THE SPREAD OF A FINITE GROUP

TIMOTHY C. BURNESS, ROBERT M. GURALNICK, AND SCOTT HARPER

ABSTRACT. A group G is said to be $\frac{3}{2}$-generated if every nontrivial element belongs to a generating pair. It is easy to see that if G has this property then every proper quotient of G is cyclic. In this paper we prove that the converse is true for finite groups, which settles a conjecture of Breuer, Guralnick and Kantor from 2008. In fact, we prove a much stronger result, which solves a problem posed by Brenner and Wiegold in 1975. Namely, if G is a finite group and every proper quotient of G is cyclic, then for any pair of nontrivial elements $x_1, x_2 \in G$, there exists $y \in G$ such that $G = \langle x_1, y\rangle = \langle x_2, y\rangle$. In other words, $s(G) \geqslant 2$, where $s(G)$ is the spread of G. Moreover, if $u(G)$ denotes the more restrictive uniform spread of G, then we can completely characterise the finite groups G with $u(G) = 0$ and $u(G) = 1$. To prove these results, we first establish a reduction to almost simple groups. For simple groups, the result was proved by Guralnick and Kantor in 2000 using probabilistic methods and since then the almost simple groups have been the subject of several papers. By combining our reduction theorem and this earlier work, it remains to handle the groups with socle an exceptional group of Lie type and this is the case we treat in this paper.

1. INTRODUCTION

In this paper we study the spread and uniform spread of finite groups. These natural invariants encode interesting generation properties and they have been the subject of numerous papers spanning a period of more than 50 years. We begin with their definitions.

Definition. Let G be a group.

(i) The *spread* of G, denoted $s(G)$, is the largest integer k such that for any nontrivial elements $x_1, \ldots, x_k$ in G, there exists $y \in G$ with $G = \langle x_i, y\rangle$ for all i.

(ii) The *uniform spread* of G, denoted $u(G)$, is the largest integer k such that there is a conjugacy class C of G with the property that for any nontrivial elements $x_1, \ldots, x_k$, there exists $y \in C$ with $G = \langle x_i, y\rangle$ for all i. Here we say C *witnesses* $u(G) \geqslant k$.

(iii) If no such largest integer exists in (i) or (ii), then we write $s(G) = \infty$ or $u(G) = \infty$, respectively.

Let us observe that for any group G we have $s(G) \geqslant u(G) \geqslant 0$, and if G is cyclic, then $s(G) = u(G) = \infty$. A group G is $\frac{3}{2}$-*generated* if every nontrivial element belongs to a generating pair, which is equivalent to the condition $s(G) \geqslant 1$. Therefore, we can view the concepts of spread and uniform spread as natural extensions of the $\frac{3}{2}$-generation property.

The notion of spread was first introduced in the 1970s by Brenner and Wiegold in [9], where numerous results on the spread of soluble groups and certain families of simple groups (such as alternating groups and linear groups of the form $\mathrm{L}_2(q)$) are established. However, it turns out that the spread of finite groups has been studied since as early as the 1930s. For instance, a 1939 paper of Piccard [59] proves that the symmetric group $G = \mathrm{Sym}_n$ has positive spread for all $n \geqslant 5$ and later work of Binder [4, 5] in the 1960s extended this to $s(G) \geqslant 2$. The more restrictive definition of uniform spread was formally introduced much more recently by Breuer, Guralnick and Kantor [10], although one finds work of Binder [6] from 1970 on the uniform spread of symmetric groups.

Date: January 15, 2021.

As a consequence of the Classification of Finite Simple Groups, we know that every nonabelian finite simple group can be generated by two elements. This is a routine exercise for the alternating groups and a theorem of Steinberg [65] for groups of Lie type. The property was verified for the sporadic groups by Aschbacher and Guralnick in [1]. In view of this fundamental result, it is natural to study the spread and uniform spread of finite simple groups and there is an extensive literature on this topic.

The first main result is due to Guralnick and Kantor [35], who proved that $u(G) \geqslant 1$ for every finite simple group G (also see Stein [64]). The proof combines powerful probabilistic methods with a detailed analysis of the conjugacy classes and subgroup structure of simple groups. It follows that every finite simple group is $\frac{3}{2}$-generated, as predicted by Steinberg in his 2-generation paper of 1962 (see [65, Section 1]). These results for simple groups G were extended in a subsequent paper by Breuer, Guralnick and Kantor [10] who showed that $u(G) \geqslant 2$, with equality if and only if

$$G \in \{\mathrm{Alt}_5,\ \mathrm{Alt}_6,\ \Omega_8^+(2),\ \mathrm{Sp}_{2r}(2)\ (r \geqslant 3)\} \tag{1}$$

(for each of these groups, it is worth noting that $s(G) = 2$). Asymptotic results on the spread and uniform spread of simple groups are established by Guralnick and Shalev in [36].

It is easy to see that if a group G is $\frac{3}{2}$-generated, then every proper quotient of G is cyclic (that is, G/N is cyclic for all nontrivial normal subgroups N of G). The converse statement is false for infinite groups since there exist infinite simple groups that are not finitely generated, such as the alternating group Alt_∞. In fact, there even exist finitely generated simple groups that are not 2-generated (see [33]). However, recent work of Donoven and Harper [27] shows that Thompson's group V, and related infinite families of finitely presented groups, are $\frac{3}{2}$-generated.

It is natural to ask if the cyclic quotient property is equivalent to $\frac{3}{2}$-generation for *finite* groups. This is a conjecture of Breuer, Guralnick and Kantor (see [10, Conjecture 1.8]).

Conjecture. *Let G be a finite group. Then $s(G) \geqslant 1$ if and only if every proper quotient of G is cyclic.*

This conjecture has been established in a handful of special cases. For example, see [9, Theorem 2.01] for soluble groups and the main theorem of [35] for simple groups. In this paper, we prove a much stronger form of the conjecture in full generality.

Theorem 1. *Let G be a finite group. Then $s(G) \geqslant 2$ if and only if every proper quotient of G is cyclic.*

As noted above, there are infinitely many finite simple groups G with $s(G) = 2$. Moreover, Corollary 2.17 shows that if G is one of the simple groups in (1), then $s(G \wr C_k) = 2$ for all $k \geqslant 1$.

In [9], Brenner and Wiegold prove that every finite soluble group G with $s(G) \geqslant 1$ satisfies the stronger bound $s(G) \geqslant 3$ (see [9, Corollary 2.02]). In [9, Problem 1.04], they seek a classification of the finite groups G with $s(G) = 1$, and they speculate that there are only finitely many such groups. As an immediate corollary to Theorem 1, we can now give the definitive solution to this problem, which has remained open since 1975: there are none.

Corollary 2. *There is no finite group G with $s(G) = 1$.*

We will prove Theorem 1 by studying the uniform spread of finite groups. The following result characterises the finite groups G with $u(G) = 0$ and $u(G) = 1$.

Theorem 3. *Let G be a finite group.*

(i) *$u(G) = 0$ if and only if G has a noncyclic proper quotient, or G is Sym_6 or $C_p \times C_p$ for a prime p.*

(ii) *$u(G) = 1$ if and only if G has a unique minimal normal subgroup*

$$N = T_1 \times \cdots \times T_k = (\mathrm{Alt}_6)^k,$$

where $k \geqslant 2$, G/N is cyclic and $N_G(T_i)/C_G(T_i) = \mathrm{Sym}_6$ for all i.

The next result is an immediate corollary (for part (ii), observe that Sym_6 can be generated by two 6-cycles).

Corollary 4. *Let G be a finite group such that every proper quotient of G is cyclic.*

(i) *If G has even order, then every involution in G belongs to a generating pair.*
(ii) *If $G \neq C_p \times C_p$ for a prime p, then G can be generated by two conjugate elements.*

Recall that a finite group G is *almost simple* if it has a unique minimal normal subgroup G_0 that is nonabelian and simple (in particular, $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ and G_0 is the socle of G). As a special case of Theorem 3, we obtain the following result, which highlights the anomaly of the symmetric group of degree 6.

Corollary 5. *Let $G = \langle G_0, g\rangle$ be a finite almost simple group with socle G_0. Then $u(G) < 2$ if and only if $G = \mathrm{Sym}_6$, in which case $s(G) = 2$ and $u(G) = 0$.*

Let G be a finite group and recall that the *generating graph* of G is an undirected graph $\Gamma(G)$ with vertices the nontrivial elements of G so that x and y are adjacent if and only if $G = \langle x, y\rangle$. This graph was first introduced by Liebeck and Shalev [52, Section 7] and it has been widely studied in recent years, especially in the setting where G is a simple group (see [13] and the references therein). The following result, which is an immediate corollary of Theorem 1, establishes a remarkable dichotomy for generating graphs of finite groups.

Corollary 6. *Let G be a finite group and let $\Gamma(G)$ be the generating graph of G. Then either*

(i) *$\Gamma(G)$ has isolated vertices; or*
(ii) *$\Gamma(G)$ is connected and has diameter at most 2.*

We now turn to a further application of spread. Let G be a finite group and let $k \geqslant d(G)$ be an integer, where $d(G)$ is the smallest size of a generating set for G. The vertices of the *product replacement graph* $\Gamma_k(G)$ are the generating k-tuples of G and the neighbours of $(x_1, \ldots, x_i, \ldots, x_k)$ in this graph are $(x_1, \ldots, x_i x_j^{\pm}, \ldots, x_k)$ and $(x_1, \ldots, x_j^{\pm} x_i, \ldots, x_k)$, for each $1 \leqslant i \neq j \leqslant k$. Two generating tuples in $\Gamma_k(G)$ are *equivalent* if they are connected by a path in $\Gamma_k(G)$. A generating tuple is *redundant* if one of the entries can be removed and the remaining entries still generate G.

This graph arises naturally in several different contexts. For example, the well known product replacement algorithm for computing random elements of G involves a random walk on $\Gamma_k(G)$ (see [18]). A straightforward argument shows that if $s(G) \geqslant 2$, then all redundant generating k-tuples of G are equivalent for $k > 2$ (see [29, Lemma 2.8]), so Theorem 1 yields the following corollary. This is related to a much more general conjecture of Pak [58, Conjecture 2.5.5], which asserts that $\Gamma_k(G)$ is connected for $k > d(G)$.

Corollary 7. *Let $k \geqslant 3$ and let G be a finite group such that every proper quotient is cyclic. Then all redundant generating k-tuples are connected in the product replacement graph $\Gamma_k(G)$.*

Let G be a finite group such that every proper quotient is cyclic. We adopt a two-step strategy for proving Theorems 1 and 3. The first step involves a reduction to almost simple groups; this is the content of Section 2. It is straightforward to reduce to the case where G has a unique minimal normal subgroup $N = T_1 \times \cdots \times T_k$ with each T_i isomorphic to a nonabelian finite simple group T. We then proceed by induction on k, applying a slightly stronger form of Corollary 5 for almost simple groups (see Theorem 2.9).

The case $k = 1$ is the base for the induction. Let $G = \langle G_0, g\rangle$ be an almost simple group with socle G_0. By the Classification of Finite Simple Groups we know that G_0 is an alternating group, a sporadic group or a group of Lie type (classical or exceptional). As previously mentioned, the result for simple groups (the case $G = G_0$) is due to Breuer, Guralnick and Kantor [10, Theorem 1.2], so we may assume $G \neq G_0$. This setting has been the focus of several recent papers and the desired result has been proved when G_0 is one of the following:

(a) Alt_n: Breuer, Guralnick & Kantor [10, Lemma 6.5], Burness & Harper [15, Theorem 4.4]

(b) Sporadic: Breuer, Guralnick & Kantor [10, Table 9]

(c) $\mathrm{L}_n(q)$: Burness & Guest [14, Theorem 2]

(d) $\mathrm{PSp}_{2m}(q)$ or $\Omega_{2m+1}(q)$: Harper [37, Theorem 1]

(e) $\mathrm{U}_n(q)$ or $\mathrm{P}\Omega^{\pm}_{2m}(q)$: Harper [38, Theorem 2].

In view of this earlier work, and with the reduction theorem in hand, it just remains to consider the case where G_0 is an exceptional group of Lie type. To complete the picture, in this paper we handle the final remaining case.

Theorem 8. *Let $G = \langle G_0, g\rangle$ be a finite almost simple group whose socle G_0 is an exceptional group of Lie type. Then $u(G) \geqslant 2$. Moreover, if (G_n) is a sequence of almost simple exceptional groups of this form such that $|G_n| \to \infty$, then $u(G_n) \to \infty$.*

The proof of Theorem 8 is given in Sections 4–9, with a number of preliminary results presented in Section 3.

By combining the asymptotic statement in Theorem 8 with similar results in [10, 14, 15, 36, 37, 38] for alternating, symmetric and classical groups, we obtain the following corollary. In the statement, $\mathcal{G}$ denotes the collection of almost simple groups of the form $G = \langle G_0, g\rangle$, where G_0 is the socle of G.

Corollary 9. *Let (G_n) be a sequence of almost simple groups such that $G_n \in \mathcal{G}$ for all n and $|G_n| \to \infty$. In addition, assume (G_n) has no infinite subsequence of groups of Lie type defined over fields of bounded size. Then either $u(G_n) \to \infty$, or (G_n) has an infinite subsequence of*

(i) *symmetric groups; or*

(ii) *alternating groups of degree all divisible by a fixed prime.*

The exceptions in Corollary 9 are genuine. In particular, for $n \geqslant 5$, [15, Theorem 2] gives

$$u(\mathrm{Sym}_n) = \begin{cases} 0 & \text{if } n = 6 \\ 2 & \text{otherwise.} \end{cases}$$

Let $G = \langle G_0, g\rangle$ be an almost simple group whose socle G_0 is an exceptional group of Lie type over $\mathbb{F}_q$. At the heart of our proof of Theorem 8 is the probabilistic method for studying uniform spread, which was introduced by Guralnick and Kantor [35]. This is encapsulated in Lemma 3.17, which states that if there exists an element $x \in G_0 g$ such that

$$\sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < \frac{1}{k}$$

for all nontrivial $z \in G$, then $u(G) \geqslant k$, witnessed by x^G. Here $\mathcal{M}(x)$ is the set of maximal overgroups of x in G and $\mathrm{fpr}(z, G/H)$ is the fixed point ratio of z, which is the proportion of cosets in G/H fixed by z with respect to the natural transitive action of G on G/H. Typically, we will aim to derive an explicit upper bound $f(q)$ on the above summation for a suitable choice of element x (and independent of z) with the property that $f(q) < \frac{1}{2}$ and $f(q) \to 0$ as q tends to infinity. In particular, the latter property is needed to prove the asymptotic statement in Theorem 8.

In order to effectively apply this approach, we need to select an appropriate element x in the coset G_0g in such a way that we can get some control on the subgroups in $\mathcal{M}(x)$. Then for each $H \in \mathcal{M}(x)$, we need to work with upper bounds on the corresponding fixed point ratios. Bounds on the relevant fixed point ratios for exceptional groups are established in [47] and this work plays a key role in our analysis (in a few cases, we need to strengthen their bounds for our application). However, several special difficulties arise in the initial step, where we select x and then determine its maximal overgroups.

In the special case $G = G_0$, Breuer, Guralnick and Kantor [10] appeal to work of Weigel [68], where a specific semisimple element $x \in G$ is identified that is contained in very few maximal subgroups (typically, $N_G(\langle x \rangle)$ is the unique maximal overgroup). However, for the almost simple groups we are considering in this paper, we need to select x in the coset G_0g and a different approach is required, which will depend on the type of automorphism g. It is worth emphasising that this constitutes a major difference between the simple groups handled in [10] and the almost simple groups we are working with in this paper. In particular, there are some substantial technical difficulties to overcome in the almost simple setting.

To handle these difficulties, we will rely heavily on the theory of Shintani descent, which was exploited in [14] to study the uniform spread of almost simple groups with socle $\mathrm{L}_n(q)$. These techniques have been subsequently extended and developed by Harper in [37, 38] and they play a key role in this paper (see Section 3.4 for further details). Needless to say, our approach will also use deep results on the maximal subgroups of exceptional groups, due to Liebeck, Seitz and others (see Theorem 3.2 for example).

Notation. Let G be a finite group and let n be a positive integer. Our group theoretic notation is fairly standard. In particular, we will write C_n, or just n, for a cyclic group of order n and G^n will denote the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$. If X is a subset of G, then $i_n(X)$ is the number of elements of order n in X and $\mathrm{meo}(X)$ is the maximal order of an element in X. We will use the notation for simple groups from [43], so we write $\mathrm{L}_n(q) = \mathrm{PSL}_n(q)$ and $E_6^-(q) = {}^2E_6(q)$, etc. For positive integers a and b, $\delta_{a,b}$ is the familiar Kronecker delta and we write (a, b) for the greatest common divisor of a and b. In this paper, all logarithms are base two.

Acknowledgements. Guralnick was partially supported by the NSF grant DMS-1901595 and Simons Foundation Fellowship 609771. Burness and Harper thank the Isaac Newton Institute for Mathematical Sciences for support and hospitality during the programme *Groups, Representations and Applications: New perspectives*, when some of the work on this paper was undertaken. This work was supported by: EPSRC grant number EP/R014604/1.

2. The reduction

In this section, we establish reduction theorems which reduce the proofs of Theorems 1 and 3 to almost simple groups. We begin by recording some preliminary results.

2.1. **Preliminaries.** Let G be a finite group and recall the definition of the *spread* and *uniform spread* of G, denoted by $s(G)$ and $u(G)$, respectively (see Section 1). Let us also recall that $s(G) \geqslant 1$ only if every proper quotient of G is cyclic. The following elementary result describes the structure of the groups with this property.

Lemma 2.1. *Let G be a finite group such that every proper quotient of G is cyclic. Then one of the following holds:*

(i) *G is cyclic and $s(G) = u(G) = \infty$.*
(ii) *$G = C_p \times C_p$ for a prime p and $s(G) = p$ and $u(G) = 0$.*
(iii) *G is nonabelian with a unique minimal normal subgroup.*

Proof. We may assume that G is noncyclic. If G is abelian then it is easy to see that (ii) holds (see [15, Remark 1(c)], for example). Now assume G is nonabelian. If N_1 and N_2 are distinct minimal normal subgroups, then G/N_i is cyclic and thus $G' \leqslant N_1 \cap N_2 = 1$, which is a contradiction. Therefore, (iii) holds. □

For the remainder of Section 2, we may assume that G is a nonabelian group with a unique minimal normal subgroup $N = T_1 \times \cdots \times T_k$, where for each i the group T_i is isomorphic to a fixed simple group T. In addition, we assume throughout that G/N is cyclic.

The case where N is abelian is easy to deal with.

Lemma 2.2. *Let G be a finite nonabelian group with a unique minimal normal subgroup N. Assume that N is abelian and G/N is cyclic. Then $s(G) = |N| - \epsilon$ and $u(G) = |N| - 1$, where $\epsilon = 0$ if $|G/N|$ is a prime, and otherwise $\epsilon = 1$. In particular, $u(G) \geqslant 2$.*

Proof. For the spread see [9, Theorem 2.01], while the uniform spread follows from [15, Theorem 1], noting that $|N| \geqslant 3$ since G is nonabelian. □

From now on we can assume that the unique minimal normal subgroup N is nonabelian. Observe that G acts transitively by conjugation on $\{T_1, \ldots, T_k\}$ and for each i we have $N_G(T_i)/C_G(T_i) \cong A$, where $A = \langle T, y\rangle$ is an almost simple group with socle T. By conjugating in $\mathrm{Aut}(N)$, we may, and will, assume that $G = G_k$, where

$$G_k = \langle N, x\rangle,\ x = (y, 1, \ldots, 1)\sigma \in \mathrm{Aut}(N),\ \sigma = (1, 2, \ldots, k) \in \mathrm{Sym}_k. \tag{2}$$

Note that if $k = 1$, then we simply have $G_k = A$ and $x = y$.

