, then G is perfect.*

(ii) *Let the finite group $G = E \rtimes H$ be a split extension, with $E \neq 1$ minimal abelian normal subgroup, H non-abelian simple, and $\mathbf{C}_G(E) = E$. Then $\mathsf{ccn}(G) < \infty$ while $\mathsf{ccn}(E) = \infty$.*

(iii) *Let L be finite quasisimple with $\mathbf{Z}(L) \neq 1$ and $L/\mathbf{Z}(L)$ a minimal simple group. Then $\mathsf{ccn}(L) = \infty$.*

Proof. (i) If G is not perfect, then by pulling back a subgroup of prime index from its abelianization, we obtain a normal subgroup $G_p \lhd G$ of index p for some prime p. Then $S(H) = \{h^p \mid h \in H\}$ defines a characteristic collection of subgroups, and it is ample since no finite simple group has exponent p. However, $S(G)^n$ is contained in G_p for all $n \in \mathbb{N}$, so $\mathsf{ccn}(G) = \infty$.

(ii) The second statement is immediate, since E is a non-trivial abelian group. To prove the first statement we apply Lemma 2.1. It suffices to show that $S(G)$ generates G for every ample characteristic collection S. By considering the natural embedding $\iota : H \hookrightarrow G$, we have that $S(H) = \iota(S(H)) \subseteq S(G)$. Since H is simple and $S(H) \neq 1$ is normal, $\langle S(H) \rangle = H$. It follows that $\langle S(G) \rangle$ is a normal subgroup of G that contains H. If $\langle S(G) \rangle = H$, then $H \lhd G$ and so $[E, H] = 1$, contradicting the assumption $\mathbf{C}_G(E) = E$. Hence $\langle S(G) \rangle > H$, and so $\langle S(G) \rangle = G$ since H is simple.

(iii) For any finite group G, let $S(G)$ be the union of all *non-abelian* simple subgroups of G. Then S is an ample characteristic collection (indeed, for any homomorphism $\varphi : G \to H$ and any simple subgroup X of G, $\varphi(X)$ is either trivial or a simple subgroup of H, and so $\varphi(X) \subseteq S(H)$). Now, if $Y \leq L$ is a non-abelian simple subgroup, then $Y \cong Y\mathbf{Z}(L)/\mathbf{Z}(L) \leq L/\mathbf{Z}(L)$ and so, by minimality of $L/\mathbf{Z}(L)$, $L = Y\mathbf{Z}(L) \cong Y \times \mathbf{Z}(L)$, contradicting the assumption that L is perfect. Hence $S(L) = \{1\}$ and $\mathsf{ccn}(L) = \infty$. $\square$

We recall that the extended covering number $\mathsf{ecn}(G)$ of a finite simple group G is the smallest integer n such that $C_1 \cdots C_n = G$ if $C_1, \dots, C_n$ is any sequence of non-trivial conjugacy classes of G.

Lemma 2.3. *If G is a finite simple group, then $\mathsf{ccn}(G) \leq \mathsf{ecn}(G) - 1$.*

Proof. If $\mathsf{ccn}(G) \geq n$, then there exist ample characteristic collections S_i, $1 \leq i \leq n-1$, such that $S_1(G) \cdots S_{n-1}(G) \neq G$. As $S_1, \dots, S_{n-1}$ are ample,

$$S_1(G) \cdots S_{n-1}(G) \supseteq C_1 \cdots C_{n-1}$$

for some sequence $C_1, \dots, C_{n-1}$ of non-trivial conjugacy classes of G. Moreover

$$1 \in S_1(G) \cdots S_{n-1}(G).$$

Therefore, there exists a non-trivial conjugacy class D such that D is disjoint from $C_1 \cdots C_{n-1}$. This implies $1 \notin C_1 \cdots C_{n-1} D^{-1}$, so $\mathsf{ecn}(G) \geq n+1$. □

Lemma 2.4. *Let $q \geq 4$ be a prime power and C_1, C_2, C_3 not necessarily distinct non-central conjugacy classes in $\mathrm{SL}_2(q)$.*

(i) *The product $C_1C_2C_3$ contains all non-central elements of $\mathrm{SL}_2(q)$.*
(ii) *If $q \neq 5$, then C_1C_2 contains elements of order $q-1$ and order $q+1$.*
(iii) *If $q = 5$, then C_1C_2 contains an element of order 4 and one of order 3 or order 6.*

Proof. Let G be a finite group. Recall that, by the extended Frobenius formula, the number of solutions to the equation $g = x_1x_2 \cdots x_k$ for a fixed $g \in G$ and $x_i \in C_i = c_i^G$ $(1 \leq i \leq k)$ is given by

$$\frac{\prod_{i=1}^{k} |C_i|}{|G|} \cdot \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(c_1) \cdots \chi(c_k)\chi(g^{-1})}{\chi(1)^{k-1}}. \tag{2.1}$$

This implies that $g \in C_1 \cdots C_k$ provided the above expression is non-zero.

The result now follows from the well known character table of $G := \mathrm{SL}_2(q)$. □

Lemma 2.5. *Let $q \geq 4$ be a prime power, d the g.c.d. of $q-1$ and 2, and C_1, C_2, C_3 not necessarily distinct non-central conjugacy classes in $G := \mathrm{PSL}_2(q)$. Let $\mathcal{C}_q$ denote the set of elements of order q.*

(i) *The product $C_1C_2C_3$ equals G.*
(ii) *The product C_1C_2 contains elements of order $(q-1)/d$ and $(q+1)/d$*
(iii) *If $q \equiv 1 \pmod 4$ is prime, then C_1C_2 contains an element of $\mathcal{C}_q$.*
(iv) *If $q \equiv 1 \pmod 4$ is prime, then $C_1\mathcal{C}_q$ contains $G \smallsetminus \{1\}$.*
(v) *If $q \equiv 3 \pmod 4$ is prime and C_1, C_2 are classes of involutions, then C_1C_2 is disjoint from $\mathcal{C}_p$.*

Proof. For q even, $\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)$, but in either case (i) and (ii) follow immediately from the corresponding statements in Lemma 2.4. For q an odd prime, $\mathcal{C}_q$ is the union of the two conjugacy classes. Conclusions (iii)–(v) follow by computing (2.1) in the relevant cases using the character table of $G := \mathrm{PSL}_2(q)$. □

From this lemma, we easily deduce Proposition 1.4.

Proof of Proposition 1.4. The two conjugacy classes in $\mathcal{C}_q$ are conjugate to one another under $\mathrm{PGL}_2(q)$, so if $S_1(G)S_2(G)$ meets $\mathcal{C}_q$ at all, it contains it. If $S_1(G)$ and $S_2(G)$ each contain a non-trivial conjugacy class of G, then by Gow's theorem [G], $S_1(G)S_2(G)$ contains all semisimple elements. If $q \equiv 1 \pmod 4$, then by Lemma 2.5 (iii), $S_1(G)S_2(G) = G$, so $\mathsf{ccn}(G) \leq 2$. On the other hand, $\mathsf{ccn}(G) \geq \mathsf{iw}(G) \geq 2$, so $\mathsf{ccn}(G) = 2$. If $q \equiv 3 \pmod 4$, then Lemma 2.5 (i) implies $\mathsf{ccn}(G) \leq 3$, and Lemma 2.5 (v) implies $\mathsf{iw}(G) \geq 3$, so $\mathsf{ccn}(G) = 3$. □

Lemma 2.6. *If $q \geq 4$ and C_1 and C_2 are non-trivial $\mathrm{PGL}_2(q)$ orbits in $\mathrm{PSL}_2(q)$, then C_1C_2 covers all split regular semisimple conjugacy classes in $\mathrm{PSL}_2(q)$.*

Proof. Again, this follows from easy character table computations. □

Lemma 2.7. (i) *If C_1, C_2, C_3 are non-trivial conjugacy classes in $\mathrm{PSL}_3(q)$, then $C_1C_2C_3$ contains all non-trivial elements of $\mathrm{PSL}_3(q)$.*

(ii) *If $2 < q \equiv -1 (\bmod\ 3)$ and C_1, C_2, C_3 are non-trivial conjugacy classes in $\mathrm{PSU}_3(q)$, then $C_1C_2C_3$ contains all non-trivial elements of $\mathrm{PSU}_3(q)$.*

(iii) *If $3 \nmid (q+1)$ and C_1, C_2, C_3 are non-trivial conjugacy classes in $\mathrm{SU}_3(q)$, then $C_1C_2C_3$ contains all elements of order q^2-q+1 in $\mathrm{SU}_3(q)$. Moreover, $\mathsf{ecn}(\mathrm{SU}_3(q)) = 5$.*

Proof. Parts (i) and (ii) follow immediately from the fact that $\mathsf{ecn}(\mathrm{PSL}_3(q)) = 4$, and that $\mathsf{ecn}(\mathrm{PSU}_3(q)) = 4$ for those q, see [O, Corollary 1.9].