Let us now present some preliminary results that we will use in the proofs of our main reduction theorems. The first two are straightforward computations and we omit their proofs.

Lemma 2.3. *Let d be a positive integer. Then x is a d-th power in $\mathrm{Aut}(N)$ if and only if $(d, k) = 1$ and y is a d-th power in $\mathrm{Aut}(T)$.*

Lemma 2.4. *Suppose $k \geqslant 2$ and let p be a prime divisor of k. Let*

$$X_i = T_i \times T_{i+p} \times \cdots \times T_{i+k-p} \cong T^{k/p} \tag{3}$$

for each $i \in \{1, \ldots, p\}$.

(i) *Then x acts transitively on $\{X_1, \ldots, X_p\}$ and x^p normalises each X_i, inducing the automorphism $(y, 1, \ldots, 1)\mu_i \in \mathrm{Aut}(X_i)$, where $\mu_i = (i, i+p, \ldots, i+k-p)$.*

(ii) *Suppose D is a diagonal subgroup of $X_1 \times \cdots \times X_p$ of the form*

$$D = \{(z, z^{\varphi_1}, \ldots, z^{\varphi_{p-1}}) : z \in X_1\} \cong T^{k/p} \tag{4}$$

with $\varphi_i \in \mathrm{Aut}(X_1)$. Then x normalises D if and only if $\varphi_i = \varphi_1^i$ for each i and $x^p = \varphi_1^p$ as automorphisms of X_1.

We will also need the next two results on the maximal subgroups of G containing x. The first one follows by combining [2, Theorems 1 and 5]. Since the proof is so much simpler in this case, we give details.

Lemma 2.5. *Let H be a maximal subgroup of G containing x. Then either*

(i) *$H = N_G((M \cap T)^k)$, where M is a maximal subgroup of A containing y; or*

(ii) *$H = N_G(D)$, where $D \cong T^{k/p}$ is a diagonal subgroup of N and p is a prime divisor of k.*

Proof. Set $J = H \cap N$ and suppose $J = 1$. Then $H = \langle x\rangle$ since G/N is cyclic. If x has order coprime to $|N|$, then x normalises a Sylow subgroup of N, otherwise $x \in N_G(C_N(z))$ for some element $z \in H$ of prime order. Plainly in both cases we get a contradiction, whence J is nontrivial.

Suppose the projection of J into T_ℓ is not surjective for some ℓ. Then x normalises $J_1 \times \cdots \times J_k$, where J_i is the image of the i-th projection, and it follows that y normalises each J_i. Replace J_1 by a maximal y-invariant subgroup of T_1 (so $M = N_A(J_1)$ is a maximal subgroup of A). Since x permutes the components transitively and y normalises each J_i, it follows that $J_i = J_1^{x^{i-1}}$ and so (i) holds.

For the remainder, we may assume that each projection of J into T_i is surjective. It follows that $J \cong S_1 \times \cdots \times S_m$ for some $m \geqslant 1$, where each S_i is isomorphic to T. Let Y_j be the direct product of the T_i such that S_j projects onto T_i. Then $N = Y_1 \times \cdots \times Y_m$ and since x acts transitively on $\{T_1, \ldots, T_k\}$, it follows that x permutes the Y_i. Therefore, $k = mr$ for some r and we have $J = D_1 \times \cdots \times D_m$, where $D_i \cong T$ is a diagonal subgroup of Y_i.

Suppose r is composite. Then the set of components in Y_1 is not a minimal block for the permutation action of x on $\{T_1, \ldots, T_k\}$. Therefore, we can write $Y_1 = Z_1 \times \cdots \times Z_s$, where the components of Z_i form a minimal block of prime size r/s, and we see that x normalises the product of the E_{ij}, where $E_{ij} \cong T$ is the inverse image of the projection of D_i into Z_j. This contradicts the maximality of H and so r is prime and $J \cong T^{k/r}$. Therefore (ii) holds and H is completely determined by D_1 (which corresponds to a minimal block of imprimitivity containing T_1). □

The next result is essentially a special case of the main results of [2]. It also follows from Lemma 2.5.

Lemma 2.6. *Let p be a prime divisor of k and define X_i as in (3). Let H be a maximal subgroup of G containing x such that the projection of $H \cap N$ onto X_1 is surjective. Then $H = N_G(D)$ where $D = D_\varphi$ is a diagonal subgroup of N of the form*

$$D_\varphi = \{(z, z^\varphi, z^{\varphi^2}, \ldots, z^{\varphi^{p-1}}) \,:\, z \in X_1\} \tag{5}$$

and φ is an automorphism of X_1 with $\varphi^p = x^p$. Moreover, p^2 does not divide k.

Proof. Since x acts transitively on $\{X_1, \ldots, X_p\}$, it follows that the projection of $H \cap N$ into each X_i is surjective. Then by applying the main theorem of [2], or by inspecting the proof of Lemma 2.5, we deduce that each maximal subgroup of G containing $H \cap N$ is the normaliser of a diagonal subgroup D of N corresponding to a minimal x-invariant partition of $\{T_1, \ldots, T_k\}$ of size r with r prime. In particular, $D \cong T^{k/r}$.

Let $Y = T_1 \times T_{k/r+1} \times \cdots \times T_{k+1-k/r} \cong T^r$ be the product of the components of N corresponding to the r conjugates of T_1 under $\langle x^{k/r} \rangle$. Suppose that either $r \neq p$ or p^2 divides k. Then $Y \leqslant X_1$ and thus D projects onto Y (since it projects onto X_1). But by the proof of Lemma 2.5 (or the main theorem of [2]), we see that the image of the projection of D into Y is isomorphic to T. This is a contradiction and we conclude that $r = p$ and p^2 does not divide k. Finally, since x normalises D, we deduce that D has the given form by applying Lemma 2.4(ii). □

Although stronger versions of the following result are available, this will be sufficient for our application.

Lemma 2.7. *Suppose $G = \langle N, z \rangle$, where $z \in \mathrm{Aut}(N)$ transitively permutes the components of N. If $G = \langle h, z \rangle$ for some $h \in N$ with $h^N = h^{\mathrm{Aut}(N)}$, then*

$$|C_{\mathrm{Aut}(N)}(z)| \leqslant |N : C_N(h)| \leqslant \frac{1}{3^k}|N|.$$

Proof. Set $Z = C_{\mathrm{Aut}(N)}(z)$. Since G contains N we have $C_{\mathrm{Aut}(N)}(G) = 1$ and thus $C_Z(h) = Z \cap C_{\mathrm{Aut}(N)}(h) = 1$. Therefore $|Z| = |h^Z| \leqslant |h^{\mathrm{Aut}(N)}| = |h^N|$. Since $h^N = h^{\mathrm{Aut}(N)}$, each coordinate of h is nontrivial and thus $|C_N(h)| \geqslant 3^k$ (there are no self-centralising involutions in T). □

Remark 2.8. We will apply Lemma 2.7 in the proof of Theorem 2.13. In this setting, we will work with an element $z \in G$ such that for any nontrivial $h \in N$ there exists $g \in G$ such that $G = \langle h^g, z\rangle$. We can then apply the lemma because there exists an involution $h \in N$ with $h^N = h^{\mathrm{Aut}(N)}$ by [31, Lemma 12.1].

The proof of our main reduction theorem (see Theorem 2.13) relies on the following deep result for almost simple groups. As explained in the proof below, this follows by combining earlier work in the literature with the proof of Theorem 8 in this paper.

Theorem 2.9. *Let $G = \langle G_0, g\rangle$ be an almost simple group with socle G_0 and assume that $G \neq \mathrm{Sym}_6$. Then $u(G) \geqslant 2$, and this is witnessed by a class y^G such that*

(i) *the order of $\langle y\rangle \cap G_0$ does not divide 4; or*
(ii) *$\langle y\rangle \cap G_0$ is nontrivial and y is not a square in $\mathrm{Aut}(G_0)$; or*
(iii) *$G = \mathrm{Alt}_6$ and y has order 4.*

Remark 2.10. As noted in the proof below, if $G = G_0 = \mathrm{Alt}_6$ then y^G with $y = (1,2,3,4)(5,6)$ is the only class to witness the bound $u(G) \geqslant 2$. Here $\langle y\rangle \cap G_0 = \langle y\rangle$ has order 4 and y is a square in $\mathrm{Aut}(G_0)$, which explains why (iii) is required in the statement of Theorem 2.9.

Proof of Theorem 2.9. First assume that $G_0 \neq \mathrm{Alt}_6$. As explained in Section 1, by combining Theorem 8 (which is of course independent of the reduction theorems we are considering here) with the main results in [10, 14, 15, 37, 38] we see that $u(G) \geqslant 2$ is witnessed by a class y^G, say. Since y is necessarily not contained in any proper normal subgroup of G, without loss of generality we may assume that $y^G \subseteq G_0 g$. Therefore, it suffices to show that y can always be chosen to satisfy one of the conditions (i) or (ii) in the statement.

First assume that G_0 is alternating or sporadic (we continue to assume that $G_0 \neq \mathrm{Alt}_6$). Suppose $G \neq G_0$, which implies that $G = \mathrm{Aut}(G_0)$ and $|G : G_0| = 2$. Here $G_0 g$ is not a square in $\mathrm{Out}(G_0)$ and therefore $y \in G_0 g$ is not a square in $\mathrm{Aut}(G_0)$. Moreover, for any involution $x \in G$ there exists $h \in G$ such that $G = \langle x, y^h\rangle$, which implies that $|y| > 2$ and thus $\langle y\rangle \cap G_0 \geqslant \langle y^2\rangle \neq 1$, so condition (ii) holds. Now assume G is simple. Here we inspect the class y^G identified in [10] that witnesses $u(G) \geqslant 2$. If $G = \mathrm{Alt}_n$, then $y = (1, \ldots, n)$ if $n \geqslant 5$ is odd (see [10, Proposition 6.7]) and $y = (1, \ldots, m-k)(m-k+1, \ldots, n)$ if $n = 2m \geqslant 8$ is even, where $k = m - (2, m-1)$ (see [10, Proposition 6.3]). If G is sporadic, then the class y^G is given in [10, Table 7]. In all cases, $|y| \geqslant 5$, so condition (i) is satisfied.

Next assume G_0 is a group of Lie type and let y^G be the class identified in the relevant reference above, which witnesses $u(G) \geqslant 2$. If $G = \mathrm{Aut}(G_0)$ and $|G : G_0|$ is even, then condition (ii) is satisfied. Otherwise, by considering each case in turn, we see that $y^{|G:G_0|} \in G_0$ has order at least 5 and thus condition (i) holds. For instance, if $G_0 = E_8(q)$ and $|G : G_0| = e > 1$, then in the proof of Theorem 5.2 we choose y such that $|y^e| = q_0^8 + q_0^7 - q_0^5 - q_0^4 - q_0^3 + q_0 + 1 \geqslant 331$, where $q = q_0^e$.

To complete the proof of the theorem, we may assume that $G = \langle G_0, g\rangle$ with $G_0 = \mathrm{Alt}_6$, and further that $G \neq \mathrm{Sym}_6$. If $G = \mathrm{Alt}_6$, then an easy computation in Magma [7] demonstrates that $u(G) \geqslant 2$ and the unique class to witness this is $(1,2,3,4)(5,6)^G$, so (iii) holds. Now assume G is a cyclic extension of G_0 isomorphic to either $\mathrm{PGL}_2(9)$ or M_{10}. Here a Magma computation shows that $u(G) \geqslant 2$, witnessed by y^G, say. Condition (ii) is satisfied as $|y| > 2$ and $y \in G_0 g$ is not square in $\mathrm{Aut}(G_0)$ since $G_0 g$ is not square in $\mathrm{Out}(G_0) = C_2 \times C_2$. □

The following result, which also follows from the main lemma of [55, Section 2], is an immediate corollary of Theorem 2.9 (note that the result is trivial for $G = \mathrm{Sym}_6$).

Corollary 2.11. *Let G be an almost simple group with socle G_0. Then for all $g \in G \setminus G_0$, there exists $h \in G_0 g$ such that the order of h is greater than the order of $G_0 g \in G/G_0$.*

2.2. **The main reduction theorem.** Let G be a finite group with a unique minimal normal subgroup $N = T_1 \times \cdots \times T_k$, where each T_i is isomorphic to a fixed nonabelian simple group T and $N_G(T_i)/C_G(T_i) \cong A = \langle T, y\rangle$ for each i. Let us assume that G/N is cyclic.

As previously explained, we may assume that $G = G_k = \langle N, x\rangle$ (see (2)), where

$$x = (y, 1, \ldots, 1)\sigma, \;\; \sigma = (1, \ldots, k) \in \mathrm{Sym}_k.$$

Moreover, in this section we will assume that $A \neq \mathrm{Sym}_6$ (the special case $A = \mathrm{Sym}_6$ will be addressed in Section 2.3). This means that we may, and will, assume that the element y in the definition of x satisfies the conclusions of Theorem 2.9, namely:

(I) For all nontrivial $r, s \in A$, there exists $z \in A$ such that $A = \langle r^z, y\rangle = \langle s^z, y\rangle$;
(II) $\langle y\rangle \cap T \neq 1$; and
(III) If y is a square in $\mathrm{Aut}(T)$, then either $|\langle y\rangle \cap T|$ does not divide 4, or $A = \mathrm{Alt}_6$ and $|y| = 4$.

In particular, for $k = 1$ we observe that x^{G_k} witnesses $u(G_k) \geqslant 2$.

Our first result handles the special case where k is a power of 2.

Theorem 2.12. *If $A \neq \mathrm{Sym}_6$ and $k = 2^e \geqslant 2$, then x^{G_k} witnesses $u(G_k) \geqslant 2$.*

Proof. We proceed by induction on e. Notice that it suffices to show that for any elements $a, b \in G_k$ of prime order, there exists $g \in G_k$ such that $G_k = \langle a, x^g\rangle = \langle b, x^g\rangle$.

First assume $e = 1$, so $G = G_2 = \langle N, x\rangle$, where $N = T_1 \times T_2$ and $x^2 = (y, y)$. The special case $A = \mathrm{Alt}_6$ can be checked by direct computation, so we will assume $A \neq \mathrm{Alt}_6$ for the remainder of the proof for $k = 2$.

Suppose $a, b \in G$ have prime order. There are two types of prime order elements in G, namely:

(i) Elements $(a_1, a_2) \in \mathrm{Aut}(T_1) \times \mathrm{Aut}(T_2)$ of prime order; and
(ii) Involutions of the form $(a_1, a_1^{-1})\sigma$ with $a_1 \in \mathrm{Aut}(T_1)$.

Note that elements of type (ii) exist if and only if $Ty \in A/T$ has odd order. These two types of prime order elements give us three separate cases to consider.

Case 1. $a = (a_1, a_2)$ and $b = (b_1, b_2)$.

Suppose that for each i, either a_i or b_i is trivial. In view of (I) above, by conjugating we may assume that $\langle a, x^2\rangle$ projects onto T_1 or T_2. By applying Lemma 2.6, it follows that any maximal overgroup of $\langle a, x\rangle$ in G is of the form $N_G(D_\varphi)$, where

$$D_\varphi := \{(z, z^\varphi) \,:\, z \in T_1\} \tag{6}$$

for some $\varphi \in \mathrm{Aut}(T_1)$. But since a has at least one trivial component, it does not normalise such a diagonal subgroup and thus $G = \langle a, x\rangle$. Similarly, we deduce that $G = \langle b, x\rangle$.

We can now assume that a_i and b_i are both nontrivial for some i. By conjugating a and b simultaneously, we may assume that a_1 and b_1 are nontrivial. By a further conjugation, and by appealing to condition (I) above, we may assume that $\langle a_1, y\rangle$ and $\langle b_1, y\rangle$ project onto T_1. Then Lemma 2.6 implies that $G \neq \langle a, x\rangle$ if and only if $\langle a, x\rangle$ normalises a diagonal subgroup D_φ of N as in (6), where $\varphi \in \mathrm{Aut}(T_1)$ and $\varphi^2 = y$ as automorphisms of T_1. Note that in this situation we have $a_2 = a_1^\varphi$ and

$$(y, y) \in \{(z, z^\varphi) \,:\, z \in \mathrm{Aut}(T_1)\},$$

so $y^\varphi = y$. Moreover, since $\langle a_1, y\rangle$ projects onto T_1, it follows that φ is uniquely determined by a_1^φ and we deduce that a is contained in the normaliser of at most one such diagonal subgroup. Similarly, b normalises at most one such subgroup.

Suppose $\langle a, x\rangle$ normalises D_φ. Let $c = (1, t) \in N$ with $t \in \langle y\rangle \cap T_2$, so $a^c = (a_1, a_2^t)$. If $G \neq \langle a^c, x\rangle$ then by arguing as above we see that $\langle a^c, x\rangle$ normalises D_θ for some $\theta \in \mathrm{Aut}(T_1)$ with $\theta^2 = y$ and $a_2^t = a_1^\theta$. Then $a_1^{\varphi t} = a_1^\theta$ and thus $\varphi t = \theta$ since both automorphisms are uniquely determined by their effect on a_1. Since t and φ commute, it follows that

$$yt^2 = \varphi^2 t^2 = (\varphi t)^2 = \theta^2 = y$$

and thus $t^2 = 1$, so either $|\langle y\rangle \cap T_2|$ is odd and $t = 1$, or there are two possibilities for t. In view of (III) above, noting that y is a square in $\mathrm{Aut}(T_1)$, we see that $|\langle y\rangle \cap T_2|$ does not divide 4. By combining these observations, it follows that if we choose $t \in \langle y\rangle \cap T_2$ at random then $t^2 = 1$ with probability at most $1/3$, whence $G = \langle a^c, x\rangle$ with probability at least $2/3$. The same argument applies with a^c replaced by b^c and we conclude that there exists $c \in N$ such that $G = \langle a^c, x\rangle = \langle b^c, x\rangle$.

Case 2. $a = (a_1, a_1^{-1})\sigma$ and $b = (b_1, b_1^{-1})\sigma$.

Suppose $a = (a_1, a_1^{-1})\sigma$ and $b = (b_1, b_1^{-1})\sigma$ are involutions in G. By conjugating, we may assume that both a_1 and b_1 are nontrivial, and then a second conjugation by a diagonal element allows us to assume that $\langle a_1, y\rangle$ and $\langle b_1, y\rangle$ both project onto T_1.

Suppose $G \neq \langle a, x\rangle$. Then Lemma 2.6 implies that $\langle a, x\rangle$ normalises a diagonal subgroup D_φ of N as in (6), where $\varphi \in \mathrm{Aut}(T_1)$ and $\varphi^2 = y$. Since $a = \sigma^{(1,a_1)}$ and the only diagonal subgroups of N normalised by σ are those of the form D_ψ with $\psi^2 = 1$, it follows that any diagonal subgroup normalised by a is of the form $D_{\psi a_1}$ with $\psi^2 = 1$, whence $\varphi = \psi a_1$ and $(\psi a_1)^2 = y$. Similarly, if $G \neq \langle b, x\rangle$ then $(\theta b_1)^2 = y$ for some $\theta \in \mathrm{Aut}(T_1)$ with $\theta^2 = 1$.