(iii) In this case, $\mathrm{GU}_3(q) = \mathrm{SU}_3(q) \times \mathbf{Z}(\mathrm{GU}_3(q))$, and so each $C_i = g_i^{\mathrm{SU}_3(q)}$ is a non-central $\mathrm{GU}_3(q)$-conjugacy class; furthermore, any element g of order $q^2 - q + 1$ belongs to a class $C_8^{(k)}$ in [O, Table 1]. By assumption, $\det(g_i) = 1$ for $1 \leq i \leq 3$, and thus condition (2) of [O, Theorem 1.3] holds. Choosing $m = 4$, we see that condition (3) of [O, Theorem 1.3] also holds; see the first remark on [O, p. 221]. Now [O, Theorem 1.3] shows that $1 \in C_1C_2C_3 \cdot (g^{-1})^{\mathrm{SU}_3(q)}$, and so $g \in C_1C_2C_3$. The last statement is contained in [O, Corollary 1.9]. □

Lemma 2.8. *Let G be a finite simple group of Lie type, and let $s, t \in G$ be two semisimple elements such that*

(i) *For any pair of ample characteristic collections S_1, S_2, the conjugacy class of s belongs to $S_1(G)S_2(G)$,*

(ii) *The product of the conjugacy class of s and the conjugacy class of t contains $G \setminus \{1\}$,*

(iii) *The element s is regular.*

Then $\mathsf{ccn}(G) \leq 6$.

Proof. By the theorem of Gow [G], every semisimple element in G, in particular t, can be written as a product of two conjugates of s. Now, if $S_3, \ldots, S_6$ are ample characteristic collections, then $s^G \subseteq S_3S_4$ and $s^G \subseteq S_5S_6$, whence t^G lies in $S_3(G)S_4(G)S_5(G)S_6(G)$. Therefore

$$G \setminus \{1\} \subset s^G \cdot t^G \subseteq S_1(G) \cdots S_6(G),$$

and it follows that $\mathsf{ccn}(G) \leq 6$. □

Lemma 2.9. *Let G be a finite group, and let $\mathfrak{d}(G)$ the lowest degree of a non-trivial character of G. Let $q \geq 4$ and $\varphi\colon \mathrm{SL}_2(q) \to G$ be a non-trivial homomorphism. Suppose that*

$$|\mathbf{C}_G(\varphi(s))|^{3/2} \leq \mathfrak{d}(G) \tag{2.2}$$

for any $s \in \mathrm{SL}_2(q)$ of order $q-1$, or for any $s \in \mathrm{SL}_2(q)$ of order $q+1$ if $q \neq 5$, or for any $s \in \mathrm{SL}_2(q)$ of order 3 or 6 if $q = 5$. Then $\mathsf{ccn}(G) \leq 6$.

Proof. By Lemma 2.5, if S_1, S_2 are ample characteristic collections, then $g := \varphi(s) \in S_1(G)S_2(G)$, where $s \in \mathrm{SL}_2(q)$ can be chosen to have order $q-1$, or $q+1$ if $q \neq 5$, or either 3 or 6 when $q = 5$. Let $C := g^G$. By the Frobenius formula, $C^3 = G$ if

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(g)|^3}{\chi(1)} < 1.$$

For any χ in the summation, $|\chi(g)| \leq |\mathbf{C}_G(g)|^{1/2}$ by the centralizer bound for character values, and $\chi(1) \geq \mathfrak{d}(G)$. Hence, by the second orthogonality relation,

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(g)|^3}{\chi(1)} < \frac{|\mathbf{C}_G(g)|^{1/2}}{\mathfrak{d}(G)} \cdot \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g)|^2 = \frac{|\mathbf{C}_G(g)|^{3/2}}{\mathfrak{d}(G)},$$

and we can deduce the needed inequality from (2.2). □

We conclude this section with two results which allow us to prove that $\mathsf{ccn}(G) \leq 4$ when G is of Lie type and is sufficiently large compared to its rank.

Proposition 2.10. *Let $\underline{G}$ denote a connected, simply connected simple algebraic group of rank r over $\mathbb{F}_q$ and G the finite simple group obtained by taking the quotient of $\underline{G}(\mathbb{F}_q)$ by its center. Let $r = r_1 + \cdots + r_k$ be a partition. If there exists a homomorphism $\phi\colon \mathrm{SL}_2(q^{r_1}) \times \cdots \times \mathrm{SL}_2(q^{r_k}) \to G$ with central kernel and if q is sufficiently large in terms of r, then $\mathsf{ccn}(G) \leq 4$.*

Proof. The number of $\mathbb{F}_q$-points on a torus of rank s is at most $(q+1)^s$. The regular elements in a maximal torus $\underline{T}$ of $\underline{G}$ lie in a union of proper subtori of $\underline{T}$ indexed by positive roots, so the number of elements in $\underline{T}(\mathbb{F}_q)$ which are not regular semisimple is less than $2r^2(q+1)^{r-1}$.

We write $H := \prod_{i=1}^k \mathrm{SL}_2(q^{r_i})/Z$, where $Z := \ker\phi$ is some subgroup of the product of the centers of the $\mathrm{SL}_2(\mathbb{F}_{q^{r_i}})$ and is therefore of order at most 2^r. The inclusion of H in G gives a homomorphism

$$\prod_{i=1}^k \mathbb{F}_{q^{r_i}}^\times \to G.$$

The image under this homomorphism of elements which are non-trivial in each coordinate is at least

$$2^{-r}(1-2q^{-1})^r q^r.$$

However, the image lies in a maximal torus T of G, i.e., the image of the $\mathbb{F}_q$-points of a maximal torus $\underline{T}$ of $\underline{G}$ in G. Lemma 2.6 therefore gives a lower bound of the form $c_r q^r$ for the cardinality of the set of regular semisimple elements of T which lie in $S_1(H)S_2(H)$

where S_1 and S_2 are ample characteristic collections. The conjugacy class of each such element meets T in at most $|W|$ elements, where W denotes the Weyl group of $\underline{G}$ with respect to $\underline{T}$, whose order is bounded in terms of r. Each conjugacy class of a regular semisimple element in $\underline{G}(\mathbb{F}_q)$ has at least $(q+1)^{-r}|\underline{G}(\mathbb{F}_q)|$ elements, so overall, we get a positive lower bound, depending only on r, for the proportion of elements of G which lie in $S_1(G)S_2(G)$. Since $S_1(G)S_2(G)$ is a normal subset of G, [LST2, Theorem A] implies that $S_1(G)S_2(G)S_3(G)S_4(G)$ contains all non-trivial elements of G. □

Note that the same argument works also for Suzuki and Ree groups.

Lemma 2.11. *Let $\underline{G}$ be a connected, simply connected simple algebraic group of rank r over $\mathbb{F}_q$ and G the quotient of $\underline{G}(\mathbb{F}_q)$ by its center. Let $\phi\colon \mathrm{SL}_2^k \to \underline{G}$ be a homomorphism of algebraic groups over $\mathbb{F}_q$ whose kernel lies in the center of SL_2^k. Let $\mathbb{G}_m^k$ denote a split maximal torus of SL_2^k, and suppose $\phi(\mathbb{G}_m^k)$ is a maximal split torus of $\underline{G}$ which contains regular $\mathbb{F}_q$-points. Then if q is sufficiently large in terms of r, we have $\mathsf{ccn}(G) \le 4$.*

Note that if $\underline{G}$ is split, then $\phi(\mathbb{G}_m^k)$ is a maximal torus, so it contains regular elements over $\mathbb{F}_q$ if q is sufficiently large. If $\underline{G}$ is not split, a maximal split torus is not a maximal torus, so $k < r$.

Proof. For q sufficiently large, there exists $(a_1,\ldots,a_k) \in (\mathbb{G}_m(\mathbb{F}_q) \smallsetminus \{1\})^k$ such that $\phi(a_1,\ldots,a_k)$ is regular. By Lemma 2.6, $(a_1,\ldots,a_k) \in S_1(\mathrm{SL}_2(q)^k)S_2(\mathrm{SL}_2(q)^k)$ if S_1 and S_2 are ample characteristic collections. By a theorem of Ellers and Gordeev [EG, Theorem 1] the product of G-conjugacy classes of any two regular semisimple elements lying in maximal split tori of G covers $G \smallsetminus \{1\}$. □

3. Classical groups

For every positive integer n, we denote by $\Phi_n(x)$ the nth cyclotomic polynomial. We recall [Zs] that for $n > 2$ and $(n,q) \neq (6,2)$, $\Phi_n(q)$ is always divisible by a Zsigmondy prime ℓ, meaning that ℓ does not divide q, which implies and the order of $q \pmod{\ell}$ is exactly n. In particular, $\ell \equiv 1 \pmod{n}$.

Theorem 3.1. *If G is a finite simple classical group, then $\mathsf{ccn}(G) \le 6$.*

Proof. We consider all the six types A_r, ${}^2A_r$, B_r, C_r, D_r, and ${}^2D_r$. Let $S_1,\ldots,S_6$ be ample characteristic collections and set $d := \gcd(2, q-1)$.

Case $G = \mathrm{PSL}_n(q)$ with $n \ge 2$ and $(n,q) \neq (2,2), (2,3)$. Note that $\mathsf{ecn}(\mathrm{PSL}_2(q)) = 4$ for $q \ge 4$ [AH, p. 2], and $\mathsf{ecn}(\mathrm{PSL}_3(q)) = 4$ [O, Corollary 1.9], so we may assume $n \ge 4$. For $(n,q) = (6,2), (7,2)$, we have $\mathrm{SL}_2(8) < G$, and any element of order 7 lies in $S_1(G)S_2(G)$ for S_i ample characteristic collections. Using the character tables for these two groups in the GAP library, we check that the square of this conjugacy class covers the non-trivial elements of the group, so $\mathsf{ccn}(G) \le 4$.

We may therefore assume that $(n,q) \neq (6,2), (7,2)$. Write $q = p^f$ for a prime p, and $m := \lfloor n/2 \rfloor$ so that $m \ge 2$ and $n \in \{2m, 2m+1\}$. By [Zs] and the assumption on (n,q), we can find a Zsigmondy prime ℓ for $(2mf, p)$. By Lemma 2.5, $S_1(\mathrm{PSL}_2(q^m))S_2(\mathrm{PSL}_2(q^m))$ contains an element of order $(q^m+1)/d$. Since $\mathrm{SL}_2(q^m) \le$

$\mathrm{SL}_{2m}(q) \leq \mathrm{SL}_n(q)$, it follows that $S_1(G)S_2(G)$ contains an element s of order divisible by $(q^m+1)/d$ which is divisible by ℓ, and so s is regular semisimple. As discussed in [GT, §2.2.1], one can find a semisimple element $t \in G$ such that $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $\mathsf{ccn}(G) \leq 6$ by Lemma 2.8.

Case $G = \mathrm{PSU}_n(q)$ with $n \geq 3$ and $(n,q) \neq (3,2)$. Note that $\mathsf{ecn}(\mathrm{PSU}_3(q)) \leq 5$ [O, Corollary 1.9], so we may assume $n \geq 4$. If $G = \mathrm{PSU}_6(2)$, then $\mathrm{SL}_2(8) < G$, and we easily check that the square of the class in G of any element of order 7 covers the nontrivial elements of G, so $\mathsf{ccn}(G) \leq 4$.

We therefore assume that $(n,q) \neq (6,2)$. Again write $m := \lfloor n/2 \rfloor$, so that $m \geq 2$ and $n \in \{2m, 2m+1\}$. By [Zs] and the assumption on (n,q), we can find a Zsigmondy prime ℓ for $(2mf, p)$ when $2|m$, and for (mf, p) when $2 \nmid m$; note that ℓ divides $q^{2m}-1$, but not $\prod_{i=1}^{2m-1}((-q)^i - 1)$. By Lemma 2.5, $S_1(\mathrm{PSL}_2(q^m))S_2(\mathrm{PSL}_2(q^m))$ contains an element of order $(q^m + (-1)^m)/d$. Note that

$$\mathrm{SL}_2(q^m) \leq \mathrm{SL}_m(q^2) < \mathrm{SU}_{2m}(q) \leq \mathrm{SU}_n(q)$$

when $2|m$, and

$$\mathrm{SL}_2(q^m) \cong \mathrm{SU}_2(q^m) \leq \mathrm{SU}_{2m}(q) \leq \mathrm{SU}_n(q)$$

when $2 \nmid m$. It follows that $S_1(G)S_2(G)$ contains an element s of order divisible by $(q^m + (-1)^m)/d$ which is divisible by ℓ, and so s is regular semisimple (as one can see by checking the eigenvalues of s). As discussed in [GT, §2.2.2], one can find a semisimple element $t \in G$ such that $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $\mathsf{ccn}(G) \leq 6$ by Lemma 2.8.

Case $G = \mathrm{PSp}_{2n}(q)$ with $n \geq 2$ and $(n,q) \neq (2,2)$. (Note that $\mathrm{Sp}_4(2)' \cong \mathrm{PSL}_2(9)$). By Lemma 2.5, $S_1(\mathrm{PSL}_2(q^n))S_2(\mathrm{PSL}_2(q^n))$ contains an element $\bar{s}$ of order $(q^n-1)/d$ and $S_3(\mathrm{PSL}_2(q^n))S_4(\mathrm{PSL}_2(q^n))$ an element $\bar{t}$ of order $(q^n+1)/d$. Since

$$\mathrm{SL}_2(q^n) \cong \mathrm{Sp}_2(q^n) < \mathrm{Sp}_{2n}(q),$$

$S_1(G)S_2(G)$ contains regular semisimple elements s of order divisible by $(q^n-1)/d$, and $S_3(G)S_4(G)$ contains a regular semisimple element of order divisible by $(q^n+1)/2$. As discussed in [GT, §2.2.3], $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $S_1(G)S_2(G)S_3(G)S_4(G) \supseteq G \smallsetminus \{1\}$, and $\mathsf{ccn}(G) \leq 4$.

Case $G = P\Omega_n^\epsilon(q)$ with $n \geq 7$ and $\epsilon = \pm$. First assume that $n = 7$ and $2 \nmid q$. Note that

$$\Omega_7(q) > \mathrm{SO}_6^+(q) > \mathrm{SL}_3(q),\ \Omega_7(q) > \mathrm{SO}_6^-(q) > \mathrm{SU}_3(q).$$

Hence, by Lemma 2.7, $S_1(G)S_2(G)S_3(G)$ contains a regular semisimple element s of order q^2+q+1 and $S_4(G)S_5(G)S_6(G)$ contains a regular semisimple element t of order divisible by $(q^2-q+1)/\gcd(3,q+1)$. As discussed in [GT, §2.2.3], $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $\mathsf{ccn}(G) \leq 6$.

We may now assume $n \geq 8$, so that $m := \lfloor n/4 \rfloor \geq 2$. Note that

$$\mathrm{PSL}_2(q^{2m}) \cong \Omega_4^-(q^m) \leq \Omega_{4m}^-(q),$$

and $S_1(\mathrm{PSL}_2(q^{2m}))S_2(\mathrm{PSL}_2(q^{2m}))$ contains an element $\tilde{s}$ of order $(q^{2m}+1)/d$. Such an element s is regular semisimple in each of the terms of

$$\Omega_{4m}^-(q) < \Omega_{4m+1}(q) < \Omega_{4m+2}^\pm(q).$$

Hence, if $G \in \{P\Omega^-_{4m}(q), \Omega_{4m+1}(q), P\Omega^\pm_{4m+2}(q)\}$, then $S_1(G)S_2(G)$ contains a regular semisimple element s of order $(q^{2m}+1)/d$. As discussed in [GT, §§2.2.3, 2.2.4], one can find a semisimple element $t \in G$ such that $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $\mathsf{ccn}(G) \le 6$ by Lemma 2.8. In particular, we are done with type ${}^2D_r$.

Consider the case of $G = P\Omega^+_{4m}(q)$, and note that

$$\mathrm{PSL}_2(q^2) \times \mathrm{PSL}_2(q^{2m-2}) \le \Omega^-_4(q) \times \Omega^-_{4m-4}(q) < \Omega^+_{4m}(q).$$

Hence, if $m \ge 3$, then applying Lemma 2.5 we see that $S_1(G)S_2(G)$ contains an element $s = (x, y)$, with $x \in S_1(\mathrm{PSL}_2(q^2))$ of order $(q^2+1)/d$ and $y \in S_2(\mathrm{PSL}_2(q^{2m-2}))$ of order $(q^{2m-2}+1)/d$. This element s is regular semisimple of type $T^{-,-}_{2,2m-2}$, and, as shown in [LST1, Proposition 7.1.1] and [GM, Theorem 7.6], there exists a semisimple element $t \in G$ such that $s^G \cdot t^G \supseteq G \smallsetminus \{1\}$. Hence $\mathsf{ccn}(G) \le 6$ by Lemma 2.8. Suppose now that $m = 2$, but $q \ge 3$. Then

$$\mathrm{SL}_3(q) < \mathrm{SO}^+_6(q) \hookrightarrow \Omega^+_8(q),\ \mathrm{SU}_3(q) < \mathrm{SO}^-_6(q) \hookrightarrow \Omega^+_8(q).$$

By Lemma 2.7, $S_1(G)S_2(G)S_3(G)$ contains an element s of order divisible by $(q^2 + q + 1)/\gcd(3, q-1)$, and such an element is regular semisimple of type $T^{+,+}_{3,1}$ in G, see [GT, §2.1]. Likewise, $S_4(G)S_5(G)S_6(G)$ contains an element t of order divisible by $(q^2 - q + 1)/\gcd(3, q+1)$, and such an element is regular semisimple of type $T^{-,-}_{3,1}$ in G (since $q \ge 3$). By [GT, Lemma 2.4], $s^G \cdot t^G = G \smallsetminus \{1\}$, whence $\mathsf{ccn}(G) \le 6$. In the case $G = \Omega^+_8(2)$, one can check directly that $\mathsf{ccn}(G) \le 4$, using an element of order 7 in $\mathrm{SL}_2(8) < G$.