If y is not a square in $\mathrm{Aut}(T)$, then $G = \langle a, x\rangle = \langle b, x\rangle$ and the result follows. So let us assume y is a square, so (III) implies that $|\langle y\rangle \cap T_2|$ does not divide 4. Let $c = (1, t) \in N$ with $t \in \langle y\rangle \cap T_2$ and note that $a^c = (a_1 t, t^{-1} a_1^{-1})\sigma$ and similarly for b^c. Suppose that a^c normalises D_φ with $\varphi^2 = y$. As above this implies that $\varphi = \psi a_1 t$ for some $\psi \in \mathrm{Aut}(T_1)$ with $\psi^2 = 1$. Then t and $\psi a_1 t$ both centralise y, so ψa_1 centralises y and therefore t as well. It follows that $t^2 = y(\psi a_1)^{-2}$. Clearly there are at most two elements in the cyclic group $\langle y\rangle \cap T_2$ with this property, so the condition in (III) implies that if we choose t at random, then the probability that $G = \langle a^c, x\rangle$ is at least $2/3$. By the same argument, $G = \langle b^c, x\rangle$ with probability at least $2/3$ and hence there exists $c \in N$ such that $G = \langle a^c, x\rangle = \langle b^c, x\rangle$.

Case 3. $a = (a_1, a_2)$ and $b = (b_1, b_1^{-1})\sigma$.

By conjugating, we may assume that $\langle a_1, y\rangle$ and $\langle b_1, y\rangle$ project onto T_1. As before, if neither a nor b normalise a diagonal subgroup, then $G = \langle a, x\rangle = \langle b, x\rangle$ and we are done.

Suppose $\langle a, x\rangle$ normalises D_φ, so $\varphi^2 = y$ and $a_2 = a_1^\varphi$. Consider an element $c = (1, t) \in N$ with $t \in \langle y\rangle \cap T_2$. By arguing as in Case 1, $G \neq \langle a^c, x\rangle$ if and only if $t^2 = 1$. Similarly, by recalling the argument in Case 2 we see that $G \neq \langle b^c, x\rangle$ if and only if b^c normalises a diagonal subgroup D_θ, where $\theta^2 = y$ and $\theta = \psi b_1 t$ with $t^2 = y(\psi b_1)^{-2}$. As explained in Cases 1 and 2, if we choose $t \in \langle y\rangle \cap T_2$ at random then with positive probability we have $t^2 \neq 1$ and $t^2 \neq y(\psi b_1)^{-2}$, so there exists $c \in N$ with $G = \langle a^c, x\rangle = \langle b^c, x\rangle$.

To complete the argument we can assume that $G = \langle a^c, x\rangle$ for all $c = (1, t) \in N$ with $t \in \langle y\rangle \cap T_2$. Then by arguing as in Case 2, if we choose such an element c at random, then $G = \langle b^c, x\rangle$ with probability at least $2/3$. The result follows.

To complete the proof of the theorem, we may assume that $k = 2^e \geqslant 4$. Write $G = G_k = \langle N, x\rangle$, where $N = X_1 \times X_2$ and

$$X_1 = T_1 \times T_3 \times \cdots \times T_{k-1}, \quad X_2 = T_2 \times T_4 \times \cdots \times T_k$$

as in Lemma 2.4 (with $p = 2$). Let us observe that every element in G of prime order normalises X_1 and X_2.

Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$ be elements in G of prime order, where $a_i, b_i \in \mathrm{Aut}(X_i)$. By simultaneously conjugating a and b by a suitable element of G, and by applying the inductive hypothesis, we may assume that both $\langle a, x^2\rangle$ and $\langle b, x^2\rangle$ project onto at least one of X_1 and X_2. Since x interchanges X_1 and X_2, Lemma 2.6 implies that the only possible maximal overgroups of $\langle a, x\rangle$ in G are the normalisers of diagonal subgroups $D_\varphi \cong T^{k/2}$ of N as in (5), where $\varphi \in \mathrm{Aut}(X_1)$ and $\varphi^2 = x^2$ as automorphisms of X_1. However, there is no such automorphism φ by Lemma 2.3 and we conclude that $G = \langle a, x\rangle$. The same argument shows that $G = \langle b, x\rangle$ and the result follows. □

We can now establish our main reduction theorem.

Theorem 2.13. *If $A \neq \mathrm{Sym}_6$ and $k \geqslant 1$, then x^{G_k} witnesses $u(G_k) \geqslant 2$.*

Proof. We proceed by induction on k. As before, it suffices to show that for any elements $a, b \in G_k$ of prime order, there exists $g \in G_k$ such that $G_k = \langle a, x^g\rangle = \langle b, x^g\rangle$.

The base case $k = 1$ is clear since $x = y$ has been chosen via Theorem 2.9 so that x^{G_1} witnesses $u(G_1) \geqslant 2$. In addition, the result follows from Theorem 2.12 if $k = 2^e \geqslant 2$. Therefore, we may assume that k is divisible by an odd prime p. As in Lemma 2.4, let

$$X_i = T_i \times T_{i+p} \times \cdots \times T_{i+k-p} \cong T^{k/p}$$

for each $i \in \{1, \ldots, p\}$. Let a and b be elements of G_k of prime order. Note that the action of a (and similarly b) on $\{X_1, \ldots, X_p\}$ is either trivial or transitive (indeed, if a normalises some X_i, then it normalises every X_i). It follows that there are three cases to consider, according to the actions of a and b on $\{X_1, \ldots, X_p\}$. For the remainder of the proof, we will write $G = G_k$.

Case 1. Both a and b act trivially on $\{X_1, \ldots, X_p\}$.

First we assume a and b both normalise some (and hence all) X_i. Write

$$a = (a_1, \ldots, a_p), \quad b = (b_1, \ldots, b_p),$$

with $a_i, b_i \in \mathrm{Aut}(X_i)$.

Suppose that for each i, either a_i or b_i is trivial. By the inductive hypothesis, we can assume that $\langle a, x^p\rangle$ projects onto X_i for some i and similarly $\langle b, x^p\rangle$ projects onto X_j some j. By applying Lemma 2.6, it follows that any maximal overgroup of $\langle a, x\rangle$ in G is of the form $N_G(D_\varphi)$, where D_φ is a diagonal subgroup of N as in (5). But we are assuming that a has at least one trivial component, so $G = \langle a, x\rangle$ since a does not normalise such a diagonal subgroup. Similarly, we deduce that $G = \langle b, x\rangle$.

Therefore, we may assume that a_i and b_i are both nontrivial for some i. By conjugating a and b simultaneously, we may assume that a_1 and b_1 are nontrivial. Then by applying the inductive hypothesis, we can conjugate a and b simultaneously so that $\langle a, x^p\rangle$ and $\langle b, x^p\rangle$ both project onto X_1. As above, the only possible maximal overgroups of $\langle a, x\rangle$ in G are the normalisers of diagonal subgroups D_φ as in (5), where $\varphi \in \mathrm{Aut}(X_1)$ and $\varphi^p = x^p$ as automorphisms of X_1. The latter equality implies that

$$(x^p, \ldots, x^p) \in \{(z, z^\varphi, \ldots, z^{\varphi^{p-1}}) : z \in \mathrm{Aut}(X_1)\}$$

and thus $(x^p)^\varphi = x^p$. Moreover, since $\langle a_1, x^p\rangle$ projects onto X_1, we see that φ is uniquely determined by a_1^φ and thus a is contained in the normaliser of at most one such diagonal subgroup. Similarly, b normalises at most one such subgroup.

Suppose $G \neq \langle a, x\rangle$ and let $N_G(D_\varphi)$ be the unique maximal overgroup of $\langle a, x\rangle$ in G. Set $c = (1, 1, c_3, \ldots, c_p) \in N$ with $c_i \in X_i$, so $a^c = (a_1, a_2, a_3^{c_3}, \ldots, a_p^{c_p})$. Since the first component of a^c is a_1, the previous argument implies that either $G = \langle a^c, x\rangle$, or $\langle a^c, x\rangle$ normalises D_φ and

we have $a_i^{c_i} = a_1^{\varphi^{i-1}}$ for $i = 3, \ldots, p$. Since there are at most $|C_{X_i}(a_i)|$ elements $c_i \in X_i$ with $a_i^{c_i} = a_1^{\varphi^{i-1}}$, if we choose such an element c at random, then the probability that $G = \langle a^c, x\rangle$ is at least

$$1 - \prod_{i=3}^{p} |X_i : C_{X_i}(a_i)|^{-1} \geqslant \frac{4}{5}.$$

In the same way, the probability that $G = \langle b^c, x\rangle$ is at least $4/5$. Therefore, there exists c as above with $G = \langle a^c, x\rangle = \langle b^c, x\rangle$ and the result follows.

Case 2. Both a and b act transitively on $\{X_1, \ldots, X_p\}$.

Here a and b have order p and we may write

$$x = (x^p, 1, \ldots, 1)\gamma \in (\mathrm{Aut}(X_1) \times \cdots \times \mathrm{Aut}(X_p)){:}\mathrm{Sym}_p,$$

where $\gamma = (1, 2, \ldots, p) \in \mathrm{Sym}_p$ and we view x^p as an automorphism of X_1 (see Lemma 2.4(i)). Then

$$a = (a_1, \ldots, a_p)\gamma, \quad b = (b_1, \ldots, b_p)\gamma,$$

with $a_i, b_i \in \mathrm{Aut}(X_i)$. Note that $\prod_i a_i = \prod_i b_i = 1$ (since $|a| = |b| = p$).

Conjugating a and b simultaneously by an element $(c_1, 1, \ldots, 1) \in N$ with $c_1 \in X_1$, we may assume that both a_1 and b_1 are nontrivial. Then conjugating by an element of the form $(c, \ldots, c) \in N$, we may (by the inductive hypothesis) assume that $\langle a_1, x^p\rangle$ and $\langle b_1, x^p\rangle$ both contain subgroups projecting onto X_1. By Lemma 2.6, it follows that the only possible maximal subgroups of G containing either $\langle a, x\rangle$ or $\langle b, x\rangle$ are the normalisers of diagonal subgroups D_φ of N as in (5).

Suppose $G \neq \langle a, x\rangle$, so $\langle a, x\rangle$ normalises D_φ. Here $\varphi^p = x^p$ as automorphisms of X_1 and as in Case 1 we note that $(x^p)^\varphi = x^p$ and φ is uniquely determined by a_1^φ. Since $ax^{-1} = (a_1x^{-p}, a_2, \ldots, a_p)$ also normalises D_φ, it follows that $a_i = a_1^{\varphi^{i-1}}x^{-p}$ for $i = 2, \ldots, p$ and thus $N_G(D_\varphi)$ is the unique maximal overgroup of $\langle a, x\rangle$ in G.

Set $c = (1, \ldots, 1, d, 1) \in N$ with $d \in X_{p-1}$, so

$$a^c = (a_1, \ldots, a_{p-2}, d^{-1}a_{p-1}, a_pd)\gamma.$$

Notice that the first component of a^c is still a_1, so either $G = \langle a^c, x\rangle$, or a^c normalises D_φ. Let us assume a^c normalises D_φ. Then a^cx^{-1} also normalises D_φ and this implies that $d^{-1}a_{p-1}$ is $C_{\mathrm{Aut}(X_1)}(x^p)$-conjugate to a_1. Let $h \in X_1$ be an involution with $h^{X_1} = h^{\mathrm{Aut}(X_1)}$ (see Remark 2.8), so by the inductive hypothesis there exists $g \in \langle X_1, x^p\rangle$ such that $\langle X_1, x^p\rangle = \langle h^g, x^p\rangle$. Then by applying Lemma 2.7 we deduce that if we choose $d \in X_{p-1}$ at random, then the probability that $d^{-1}a_{p-1}$ is $C_{\mathrm{Aut}(X_1)}(x^p)$-conjugate to a_1 is at most $1/3$. In particular, the probability that $G = \langle a^c, x\rangle$ is at least $2/3$ and an entirely similar argument gives the same conclusion with a^c replaced by b^c. Therefore, there exists $c \in N$ as above such that $G = \langle a^c, x\rangle = \langle b^c, x\rangle$.

Case 3. a acts trivially and b act transitively on $\{X_1, \ldots, X_p\}$.

As above, we may write

$$a = (a_1, \ldots, a_p), \quad b = (b_1, \ldots, b_p)\gamma,$$

where $a_i, b_i \in \mathrm{Aut}(X_i)$ and $\gamma = (1, \ldots, p) \in \mathrm{Sym}_p$. By applying the inductive hypothesis, and by replacing a and b by suitable (simultaneous) conjugates, we may assume that $\langle a_1, x^p\rangle$ and $\langle b_1, x^p\rangle$ both project onto X_1. Then either $G = \langle a, x\rangle$, or $\langle a, x\rangle$ normalises a diagonal subgroup D_φ as in (5), where $\varphi \in C_{\mathrm{Aut}(X_1)}(x^p)$ and φ is uniquely determined by a_1^φ. And similarly for $\langle b, x\rangle$.

Set $c = (1, \ldots, 1, c_{p-1}, c_p) \in N$, where $c_{p-1} \in X_{p-1}$ and $c_p \in X_p \cap \langle x^p \rangle$. Then

$$b^c x^{-1} = (b_1 c_p x^{-p}, b_2, \ldots, b_{p-2}, c_{p-1}^{-1} b_{p-1}, c_p^{-1} b_p c_{p-1})$$

and we note that $\langle x^p, b_1 c_p \rangle$ projects onto X_1 (since $c_p \in \langle x^p \rangle$).

If $G \neq \langle b^c, x \rangle$ then $b^c x^{-1}$ must normalise a diagonal subgroup D_φ and thus $c_{p-1}^{-1} b_{p-1}$ is $C_{\mathrm{Aut}(X_1)}(x^p)$-conjugate to $b_1 c_p x^{-p}$. As we argued in Case 2, if we fix $c_p \in X_p \cap \langle x^p \rangle$ and we choose $c_{p-1} \in X_{p-1}$ at random, then the probability that $c_{p-1}^{-1} b_{p-1}$ is $C_{\mathrm{Aut}(X_1)}(x^p)$-conjugate to $b_1 c_p x^{-p}$ is at most $1/3$. In particular, the probability that $G = \langle b^c, x \rangle$ is at least $2/3$.

If $G \neq \langle a^c, x \rangle$ then a^c normalises some D_θ, where $a_p^{c_p} = a_1^{\theta^{p-1}}$ and θ is uniquely determined by a_1^θ. Since $(x^p)^\theta = x^p$ and $\langle a_1, x^p \rangle$ projects onto X_1, it follows that $\langle a_p, x^p \rangle$ projects onto X_p and thus the conjugates $a_p^{c_p}$ are distinct as c_p runs through $X_p \cap \langle x^p \rangle$. In particular, there is at most one c_p such that $a_p^{c_p} = a_1^{\theta^{p-1}}$. Therefore, if we fix $c_{p-1} \in X_{p-1}$ and choose $c_p \in X_p \cap \langle x^p \rangle$ at random, then the probability that $G = \langle a^c, x \rangle$ is at least $1 - |\langle x^p \rangle \cap X_p|^{-1} \geqslant 1/2$ (note that $\langle x^p \rangle \cap X_p \neq 1$ by condition (II) above).

Finally, by combining the two previous arguments we conclude that there exists $c \in N$ such that $G = \langle a^c, x \rangle = \langle b^c, x \rangle$. □

Subject to proving Theorem 8, by Theorem 2.13 we conclude that the proofs of Theorems 1 and 3 are complete, unless $A = \mathrm{Sym}_6$. The groups G_k for which $A = \mathrm{Sym}_6$ are handled in Theorem 2.15 in the following section.

2.3. **The special case $A = \mathrm{Sym}_6$.** For the proof of Theorem 2.15, it will be useful to introduce some additional notation. Let G be a finite group with a unique minimal normal subgroup N. Write $s_0(G)$ for the largest integer $k \geqslant 0$ such that for any nontrivial elements $x_1, \ldots, x_k$ of N, there exists $y \in G$ with $G = \langle x_i, y \rangle$ for all i. Define $u_0(G)$ in the same way, with the condition $y \in G$ replaced by $y \in C$, where C is a specified conjugacy class of G. Clearly, we have $s(G) \leqslant s_0(G)$ and $u(G) \leqslant u_0(G)$.

The following observation will be useful. Here G_k is defined as in (2).

Lemma 2.14. *We have $s_0(G_k) \leqslant s_0(A)$ and $u_0(G_k) \leqslant u_0(A)$.*

Proof. We prove the first inequality; the proof of the second is essentially the same. Write $s_0(A) = m - 1$ and fix nontrivial elements $y_1, \ldots, y_m \in T$ such that no element of A generates with each of the y_i. Seeking a contradiction, suppose that $s_0(G_k) \geqslant m$.

For each i, let $x_i = (y_i, 1, \ldots, 1) \in N$. Suppose that w generates with each x_i. Since w necessarily permutes the k factors of N transitively, by replacing w with a suitable power, we can assume that $w = (w_1, \ldots, w_k)\sigma$. Set $g = (1, w_2 w_3 \cdots w_k, w_3 \cdots w_k, \ldots, w_k) \in A^k$ and $v = w_1 \cdots w_k \in A$. Then $w^g = (v, 1, \ldots, 1)\sigma$ and $x_i^g = x_i$, whence $G_k^g = \langle x_i, w^g \rangle$ for all i. Since $\langle N, x^k \rangle = \langle N, x^k \rangle^g \leqslant G_k^g$, we deduce that $A = \langle y_i, v \rangle$ for all i and we have reached a contradiction. □

We now complete our reduction.

Theorem 2.15. *Suppose $G = G_k$ and $A = \mathrm{Sym}_6$. Then $s(G) = 2$ and $u(G) = 1 - \delta_{1,k}$.*

Proof. We begin by establishing upper bounds on $s(G)$ and $u(G)$. By Lemma 2.14 we have $s(G) \leqslant s_0(G) \leqslant s_0(A)$ and it is easy to check that $s_0(A) \leqslant 2$. For example, if we take $x_1 = (1,2)(3,4)$, $x_2 = (1,2)(5,6)$ and $x_3 = (3,4)(5,6)$ then there is no $y \in A$ such that $A = \langle x_i, y \rangle$ for all i. Similarly, it is easy to check that y^A witnesses $u_0(A) \geqslant 1$ if and only if y has order 6. But if we take $y = (1,2,3)(4,5)$, $x_1 = (1,2,3)$ and $x_2 = (4,5,6)$, then there is no $c \in A$ such that $G = \langle x_1, y^c \rangle = \langle x_2, y^c \rangle$. By applying an outer automorphism of A, we see that the class of 6-cycles in A also fails to witness $u_0(A) \geqslant 2$ and we conclude that $u(G) \leqslant u_0(G) \leqslant u_0(A) \leqslant 1$. We have now shown that $s(G) \leqslant 2$ and $u(G) \leqslant 1$.

The case $k = 1$ is an easy computation and it is also a special case of [15, Theorem 2(i)], which gives the exact spread and uniform spread of all symmetric groups (see also Remark 2.16). Similarly, if $k = 2$ then it is straightforward to verify the bounds $s(G) \geqslant 2$ and $u(G) \geqslant 1$ by direct computation, which gives $s(G) = 2$ and $u(G) = 1$. For the remainder of the proof, let us assume $k \geqslant 3$.

To show that $s(G) \geqslant 2$, which gives $s(G) = 2$, the argument is essentially identical to the general case handled above. As before we choose $y \in A$ such that $A = \langle T, y\rangle$ and we write $G = \langle N, x\rangle$ with $x = (y, 1, \ldots, 1)\sigma$ and $\sigma = (1, \ldots, k) \in \mathrm{Sym}_k$. Given elements $a, b \in G$ of prime order, the goal is to show that there exists $c \in G$ such that $G = \langle a^c, x\rangle = \langle b^c, x\rangle$. Since $s(A) = 2$ and $u(A) = 0$, the difference here is that we choose y (and hence x) according to the choice of a and b, rather than picking it uniformly as we did before.