Consider the case of $G = \Omega_{4m+3}(q)$ with $m \ge 2$, and note that

$$\mathrm{PSL}_2(q^{2m}) < \Omega^-_{4m}(q) \times \Omega_3(q) < \Omega^+_{4m+3}(q).$$

Again using Lemma 2.5 we see that $S_1(G)S_2(G)$ contains an element $s \in S_1(\mathrm{PSL}_2(q^{2m}))$ of order $(q^{2m}+1)/d$. Note that

$$\mathbf{C}_{\mathrm{SO}_{4m+3}(q)}(s) = T \times \mathrm{SO}_3(q),$$

where $T < \mathrm{SO}^-_{4m}(q)$ has order $q^{2m}+1$. Since $\mathrm{SO}_3(q) \cap G = \Omega_3(q)$ has index 2 in $\mathrm{SO}_3(q)$, it follows that

$$|\mathbf{C}_G(s)| = (q^{2m}+1)(q^3-q)/2.$$

Let $B := q^{8m-4}$. By [LOST, Corollary 5.8], Ω has exactly $q+4$ nontrivial irreducible characters of degree $\le B$, which are the characters D°_α with $\alpha \in \mathrm{Irr}(\mathrm{Sp}_2(q))$, listed in [LOST, Proposition 5.7]. The proof of Lemma 2.9 shows that

(3.1)

$$\sum_{\chi \in \mathrm{Irr}(G),\ \chi(1) > B} \frac{|\chi(s)|^3}{\chi(1)} < \frac{|\mathbf{C}_G(s)|^{3/2}}{B} \le \frac{\big((q^{2m}+1)(q^3-q)/2\big)^{3/2}}{q^{8m-4}} < \frac{2^{-3/2}}{q^{5m-17/2}} < 0.07.$$

The degrees of D°_α are listed in [LOST, Table I], showing that two of them have ℓ-defect 0 for ℓ a Zsigmondy prime for $(n-3, q)$ and so vanish at s. Next we estimate $|\chi(s)|$ for the remaining $q+2$ characters. Note that, in the action of s on the natural G-module $\mathbb{F}_q^n$, s has a unique eigenvalue λ that belongs to $\mathbb{F}_{q^2}$, and this eigenvalue is $\lambda = 1$ and has multiplicity 3. Consider the action of $x \otimes s$ on $V := \mathbb{F}_q^2 \otimes \mathbb{F}_q^n$ for any $x \in \mathrm{Sp}_2(q)$ and $\mathbb{F}_q^2$ being the natural module for $\mathrm{Sp}_2(q)$. Then the fixed point subspace of $x \otimes s$ on V

has dimension 6 if $x = 1$, 3 if $1 \neq x$ is unipotent, and 0 otherwise. It follows from the formula [LOST, Lemma 5.5] for D_α that

$$(3.2)\ \ |D_\alpha(s)| \leq \frac{\alpha(1)}{q(q^2-1)}\big(q^3 + q^{3/2}(q^2-1) + q(q^2-1) - q^2\big) = \alpha(1)(q^{1/2} + 2q/(q+1)).$$

Note that $D^\circ_\alpha = D_\alpha$, unless $\alpha(1) = (q+1)/2$ in which case $D^\circ_\alpha = D_\alpha - 1_G$. Now, if $q = 3$, then $\alpha(1) \leq 3$, and so (3.2) shows that $|D^\circ_\alpha(s)| < 10.5$. Since $D^\circ_\alpha(1) \geq 7260$, it follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)\leq B} \frac{|\chi(s)|^3}{\chi(1)} \leq \frac{5 \cdot (10.5)^3}{7260} < 0.8.$$

If $q \geq 5$, then since $\alpha(1) \leq q+1$, (3.2) shows that $|D^\circ_\alpha(s)| \leq 2q + q^{1/2}(q+1)$. As $D^\circ_\alpha(1) > q^8$, it follows that

$$\sum_{\chi \in \mathrm{Irr}(G),\ 1<\chi(1)\leq B} \frac{|\chi(s)|^3}{\chi(1)} \leq \frac{(q+2)\cdot\big(2q + q^{1/2}(q+1)\big)^3}{q^8} < 0.2.$$

Together with (3.1), we have shown that

$$\sum_{1_G \neq \chi \in \mathrm{Irr}(G)} \frac{|\chi(s)|^3}{\chi(1)} < 0.87,$$

and so $(s^G)^3 \supseteq G \smallsetminus \{1\}$ by the Frobenius formula. Consequently, $\mathsf{ccn}(G) \leq 6$. □

Proposition 3.2. *If G is a classical group and the order of G is sufficiently large in terms of the rank of G, then $\mathsf{ccn}(G) \leq 4$.*

Proof. We do a case analysis.

Case $G = \mathrm{PSL}_n(q)$. Let $m = \lfloor n/2 \rfloor$. The obvious homomorphism $\mathrm{SL}_2(q)^m \to \mathrm{SL}_n(q)$ maps $(x_1, \ldots, x_m)$ to a regular semisimple element in a split maximal torus of SL_n over $\mathbb{F}_q$ and hence to a split regular semisimple element of G, whenever the x_i are regular semisimple elements with eigenvalues $\lambda_i^{\pm 1}$, $\lambda_i \in \mathbb{F}_q^\times$, and $\lambda_i \neq \lambda_j^{\pm 1}$ for all i, j. This case now follows from Lemma 2.11.

Case $G = \mathrm{PSU}_n(q)$. Let $m = \lfloor n/2 \rfloor$. We proceed exactly as before, using the obvious homomorphism from $\mathrm{SL}_2(q)^m = \mathrm{SU}_2(q)^m$ to $\mathrm{SU}_n(q)$. An m-tuple of regular semisimple elements such that $\lambda_i \neq \lambda_j^{\pm 1}$ for all i, j maps to an element in an m-dimensional split torus of G, and this is a maximal split torus [T, Table 2].

Case $G = \mathrm{PSp}_{2n}(q)$. We proceed as before, using the obvious homomorphism from $\mathrm{SL}_2(q)^n \cong \mathrm{Sp}_2(q)^n$ to $\mathrm{Sp}_{2n}(q)$, which maps any split maximal torus of SL_2^n to a split maximal torus of Sp_{2n}.

Case $G = P\Omega_{2n+1}(q)$. If $n = 2m$, we proceed as before, using composition of the obvious homomorphisms from $\mathrm{SL}_2(q)^n$ to

$$\mathrm{Spin}_5(q) * \underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m-1} \cong \mathrm{Sp}_4(q) * \underbrace{\mathrm{SL}_2(q) * \ldots * \mathrm{SL}_2(q)}_{n-2}$$

and $\mathrm{Spin}_5(q) * \underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m-1} \to \mathrm{Spin}_{2n+1}(q)$. If $n = 2m+1$, we map $\mathrm{SL}_2(q)^n$ onto $\mathrm{Spin}_3(q) * \underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m}$ and maps the latter to $\mathrm{Spin}_{2n+1}(q)$.

Case $G = P\Omega_{2n}^+(q)$. If $n = 2m$, we map $\mathrm{SL}_2(q)^n$ onto $\underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m}$ and map the latter to $\mathrm{Spin}_{2n}^+(q)$. If $n = 2m+1$, we map $\mathrm{SL}_2(q)^{n-1}$ to

$$\mathrm{SL}_4(q) * \underbrace{\mathrm{SL}_2(q) * \ldots * \mathrm{SL}_2(q)}_{n-3} \cong \mathrm{Spin}_6^+(q) * \underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m-1},$$

which embeds in the usual way in $\mathrm{Spin}_{2n}^+(q)$.

Case $G = P\Omega_{2n}^-(q)$. If $n = 2m+1$, we map $\mathrm{SL}_2(q)^{n-1} = \mathrm{SU}_2(q)^2 \times \mathrm{SL}_2(q)^{n-3}$ onto

$$\mathrm{SU}_4(q) * \underbrace{\mathrm{SL}_2(q) * \ldots * \mathrm{SL}_2(q)}_{n-3} \cong \mathrm{Spin}_6^-(q) * \underbrace{\mathrm{Spin}_4^+(q) * \ldots * \mathrm{Spin}_4^+(q)}_{m-1},$$

which embeds in the usual way in $\mathrm{Spin}_{2n}^-(q)$. Note that an ordered pair of regular semisimple elements of $\mathrm{SU}_2(q)$ with distinct eigenvalue pairs gives a regular semisimple element of $\mathrm{SU}_4(q)$, and it follows that the image of a maximal torus of SL_2^{n-1} in $\mathrm{Spin}_{2n}^-(q)$ meets the regular semisimple locus. As Spin_{2n}^- is not split, it cannot have a split torus of rank n, so any split torus of rank $n-1$ must be a maximal split torus. It follows that the image of a split maximal torus of SL_2^{n-1} is a maximal split torus of Spin_{2n}^-.

If $n = 2m$, we identify $\mathrm{Spin}_4^-(q)$ with $\mathrm{SL}_2(q^2)$ and map $\mathrm{SL}_2(q^2) \times \mathrm{SL}_2(q)^{n-2}$ into $\mathrm{Spin}_{2n}^-(q)$. This maps $(y, x_1, \ldots, x_{n-2})$ to a regular semisimple element when y and the x_i are regular semisimple, the eigenvalues of all x_i lie in $\mathbb{F}_q$, the eigenvalues of y do not lie in $\mathbb{F}_q$, and no two x_i have an eigenvalue in common. We can no longer use the Ellers-Gordeev method, but Proposition 2.10 applies, so we still obtain $\mathsf{ccn}(G) \leq 4$. □

From this, we easily deduce Proposition 1.6.

Proof of Proposition 1.6. Because n and $q-1$ are relatively prime, $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)$, so

$$4 = \mathsf{iw}(\mathrm{SL}_n(q)) = \mathsf{iw}(\mathrm{PSL}_n(q)) \leq \mathsf{ccn}(\mathrm{PSL}_n(q)) \leq 4.$$

□

At present, weakening the assumption "the order of G is sufficiently large in terms of the rank of G" in Proposition 3.2 even to "the order of G is sufficiently large" seems challenging.

4. Exceptional groups of Lie type

The following lemma will be useful for us.

Lemma 4.1. *Let G be an exceptional group of Lie type and s an element of G whose order is divisible by a prime ℓ which is Zsigmondy for (n, q). Then*

(i) *If $G = F_4(q)$ and $n = 8$, then s is regular semisimple with centralizer order $q^4 + 1$.*

(ii) *If $G = {}^2F_4(q)$ with $q \geq 8$, $n = 4$, and $\ell > 5$, then s is regular semisimple with centralizer order $q^2 + 1$.*
(iii) *If $G = E_6(q)$ or $G = {}^2E_6(q)$, and $n = 8$, then s is regular semisimple with centralizer order $(q^2 - 1)(q^4 + 1)$.*
(iv) *If $G = E_7(q)$ and $n = 7$, then s is regular semisimple with centralizer order $q^7 - 1$.*
(v) *If $G = E_8(q)$ and $n = 7$, then s has centralizer order dividing $(q^3 - q)(q^7 - 1)$.*

Proof. In all five cases, $\ell - 1$ has a divisor ≥ 5, so $\ell \geq 11$. Let t denote a power of s of exact order ℓ, so t is semisimple. By [MT, Lemma 2.2], the connected center T of the centralizer of t has order divisible by ℓ. It suffices to prove the stated claims for t, since the centralizer of t contains the centralizer of s. In general, ℓ divides $\Phi_m(q)$ only if m is n times a power of ℓ. The order of every torus T in G can be written $\prod_j \Phi_{i_j}(q)$, where $\sum \phi(i_j)$ is the rank of the torus; in particular, $\phi(i_j) \leq 8$, which implies that $i_j < n\ell$, so if ℓ divides $|T$, then $i_j = n$ for some i_j.

In the F_4 case, $\phi(8) = 4$ so T must have order $\Phi_8(t)$, so t must be regular semisimple. The same argument applies to ${}^2F_4(q)$ (which is ${}^2F_4(r^2)$ with $r = q^{1/2}$). In the E_6 and ${}^2E_6$ cases, we consult the connected centralizers in the E_6 table in [FJ1] and conclude that t must be regular semisimple and associated to w_{19}, implying the stated centralizer order. The E_7-table in [FJ1] has a $\Phi_7(q)$ factor in the connected centralizer of t only for the regular semisimple case associated to w_{39}. The E_8-table in [FJ2] has a $\Phi_7(q)$ factor in three cases: the regular semisimple classes associated to w_{37} and w_{55}, with centralizer orders $(q-1)(q^7-1)$ and $(q+1)(q^7-1)$ respectively and the (A_1, w_{51}) class, with centralizer order $(q^3 - q)(q^7 - 1)$. □

Theorem 4.2. *If G is a finite simple group of exceptional Lie type, then* $\mathsf{ccn}(G) \leq 6$.

Proof. We consider each of the ten possibilities.

Case ${}^2B_2(q)$. As G is a finite simple group, we have $q \geq 8$. By [AH, p. 2], $\mathsf{ecn}(G) = 4$, so by Lemma 2.3, $\mathsf{ccn}(G) \leq 3$.

Case $G_2(q)'$. The character table for $q = 2$ is in the GAP library, and we easily compute that the extended covering number of this group is 5, so $\mathsf{ccn}(G) \leq 4$. Otherwise, $q \geq 3$, so $G_2(q)' = G_2(q)$. By [LSS, Table 5.1], we have $\mathrm{SL}_3(q) < G_2(q)$. Let $e := \gcd(3, q-1) = \gcd(3, q^2 + q + 1)$. By Lemma 2.7, for all S_1, S_2, S_3, every element $\overline{s}$ of order $\frac{q^2+q+1}{e}$ in $\mathrm{PSL}_3(q)$ belongs to $S_1(\mathrm{PSL}_3(q))S_2(\mathrm{PSL}_3(q))S_3(\mathrm{PSL}_3(q))$, and let s be any lift of $\overline{s}$ to $\mathrm{SL}_3(q)$. By [GM, Table 10], every non-trivial element of G is a product of two such elements s, so $\mathsf{ccn}(G_2) \leq 6$.

Case ${}^2G_2(q)'$. When $q = 3$, this is $\mathrm{PSL}_2(8)$, so we have $\mathsf{ccn}(G) \leq 3$. When $q \geq 27$, ${}^2G_2(q)$ is already simple. By [LSS, Table 5.1], $\mathrm{PSL}_2(q) < G$, so by Lemma 2.5, any $S_1(G)S_2(G)$ contains an element s of order $\frac{q+1}{2}$, and by [GM, Theorem 7.1], every element of $G \smallsetminus \{1\}$ is a product of two conjugates of s. Thus $\mathsf{ccn}(G) \leq 4$.

Case ${}^3D_4(q)$. We compute

$$\mathsf{ecn}({}^3D_4(2)) = 7, \ \mathsf{ecn}({}^3D_4(3)) = 6,$$

using the character table in the GAP library for the former and Frank Lübeck's character table, computed using the generic character table for ${}^3D_4$ in CHEVIE [GHLMP], for the latter. So we may assume $q \geq 4$.

By [LSS, Table 5.1], we have $\mathrm{SL}_2(q) \times \mathrm{SL}_2(q^3) < {}^3D_4(q)$ if q is even and the central product $\mathrm{SL}_2(q) * \mathrm{SL}_2(q^3)$ if q is odd. In either case, by Lemma 2.4, given ample characteristic collections S_1 and S_2, this subgroup contains an element s of $S_1(G)S_2(G)$ of order $(q-1)(q^3+1)/d$ where $d := \gcd(2, q-1)$. This element is regular semisimple of type s_{11} in the Deriziotis-Michler classification [DM, Table 2.1]; it follows that the order of its centralizer is $(q-1)(q^3+1) < q^4$. From Lübeck's table of degrees for ${}^3D_4(q)$ [Lu], we know that except for the trivial character and a character χ_1 of degree $q\Phi_{12}(q)$, all other irreducible characters of ${}^3D_4(q)$ have degree greater than $q^8/2$ when $q \geq 4$. By [Sp, Table 2], the value of χ_1 at a regular semisimple element with centralizer $(q-1)(q^3+1)$ is 1. Certainly, $\sum_{\chi \in \mathrm{Irr}(G)} |\chi(s)|^2 = |\mathbf{C}_G(s)| < q^4$, and $|\chi(s)| < ((q-1)(q^3+1))^{1/2} < q^2$ for all $1_G \neq \chi \in \mathrm{Irr}(G)$. We conclude that

$$\begin{aligned}\sum_{\chi \neq 1} \frac{|\chi(s)|^3}{\chi(1)} &< \frac{1}{q\Phi_{12}(q)} + \sum_{\chi(1) > \epsilon_1(1)} \frac{|\chi(s)|^3}{\chi(1)} \\ &< \frac{2}{q^5} + \frac{q^2}{q^8/2} \sum_{\chi} |\chi(s)|^2 \\ &< \frac{2}{q^5} + \frac{2}{q^2} < 1,\end{aligned}$$

so the Frobenius formula implies that $(s^G)^3 = G$.

Case $F_4(q)$. By [LSS, Table 5.1], $\mathrm{Sp}_4(q^2) < F_4(q)$. Therefore, $\mathrm{SL}_2(q^4) < F_4(q)$. We are therefore guaranteed elements s of order q^4+1 in $S_1(F_4(q))S_2(F_4(q))$. By Lemma 4.1, such elements are regular semisimple. By [GM, Table 11], If t is any element of order $\Phi_{12}(t)$, then the product of the conjugacy class of s and the conjugacy class of t covers $F_4(q) \setminus \{1\}$. Thus, Lemma 2.8 implies $\mathsf{ccn}(F_4(q)) \leq 6$.