To complete the proof, it remains to show that $u(G) \geqslant 1$ for $k \geqslant 3$. To do this, write $A = \langle T, y\rangle$ and $G = \langle N, x\rangle$, where $x = (y, 1, \ldots, 1)\sigma$ and $\sigma = (1, \ldots, k) \in \mathrm{Sym}_k$. We will show that if $a \in G$ has prime order, then there exists $c \in G$ such that $G = \langle a^c, x\rangle$.

First assume k is a prime and set $y = (1, 2, 3)(4, 5) \in A$. One checks that if $z \in A$ is nontrivial and not a transposition, then $A = \langle y^c, z\rangle$ for some $c \in A$. Therefore, we can proceed as in the proof of Theorem 2.13, unless $a = (a_1, \ldots, a_k) \in \mathrm{Aut}(T)^k$ and each a_i is a transposition. By conjugating by an element of $N = T^k$, we can assume that $A = \langle a_1, a_2, y\rangle$ and $a_3 = y^3 = (4, 5)$. In addition, we may assume that the projections of $\langle a, x^k\rangle$ on to T_1 and T_2 are $H_1 = \mathrm{Alt}_5$ (intransitive) and $H_2 = C_3 \times C_3$, respectively. Since $\mathrm{Alt}_6 = \langle H_1, H_2\rangle$ and x acts transitively on $\{T_1, \ldots, T_k\}$, it follows that $\langle a, x\rangle \cap N$ is a subdirect product of N and so either $G = \langle a, x\rangle$, or $\langle a, x\rangle$ normalises a diagonal subgroup D_φ of N. If $\langle a, x\rangle$ normalises D_φ, then $y^\varphi = y$ and $a_i = a_1^{\varphi^{i-1}}$ for $i = 2, \ldots, k$, so

$$A = \langle y^\varphi, a_1^\varphi, a_2^\varphi\rangle = \langle y, a_2, y^3\rangle = \langle y, a_2\rangle.$$

But this is a contradiction since $A \neq \langle y, z\rangle$ for all transpositions $z \in A$. The result follows.

Finally, if $k \geqslant 4$ is composite, then a suitably modified version of the induction proof for Theorem 2.13 goes through (but the argument here is easier since we only need to deal with a single element rather than a pair). □

Remark 2.16. For completeness, let us present a direct argument to show that $u(\mathrm{Sym}_6) = 0$. Let $G = \mathrm{Sym}_n$, where $n \geqslant 6$ is even. Suppose that $u(G) > 0$ is witnessed by the class x^G. Since a conjugate of x generates with $(1, 2, 3)$, x must be odd. Similarly, since a conjugate of x generates with $(1, 2)$, we see that x must have at most two cycles. Since n is even, it follows that x is a n-cycle. However, if $n = 6$ and $\varphi \in \mathrm{Aut}(G) \setminus G$, then $x^\varphi \in (1, 2, 3)(4, 5)^G$ also witnesses $u(G) > 0$, which is a contradiction.

We close this section by establishing, subject to proving Theorem 3, that there are infinitely many groups with spread two that are not almost simple.

Corollary 2.17. *Let $G = T \wr C_k$ where $k \geqslant 1$ and T is Alt_5, Alt_6, $\Omega_8^+(2)$ or $\mathrm{Sp}_{2r}(2)$ with $r \geqslant 3$. Then $s(G) = u(G) = 2$.*

Proof. As noted in (1), $s(T) = u(T) = 2$ by [10], so Lemma 2.14 implies that $u(G) \leqslant s(G) \leqslant 2$. Combining this with Theorem 3, we see that $u(G) \geqslant 2$ and hence $s(G) = u(G) = 2$. □

In view of the main results in this section, we have now reduced the proofs of Theorems 1 and 3 to the proof of Theorem 8. Strictly speaking, we need the slightly stronger conclusion given in Theorem 2.9, but this will follow easily from our proof. Therefore, for the remainder of the paper, our goal is to prove Theorem 8. We begin by recording some preliminary results for exceptional groups of Lie type.

3. Preliminaries on exceptional groups

In this section, we collect together some general results on almost simple exceptional groups of Lie type that will be crucial to our proof of Theorem 8. In addition, we will introduce the probabilistic approach for bounding the uniform spread of a finite group, which is at the heart of our proof, and we will discuss the relevant notation and set up for applying Shintani descent in this context.

For this discussion, it will be convenient to partition the finite simple exceptional groups over $\mathbb{F}_q$ into two collections:

$$\mathcal{A} = \{{}^2B_2(q),\ {}^2G_2(q)',\ {}^2F_4(q)',\ G_2(q)'\}$$
$$\mathcal{B} = \{E_8(q),\ E_7(q),\ E_6^\epsilon(q),\ F_4(q),\ {}^3D_4(q)\}.$$

The proof of Theorem 8 for the low rank groups with socle in $\mathcal{A}$ will be given in Section 4 and the remaining groups whose socle is in $\mathcal{B}$ will be handled in Sections 5–9.

Remark 3.1. In this paper, we always use expressions such as $E_7(q)$ and ${}^2E_6(q)$ to denote the corresponding *simple* groups.

3.1. **Subgroup structure.** Let G be a finite almost simple exceptional group of Lie type over $\mathbb{F}_q$ with socle G_0. Write $q = p^f$ with p prime. Let $\mathcal{M}$ be the set of maximal subgroups H of G with $G = HG_0$.

First assume $G_0 \in \mathcal{A} \cup \{{}^3D_4(q)\}$. In each of these cases, the maximal subgroups of G have been determined up to conjugacy. For $G_0 = {}^2F_4(q)'$ this is due to Malle [56] and in the other cases we refer the reader to the relevant table in [8, Chapter 8] for a convenient list of the subgroups that arise. These tables reproduce the original results of Suzuki [66] for ${}^2B_2(q)$, Cooperstein [22] for $G_2(q)'$ (q even) and Kleidman [41, 42] for $G_2(q)$ (q odd), ${}^2G_2(q)'$ and ${}^3D_4(q)$. We will make extensive use of this work in the proof of Theorem 8.

For the remainder of Section 3.1, we will assume $G_0 \in \mathcal{B}'$, where

$$\mathcal{B}' = \{E_8(q),\ E_7(q),\ E_6^\epsilon(q),\ F_4(q)\}.$$

Here we only have a complete description of the maximal subgroups of G up to conjugacy when G_0 is one of

$$E_7(2),\ E_6(2),\ {}^2E_6(2),\ F_4(2)$$

(see [3], [44], [21, 70] and [57], respectively). However, as described below, we are able to appeal to some powerful reduction theorems to obtain a very useful description of the maximal subgroups in the general cases.

Write $G_0 = (\bar{G}_\sigma)'$, where $\bar{G}$ is a simple algebraic group of adjoint type over the algebraic closure of $\mathbb{F}_p$ and σ is an appropriate Steinberg endomorphism of $\bar{G}$. The subgroups in $\mathcal{M}$ fall into several families according to the following fundamental theorem (see [49, Theorem 2]).

Theorem 3.2. *Let G be an almost simple group with socle $G_0 = (\bar{G}_\sigma)' \in \mathcal{B}'$ and let $H \in \mathcal{M}$. Then one of the following holds:*

(I) *$H = N_G(\bar{H}_\sigma)$ for a maximal closed σ-stable positive dimensional subgroup $\bar{H}$ of $\bar{G}$;*
(II) *H is of the same type as G (possibly twisted) over a subfield of $\mathbb{F}_q$;*
(III) *H is an exotic local subgroup (see [20]);*
(IV) *$G_0 = E_8(q)$, $p \geqslant 7$ and $H \cap G_0 = (\mathrm{Alt}_5 \times \mathrm{Alt}_6).2^2$;*
(V) *H is almost simple and not of type (I) or (II).*

In view of Theorem 3.2, it will be convenient to write

$$\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3 \tag{7}$$

where $\mathcal{M}_1$ comprises the maximal subgroups of type (I)–(IV) and $\mathcal{M}_2 \cup \mathcal{M}_3$ is the remaining collection of almost simple subgroups of type (V). Specifically, if H is a type (V) subgroup

with socle S and $\mathrm{Lie}(p)$ denotes the set of finite simple groups of Lie type over a field of characteristic p, then we write $H \in \mathcal{M}_2$ if $S \in \mathrm{Lie}(p)$ and $H \in \mathcal{M}_3$ otherwise.

Through the work of numerous authors, the subgroups comprising $\mathcal{M}_1$ are well understood and they have been determined up to conjugacy. However, there is no equivalent result for the subgroups in $\mathcal{M}_2 \cup \mathcal{M}_3$, although there has been some substantial progress. In particular, there is a short list of possibilities for S up to isomorphism (see Theorem 3.4 below for $\mathcal{M}_2$ and [50, 53] for $\mathcal{M}_3$), but the conjugacy problem remains open in general. Extensive ongoing work of Craven [23, 24, 25] seeks to significantly shorten the list of candidate subgroups in $\mathcal{M}_2 \cup \mathcal{M}_3$, with the ultimate goal of a complete classification.

The remainder of this section is dedicated to deducing the information we need on the subgroups in $\mathcal{M}$ for the proof of Theorem 8. We begin by studying the conjugacy classes of subgroups in $\mathcal{M}_1$. Recall our convention that logarithms are base two.

Proposition 3.3. *The number of $\bar{G}_\sigma$-classes of subgroups in $\mathcal{M}_1$ is at most $a(G_0) + \log\log q$, where*

G_0	$F_4(q)$	$E_6^\epsilon(q)$	$E_7(q)$	$E_8(q)$
$a(G_0)$	25	25	30	49

Proof. The argument is similar in each case and we just give details for $G_0 = E_8(q)$. First consider the subgroups of type (I) in Theorem 3.2, so $H = N_G(\bar{H}_\sigma)$. Clearly, there are 8 classes of maximal parabolic subgroups (one for each node in the Dynkin diagram) and by inspecting [48] we find that there are at most 29 additional classes of maximal subgroups of type (I) with $\bar{H}$ of maximal rank. The remaining possibilities for H are listed in [51, Table 3], together with the case recorded in [51, Theorem 8(I)(d)]; this gives at most 9 further classes. Altogether, this demonstrates that there are at most 46 classes of maximal subgroups in $\mathcal{M}_1$ of type (I). The subgroups of type (II) are subfield subgroups; there is a unique class for each maximal subfield of $\mathbb{F}_q$ and there are at most $\log\log q$ such subfields (this is an upper bound on the number of prime divisors of f, where $q = p^f$). By the main theorem of [20], there are at most 2 classes of subgroups of type (III) and there is at most 1 additional class of type (IV). By bringing the above estimates together, we conclude that there are at most $49 + \log\log q$ distinct $\bar{G}_\sigma$-classes of subgroups in $\mathcal{M}_1$. □

Now assume that $H \in \mathcal{M}_2 \cup \mathcal{M}_3$ and let S be the socle of H. Note that S is a subgroup of G_0. The following result significantly restricts the subgroups in $\mathcal{M}_2$ (see [51, Theorem 8], noting that the value of $b(E_8(q))$ in part (iii) is taken from [45]). In the statement, if X is a simple group of Lie type, then $\mathrm{rk}(X)$ denotes the untwisted Lie rank of X (that is, $\mathrm{rk}(X)$ is the rank of the ambient simple algebraic group).

Theorem 3.4. *Suppose that $H \in \mathcal{M}_2$ has socle S, a simple group of Lie type over $\mathbb{F}_t$, where t is a power of p. Then $\mathrm{rk}(S) \leqslant \frac{1}{2}\mathrm{rk}(G_0)$ and one of the following holds:*

(i) $t \leqslant 9$;
(ii) $S = \mathrm{L}_3^\epsilon(16)$;
(iii) $S \in \{\mathrm{L}_2(t), {}^2B_2(t), {}^2G_2(t)\}$, *where* $t \leqslant (2, q-1)\, b(G_0)$ *and*

G_0	$F_4(q)$	$E_6^\epsilon(q)$	$E_7(q)$	$E_8(q)$
$b(G_0)$	68	124	388	1312

It remains to discuss the situation where $H \in \mathcal{M}_3$. In this case, the possibilities for S (up to isomorphism) are described in [50] (see [50, Tables 10.1–10.4]) and we note that substantial refinements are established in [23, 24, 25, 53]. For instance, the main theorem of [23] states that if $S = \mathrm{Alt}_n$ then $n = 6$ and $n = 7$ are the only options, whereas [50] gives $n \leqslant 18$.

TABLE 1. Bounds on $\mathrm{meo}(\mathrm{Aut}(S))$, S exceptional, $\mathrm{rk}(S) \leqslant 4$

S	$c(S)$
$F_4(t)$	$32(t+1)(t^3-1)\log t$
$G_2(t)$	$8(t^2+t+1)\log t$
${}^2F_4(t)$, $t = 2^{2k+1}$, $k \geqslant 1$	$16(2k+1)(2^{4k+2}+2^{3k+2}+2^{2k+1}+2^{k+1}+1)$
${}^2F_4(2)'$	20
${}^3D_4(t)$	$24(t^3-1)(t+1)\log t$
${}^2G_2(t)$, $t = 3^{2k+1}$, $k \geqslant 1$	$(2k+1)(3^{2k+1}+3^{k+1}+1)$
${}^2G_2(3)'$	9
${}^2B_2(t)$, $t = 2^{2k+1}$, $k \geqslant 1$	$(2k+1)(2^{2k+1}+2^{k+1}+1)$

We conclude this section by studying the maximal order of an element in a subgroup contained in $\mathcal{M}_2 \cup \mathcal{M}_3$. Given a subset X of a finite group, set

$$\mathrm{meo}(X) = \max\{|x| : x \in X\}.$$

The following result gives an upper bound on $\mathrm{meo}(H)$, where H is almost simple and either classical or a low rank exceptional group.

Proposition 3.5. *Let S be a finite simple group of Lie type over $\mathbb{F}_t$ with $\mathrm{rk}(S) = m$.*

(i) *If S is a classical group, then either*

$$\mathrm{meo}(\mathrm{Aut}(S)) \leqslant \frac{t^{m+1}}{t-1},$$

or $S = \mathrm{PSp}_4(2)'$ and $\mathrm{meo}(\mathrm{Aut}(S)) = 10$.

(ii) *If S is an exceptional group with $m \leqslant 4$, then $\mathrm{meo}(\mathrm{Aut}(S)) \leqslant c(S)$, where $c(S)$ is given in Table 1.*

Proof. Part (i) is an immediate corollary of [34, Theorem 2.16]. For (ii), we argue as in the proof of [34, Theorem 1.2] (see [34, p.7683]). If t is odd, then $\mathrm{meo}(S)$ is given in [39, Table A.7] and the result follows from the trivial bound

$$\mathrm{meo}(\mathrm{Aut}(S)) \leqslant |\mathrm{Out}(S)|\,\mathrm{meo}(S). \tag{8}$$

Now assume t is even. For $S = {}^2B_2(t)$ with $t = 2^{2k+1} > 2$, we have $\mathrm{meo}(S) = 2^{2k+1}+2^{k+1}+1$ (see [66, Proposition 16]) and the bound in Table 1 follows via (8). In the remaining cases, we use

$$\mathrm{meo}(\mathrm{Aut}(S)) \leqslant \alpha\beta|\mathrm{Out}(S)|,$$

where α and β are upper bounds on the maximal orders of semisimple and unipotent elements in S, respectively (see the proof of [34, Theorem 1.2]). Expressions for α and β are given in [34, Table 5] and the desired result follows. □

Remark 3.6. For $S = \mathrm{L}_d^\epsilon(t)$, the precise value of $\mathrm{meo}(\mathrm{Aut}(S))$ is recorded in [34, Table 3]. In particular, we note that $\mathrm{meo}(\mathrm{Aut}(\mathrm{L}_3(16))) = 273$ and $\mathrm{meo}(\mathrm{Aut}(\mathrm{U}_3(16))) = 255$.

For the subgroups in $\mathcal{M}_3$, we have the following result on element orders.

Proposition 3.7. *Suppose $H \in \mathcal{M}_3$. Then $\mathrm{meo}(H) \leqslant d(G_0)$, where*

G_0	$F_4(q)$	$E_6^\epsilon(q)$	$E_7(q)$	$E_8(q)$
$d(G_0)$	40	60	63	210

Proof. Let S be the socle of H. As previously noted, the possibilities for S (up to isomorphism) are recorded in [50, Tables 10.1–10.4] and it is straightforward to determine $\mathrm{meo}(\mathrm{Aut}(S))$ in every case, either via MAGMA [7] or by inspecting the ATLAS [21]. □

We will also need the following result to handle some special cases.

Proposition 3.8. *If* $S \in \{\mathrm{L}_4(8), \mathrm{U}_5(8), \mathrm{PSp}_6(8), G_2(8), G_2(9)\}$, *then*

$$\mathrm{meo}(\mathrm{Aut}(S) \setminus S) \leqslant e(S),$$

where

S	$\mathrm{L}_4(8)$	$\mathrm{U}_5(8)$	$\mathrm{PSp}_6(8)$	$G_2(8)$	$G_2(9)$
$e(S)$	130	130	45	36	36

Proof. This can be verified with MAGMA [7], using `AutomorphismGroupSimpleGroup` to construct suitable permutation representations of the relevant automorphism groups. □

3.2. **Automorphisms.** Continue to assume that G_0 is a finite simple exceptional group of Lie type over $\mathbb{F}_q$ and write $q = p^f$ where p is prime. In this section we determine the precise list of almost simple groups with socle G_0 that we need to consider in order to prove Theorem 8. Naturally, this will involve a careful study of the automorphisms of G_0 and the structure of the outer automorphism group $\mathrm{Out}(G_0) = \mathrm{Aut}(G_0)/G_0$. Our main result to this end is Proposition 3.15.

In this discussion, for clarity of exposition, we will assume that G_0 is not one of

$$G_2(2)' \cong \mathrm{U}_3(3),\ {}^2F_4(2)',\ {}^2G_2(3)' \cong \mathrm{L}_2(8). \tag{9}$$

(In the first two cases, $\mathrm{Aut}(G_0) = G_0.2$ and in the latter we have $\mathrm{Aut}(G_0) = G_0.3$.) Let us partition the remaining possibilities for G_0 into three classes:

$$E_8(q),\ E_7(q),\ E_6^{\epsilon}(q),\ F_4(q)\,(p \neq 2),\ G_2(q)\,(p \neq 3),\ {}^3D_4(q) \tag{10}$$

$$F_4(2^f),\ G_2(3^f) \tag{11}$$

$${}^2F_4(2^{2k+1}),\ {}^2G_2(3^{2k+1}),\ {}^2B_2(2^{2k+1}). \tag{12}$$

We begin by describing $\mathrm{Aut}(G_0)$, where we follow [32, Chapter 2.5] (see [32, Theorem 2.5.12] in particular). Write $G_0 = (\bar{G}_\sigma)'$, where $\bar{G}$ is a simple algebraic group over $k = \bar{\mathbb{F}}_p$ of adjoint type and σ is a Steinberg endomorphism. We refer to $\bar{G}_\sigma$ as the *innerdiagonal group* of automorphisms of G_0 and we write $\bar{G}_\sigma = \mathrm{Inndiag}(G_0)$. We refer to the elements in $\mathrm{Inndiag}(G_0) \setminus G_0$ as *diagonal automorphisms*. Then $\mathrm{Aut}(G_0)$ is a split extension of $\mathrm{Inndiag}(G_0)$ by a soluble group generated by *field*, *graph* and *graph-field automorphisms* that are defined naturally from automorphisms of the underlying field $\mathbb{F}_q$ and symmetries of the Dynkin diagram of $\bar{G}$.