Case ${}^2F_4(q)'$. For $q = 2$, this is the Tits group. In this case, we can use the character table in GAP to compute the extended covering number, which is 5, so $\mathsf{ccn}(G) \leq 4$. We may therefore assume $q \geq 8$, so ${}^2F_4(q)$ is already perfect. By [LSS, Table 5.1], $\mathrm{SL}_2(q^2) < \mathrm{Sp}_4(q) < {}^2F_4(q)$. Thus, ${}^2F_4(q)$ contains regular semisimple elements s of order q^2+1 by Lemma 4.1. The centralizer of s in ${}^2F_4(q)$ has order q^2+1, and by [LS] we have $\mathfrak{d}(G) \geq 2^{-1/2}(1-q^{-1})q^{11/2}$. Lemma 2.9 now implies that $\mathsf{ccn}(G) \leq 6$ for $q \geq 8$.

Cases $E_6(q)$ and ${}^2E_6(q)$. As $F_4(q) < G$, we have $\mathrm{SL}_2(q^4) < G$, and proceeding as in the $F_4(q)$ case, we are guaranteed elements s of order q^4+1 in $S_1(G)S_2(G)$. These elements are regular semisimple by Lemma 4.1. By [GM, Table 11], there exists a semisimple element t such that the product of the conjugacy classes of s and t cover $G \setminus \{1\}$. Thus, $\mathsf{ccn}(G) \leq 6$ by Lemma 2.8.

Case $E_7(q)$. By [LSS, Table 5.1], $E_7(q)$ contains $\mathrm{PSL}_2(q^7)$. If S_1 and S_2 are ample characteristic collections, then $S_1(\mathrm{PSL}_2(q^7))S_2(\mathrm{PSL}_2(q^7))$ contains an element s of order q^7-1 or $\frac{q^7-1}{2}$. By Lemma 4.1, this element is regular semisimple. In [GM, Table 11] is it shown that there exists an order x_2 prime to q such that the product of any conjugacy class of order $x_1 = q^7 - 1$ and any conjugacy class of order x_2 covers $G \smallsetminus \{1\}$. The proof depends only on the divisibility of x_1 by a Zsigmondy prime and therefore goes through unchanged if $x_1 = \frac{q^7-1}{2}$. Lemma 2.8 now implies that $\mathsf{ccn}(E_7(q)) \le 6$.

Case $E_8(q)$. By [LSS, Table 5.1], $E_8(q)$ contains a $E_7^{\mathrm{sc}}(q)$, which, in turn, contains a perfect central extension $\tilde{H}$ of $H = \mathrm{PSL}_2(q^7)$. We can therefore regard $\tilde{H}$ as a central quotient of $\mathrm{SL}_2(q^7)$. If S_1 and S_2 are ample characteristic collections, then $S_1(\tilde{H})S_2(\tilde{H})$ contains an element s of order $q^7 - 1$ or $\frac{q^7-1}{2}$. This element is therefore semisimple, and by Lemma 4.1, the order of its centralizer divides $(q^3 - q)(q^7 - 1)$. By [LS], $\mathfrak{d}(G) \ge q^{27}(q^2 - 1) \ge q^{28}$. As $(q^{10})^{3/2} = q^{15} < q^{28}$, Lemma 2.9 implies $\mathsf{ccn}(E_8(q)) \le 6$. □

In most cases, we can prove the improved bound of 4.

Proposition 4.3. *If G is a sufficiently large finite simple group of exceptional Lie type, then* $\mathsf{ccn}(G) \le 4$.

Proof. For each series of exceptional groups of Lie type with the exception of ${}^2B_2$ (which is already covered by Theorem 4.2), E_6 and ${}^2E_6$, [LSS, Table 5.1] gives a subgroup of the type for which Proposition 2.10 applies.

Suppose G is of type E_6, i.e., it is the quotient of $\underline{G}(\mathbb{F}_q)$ by its center, where $\underline{G}$ is the split simply connected group group over $\mathbb{F}_q$ of type E_6. As $A_1 \times A_5$ can be obtained from the extended Dynkin diagram of E_6 by deleting a vertex, it follows that there exists a homomorphism $\mathrm{SL}_2 \times \mathrm{SL}_6 \to \underline{G}$ of algebraic groups over $\mathbb{F}_q$, and a maximal torus of the former maps to a maximal torus of the later. Thus, there exists a homomorphism $\phi\colon \mathrm{SL}_2^4 \to \underline{G}$ which factors through $\mathrm{SL}_2 \times \mathrm{SL}_6 \to \underline{G}$, which maps a split maximal torus into a split maximal torus, and whose image contains regular elements if q is sufficiently large. The proposition now follows from Lemma 2.11.

Finally suppose G is of type ${}^2E_6$. Let $\underline{G}$ be a simply connected non-split group of type E_6 over $\mathbb{F}_q$. By [T, Table 2], it is of rank 4 over $\mathbb{F}_q$. The rank of $\mathrm{SL}_2 \times \mathrm{SU}_6$ over $\mathbb{F}_q$ is also 4, so there is a homomorphism $\mathrm{SL}_2 \times \mathrm{SU}_6 \to \underline{G}$ mapping a maximal split torus to a maximally split maximal torus. Using $\mathrm{SL}_2^3 = \mathrm{SU}_2^3 \to \mathrm{SU}_6$, we obtain a morphism of algebraic groups over $\mathbb{F}_q$ from SL_2^4 to $\underline{G}$ which sends any split maximal torus of SL_2^4 to a maximal split torus of $\underline{G}$ and whose image in $\underline{G}$ contains regular semisimple elements. The proposition again follows from Lemma 2.11. □

5. Alternating groups and sporadic groups

Proposition 5.1. *For $n \ge 5$ we have* $\mathsf{ccn}(\mathsf{A}_n) \le 4$.

Proof. By [AH, p. 1], we have $\mathsf{ecn}(\mathsf{A}_n) \le 5$ for $n \le 9$, so by Lemma 2.3, we may assume $n \ge 10$.

If p is a prime, the permutation representation on $\mathbb{P}^1(\mathbb{F}_p)$ embeds $\mathrm{PSL}_2(p)$ in A_{p+1}. Every element of order p maps to a p-cycle in A_{p+1} and therefore to a p-cycle in A_n for all $n \ge p + 1$. By Lemma 2.5, if $p \equiv 1 \pmod 4$, then there exist elements

$$s \in S_1(\mathrm{PSL}_2(p))S_2(\mathrm{PSL}_2(p)),\ t \in S_3(\mathrm{PSL}_2(p))S_4(\mathrm{PSL}_2(p))$$

of order p. Hence every element in A_n which is a product of two p-cycles lies in $S_1(\mathsf{A}_n)\cdots S_4(\mathsf{A}_n)$.

By a theorem of Bertrand [B], if $\lfloor \frac{3n}{4} \rfloor \leq p \leq n$, then every element of A_n is a product of two p-cycles. Therefore, $\mathsf{ecn}(\mathsf{A}_n) \leq 4$ whenever there exists a prime which is 1 (mod 4) in the interval $[\lfloor 3n/4 \rfloor, n-1]$. Applying this for $p = 13$ and $p = 17$, we get the desired inequality for n in $\{14, 15, 16, 17\}$ and $\{18, 19, 20, 21, 22, 23\}$ respectively. The following table gives primes which together cover all values of $n \in [30, 1.3 \cdot 10^{10}]$.

29	37	41	53	61
73	97	113	149	197
257	337	449	593	773
1021	1361	1801	2393	3181
4241	5653	7537	10037	13381
17837	23773	31657	42209	56269
75017	99989	133277	177677	236897
315857	421133	561461	748613	998117
1330789	1774373	2365829	3154433	4205909
5607853	7477121	9969457	13292593	17723449
23631253	31508329	42011093	56014789	74686357
99581809	132775693	177034217	236045497	314727293
419636389	559515161	746020213	994693597	

By a theorem of Ramaré and Rumely [RR], if $n \geq 10^{10}$, then the sum of $\log p$ over all $p < n$ which are 1 (mod 4) lies between $.495n$ and $.505n$. It follows that there is at least one such prime in the interval $[n, 1.1n]$ for all $n > 10^{10}$, and this is enough to show $\mathsf{ccn}(\mathsf{A}_n) \leq 4$ for all $n > 10^{10}$.