Let us fix our notation for automorphisms of G_0. In part (iii) of the following definition, we write D_4 for the adjoint group $\mathrm{PSO}_8(k)$.

Definition 3.9. Let $G_0 = (\bar{G}_\sigma)' = {}^dX(q)$ be a finite simple exceptional group as above and let φ be a standard Frobenius endomorphism of $\bar{G}$.

(i) If G_0 is not in (12), then we identify φ with the restriction $\varphi|_{G_0}$. Then $\varphi \in \mathrm{Aut}(G_0)$ is a field or graph automorphism such that $|\varphi| = df$.

(ii) If G_0 is in (11) or (12), then let ρ be the Steinberg endomorphism of $\bar{G}$ such that $\rho^2 = \varphi$ and identify ρ with the restriction $\rho|_{G_0}$. Then $\rho \in \mathrm{Aut}(G_0)$ is a graph-field automorphism with $|\rho| = 2f/d$.

(iii) Let γ be an involutory graph automorphism of $\bar{G} = E_6$ such that $[\varphi, \gamma] = 1$ and $C_{E_6}(\gamma) = F_4$, and identify γ with the restriction $\gamma|_{E_6^{\epsilon}(q)}$. Similarly, let τ be an order 3 triality graph automorphism of $\bar{G} = D_4$ with $[\varphi, \tau] = 1$ and $C_{D_4}(\tau) = G_2$, and identify τ with the restriction $\tau|_{{}^3D_4(q)}$.

(iv) If $G_0 = E_7(q)$ and q is odd, then fix a diagonal automorphism $\delta \in \mathrm{Inndiag}(G_0)$ of order 2. Similarly, if $G_0 = E_6^{\epsilon}(q)$ and $q \equiv \epsilon \pmod 3$, then let $\delta \in \mathrm{Inndiag}(G_0)$ be a diagonal automorphism of order 3.

TABLE 2. $\mathrm{Out}(G_0)$ for a finite simple exceptional group G_0

G_0		$\mathrm{Out}(G_0)$		Comments
$E_8(q)$		$\langle \ddot{\varphi} \rangle$	C_f	
$E_7(q)$	$p \neq 2$	$\langle \ddot{\delta} \rangle \times \langle \ddot{\varphi} \rangle$	$C_2 \times C_f$	
	$p = 2$	$\langle \ddot{\varphi} \rangle$	C_f	
$E_6(q)$	$q \not\equiv 1 \pmod 3$	$\langle \ddot{\gamma} \rangle \times \langle \ddot{\varphi} \rangle$	$C_2 \times C_f$	
	$q \equiv 1 \pmod 3$	$\langle \ddot{\delta}, \ddot{\gamma}, \ddot{\varphi} \rangle$	$\mathrm{Sym}_3 \times C_f$	See Lemma 3.10
${}^2E_6(q)$	$q \not\equiv 2 \pmod 3$	$\langle \ddot{\varphi} \rangle$	C_{2f}	$\ddot{\varphi}^f = \ddot{\gamma}$
	$q \equiv 2 \pmod 3$	$\langle \ddot{\delta}, \ddot{\varphi} \rangle$	$\mathrm{Sym}_3 \times C_f$	See Lemma 3.12
$F_4(q)$	$p \neq 2$	$\langle \ddot{\varphi} \rangle$	C_f	
	$p = 2$	$\langle \ddot{\rho} \rangle$	C_{2f}	$\ddot{\rho}^2 = \ddot{\varphi}$
$G_2(q)$	$p \neq 3, q > 2$	$\langle \ddot{\varphi} \rangle$	C_f	
	$p = 3$	$\langle \ddot{\rho} \rangle$	C_{2f}	$\ddot{\rho}^2 = \ddot{\varphi}$
${}^3D_4(q)$		$\langle \ddot{\varphi} \rangle$	C_{3f}	$\ddot{\varphi}^f = \ddot{\tau}$
${}^2F_4(q)$	$q > 2$	$\langle \ddot{\rho} \rangle$	C_f	
${}^2G_2(q)$	$q > 3$	$\langle \ddot{\rho} \rangle$	C_f	
${}^2B_2(q)$		$\langle \ddot{\rho} \rangle$	C_f	

For $g \in \mathrm{Aut}(G_0)$, we write $\ddot{g}$ for the coset $G_0 g$, so

$$\mathrm{Out}(G_0) = \{\ddot{g} : g \in \mathrm{Aut}(G_0)\}.$$

If G_0 is not $E_6^\epsilon(q)$, then the structure of $\mathrm{Out}(G_0)$ can be immediately deduced from [32, Theorem 2.5.12] and we present the details in Table 2. The structure of $\mathrm{Out}(E_6^\epsilon(q))$ is given in Lemmas 3.10 and 3.12 in the untwisted and twisted cases, respectively.

Lemma 3.10. *Let $G_0 = E_6(q)$. Then*

$$\mathrm{Out}(G_0) = \begin{cases} \langle \ddot{\gamma} \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_f & \text{if } q \not\equiv 1 \pmod 3 \\ \langle \ddot{\delta}, \ddot{\gamma}, \ddot{\varphi} \rangle \cong \mathrm{Sym}_3 \times C_f & \text{if } q \equiv 1 \pmod 3. \end{cases}$$

Proof. According to [32, Theorem 2.5.12(a)], we have $\mathrm{Aut}(G_0) = \mathrm{Inndiag}(G_0){:}\langle \gamma, \varphi \rangle$. In particular, if $q \not\equiv 1 \pmod 3$ then

$$\mathrm{Out}(G_0) = \langle \ddot{\gamma}, \ddot{\varphi} \rangle = \langle \ddot{\gamma} \rangle \times \langle \ddot{\varphi} \rangle \cong C_2 \times C_f$$

as claimed.

For the remainder, we may assume $q \equiv 1 \pmod 3$. Here

$$\mathrm{Out}(G_0) = \langle \ddot{\delta}, \ddot{\gamma}, \ddot{\varphi} \rangle \text{ and } |\ddot{\delta}| = 3,\ |\ddot{\gamma}| = 2,\ |\ddot{\varphi}| = f,\ [\ddot{\gamma}, \ddot{\varphi}] = 1,\ \ddot{\delta}^{\ddot{\gamma}} = \ddot{\delta}^{-1},\ \ddot{\delta}^{\ddot{\varphi}} = \ddot{\delta}^p \tag{13}$$

(for the final two claims, see [32, Theorem 2.5.12(i)] and [32, Theorem 2.5.12(g)], respectively). If $p \equiv 1 \pmod 3$, then $[\ddot{\delta}, \ddot{\varphi}] = 1$ and thus

$$\mathrm{Out}(G_0) = \langle \ddot{\delta}, \ddot{\gamma} \rangle \times \langle \ddot{\varphi} \rangle \cong \mathrm{Sym}_3 \times C_f.$$

Now assume that $p \equiv 2 \pmod 3$. Here the condition $q \equiv 1 \pmod 3$ implies that f is even, so $|\ddot{\gamma}\ddot{\varphi}| = f$. In addition, $[\ddot{\gamma}, \ddot{\gamma}\ddot{\varphi}] = 1$ and $[\ddot{\delta}, \ddot{\gamma}\ddot{\varphi}] = 1$, where the latter claim holds since $\ddot{\delta}^{\ddot{\gamma}\ddot{\varphi}} = (\ddot{\delta}^{-1})^{\ddot{\varphi}} = \ddot{\delta}$. Therefore,

$$\mathrm{Out}(G_0) = \langle \ddot{\delta}, \ddot{\gamma} \rangle \times \langle \ddot{\gamma}\ddot{\varphi} \rangle \cong \mathrm{Sym}_3 \times C_f. \qquad \square$$

For future reference, it will be convenient to record the following set of conditions:

$$p \equiv 2 \pmod 3,\ f \text{ is even and } i \text{ is odd.} \tag{14}$$

Lemma 3.11. *Let $G_0 = E_6(q)$ with $q \equiv 1 \pmod 3$ and fix an integer $0 \leqslant i < f$. Then the following hold:*

(i) $\ddot{\delta}\ddot{\varphi}^i$ *and* $\ddot{\delta}^2\ddot{\varphi}^i$ *are* $\mathrm{Out}(G_0)$*-conjugate.*

(ii) $\ddot{\delta}\ddot{\gamma}\ddot{\varphi}^i$ *and* $\ddot{\delta}^2\ddot{\gamma}\ddot{\varphi}^i$ *are* $\mathrm{Out}(G_0)$*-conjugate.*

(iii) $\ddot{\varphi}^i$ *and* $\ddot{\delta}\ddot{\varphi}^i$ *are* $\mathrm{Out}(G_0)$*-conjugate if each condition in* (14) *holds.*

(iv) $\ddot{\gamma}\ddot{\varphi}^i$ *and* $\ddot{\delta}\ddot{\gamma}\ddot{\varphi}^i$ *are* $\mathrm{Out}(G_0)$*-conjugate if any of the conditions in* (14) *fail to hold.*

Proof. Let $A = \langle \ddot{\delta}, \ddot{\gamma} \rangle \cong \mathrm{Sym}_3$ and note that the conjugacy classes of A are as follows:

$$\{\ddot{1}\},\ \{\ddot{\delta}, \ddot{\delta}^2\},\ \{\ddot{\gamma}, \ddot{\delta}\ddot{\gamma}, \ddot{\delta}^2\ddot{\gamma}\}.$$

If any one of the conditions in (14) is not satisfied, then $\ddot{\varphi}^i \in Z(\mathrm{Out}(G_0))$ and (i), (ii) and (iv) follow. On the other hand, if all the conditions in (14) are satisfied, then $\ddot{\gamma}\ddot{\varphi}^i \in Z(\mathrm{Out}(G_0))$ and by writing

$$\begin{gathered}\ddot{\delta}\ddot{\varphi}^i = \ddot{\delta}\ddot{\gamma}(\ddot{\gamma}\ddot{\varphi}^i) \text{ and } \ddot{\delta}^2\ddot{\varphi}^i = \ddot{\delta}^2\ddot{\gamma}(\ddot{\gamma}\ddot{\varphi}^i) \\ \ddot{\delta}\ddot{\gamma}\ddot{\varphi}^i = \ddot{\delta}(\ddot{\gamma}\ddot{\varphi}^i) \text{ and } \ddot{\delta}^2\ddot{\gamma}\ddot{\varphi}^i = \ddot{\delta}^2(\ddot{\gamma}\ddot{\varphi}^i) \\ \ddot{\varphi}^i = \ddot{\gamma}(\ddot{\gamma}\ddot{\varphi}^i) \text{ and } \ddot{\delta}\ddot{\varphi}^i = \ddot{\delta}\ddot{\gamma}(\ddot{\gamma}\ddot{\varphi}^i)\end{gathered}$$

we deduce that (i), (ii) and (iii) hold. □

We now turn to the twisted version of E_6.

Lemma 3.12. *Let $G_0 = {}^2E_6(q)$. Then*

$$\mathrm{Out}(G_0) = \begin{cases} \langle \ddot{\varphi} \rangle \cong C_{2f} & \text{if } q \not\equiv 2 \pmod 3 \\ \langle \ddot{\delta}, \ddot{\varphi} \rangle \cong \mathrm{Sym}_3 \times C_f & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

Proof. By [32, Theorem 2.5.12(a)], we have $\mathrm{Aut}(G_0) = \mathrm{Inndiag}(G_0){:}\langle\varphi\rangle$. Therefore, if $q \not\equiv 2 \pmod 3$, then $\mathrm{Out}(G_0) = \langle \ddot{\varphi} \rangle \cong C_{2f}$. For the remainder, let us assume $q \equiv 2 \pmod 3$. Here $p \equiv 2 \pmod 3$, f is odd and

$$\mathrm{Out}(G_0) = \langle \ddot{\delta}, \ddot{\varphi} \rangle \text{ and } |\ddot{\delta}| = 3,\ |\ddot{\varphi}| = 2f,\ \ddot{\delta}^{\ddot{\varphi}} = \ddot{\delta}^{-1} \tag{15}$$

(see [32, Theorem 2.5.12(g)] for the final claim). Since $\langle \varphi \rangle = \langle \varphi^f \rangle \times \langle \varphi^2 \rangle$, we obtain

$$\mathrm{Out}(G_0) = \langle \ddot{\delta}, \ddot{\varphi}^f \rangle \times \langle \ddot{\varphi}^2 \rangle \cong \mathrm{Sym}_3 \times C_f.$$ □

Lemma 3.13. *Let $G_0 = {}^2E_6(q)$ with $q \equiv 2 \pmod 3$ and fix an integer $0 \leqslant i < 2f$. Then the following hold:*

(i) $\ddot{\delta}\ddot{\varphi}^i$ *and* $\ddot{\delta}^2\ddot{\varphi}^i$ *are* $\mathrm{Out}(G_0)$*-conjugate.*

(ii) *If i is odd, then $\ddot{\varphi}^i$ and $\ddot{\delta}\ddot{\varphi}^i$ are* $\mathrm{Out}(G_0)$*-conjugate.*

Proof. By (15), we have $(\ddot{\delta}\ddot{\varphi}^i)^{\ddot{\varphi}} = \ddot{\delta}^2\ddot{\varphi}^i$. Moreover, if i is odd then

$$(\ddot{\varphi}^i)^{\ddot{\delta}} = \ddot{\delta}^{-1}\ddot{\varphi}^i\ddot{\delta} = \ddot{\delta}^{-1}\ddot{\delta}^{\ddot{\varphi}^{-i}}\ddot{\varphi}^i = \ddot{\delta}^{-1}\ddot{\delta}^{-1}\ddot{\varphi}^i = \ddot{\delta}\ddot{\varphi}^i$$

and the result follows. □

The following elementary lemma will be useful in the proof of Proposition 3.15 (for a proof, see [38, Lemma 5.2.1]).

Lemma 3.14. *Let $\langle a \rangle{:}\langle b \rangle$ be a semidirect product of finite cyclic groups. For all $i > 0$, there exist nonnegative integers j and k such that $\langle ab^i \rangle = \langle a^j b^k \rangle$ and k divides $|b|$.*

We now use the above information on $\mathrm{Out}(G_0)$ to determine the specific groups we need to consider in order to prove Theorem 8. Note that in Table 3, i is a proper divisor of f and the symbols $\star$ and † refer to notes presented in Remark 3.16.

TABLE 3. The automorphisms of $G_0 = E_6^\epsilon(q)$ in Proposition 3.15(iv)

ϵ	$\pm$	$\pm$	$+$	$+$	$+$	$-$	$-$	
g		γ	φ^i	$\gamma\varphi^i$	$\gamma\varphi^i$	$\gamma\varphi^i$	φ^i	(R1)
	δ		$\delta^\pm\varphi^i$	$\delta^\pm\gamma\varphi^i$		$\delta^\pm\gamma\varphi^i$		(R2)
f/i			any	even	odd	odd	any	
notes			$\star$	†				

Proposition 3.15. *Let G_0 be a finite simple exceptional group over $\mathbb{F}_q$, where $q = p^f$ with p prime. Assume G_0 is not one of the groups in* (9) *and let h be a non-inner automorphism of G_0. Then $\langle G_0, h\rangle$ is $\mathrm{Aut}(G_0)$-conjugate to $\langle G_0, g\rangle$, where $g \in \mathrm{Aut}(G_0)$ is one of the following:*

(i) *G_0 is in* (12) *and $g = \rho^i$ for a proper divisor i of f.*
(ii) *G_0 is in* (11) *and either*
  (a) *$g = \varphi^i$ for a proper divisor i of f; or*
  (b) *$g = \rho^i$ for an odd divisor i of f.*
(iii) *G_0 is in* (10)*, $G_0 \neq E_6^\epsilon(q)$, and either*
  (a) *$g = \varphi^i$ for a proper divisor i of f;*
  (b) *$G_0 = {}^3D_4(q)$ and $g = \tau\varphi^i$ for a divisor i of f; or*
  (c) *$G_0 = E_7(q)$ with q odd and g is δ or $\delta\varphi^i$ for a proper divisor i of f.*
(iv) *$G_0 = E_6^\epsilon(q)$ and either*
  (a) *g is in Row* (R1) *of Table 3; or*
  (b) *$q \equiv \epsilon \pmod 3$ and g is in Row* (R2) *of Table 3.*

Remark 3.16. In Table 3, the symbol $\delta^\pm$ denotes that we may consider either δ or δ^{-1} (but there is no need to consider both). The notes labelled $\star$ and † impose further restrictions on the automorphisms we need to consider:

- $\star$ We need only consider one of the automorphisms in $\{\varphi^i, \delta\varphi^i, \delta^2\varphi^i\}$ in the very special case when all the conditions in (14) are satisfied.
- † We need only consider one automorphism in $\{\gamma\varphi^i, \delta\gamma\varphi^i, \delta^2\gamma\varphi^i\}$ *unless* all the conditions in (14) hold.

Proof of Proposition 3.15. Since $\langle G_0, g\rangle$ and $\langle G_0, h\rangle$ are $\mathrm{Aut}(G_0)$-conjugate if and only if $\langle \ddot{g}\rangle$ and $\langle \ddot{h}\rangle$ are $\mathrm{Out}(G_0)$-conjugate, we must determine the conjugacy classes of cyclic subgroups of $\mathrm{Out}(G_0)$. Fix an automorphism $h \in \mathrm{Aut}(G_0) \setminus G_0$.

If G_0 is in (12) or (11), then Table 2 indicates that G_0 has a graph-field automorphism ρ such that $\mathrm{Out}(G_0) = \langle \ddot{\rho}\rangle$. Moreover, if G_0 is in (12), then $|\ddot{\rho}| = f$, so $\langle \ddot{h}\rangle = \langle \ddot{\rho}^i\rangle$ for some proper divisor i of f, as we claim. Similarly, if G_0 is in (11), then $|\ddot{\rho}| = 2f$, so $\langle \ddot{h}\rangle = \langle \ddot{\rho}^i\rangle$ for some proper divisor i of $2f$. In particular, $\langle \ddot{h}\rangle$ is either equal to $\langle \ddot{\rho}^i\rangle$ for some odd divisor i of f (as in (ii)(b)), or $\langle \ddot{\rho}^{2i}\rangle = \langle \ddot{\varphi}^i\rangle$ for some proper divisor i of f (as in (ii)(a)).

Next assume G_0 is in (10) with $G_0 \neq E_6^\epsilon(q)$. First assume that $\mathrm{Out}(G_0) = \langle \ddot{\varphi}\rangle$, so $\langle \ddot{h}\rangle = \langle \ddot{\varphi}^i\rangle$ for some proper divisor i of $|\varphi|$. If $G_0 \neq {}^3D_4(q)$, then $|\varphi| = f$ and we are in case (iii)(a). Now suppose $G_0 = {}^3D_4(q)$, so $\langle \ddot{h}\rangle = \langle \ddot{\varphi}^i\rangle$ for some divisor of i of $|\varphi| = 3f$. If 3 divides $3f/i$, then i divides f and we are in (iii)(a) once again. Otherwise, 3 divides i and f/j is not divisible by 3, where $j = i/3$. Here $3f/(3f, f+j) = 3f/(3f, j)$ and

$$\langle \ddot{h}\rangle = \langle \ddot{\varphi}^i\rangle = \langle \ddot{\varphi}^{f+j}\rangle = \langle \ddot{\tau}\ddot{\varphi}^j\rangle,$$

which puts us in case (iii)(b). Finally, if $\mathrm{Out}(G_0) \neq \langle \ddot{\varphi}\rangle$ then $G_0 = E_7(q)$ is the only option (see Table 2), where q is odd and $\mathrm{Out}(G_0) = \langle \ddot{\delta}\rangle \times \langle \ddot{\varphi}\rangle$. Here Lemma 3.14 implies that

$\langle \ddot{h} \rangle = \langle \ddot{\varphi}^i \rangle$ or $\langle \ddot{\delta}\ddot{\varphi}^i \rangle$ for some divisor i of f, and these possibilities are covered by cases (iii)(a) and (iii)(c), respectively.

To complete the proof, we may assume that $G_0 = E_6^\epsilon(q)$. First we handle the case $\epsilon = +$. Here $\langle \ddot{h} \rangle = \langle \ddot{h}_0 \varphi^i \rangle$, where h_0 is a product of diagonal and graph automorphisms, and by Lemma 3.14 we may assume that $i = 0$ or i divides f. If $q \not\equiv 1 \pmod 3$, then $h_0 \in \{1, \gamma\}$, so $\langle \ddot{h} \rangle = \langle \ddot{g} \rangle$ for an automorphism g in Row (R1) of Table 3. Now assume $q \equiv 1 \pmod 3$. Here $h_0 = \delta^j \gamma^k$ with $j \in \{0, 1, 2\}$ and $k \in \{0, 1\}$; we claim that $\langle \ddot{h} \rangle$ is $\mathrm{Out}(G_0)$-conjugate to $\langle \ddot{g} \rangle$ for an automorphism g in Table 3. To see this, first observe that $\ddot{\delta}\ddot{\varphi}^i$ and $\ddot{\delta}^2\ddot{\varphi}^i$ are $\mathrm{Out}(G_0)$-conjugate and so are $\ddot{\delta}\ddot{\gamma}\ddot{\varphi}^i$ and $\ddot{\delta}^2\ddot{\gamma}\ddot{\varphi}^i$ (see parts (i) and (ii) in Lemma 3.11). Therefore, it remains to prove the claim when $h \in \{\delta\gamma\varphi^i, \delta^2\gamma\varphi^i\}$ and $i = 0$ or f/i is odd, together with the additional claims in $\star$ and † (see Remark 3.16). If $i = 0$ or f/i is odd, then (14) does not hold, so Lemma 3.11(iv) implies that $\ddot{h}$ is $\mathrm{Out}(G_0)$-conjugate to $\ddot{\gamma}$. In addition, the claims in $\star$ and † follow immediately from parts (iv) and (iii) in Lemma 3.11, respectively.

Finally, let us assume $G_0 = {}^2E_6(q)$. Here $\langle \ddot{g} \rangle$ is $\mathrm{Out}(G_0)$-conjugate to $\langle \ddot{h}\ddot{\varphi}^i \rangle$ where h is trivial or diagonal, and i is either 0 or a divisor of $2f$. If $i > 0$ and $2f/i$ is even, then i divides f. On the other hand, if $i > 0$ and $2f/i$ is odd, then f/j is odd for $j = i/2$ and we note that $2f/(2f, i) = 2f/(2f, f + j)$. Therefore, $\langle \ddot{\gamma} \rangle$ is $\mathrm{Out}(G_0)$-conjugate to one of $\langle \ddot{h} \rangle$, $\langle \ddot{h}\ddot{\varphi}^f \rangle = \langle \ddot{h}\ddot{\gamma} \rangle$ or $\langle \ddot{h}\ddot{\varphi}^i \rangle$, where i is a proper divisor of f, or $\langle \ddot{h}\ddot{\varphi}^{f+j} \rangle = \langle \ddot{h}\ddot{\gamma}\ddot{\varphi}^j \rangle$ and j is a proper divisor of f such that f/j is odd. Therefore, $\langle \ddot{h} \rangle$ is $\mathrm{Out}(G_0)$-conjugate to $\langle \ddot{g} \rangle$ for an automorphism g in Table 3 and for the case $q \equiv 2 \pmod 3$ we conclude by appealing to Lemma 3.13. □

3.3. **Probabilistic method.** In this section, we discuss a probabilistic approach for bounding the uniform spread of a finite group, which was introduced by Guralnick and Kantor [35]. This approach plays a central role in the sequence of papers [10, 14, 35, 37, 38], and it is also a core technique in our proof of Theorem 8 in this paper. Here we recall the general set up and we introduce the relevant notation.

Let G be a finite group, let H be a subgroup of G and consider the natural transitive action of G on the set of cosets G/H. In terms of this action, the *fixed point ratio* of $z \in G$ is

$$\mathrm{fpr}(z, G/H) = \frac{|\{\omega \in G/H \,:\, \omega z = \omega\}|}{|G/H|} = \frac{|z^G \cap H|}{|z^G|}.$$

For $z, x \in G$, let $P(z, x)$ be the probability that z and a uniformly randomly chosen conjugate of x do *not* generate G, that is,

$$P(z, x) = \frac{|\{y \in x^G \,:\, \langle z, y \rangle \neq G\}|}{|x^G|}.$$

Now let us specialise to the case where G is an almost simple group with socle G_0. Recall that $\mathcal{M}$ is the set of maximal subgroups H of G such that $G = HG_0$. For an element $x \in G$, write $\mathcal{M}(x)$ for the set of subgroups $H \in \mathcal{M}$ that contain x. Notice that if the conjugacy class x^G witnesses $u(G) \geqslant 1$, then we must have $G/G_0 = \langle G_0 x \rangle$ and thus $\mathcal{M}(x)$ is simply the set of all maximal subgroups of G that contain x. Given this observation, the following result is a combination of [14, Lemmas 2.1 and 2.2].

Lemma 3.17. *Let G be an almost simple group with socle G_0. Let $x \in G$ with $G/G_0 = \langle G_0 x \rangle$.*

(i) *For $z \in G$, we have*

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H).$$

(ii) *If $P(z, x) < 1/k$ for all nontrivial $z \in G$, then $u(G) \geqslant k$, witnessed by x^G.*

Roughly speaking, in order to effectively apply Lemma 3.17 we need to do two things:

(a) First we must identify an appropriate element $x \in G$ such that $G/G_0 = \langle G_0 x \rangle$ and we have some control on the set of maximal overgroups $\mathcal{M}(x)$;
(b) Then we need to compute upper bounds on the fixed point ratios $\mathrm{fpr}(z, G/H)$ for all $H \in \mathcal{M}(x)$ and all nontrivial $z \in G$.

In the case where G_0 is a simple exceptional group of Lie type, upper bounds on $\mathrm{fpr}(z, G/H)$ for all maximal subgroups H of G are determined by Lawther, Liebeck and Seitz in [47] and we will make extensive use of their work (and in a few cases, we will need to strengthen the bounds in [47]).

To handle the problem identified in (a), we will often appeal to the theory of *Shintani descent*, both to find an element x and to control the maximal subgroups containing x. We discuss this approach in the next section.

3.4. **Shintani descent.** To close this preliminary section, we briefly recall the general theory of Shintani descent, which is our principal method for identifying and studying elements in the nontrivial cosets of the socle of an almost simple group of Lie type. The general method was introduced by Shintani [62] and Kawanaka [40] in the 1970s and it has found important applications in character theory. It was first adapted for studying the uniform spread of almost simple groups in [14] and we refer the reader to [38, Chapter 3] for a convenient overview of the relevant techniques.

To describe the general set up, let $\bar{G}$ be a connected algebraic group over an algebraically closed field and let σ be a Steinberg endomorphism of $\bar{G}$. Fix an integer $e > 1$. By identifying σ with its restriction to $\bar{G}_{\sigma^e}$, we can consider the finite semidirect product $\bar{G}_{\sigma^e}{:}\langle\sigma\rangle = \bar{G}_{\sigma^e}.e$.

Definition 3.18. A *Shintani map* of $(\bar{G}, \sigma, e)$ is a map of conjugacy classes of the form

$$F\colon \{(g\sigma)^{\bar{G}_{\sigma^e}} \,:\, g \in \bar{G}_{\sigma^e}\} \to \{y^{\bar{G}_\sigma} \,:\, y \in \bar{G}_\sigma\},\ \ (g\sigma)^{\bar{G}_{\sigma^e}} \mapsto (a^{-1}(g\sigma)^e a)^{\bar{G}_\sigma}$$

where $a \in \bar{G}$ satisfies $g = aa^{-\sigma^{-1}}$ (such an element a exists by the Lang-Steinberg theorem, see [32, Theorem 2.1.1]).

We now present the main theorem of Shintani descent (see [40, Lemma 2.2]).

Theorem 3.19. *Let F be a Shintani map of $(\bar{G}, \sigma, e)$. Then F is a well-defined bijection from the set of $\bar{G}_{\sigma^e}$-conjugacy classes in the coset $\bar{G}_{\sigma^e}\sigma$ to the set of conjugacy classes in $\bar{G}_\sigma$. Moreover, F does not depend on the choice of element $a \in \bar{G}$.*

In light of Theorem 3.19, we refer to F as *the* Shintani map of $(\bar{G}, \sigma, e)$. To simplify the notation, if the setting is understood, we will write $F\colon \bar{G}_{\sigma^e}\sigma \to \bar{G}_\sigma$ for the Shintani map and $F(g\sigma)$ for a representative of the $\bar{G}_\sigma$-class $F((g\sigma)^{\bar{G}_{\sigma^e}})$. We refer to $g\sigma$ as a *Shintani correspondent* of $F(g\sigma)$.

The following elementary observation highlights the relationship between the order of an element in $\bar{G}_\sigma$ and the order of a Shintani correspondent in the coset $\bar{G}_{\sigma^e}\sigma$.

Lemma 3.20. *Let $y \in \bar{G}_\sigma$ and let $g \in \bar{G}_{\sigma^e}$ such that $F(g\sigma) = y$. Then $|g\sigma| = e|y|$.*

Proof. Since $g\sigma \in \bar{G}_{\sigma^e}{:}\langle\sigma\rangle$, it follows that e divides the order of $g\sigma$. Therefore, $|g\sigma| = e|(g\sigma)^e|$ and we conclude that $|g\sigma| = e|y|$ since $(g\sigma)^e$ is $\bar{G}$-conjugate to y. □

We will need the following technical result [38, Corollary 3.2.3] (in the statement, for a finite group X we write $O^{p'}(X)$ for the normal subgroup generated by the p-elements of X).

Lemma 3.21. *Let $\bar{G}$ be a simple algebraic group over $\bar{\mathbb{F}}_p$ of adjoint type and set $G_0 = (\bar{G}_{\sigma^e})'$. If $\langle G_0, \sigma\rangle \trianglelefteqslant \langle \bar{G}_{\sigma^e}, \sigma\rangle$, then the Shintani map F of $(\bar{G}, \sigma, e)$ restricts to a bijection*

$$\{(g\sigma)^{\bar{G}_{\sigma^e}} \,:\, g \in G_0\} \to \{y^{\bar{G}_\sigma} \,:\, y \in O^{p'}(\bar{G}_\sigma)\}.$$

Let us provide an example to demonstrate how we will use Lemma 3.21.

Example 3.22. Here we explain how we use Shintani descent to identify a conjugacy class in the coset $E_7(q)h$, where $q = p^f$ and h is a field automorphism.

Let $\bar{G}$ be the adjoint algebraic group of type E_7 over $\bar{\mathbb{F}}_p$. Let φ be a standard Frobenius endomorphism of $\bar{G}$, let $\sigma = \varphi^i$ for a proper divisor i of f and set $e = f/i > 1$. Write $q = q_0^e$ and let F be the Shintani map of $(\bar{G}, \sigma, e)$.

If q is even, then $\bar{G}_{\sigma^e}$ and $\bar{G}_\sigma$ are the simple groups $E_7(q)$ and $E_7(q_0)$, respectively, so

$$F\colon \{(g\varphi^i)^{E_7(q)} \,:\, g \in E_7(q)\} \to \{y^{E_7(q_0)} \,:\, y \in E_7(q_0)\}.$$

Therefore, we may select an element in the coset $E_7(q)\varphi^i$ by identifying an element in the subgroup $E_7(q_0)$ and taking its Shintani correspondent. However, if q is odd, then $|\bar{G}_{\sigma^e} : E_7(q)| = |\bar{G}_\sigma : E_7(q_0)| = 2$ and the Shintani map

$$F\colon \{(g\varphi^i)^{\bar{G}_{\sigma^e}} \,:\, g \in \bar{G}_{\sigma^e}\} \to \{y^{\bar{G}_\sigma} \,:\, y \in \bar{G}_\sigma\}$$

allows us to identify an element in $\bar{G}_{\sigma^e}\varphi^i$ but it does not tell us which coset of $E_7(q)$ this element is contained in. This is where Lemma 3.21 comes into play.

Observe that $E_7(q) = (\bar{G}_{\sigma^e})'$ and $E_7(q_0) = O^{p'}(\bar{G}_\sigma)$. Moreover, $\langle \ddot{\sigma} \rangle$ is an index two subgroup of $\langle \ddot{\delta}, \ddot{\sigma} \rangle = \langle \bar{G}_{\sigma^e}, \sigma \rangle / G_0$ (see Table 2), so $\langle G_0, \sigma \rangle \trianglelefteq \langle \bar{G}_{\sigma^e}, \sigma \rangle$. Therefore, Lemma 3.21 implies that F restricts to a bijection

$$\{(g\varphi^i)^{\bar{G}_{\sigma^e}} \,:\, g \in E_7(q)\} \to \{y^{\bar{G}_\sigma} \,:\, y \in E_7(q_0)\}.$$

This means that the coset of $E_7(q_0)$ in $\bar{G}_\sigma$ containing a given element $y \in \bar{G}_\sigma$ controls the coset of $G_0 = E_7(q)$ in $\mathrm{Aut}(G_0)$ that contains the Shintani correspondent of y.

It is important to observe that the Shintani map gives more than just the bijection between conjugacy classes stated in Theorem 3.19. Indeed, we can use it to shed light on the overgroups in $\langle \bar{G}_{\sigma^e}, \sigma \rangle$ of an element in the coset $\bar{G}_{\sigma^e}\sigma$. This is encapsulated in Lemmas 3.23 and 3.25 below, which coincide with Lemmas 3.3.2 and 3.3.4 in [38] (in turn these results are closely related to Corollary 2.15 and Proposition 2.16(i) in [14]).

Lemma 3.23. *Let $\bar{H}$ be a closed connected σ-stable subgroup of $\bar{G}$ such that $N_{\bar{G}_\sigma}(\bar{H}_\sigma) = \bar{H}_\sigma$ and $N_{\bar{G}_{\sigma^e}}(\bar{H}_{\sigma^e}) = \bar{H}_{\sigma^e}$. Then for all $g \in \bar{G}_{\sigma^e}$, the number of $\bar{G}_{\sigma^e}$-conjugates of $\bar{H}_{\sigma^e}$ normalised by $g\sigma$ equals the number of $\bar{G}_\sigma$-conjugates of $\bar{H}_\sigma$ containing $F(g\sigma)$.*

Corollary 3.24. *Let $\bar{G}$ be a simple algebraic group and let $g \in \bar{G}_{\sigma^e}$. Then the number of maximal parabolic subgroups of $G = \langle \bar{G}_{\sigma^e}, \sigma \rangle$ that contain $g\sigma$ is equal to the number of maximal parabolic subgroups of $\bar{G}_\sigma$ that contain $F(g\sigma)$.*

Proof. Let $\bar{H}$ be a maximal σ-stable parabolic subgroup of $\bar{G}$, so $\bar{H}$ is connected and self-normalising. Then $\bar{H}_\sigma$ is a maximal parabolic subgroup of $\bar{G}_\sigma$ and we have $N_{\bar{G}_\sigma}(\bar{H}_\sigma) = \bar{H}_\sigma$. Similarly, $H = N_G(\bar{H}_{\sigma^e}) = \langle \bar{H}_{\sigma^e}, \sigma \rangle$ is a maximal parabolic subgroup of G and $N_G(H) = H$. Therefore, Lemma 3.23 implies that the number of G-conjugates of H that contain $g\sigma$ equals the number of $\bar{G}_\sigma$-conjugates of $\bar{H}_\sigma$ that contain $F(g\sigma)$.

Let us now explain why this gives the desired result. First observe that every maximal parabolic subgroup of $\bar{G}_\sigma$ is $\bar{G}_\sigma$-conjugate to $\bar{H}_\sigma$ for a maximal σ-stable parabolic subgroup $\bar{H}$ of $\bar{G}$, and similarly, every maximal parabolic subgroup of G is G-conjugate to $N_G(\bar{H}_{\sigma^e})$ for a maximal σ-stable parabolic subgroup $\bar{H}$ of $\bar{G}$ (in the latter case, $\bar{H}$ is σ-stable, not just σ^e-stable, because otherwise $N_G(\bar{H}_{\sigma^e})$ would not be maximal in $G = \langle \bar{G}_{\sigma^e}, \sigma \rangle$). Moreover, if $\bar{H}$ and $\bar{K}$ are two different maximal σ-stable parabolic subgroups of $\bar{G}$, then $\bar{H}_\sigma$ and $\bar{K}_\sigma$ are $\bar{G}_\sigma$-conjugate if and only if $N_G(\bar{H}_{\sigma^e})$ and $N_G(\bar{K}_{\sigma^e})$ are G-conjugate, since both of these conditions are equivalent to $\bar{H}$ and $\bar{K}$ being $\bar{G}$-conjugate. The result follows. □

Lemma 3.25. *If $g \in \bar{G}_{\sigma^e}$ and $H \leqslant \langle \bar{G}_{\sigma^e}, \sigma \rangle$, then $g\sigma$ is contained in at most $|C_{\bar{G}_\sigma}(F(g\sigma))|$ distinct $\langle \bar{G}_{\sigma^e}, \sigma \rangle$-conjugates of H.*

In the proof of Theorem 8, there will be some cases where we will be unable to apply Shintani descent directly (for instance, see Example 3.28). In such a situation, we will often appeal to the following result (see [38, Lemma 3.4.1]). In the statement of the lemma, by an automorphism ρ of $\bar{G}$ we mean an *algebraic* automorphism, in the sense that both ρ and ρ^{-1} are morphisms of varieties.

Lemma 3.26. *Let ρ be an automorphism of $\bar{G}$ and let $\bar{K}$ be a closed connected σ-stable subgroup of $C_{\bar{G}}(\rho)$. Set $G = \bar{G}_{\rho\sigma^e}{:}\langle\rho,\sigma\rangle$ and let $y \in \bar{K}_\sigma \leqslant \bar{G}_{\rho\sigma^e}$.*

(i) *There exists $g \in \bar{K}_{\sigma^e} \leqslant \bar{G}_{\rho\sigma^e}$ such that $(g\sigma)^e$ and $y\rho^{-1}$ are $\bar{G}$-conjugate elements of G.*

(ii) *Suppose there is a positive integer d such that $(\rho\sigma^e)^d = \sigma^{ed}$ as endomorphisms of $\bar{G}$.*

  (a) *For each subgroup H of $\langle \bar{G}_{\rho\sigma^e}, \sigma\rangle$, $g\sigma$ is contained in at most $|C_{\bar{G}_\sigma}(y^d)|$ distinct $\bar{G}_{\rho\sigma^e}$-conjugates of H.*

  (b) *For all closed connected σ-stable subgroups $\bar{H}$ of $\bar{G}$ such that $N_{\bar{G}_\sigma}(\bar{H}_\sigma) = \bar{H}_\sigma$ and $N_{\bar{G}_{\sigma^{de}}}(\bar{H}_{\sigma^{de}}) = \bar{H}_{\sigma^{de}}$, the number of $\bar{G}_{\sigma^{de}}$-conjugates of $\bar{H}_{\sigma^{de}}$ normalised by $g\sigma$ is equal to the number of $\bar{G}_\sigma$-conjugates of $\bar{H}_\sigma$ containing y^d.*

Remark 3.27. Adopt the notation in Lemma 3.26 and fix an appropriate element $g \in \bar{G}_{\rho\sigma^e}$ as in part (i). Now e divides $|g\sigma|$ and $(g\sigma)^e$ is $\bar{G}$-conjugate to $y\rho^{-1}$, so $|g\sigma| = e|y\rho^{-1}|$. Since $y \in C_{\bar{G}}(\rho)$ we have $|y\rho^{-1}| = |y||\rho|/(|y|,|\rho|)$ and thus $|g\sigma| = e|y||\rho|/(|y|,|\rho|)$.