If q is any odd prime power, then for C_1 and C_2 non-trivial conjugacy classes in $\mathrm{PSL}_2(q)$, there is an element of order $\frac{q+1}{2}$ in C_1C_2. This maps into a product of two disjoint $\frac{q+1}{2}$ cycles. A theorem of Xu [X] asserts that if $n-1 \leq r+s \leq n$, then every element of A_n is a product of two elements, each consisting of two disjoint cycles of length r and s. Applying this for $q = 9$, $q = 11$, $q = 23$, $q = 25$, and $q = 27$ we get $\mathsf{ccn}(\mathsf{A}_n) \leq 4$ for n in $\{10, 11\}$, $\{12, 13\}$, $\{24, 25\}$, $\{26, 27\}$, and $\{28, 29\}$ respectively, so all cases are covered. □

To deal with A_n for large n, it is useful to have the following lemma:

Lemma 5.2. *Let p be a prime, k and n positive integers, $n \geq kp$, and*

$$u_1, \ldots, u_k, v_1, \ldots, v_k \in \{1, \ldots, n\}$$

such that $u_i \neq u_j$, $v_i \neq v_j$, and $u_i \neq v_j$ when $i \neq j$. Then there exists an element $\sigma \in \mathsf{S}_n$ such that $\sigma(u_i) = v_i$ for $1 \leq i \leq k$ and σ^p is the identity.

Proof. For each i such that $u_i = v_i$, let $X_i = \{u_i\}$, and for each i such that $u_i \neq v_i$, let X_i be a p-element set containing u_i and v_i and such that the X_i are disjoint from one another. We define σ to be the identity on $\{1, \ldots, n\} \smallsetminus \bigcup X_i$ and to cyclically permute the elements of each X_i such that $\sigma(u_i) = v_i$. □

We can now prove Proposition 1.5.

Proof of Proposition 1.5. First we note by [TZ, Theorem 1.2] that $\mathsf{iw}(\mathsf{A}_n) \geq 3$ when $n \geq 15$: indeed, not every element in A_n with $n \geq 15$ is a product of two involutions. Hence it suffices to show that $\mathsf{ccn}(\mathsf{A}_n) \leq 3$ when n is large enough.

We say a characteristic collection S if of *type* r if r is the smallest prime such that $S(\mathsf{A}_5)$ contains an element of order r. If S is ample it must be of type 2, type 3, or type 5. For any positive integer n and $0 \leq m \leq \lfloor n/5 \rfloor$, the embedding $\mathsf{A}_5^m < \mathsf{A}_n$ guarantees that $S(\mathsf{A}_n)$ contains an element of cycle type $1^{5-4m}2^{2m}$ if S is of type 2, $1^{5-3m}3^m$ if S is of type 3, and $1^{5-5m}5^m$, if S is of type 5.

For $p \equiv \pm 1 \pmod{10}$, $\mathsf{A}_5 < \mathrm{PSL}_2(p) < \mathsf{A}_{p+1}$, and every element of A_5 of order r, when regarded as an element x of A_{p+1}, has at most 2 fixed points and otherwise consists entirely of r-cycles. For $p = 59$, x is therefore a permutation of the form $r^{60/r}$. If S is of type 2, the embedding $\mathsf{A}_{60}^i \times \mathsf{A}_{n-60i} < \mathsf{A}_n$ gives $S(\mathsf{A}_n)$ elements of cycle type $1^{5-4m}2^{2m}$ whenever m belongs to

$$I_i = \Big[15i, 15i + \lfloor \frac{n-60i}{5} \rfloor\Big].$$

When $75+60k \leq n < 75+60(k+1)$, the consecutive intervals in the sequence $I_0, \dots, I_k$ overlap, so for $0 \leq m \leq 15k$, all elements of cycle type $1^{5-4m}2^{2m}$ belong to $S(\mathsf{A}_n)$. This means that every even permutation of order 2 with at least $B_2 = 75$ fixed points lies in $S(\mathsf{A}_n)$. By the same reasoning, for $B_3 = 100$ and $B_5 = 60$, all elements of order 3 and 5 in A_n with at least B_3 and B_5 fixed points respectively lie in $S(\mathsf{A}_n)$ if S is respectively of type 3 or 5.

By [LS1, Theorem 1.2(ii)], if x is an element of S_n of prime order r and a bounded number of fixed points, then for every irreducible character χ of S_n, $|\chi(x)| \leq \chi(1)^{1/r+o(1)}$. Therefore, if n is sufficiently large and x_1, x_2, x_3 are three such elements in A_n, of orders r_1, r_2, r_3 respectively, and

$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} < 1,$$

then the product of the S_n-conjugacy classes of the x_i cover $\mathsf{A}_n \smallsetminus \{1\}$. (Indeed, note that we have $1/r_1 + 1/r_2 + 1/r_3 \leq 41/42$ in such a case, and so, by [LiSh2, Theorem 2.6],

$$\sum_{\chi \in \mathrm{Irr}(\mathsf{S}_n),\ \chi(1)>1} \frac{|\chi(x_1)\chi(x_2)\chi(x_3)|}{\chi(1)} < \sum_{\chi \in \mathrm{Irr}(\mathsf{S}_n),\ \chi(1)>1} \frac{1}{\chi(1)^{1/42}} \to 0$$

when $n \to \infty$.) We may assume without loss of generality that $r_1 \leq r_2 \leq r_3$, so we need only consider the cases $(r_1, r_2) = (2, 2)$, $(r_1, r_2) = (2, 3)$, and $r_1 = r_2 = r_3 = 3$. We proceed by case analysis.

Case $(2, 2, r_3)$. For any $k \geq 1$, let

$$\sigma_k = (1, 2) \cdots (2k-1, 2k) \in \mathsf{S}_{2k},\ \ \tau_k = (2, 3) \cdots (2k, 2k+1) \in \mathsf{S}_{2k+1}.$$

Thus, $\sigma_k\tau_k$ is a $(2k+1)$-cycle, while $\sigma_k\tau_{k-1}$ is a $2k$-cycle. Applying this to any cycle, we see that every element in S_n can be written as a product of two involutions. Regarding S_{n-2} as the stabilizer in A_n of $\{n-1, n\}$, we see that every element of A_n which fixes $n-1$ and n can be written as a product of two involutions in A_n. More generally, every element of A_n with at least $2 + B_2$ fixed points can be written as a product of even involutions, each of which has at least B_2 fixed points and hence belongs to $S(\mathsf{A}_n)$.

We claim that if n is sufficiently large, for every $\rho \in \mathsf{A}_n$ and $p \in \{2, 3, 5\}$ there exists $\pi \in \mathsf{A}_n$ of order dividing p with at least B_p fixed points such that $\pi\rho$ has at least $2+B_2$ fixed points. We choose a sequence $x_1, \dots, x_{2+B_2}$ of distinct elements of $\{1, \dots, n\}$ such that $\rho(x_i) \neq x_j$ for $i \neq j$ and then a sequence $y_1, \dots, y_{B_p}$ of distinct elements of $\{1, \dots, n\} \setminus \{\rho(x_1), \dots, \rho(x_{2+B_2})\}$. By Lemma 5.2, if n is sufficiently large, there exists an even permutation π of order 1 or p which fixes each y_i and maps each $\rho(x_j)$ to x_j. By the above discussion, $\pi\rho \in S(\mathsf{A}_n)S(\mathsf{A}_n)$ and $\pi^{-1} \in S(\mathsf{A}_n)$, hence $\rho \in S(\mathsf{A}_n)S(\mathsf{A}_n)S(\mathsf{A}_n)$.

Case $(2, 3, r_3)$. Let

$$\begin{aligned}
\sigma_k &= (1, 2)(4, 5) \cdots (3k-2, 3k-1),\\
\sigma'_k &= (3, 4)(6, 7) \cdots (3k, 3k+1),\\
\tau_k &= (2, 3, 4)(5, 6, 7) \cdots (3k-1, 3k, 3k+1),\\
\tau'_k &= (1, 2, 3)(4, 5, 6) \cdots (3k-2, 3k-1, 3k).
\end{aligned}$$

Then $\sigma_k\tau_k$ is a $(3k+1)$-cycle, $\sigma_{k+1}\tau_k$ is a $(3k+2)$-cycle, and $\sigma'_k\tau'_{k+1}$ is a $(3k+3)$-cycle. Thus, every element of S_n is a product of an involution σ and an element τ of order 1 or 3. Since any such τ lies in A_n, the same statement holds in A_n, and if the product has at least $\max(B_2, B_3)$ fixed points, the same can be assumed of σ and τ. Applying Lemma 5.2 as before, we can guarantee for each $\rho \in \mathsf{A}_n$ the existence of an element $\pi \in \mathsf{A}_n$ of order dividing r_3 with at least B_{r_3} fixed points such that $\pi\rho$ has at least $\max(B_2, B_3)$ fixed points, and then finish as in the previous case.

Case $(3, 3, 3)$. It suffices to prove that every element of A_n can be written as a product of two elements of order dividing 3. Let

$$\begin{aligned}
\sigma_{k,l} = {}&(1, 2, 3)(5, 6, 7) \cdots (4k-7, 4k-6, 4k-5)(4k-3, 4k-2, 4k-1)\\
&(4k, 4k+1, 4k+2)(4k+4, 4k+5, 4k+6) \cdots (4l, 4l+1, 4l+2),\\
\tau_{k,l} = {}&(3, 4, 5)(7, 8, 9) \cdots (4k-5, 4k-4, 4k-3)(4k-1, 4k, 4k+1)\\
&(4k+2, 4k+3, 4k+4)(4k+6, 4k+7, 4k+8) \cdots (4l+2, 4l+3, 4l+4),
\end{aligned}$$

where the first line in each expression is omitted if $k = 0$ and the second line is omitted if $l = k-1$. Then $\sigma_{k,k-1}\tau_{k-1,k-2}$ is a $(4k-1)$-cycle, and $\sigma_{k,k-1}\tau_{k,k-1}$ is a $(4k+1)$-cycle, so all odd cycles can be written as a product of two elements of order dividing 3. For $l \geq k \geq 0$ and $k + l \geq 1$, $\sigma_{k,l}\tau_{k,l}$ is a disjoint product of a $4k$-cycle and a $(4l+4-4k)$-cycle; $\sigma_{k,l}\tau_{k-1,l}$ is a disjoint product of a $(4k-2)$-cycle and a $(4l+6-4k)$-cycle; $\sigma_{k,l}\tau_{k,l-1}$ is a disjoint product of a $4k$-cycle and a $(4l+2-4k)$-cycle; and $\sigma_{k,l}\tau_{k-1,l-1}$ is a disjoint product of a $(4k-2)$-cycle and a $(4l+4-4k)$-cycle. Thus, all possible permutations that are products of two disjoint even-length cycles can be written as a product of two permutations of order dividing 3. □

Proposition 5.3. *For all sporadic finite simple groups we have* $\mathsf{ccn}(G) \leq 4$.

Proof. By a theorem of Zisser [Zi], we have $\mathsf{ecn}(G) \leq 5$ for all sporadic groups except Fi_{22} and Fi_{23}, so it suffices to consider these two cases. It is known [ATLAS, pp. 74, 163] that there are inclusions $\mathrm{PSL}_2(25) < {}^2F_4(2)' < \mathrm{Fi}_{22}$. By Lemma 2.5, if S_1 and S_2 are ample characteristic collections, then $S_1(\mathrm{PSL}_2(25))S_2(\mathrm{PSL}_2(25))$ has an element of order 13, and a machine computation shows that the product of any two conjugacy classes of elements of order 13 in Fi_{22} contains $\mathrm{Fi}_{22} \smallsetminus \{1\}$. It is also known [ATLAS, p. 177] that $\mathrm{PSL}_2(17) < \mathrm{Fi}_{23}$. By Lemma 2.5, the product $S_1(\mathrm{PSL}_2(17))S_2(\mathrm{PSL}_2(17))$ contains an element of order 17; a machine computation shows that the square of the unique conjugacy class of order 17 in Fi_{23} is the whole group. $\square$

Together with Theorems 3.1 and 4.2, Propositions 5.1 and 5.3 complete the proof of Theorem A. Theorem E follows from results 5.1, 5.3, 3.2 and 4.3.

References

[AH] Z. Arad and M. Herzog, Powers and products of conjugacy classes in groups. Lecture Notes in Math., 1112, Springer, Berlin, 1985.

[B] E. Bertram, Even permutations as a product of two conjugate cycles. *J. Combinatorial Theory Ser. A* **12** (1972), 368–380.

[Bo] A. Borel, On free subgroups of semisimple groups, *Enseign. Math.* **29** (1983), 151–164.

[B1] A. Bors, Fibers of automorphic word maps and an application to composition factors, *J. Group Theory* **20** (2017), no. 6, 1103–1134.

[B2] A. Bors, Fibers of word maps and the multiplicities of nonabelian composition factors, *Internat. J. Algebra Comput.* **27**, (2017), no. 8, 1121–1148.

[ATLAS] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.

[DM] D. I. Deriziotis and 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.

[EG] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), no. 9, 3657–3671.

[FJ1] P. Fleischmann and I. Janiszczak, The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7. *Comm. Algebra* **21** (1993), no. 1, 93–161.

[FJ2] P. Fleischmann and I. Janiszczak, The semisimple conjugacy classes and the generic class number of the finite simple groups of Lie type E_8. *Comm. Algebra* **22** (1994), no. 6, 2221–2303.

[GHLMP] M. Geck, G. Hiss, F. Lübeck, G. Malle, and G. Pfeiffer, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), 175–210.

[G] R. Gow, Commutators in finite simple groups of Lie type. *Bull. London Math. Soc.* **32** (2000), no. 3, 311–315.

[GLOST] R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, Surjective word maps and Burnside's p^aq^b theorem. *Invent. Math.* **213** (2018), no. 2, 589–695.

[GM] R. M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.* **25** (2012), no. 1, 77–121.

[GT] R. M. Guralnick and P. H. Tiep, Effective results on the Waring problem for finite simple groups. *Amer. J. Math.* **137** (2015), 1401–1430.

[KaN] M. Kassabov and N. Nikolov, Words with few values in finite simple groups. *Quarterly J. Math.* **64** (2013), 1161–1166.

[KnN] F. Knüppel and K. Nielsen, $SL(V)$ is 4-reflectional. *Geom. Dedicata* **38** (1991), no. 3, 301–308.

[LS] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443.

[La] M. Larsen, Word maps have large image. *Israel J. Math.* **139** (2004), 149–156.

[LS1] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), 645–687.

[LS2] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), 437–466.

[LST1] M. Larsen, A. Shalev and P. H. Tiep, The Waring problem for finite simple groups. *Annals of Math.* **174** (2011), 1885–1950.

[LST2] M. Larsen, A. Shalev and P. H. Tiep, Products of normal subgroups and derangements, arXiv:2003.12882.

[LOST] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, The Ore conjecture. *J. Europ. Math. Soc.* **12** (2010), 939–1008.

[LOST2] M. W. Liebeck, E .A. O'Brien, A. Shalev and P .H. Tiep, Products of squares in simple groups. *Proc. Amer. Math. Soc.* **140** (2012), 21–33.

[LSS] M. W. Liebeck, J. Saxl, G. M. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type. *Proc. London Math. Soc. (3)* **65** (1992), no. 2, 297–325.

[LiSh1] M. W. Liebeck and A. Shalev, Diameter of simple groups: sharp bounds and applications. *Annals of Math.* **154** (2001), 383–406.

[LiSh2] M. W. Liebeck, A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601.

[Lu] F. Lübeck, `http://www.math.rwth-aachen.de/~Frank.Luebeck`.

[Ma] A. J. Malcolm, The involution width of finite simple groups. *J. Algebra* **493** (2018), 297–340.

[Ma2] A. J. Malcolm, On the p-width of finite simple groups, arXiv:2003.00755.

[MZ] C. Martinez and E. I. Zelmanov, Products of powers in finite simple groups. *Israel J. Math.* **96** (1996), 469–479.

[MT] A. Moretó and P. H. Tiep, Prime divisors of character degrees. *J. Group Theory* **11** (2008), no. 3, 341–356.

[O] S. Yu. Orevkov, Products of conjugacy classes in finite unitary groups $\mathrm{GU}(3, q^2)$ and $\mathrm{SU}(3, q^2)$. *Ann. Fac. Sci. Toulouse Math. (6)* **22** (2013), no. 2, 219–251.

[RR] O. Ramaré and R. Rumely, Primes in arithmetic progressions. *Math. Comp.* **65** (1996), no. 213, 397–425.

[SW] J. Saxl and J. S. Wilson, A note on powers in simple groups, *Math. Proc. Cambridge Philos. Soc.*, **122** (1997), 91–94.

[Se] D. Segal, *Words: Notes on Verbal Width in Groups*. London Mathematical Society Lecture Note Series **361**, Cambridge University Press, Cambridge, 2009.

[Sh1] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem. *Annals of Math.* **170** (2009), 1383–1416.

[Sh2] A. Shalev, Some problems and results in the theory of word maps, *Erdős Centennial*, eds: Lovász et al., Bolyai Soc. Math. Studies **25** (2013), pp. 611–649.

[Sp] N. Spaltenstein, Caractères unipotents de ${}^3D_4(\mathbb{F}_q)$. *Comment. Math. Helv.* **57** (1982), no. 4, 676–691.

[TZ] P. H. Tiep and A.E. Zalesskii, Real conjugacy classes in algebraic groups and finite groups of Lie type, *J. Group Theory* **8** (2005), 291–315.

[T] J. Tits, Classification of algebraic semisimple groups. 1966 Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965) pp. 33–62, Amer. Math. Soc., Providence, R.I., 1966.

[X] C.-H. Xu, The commutators of the alternating group. *Sci. Sinica* **14** (1965), 339–342.

[Zi] I. Zisser, The covering numbers of the sporadic simple groups. *Israel J. Math.* **67** (1989), no. 2, 217–224.

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

E-mail address: `mjlarsen@indiana.edu`

Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.

E-mail address: shalev@math.huji.ac.il

Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel

E-mail address: pht19@math.rutgers.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854-8019, U.S.A.