The following example explains why Lemma 3.26 will be useful in the proof of Theorem 8.

Example 3.28. Here we explain how we can use Shintani descent to identify a conjugacy class in the coset $E_6(q)h$, where $q = 3^f$ and h is a graph-field automorphism.

Let $\bar{G}$ be the adjoint simple algebraic group E_6 over $\bar{\mathbb{F}}_3$. Let φ and γ be the standard Frobenius endomorphism and graph automorphism of $\bar{G}$, respectively, so $[\gamma,\varphi] = 1$ (see Definition 3.9). Write $\sigma = \gamma\varphi^i$, where i divides f, and set $e = f/i > 1$. Write $q = q_0^e$ and let F be the Shintani map of $(\bar{G},\sigma,e)$.

If e is even, then $\bar{G}_{\sigma^e} = \bar{G}_{\varphi^f} = E_6(q)$ and $\bar{G}_\sigma = \bar{G}_{\gamma\varphi} = {}^2E_6(q_0)$. Therefore,

$$F\colon \{(g\gamma\varphi^i)^{E_6(q)} : g \in E_6(q)\} \to \{y^{{}^2E_6(q_0)} : y \in {}^2E_6(q_0)\}$$

and we can use F to choose an element in the coset $E_6(q)\gamma\varphi^i$ as desired.

However, if e is odd, then $\bar{G}_{\sigma^e} = \bar{G}_{\gamma\varphi^f} = {}^2E_6(q)$ and the Shintani map

$$F\colon \{(g\gamma\varphi^i)^{{}^2E_6(q)} : g \in {}^2E_6(q)\} \to \{y^{{}^2E_6(q_0)} : y \in {}^2E_6(q_0)\}$$

provides no information about the coset $E_6(q)\gamma\varphi^i$. In this case we apply Lemma 3.26, with $\rho = \gamma$. To this end, let $\bar{K} = C_{\bar{G}}(\gamma) = F_4$, which is connected. Then Lemma 3.26 allows us to choose an element in the coset $E_6(q)\gamma\varphi^i$. More precisely, part (i) of the lemma implies that for all $y \in F_4(q_0) \leqslant {}^2E_6(q_0)$, there exists $g \in E_6(q)$ such that $(g\gamma\varphi^i)^e$ is $\bar{G}$-conjugate to $y\gamma$. In addition, part (ii) provides information on the maximal overgroups of $g\gamma\varphi^i$.

4. Proof of Theorem 8: low rank groups

We now turn to the proof of Theorem 8, which will be spread across Sections 4–9. Since the theorem for simple exceptional groups is proved in [10], we will always assume that G is almost simple, but not simple.

We begin in this section by handling the low rank almost simple groups G with socle

$$G_0 \in \{{}^2B_2(q),\ {}^2G_2(q)',\ {}^2F_4(q)',\ G_2(q)'\}. \tag{16}$$

First we establish Theorem 8 in some special cases.

TABLE 4. The relevant groups $G = \langle G_0, g\rangle$ for G_0 in (16)

Case	G_0	g	Conditions
(a)	$G_2(q)$	φ^i	i is a proper divisor of f
(b)	$G_2(q)$	ρ^i	i is an odd divisor of f & $p = 3$
(c)	${}^2B_2(q), {}^2G_2(q), {}^2F_4(q)$	ρ^i	i is a proper divisor of f

Proposition 4.1. *The conclusion to Theorem 8 holds when*

$$G_0 \in \{{}^2B_2(8), {}^2G_2(3)', {}^2F_4(2)', G_2(2)', G_2(3), G_2(4)\}. \tag{17}$$

Proof. In each of these cases, we may assume that $G = \mathrm{Aut}(G_0)$ since this is the only almost simple group G with $\mathrm{soc}(G) = G_0$ and $G \neq G_0$. We prove the result by way of computation in MAGMA [7].

To do this, we first construct G using the command `AutomorphismGroupSimpleGroup` and we note that $|G : G_0|$ is prime. Our method for studying $u(G)$ computationally is described in [37, Section 2.3] and the relevant code is given in [38, Appendix A]. In this way, we can verify that the bound $u(G) \geqslant k$ is witnessed by the conjugacy class x^G, where k and x^G are are as follows (in terms of the ATLAS [21] notation):

G_0	${}^2B_2(8)$	${}^2G_2(3)'$	${}^2F_4(2)'$	$G_2(2)'$	$G_2(3)$	$G_2(4)$
$\lvert G : G_0\rvert$	3	3	2	2	2	2
x^G	`15A`	`9D`	`12C`	`12C`	`18A`	`24B`
k	90	6	18	3	23	10

(The computations were carried out using MAGMA 2.24-4 on a 2.7 GHz machine with 128 GB RAM. The largest computation took 2 seconds and 32 MB of memory.) □

Suppose $G = \langle G_0, g\rangle$ with G_0 as in (16) and write $q = p^f$ where p is prime. In view of Proposition 4.1, we may (and will) assume for the remainder of this section that G_0 is not one of the groups in (17). Then by Proposition 3.15, it suffices to consider the groups recorded in Table 4. In the table (and the proofs below), we refer freely to the notation for automorphisms in Definition 3.9.

Proposition 4.2. *The conclusion to Theorem 8 holds in case (a) of Table 4.*

Proof. Let $G_0 = G_2(q)$ where $q = p^f$ with $f > 1$ and $q \geqslant 8$. Let $\bar{G}$ be the simple algebraic group G_2 over the algebraic closure of $\mathbb{F}_p$ and let φ be a standard Frobenius endomorphism of $\bar{G}$. Let $\sigma = \varphi^i$ and write $e = f/i$ and $q_0 = p^i$, so $q = q_0^e$ and $e > 1$. Then $\bar{G}_\sigma = G_2(q_0)$ and $\bar{G}_{\sigma^e} = G_2(q)$, and by identifying σ with its restriction to $\bar{G}_{\sigma^e}$ we see that $\sigma = g$. Let $F\colon G_2(q)g \to G_2(q_0)$ be the Shintani map of $(\bar{G}, \sigma, e)$ (see Definition 3.18) and choose $y \in G_2(q_0)$ such that

$$|y| = \begin{cases} q_0^2 - q_0 + 1 & \text{if } q_0 > 2 \\ 7 & \text{if } q_0 = 2. \end{cases}$$

Note that $C_{G_2(q_0)}(y) = \langle y\rangle$ (see [19, 28]). By Theorem 3.19, fix $x \in G_0 g$ such that $F(x) = y$.

Recall that $\mathcal{M}$ is the set of maximal subgroups H of G with $G = HG_0$ and $\mathcal{M}(x)$ is the collection of subgroups in $\mathcal{M}$ containing x. The maximal subgroups of G are recorded in [8, Tables 8.30, 8.41 and 8.42]. The element y is not contained in any maximal parabolic subgroup of $G_2(q_0)$ since $|y|$ does not divide the order of any such subgroup. Therefore, Corollary 3.24 informs us that there are no maximal parabolic subgroups in $\mathcal{M}(x)$. Consequently, by inspecting the relevant tables in [8, Chapter 8], we see that there are at most $6 - 3\delta_{2,p} + \log\log q$

conjugacy classes of subgroups in $\mathcal{M}(x)$. Moreover, if H is any subgroup of G, then Lemma 3.25 implies that x is contained in at most $|C_{G_2(q_0)}(y)| = |y|$ distinct G-conjugates of H. Therefore,

$$|\mathcal{M}(x)| \leqslant (6 - 3\delta_{2,p} + \log\log q) \cdot |y|.$$

Let $z \in G$ be nontrivial. Then [47, Theorem 1] gives $\mathrm{fpr}(z, G/H) \leqslant (q^2 - q + 1)^{-1}$ for all $H \in \mathcal{M}$ and thus Lemma 3.17(i) yields

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (6 - 3\delta_{2,p} + \log\log q) \cdot |y| \cdot (q^2 - q + 1)^{-1}.$$

For $q > 49$, this upper bound proves that $P(z,x) < q^{-1/2}$, so $P(z,x) \to 0$ as $q \to \infty$. In view of Lemma 3.17(ii), we conclude that $u(G) \to \infty$ as $q \to \infty$.

Moreover, since $q \geqslant 8$, one checks that this upper bound is less than $\frac{1}{2}$ unless $q \in \{8, 9\}$. If $q = 9$, then $|y| = 7$ and we check that there are only 3 conjugacy classes of subgroups in $\mathcal{M}$ with order divisible by 7 (here we are using the fact that G does not contain any graph-field automorphisms). This allows us to replace the leading factor $6 + \log\log q$ in the above bound by 3 and this is sufficient to see that $P(z,x) < \frac{1}{2}$. Similarly, if $q = 8$ then we can replace $3 + \log\log q$ by 4, which yields

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant 4 \cdot 7 \cdot \frac{1}{57} = \frac{28}{57} < \frac{1}{2}.$$

Therefore, $P(z,x) < \frac{1}{2}$ in all cases and thus Lemma 3.17(ii) implies that $u(G) \geqslant 2$. □

Proposition 4.3. *The conclusion to Theorem 8 holds in case (b) of Table 4.*

Proof. Let $G_0 = G_2(q)$ where $q = 3^f$ and $f > 1$. Let $\bar{G} = G_2$ and let ρ be the Steinberg endomorphism of $\bar{G}$ from Definition 3.9(ii). Let $\sigma = \rho^i$ and write $e = f/i$ and $q_0 = 3^i$, so $q = q_0^e$ and $e \geqslant 1$. Let $F\colon G_2(q)g \to {}^2G_2(q_0)$ be the Shintani map of $(\bar{G}, \sigma, 2e)$, and fix $y \in {}^2G_2(q_0)$ with

$$|y| = q_0 + \sqrt{3q_0} + 1.$$

Note that $C_{{}^2G_2(q_0)}(y) = \langle y \rangle$ (see (3) in the main theorem of [67]). Let $x \in G$ satisfy $F(x) = y$.

By [42], there are at most $7 + \log\log q$ classes of subgroups in $\mathcal{M}$ and by Lemma 3.25, $\mathcal{M}(x)$ contains at most $|C_{{}^2G_2(q_0)}(y)| = |y|$ conjugates of any given subgroup H of G. Let $z \in G$ be nontrivial. Then [47, Theorem 1] gives $\mathrm{fpr}(z, G/H) \leqslant (q^2 - q + 1)^{-1}$ for all $H \in \mathcal{M}$, so

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (7 + \log\log q) \cdot |y| \cdot (q^2 - q + 1)^{-1}.$$

This upper bound is less than $\frac{1}{2}$ for $q > 9$ and less than $q^{-1/2}$ for $q > 27$. Finally, if $q = 9$ then there are only 2 classes of subgroups in $\mathcal{M}$ with order divisible by $|y| = 7$ and we obtain $P(z,x) < \frac{1}{2}$ by replacing the $7 + \log\log q$ factor in the above bound by 2. The result now follows by Lemma 3.17. □

Proposition 4.4. *The conclusion to Theorem 8 holds in case (c) of Table 4.*

Proof. Let $G_0 \in \{{}^2B_2(q), {}^2G_2(q), {}^2F_4(q)\}$. As usual, let $q = p^f$ where p is prime, and note that $f \geqslant 3$ is odd. In each case, let $\bar{G}$ be the ambient simple algebraic group and let ρ be the Steinberg endomorphism of $\bar{G}$ from Definition 3.9(ii). Let $\sigma = \rho^i$ and write $e = f/i$ and $q_0 = p^i$, so $q = q_0^e$ and $e \geqslant 3$ is odd. Let $F : G_0 g \to \bar{G}_\sigma$ be the Shintani map of $(\bar{G}, \sigma, e)$.

Choose $y \in \bar{G}_\sigma$ as in Table 5 and let $x \in G$ be a Shintani correspondent of y. By inspecting [42, 56, 66], we see that there are at most $m + \log\log q$ classes of subgroups in $\mathcal{M}$, where m is given in Table 5. Moreover, $C_{\bar{G}_\sigma}(y) = \langle y \rangle$ (see [61, 66, 67]), so $|\mathcal{M}(x)| \leqslant (m + \log\log q) \cdot |y|$ by Lemma 3.25. In addition, [47, Theorem 1] gives $\mathrm{fpr}(z, G/H) \leqslant a(q)$ for all $H \in \mathcal{M}$ and all

TABLE 5. Data for the groups in case (c) of Table 4

G_0	$\lvert y\rvert$	m	$a(q)$
${}^2B_2(q)$	$q_0+\sqrt{2q_0}+1$	4	$(q^{2/\ell}+1)/(q^2+1)$
${}^2G_2(q)$	$q_0+\sqrt{3q_0}+1$	5	$(q^2-q+1)^{-1}$
${}^2F_4(q)$	$q_0^2+\sqrt{2q_0^3}+q_0+\sqrt{2q_0}+1$	11	q^{-4}

nontrivial $z \in G$, where $a(q)$ is presented in Table 5 (note that in the first row of Table 5, ℓ is the least prime divisor of f). Therefore,

$$P(z,x) \leqslant \sum_{H\in\mathcal{M}(x)} \mathrm{fpr}(z,G/H) \leqslant (m+\log\log q)\cdot|y|\cdot a(q).$$

One can check that this bound gives $P(z,x) < \frac{1}{2}$ and $P(z,x) < q^{-1/6}$, whence $u(G) \geqslant 2$ and $u(G) \to \infty$ as $q \to \infty$. □

By combining Propositions 4.1–4.4, we have now established the following theorem.

Theorem 4.5. *The conclusion to Theorem 8 holds when G_0 is one of the groups in* (16).

In the next five sections, we will complete the proof of Theorem 8 by handling the remaining groups with $G_0 \in \{E_8(q), E_7(q), E_6^\epsilon(q), F_4(q), {}^3D_4(q)\}$.

5. PROOF OF THEOREM 8: $G_0 = E_8(q)$

In this section, we prove Theorem 8 for almost simple groups G with socle $G_0 = E_8(q)$, where $q = p^f$. By Proposition 3.15, we may assume that $G = \langle G_0, g\rangle$, where $g = \varphi^i$ for the field automorphism φ in Definition 3.9(i) and a proper divisor i of f.

Let $\bar{G}$ be the algebraic group E_8 over $\bar{\mathbb{F}}_p$, let σ be the Frobenius endomorphism φ^i of $\bar{G}$ and let $e = f/i$, so $G_0 = \bar{G}_{\sigma^e}$. Set $q = q_0^e$ and let $F\colon E_8(q)g \to E_8(q_0)$ be the Shintani map of $(\bar{G},\sigma,e)$.

Fix an element $y \in E_8(q_0)$ such that

$$|y| = q_0^8+q_0^7-q_0^5-q_0^4-q_0^3+q_0+1$$

and $C_{E_8(q_0)}(y) = \langle y\rangle$ (see [54] or [30, Section 3]). Let $x \in G$ be a Shintani correspondent of y (that is, choose $x \in G$ such that $F(x) = y$). Then by Lemma 3.20, we have $|x| = e|y|$ and we note that $|y| = 331$ if $q_0 = 2$ and $|y| \geqslant 8401$ if $q_0 \geqslant 3$.

Recall that for integers $a, b \geqslant 2$, a prime r is said to be a *primitive prime divisor* of a^b-1 if r divides a^b-1 but r does not divide a^i-1 for all $1 \leqslant i < b$. A theorem of Zsigmondy [71] asserts that a^b-1 has at least one primitive prime divisor for all integers $a, b \geqslant 2$ unless $(a,b) = (2,6)$, or a is a Mersenne prime and $b = 2$. In particular, $q_0^{30}-1$ has a primitive prime divisor, and by considering the factorisation of $q_0^{30}-1$ as a product of cyclotomic polynomials, we see that such a primitive prime divisor necessarily divides $|y|$.

As usual, we write $\mathcal{M}$ for the set of maximal subgroups H of G with $G = HG_0$ and $\mathcal{M}(x)$ for the collection of subgroups in $\mathcal{M}$ containing x. In the analysis below, we will refer repeatedly to the partition $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$ in (7).

Proposition 5.1. *We have $\mathcal{M}(x) \subseteq \mathcal{M}_1$.*

Proof. Let $H \in \mathcal{M}(x)$. If $H \in \mathcal{M}_3$, then Proposition 3.7 gives $\mathrm{meo}(H) \leqslant 210$, which is incompatible with the bound $|x| \geqslant 331e$. Therefore, we may assume $H \in \mathcal{M}_2$. Let S be the socle of H, which is a simple group of Lie type over a field $\mathbb{F}_t$ of characteristic p. We proceed by considering the possibilities for S given in Theorem 3.4.

TABLE 6. The relevant groups $G = \langle G_0, g\rangle$ for $G_0 = E_7(q)$

Case	g	Conditions	
(a)	δ	q odd	
(b)	φ^i		$i \in \Delta(f)$
(c)	$\delta\varphi^i$	q odd	$i \in \Delta(f)$

If $S = \mathrm{L}_3^\epsilon(16)$, then Proposition 3.5 gives $\mathrm{meo}(H) \leqslant 273 < |x|$, so this case does not arise. Next assume that $S = \mathrm{L}_2(t)$ and $t \leqslant 1312(2, t-1)$. By applying Proposition 3.5, we reduce to the case $q_0 = 2$, so $|x| = 331e$ and $t = 2^k$ with $k \leqslant 10$. However, for each k, it is easy to check that $|S|$ is indivisible by 331, so this case does not arise. Next assume that $S = {}^2B_2(t)$, so $p = 2$ and $t = 2^{2k+1}$ with $k \leqslant 4$. Here Proposition 3.5 gives $\mathrm{meo}(H) \leqslant 4905$, so we immediately reduce to the case $q_0 = 2$ and one checks that $|S|$ is indivisible by 331. Similarly, if $S = {}^2G_2(t)'$, then $t = 3^{2k+1}$ with $k \leqslant 3$ and $\mathrm{meo}(H) \leqslant 15883 < 8401e$, so this case is also ruled out.

To complete the proof of the proposition, we may assume that $\mathrm{rk}(S) \in \{2, 3, 4\}$ and $t \leqslant 9$. We consider each possibility for S in turn, excluding ${}^2B_2(t)$ and ${}^2G_2(t)'$ since these groups were handled above.

To get started, let us assume $\mathrm{rk}(S) = 4$, so

$$S \in \{\mathrm{L}_5^\epsilon(t),\ \mathrm{PSp}_8(t),\ \mathrm{P\Omega}_8^\epsilon(t),\ \Omega_9(t),\ F_4(t),\ {}^2F_4(t),\ {}^3D_4(t)\}.$$

If S is a classical group, Proposition 3.5 gives $\mathrm{meo}(H) \leqslant t^5/(t-1)$ and we immediately reduce to the case $(t, q_0) = (8, 2)$. Here one checks that $|S|$ is divisible by 331 if and only if $S = \mathrm{U}_5(8)$, but this case is ruled out by Proposition 3.8. Now assume that $S = F_4(t)$. By applying the bound on $\mathrm{meo}(H)$ from Proposition 3.5, we may assume that either $q_0 = 2$, or $q_0 = 3$ and $t = 9$. For $q_0 = 2$ we have $t \in \{2, 4, 8\}$ and $|S|$ is indivisible by 331. Similarly, if $q_0 = 3$, then $|y| = 8401 = 31 \cdot 271$, but $|S|$ is indivisible by 31. The cases where S is ${}^2F_4(t)'$ and ${}^3D_4(t)$ are very similar. For example, if $S = {}^2F_4(t)'$, then we reduce to the case $t = 8$ with $q_0 = 2$ and one checks that $|{}^2F_4(8)|$ is indivisible by 331.

Now assume $\mathrm{rk}(S) \in \{2, 3\}$. If S is classical, then the bound in Proposition 3.5 implies that $\mathrm{meo}(H) < |x|$. Finally, if $S = G_2(t)'$, then Proposition 3.5 gives $\mathrm{meo}(H) \leqslant 8(t^2 + t + 1)\log t$, which is less than $|x|$ unless $(t, q_0) = (8, 2)$. But $|G_2(8)|$ is indivisible by 331, so this case does not arise and the proof is complete. □

Theorem 5.2. *The conclusion to Theorem 8 holds when $G_0 = E_8(q)$.*

Proof. We will apply Lemma 3.17. Recall that $y \in E_8(q_0)$ and x is a Shintani correspondent of y. Let $H \in \mathcal{M}(x)$, so Proposition 5.1 gives $H \in \mathcal{M}_1$ and Lemma 3.25 implies that at most $|C_{E_8(q_0)}(y)| = |y|$ distinct G_0-conjugates of H are contained in $\mathcal{M}(x)$. Finally, if $z \in G$ is nontrivial then [47, Theorem 1] gives $\mathrm{fpr}(z, G/H) \leqslant q^{-8}(q^4 - 1)^{-1}$ and therefore Proposition 3.3 implies that

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < (49 + \log\log q) \cdot |y| \cdot \frac{1}{q^8(q^4 - 1)} < \frac{1}{q},$$

noting that $q_0 \leqslant q^{1/2}$. The result follows. □

6. PROOF OF THEOREM 8: $G_0 = E_7(q)$

Let $G = \langle G_0, g\rangle$, where $G_0 = E_7(q)$ and $g \in G \setminus G_0$. As usual, write $q = p^f$ with p prime. According to Proposition 3.15, it is enough to prove Theorem 8 for the cases recorded in Table 6. In the table, we write $\Delta(f)$ for the set of proper positive divisors of f.

Proposition 6.1. *The conclusion to Theorem 8 holds in case (a) of Table 6.*

Proof. Here q is odd and $G = \langle G_0, \delta\rangle = \mathrm{Inndiag}(G_0)$. Fix an element $x \in G \setminus G_0$ of order $(q+1)(q^6-q^3+1)$. As explained in [68, Section 4(i)], x is contained in a unique maximal subgroup of G (namely, a maximal rank subgroup of type ${}^2E_6(q) \times (q+1)$). Therefore [47, Theorem 1] implies that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (q^6-q^3+1)^{-1}$$

for all nontrivial $z \in G$ and the result follows. □

For the remainder of this section, we will assume that we are in cases (b) and (c) of Table 6. Therefore, fix a proper divisor i of f and write $e = f/i$ and $q = q_0^e$. Let $\bar{G}$ be the adjoint algebraic group of type E_7 over $\bar{\mathbb{F}}_p$, let σ be the Steinberg endomorphism φ^i and let

$$F\colon \mathrm{Inndiag}(E_7(q))\varphi^i \to \mathrm{Inndiag}(E_7(q_0))$$

be the Shintani map of $(\bar{G}, \sigma, e)$.

If q is even, then we are necessarily in case (b) and we have $F\colon E_7(q)g \to E_7(q_0)$, which means that we can proceed as in Section 5. The following lemma will allow us to handle cases (b) and (c) simultaneously when q is odd.

Lemma 6.2. *If q is odd, then the Shintani map F restricts to bijections*

$$\{(t\varphi^i)^{\mathrm{Inndiag}(E_7(q))} : t \in E_7(q)\} \to \{y^{\mathrm{Inndiag}(E_7(q_0))} : y \in E_7(q_0)\}$$
$$\{(t\delta\varphi^i)^{\mathrm{Inndiag}(E_7(q))} : t \in E_7(q)\} \to \{y^{\mathrm{Inndiag}(E_7(q_0))} : y \in \mathrm{Inndiag}(E_7(q_0)) \setminus E_7(q_0)\}.$$

Proof. This was essentially proved in Example 3.22. First observe that $E_7(q) = (\bar{G}_{\sigma^e})'$ and $E_7(q_0) = O^{p'}(\bar{G}_\sigma) = (\bar{G}_\sigma)'$. Let us also note that $\langle G_0, \sigma\rangle = \langle E_7(q), \varphi^i\rangle$ is an index two (and hence normal) subgroup of $\langle \bar{G}_{\sigma^e}, \sigma\rangle = \langle \mathrm{Inndiag}(E_7(q)), \varphi^i\rangle$. Therefore, Lemma 3.21 implies that the Shintani map F restricts to the bijection

$$F_1\colon \{(t\varphi^i)^{\mathrm{Inndiag}(E_7(q))} : t \in E_7(q)\} \to \{y^{\mathrm{Inndiag}(E_7(q_0))} : y \in E_7(q_0)\},$$

while the restriction of F to the complement of the domain of F_1 is the bijection

$$F_2\colon \{(t\delta\varphi^i)^{\mathrm{Inndiag}(E_7(q))} : t \in E_7(q)\} \to \{y^{\mathrm{Inndiag}(E_7(q_0))} : y \in \mathrm{Inndiag}(E_7(q_0)) \setminus E_7(q_0)\}.$$

The result follows. □

Fix an element $y \in \mathrm{Inndiag}(E_7(q_0))$ such that

$$|y| = \begin{cases} (q_0+1)(q_0^6-q_0^3+1) & \text{if } q_0 > 2 \\ 129 & \text{if } q_0 = 2 \end{cases}$$

and $C_{\mathrm{Inndiag}(E_7(q_0))}(y^2) = \langle y\rangle$ (see [54]). Let $x \in \langle \mathrm{Inndiag}(E_7(q)), \varphi^i\rangle$ such that $F(x)$ is y^2 in case (b) and y in case (c).

If q is even, then we are in case (b) and we have $y \in E_7(q_0)$ and $x \in G = \langle G_0, \varphi^i\rangle$. If q is odd, then $y \in \mathrm{Inndiag}(E_7(q_0)) \setminus E_7(q_0)$ and $y^2 \in E_7(q_0)$, so Lemma 6.2 implies that $x \in G = \langle G_0, g\rangle$ in both cases (b) and (c). By Lemma 3.20, if we are in case (b) with q odd, then $|x| = e|y^2| = \frac{1}{2}e|y|$, whereas $|x| = e|y|$ in every other case (note that $|y| = |y^2|$ if q is even). Let us also note that $|y^2| = 1406$ if $q_0 = 3$ and $|y^2| \geqslant 20165$ if $q_0 \geqslant 4$.

Proposition 6.3. *Let $H \in \mathcal{M}(x)$. Then $H \in \mathcal{M}_1$ and H is non-parabolic.*

Proof. We proceed as in the proof of Proposition 5.1. By applying Proposition 3.7, we see that $H \notin \mathcal{M}_3$. Now assume $H \in \mathcal{M}_2$ and let S be the socle of H. We need to consider the possibilities for S described in Theorem 3.4.

First assume that $S = \mathrm{L}_3^\epsilon(16)$. Here $|S|$ is indivisible by 43, so $q_0 \geqslant 3$ and consequently $\mathrm{meo}(H) \leqslant 273 < |x|$. Next assume $S = \mathrm{L}_2(t)$ with $t \leqslant 388(2, t-1)$, so $t \leqslant 2^8$ if t is even. This case is ruled out since Proposition 3.5 gives $\mathrm{meo}(H) \leqslant t^2/(t-1) < |x|$. Now assume

TABLE 7. The relevant groups $G = \langle G_0, g\rangle$ for $G_0 = E_6^\epsilon(q)$

Case	g	Conditions		
(a)	δ	$q \equiv \epsilon \pmod 3$		
(b)(i)	φ^i		$\epsilon = +$	$i \in \Delta(f)$
(b)(ii)	$\gamma\varphi^i$		$\epsilon = (-)^{f/i}$	$i \in \Delta(f)$
(b)(iii)	$\delta^{\pm}\varphi^i$	$q \equiv 1 \pmod 3$	$\epsilon = +$	$i \in \Delta(f)$
(b)(iv)	$\delta^{\pm}\gamma\varphi^i$	$q \equiv \epsilon \pmod 3$	$\epsilon = (-)^{f/i}$	$i \in \Delta(f)$
(c)(i)	φ^i		$\epsilon = -$	$i \in \Delta(f)$
(c)(ii)	$\gamma\varphi^i$		$\epsilon = +$	$i \in \Delta(f)$ & f/i odd
(d)	γ			

$S = {}^2B_2(t)$ with $t = 2^{2k+1}$ and $k \leqslant 3$. Here $\mathrm{meo}(H) \leqslant 1035$ and we may assume $q_0 = 2$ and $t = 2^7$, but one checks that $|S|$ is indivisible by 43, so this case does not arise. Similarly, if $S = {}^2G_2(t)'$ with $t = 3^{2k+1}$ and $k \leqslant 2$, then $\mathrm{meo}(H) \leqslant 1355 < |x|$.

Now assume that $\mathrm{rk}(S) \in \{2, 3\}$ and $t \leqslant 9$. If $\mathrm{rk}(S) = 3$, then $\mathrm{meo}(H) \leqslant t^4/(t-1)$ and we reduce to the case $t = 8$ with $q_0 = 2$, but in every case, one checks that $|S|$ is indivisible by 43. Finally, let us assume $\mathrm{rk}(S) = 2$. If S is classical, then Proposition 3.5 implies that $\mathrm{meo}(H) < |x|$. If $S = G_2(t)'$, then $\mathrm{meo}(H) \leqslant 8(t^2+t+1)\log t$ and this upper bound is less than $|x|$ unless $q_0 = 2$ and $t \in \{4, 8\}$, but in both cases, $|S|$ is indivisible by 43.

To complete the proof, let us observe that $y^2 \in E_7(q_0)$ is contained in a unique maximal subgroup of $E_7(q_0)$ (see [35, Tables III and IV]). In particular, y is not contained in a maximal parabolic subgroup of $E_7(q_0)$, so by applying Corollary 3.24, we deduce that x is not contained in a maximal parabolic subgroup of G. □

Proposition 6.4. *The conclusion to Theorem 8 holds in cases (b) and (c) of Table 6.*

Proof. We proceed as usual, via Lemma 3.17. Let $H \in \mathcal{M}(x)$ and let $z \in G$ be nontrivial. Then Proposition 6.3 implies that $H \in \mathcal{M}_1$ and H is not a parabolic subgroup, so [47, Theorem 2] gives $\mathrm{fpr}(z, G/H) \leqslant 2q^{-12}$. Now

$$|C_{\mathrm{Inndiag}(E_7(q_0))}(y^2)| = |y| \leqslant (q_0+1)(q_0^6 - q_0^3 + 1)$$

and by applying Proposition 3.3 and Lemma 3.25, we deduce that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < (30 + \log\log q) \cdot (q_0+1)(q_0^6 - q_0^3 + 1) \cdot 2q^{-12} < q^{-1}.$$

The result follows. □

By combining Propositions 6.1 and 6.4, we get the following.

Theorem 6.5. *The conclusion to Theorem 8 holds when $G_0 = E_7(q)$.*

7. Proof of Theorem 8: $G_0 = E_6^\epsilon(q)$

In this section we study the almost simple groups $G = \langle G_0, g\rangle$, where $G_0 = E_6^\epsilon(q)$ for some sign $\epsilon \in \{+, -\}$. The description of $\mathrm{Out}(G_0)$ in Section 3.2 shows that there are several different types of automorphism g that we must consider in order to prove Theorem 8 in this setting. More precisely, in light of Proposition 3.15, it suffices to consider the groups recorded in Table 7 (as before, we write $\Delta(f)$ for the set of proper positive divisors of f).

Let us briefly comment on the distinction between cases (b) and (c) in Table 7. The elements g that arise in these two cases are precisely the automorphisms of G_0 that are not

contained in $\langle \mathrm{Inndiag}(G_0), \gamma\rangle$. One can check that such an automorphism features in case (b) if and only if

$$\langle G_0, g\rangle \cap \langle \mathrm{Inndiag}(G_0), \gamma\rangle \leqslant \mathrm{Inndiag}(G_0).$$

We will see that Shintani descent applies in the usual way in case (b), but in case (c) we need to apply Lemma 3.26 (see Example 3.28, which contrasts cases (b)(ii) and (c)(ii) when $\epsilon = +$ and $p = 3$).

Recall that Remark 3.16 (in particular, the notes labelled $\star$ and †) permits us to omit some of the cases in Table 7 if certain conditions on p, f and i are satisfied. We will consider cases (a)–(d) in Sections 7.1–7.4, respectively.

It will be useful to note that if G is any almost simple group with socle $E_6^\epsilon(q)$, then [47, Theorem 1] gives

$$\mathrm{fpr}(z, G/H) \leqslant \begin{cases} (q^4 - q^2 + 1)^{-1} & \text{if } \epsilon = + \\ (q^6 - q^3 + 1)^{-1} & \text{if } \epsilon = - \end{cases} \tag{18}$$

for all $H \in \mathcal{M}$ and all nontrivial $z \in G$.

7.1. **Case (a): diagonal automorphisms.** We begin by handling the case where g is a diagonal automorphism.

Proposition 7.1. *The conclusion to Theorem 8 holds in case (a) of Table 7.*

Proof. Here $q \equiv \epsilon \pmod 3$ and $G = \langle G_0, \delta\rangle = \mathrm{Inndiag}(G_0)$. Fix an element $x \in G \setminus G_0$ of order $q^6 + \epsilon q^3 + 1$. By [68, Sections 4(g) and (h)], x is contained in a unique maximal subgroup of G (namely, a subgroup of type $\mathrm{SL}_3^\epsilon(q^3).3$). Therefore, with the bound in (18), we get

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (q^4 - q^2 + 1)^{-1}$$

for all nontrivial $z \in G$ and the result follows. □

7.2. **Case (b): Shintani descent.** Here we consider cases (b)(i)–(b)(iv) in Table 7. Fix a proper divisor i of f and write $e = f/i$ and $q = q_0^e$. Recall that in cases (iii) and (iv), e is even if $\epsilon = +$ and e is odd if $\epsilon = -$. Let $\bar{G}$ be the adjoint algebraic group of type E_6 over $\bar{\mathbb{F}}_p$ and define

$$(\sigma, \eta) = \begin{cases} (\varphi^i, +) & \text{in cases (i) and (iii)} \\ (\gamma\varphi^i, -) & \text{in cases (ii) and (iv).} \end{cases}$$

Notice that $\epsilon = \eta^e$ and $\bar{G}_\sigma = \mathrm{Inndiag}(E_6^\eta(q_0))$. Let

$$F\colon\ \mathrm{Inndiag}(E_6^\epsilon(q))\sigma \to \mathrm{Inndiag}(E_6^\eta(q_0))$$

be the Shintani map of $(\bar{G}, \sigma, e)$. The following result is the analogue of Lemma 6.2.

Lemma 7.2. *If $q_0 \equiv \eta \pmod 3$, then the Shintani map F restricts to bijections*

$$\{(t\sigma)^{\mathrm{Inndiag}(E_6^\epsilon(q))} : t \in E_6^\epsilon(q)\} \to \{y^{\mathrm{Inndiag}(E_6^\eta(q_0))} : y \in E_6^\eta(q_0)\}$$
$$\{(t\delta\sigma)^{\mathrm{Inndiag}(E_6^\epsilon(q))} : t \in E_6^\epsilon(q)\} \to \{y^{\mathrm{Inndiag}(E_6^\eta(q_0))} : y \in \mathrm{Inndiag}(E_6^\eta(q_0)) \setminus E_6^\eta(q_0)\}.$$

Proof. By hypothesis $q_0 \equiv \eta \pmod 3$, which implies that $q = q_0^e \equiv \eta^e = \epsilon \pmod 3$ and thus

$$|\,\mathrm{Inndiag}(E_6^\epsilon(q)) : E_6^\epsilon(q)| = |\,\mathrm{Inndiag}(E_6^\eta(q_0)) : E_6^\eta(q_0)| = 3.$$

We have already noted that $\bar{G}_{\sigma^e} = \mathrm{Inndiag}(E_6^\epsilon(q))$ and $\bar{G}_\sigma = \mathrm{Inndiag}(E_6^\eta(q_0))$. Also observe that $E_6^\epsilon(q) = (\bar{G}_{\sigma^e})'$ and $E_6^\eta(q_0) = O^{p'}(\bar{G}_\sigma) = (\bar{G}_\sigma)'$. Therefore, in order to apply Lemma 3.21 it remains to check that $\langle G_0, \sigma\rangle \trianglelefteqslant \langle \bar{G}_{\sigma^e}, \sigma\rangle$. In cases (i) and (iii) we have $\sigma = \varphi^i$ and $\epsilon = \eta = +$, so $p^i = q_0 \equiv 1 \pmod 3$. From (13) we see that $[\ddot{\varphi}^i, \ddot{\delta}] = \ddot{\delta}^{p^i - 1} = 1$, whence $\langle \ddot{\sigma}\rangle \trianglelefteqslant \langle \ddot{\sigma}, \ddot{\delta}\rangle = \langle \bar{G}_{\sigma^e}, \sigma\rangle/G_0$ and consequently $\langle G_0, \sigma\rangle \trianglelefteqslant \langle \bar{G}_{\sigma^e}, \sigma\rangle$. Similarly, $\sigma = \gamma\varphi^i$ and $p^i = q_0 \equiv 2 \pmod 3$ in cases (ii) and (iv). Here (13) and (15) give $[\ddot{\gamma}\ddot{\varphi}^i, \ddot{\delta}] = \ddot{\delta}^{-p^i - 1} = 1$, so

we again obtain $\langle \ddot{\sigma} \rangle \trianglelefteqslant \langle \ddot{\sigma}, \ddot{\delta} \rangle$ and $\langle G_0, \sigma \rangle \trianglelefteqslant \langle \bar{G}_{\sigma^e}, \sigma \rangle$. By applying Lemma 3.21, we see that the Shintani map F restricts to the bijections in the statement. $\square$

Fix a regular semisimple element $y \in \mathrm{Inndiag}(E_6^\eta(q_0))$ such that

$$|y| = q_0^6 + \eta q_0^3 + 1$$

and

$$C_{\mathrm{Inndiag}(E_6^\eta(q_0))}(y^3) = \langle y \rangle$$

(see [54]). Choose $x \in \langle \mathrm{Inndiag}(E_6^\epsilon(q)), \varphi^i \rangle$ such that

$$F(x) = \begin{cases} y^3 & \text{in cases (i) and (ii)} \\ y & \text{in cases (iii) and (iv).} \end{cases}$$

If $q \not\equiv \epsilon \pmod 3$, then we are in case (i) or (iii) and we have $y \in E_6^\eta(q_0)$ and $x \in G = \langle G_0, g \rangle$. If $q_0 \equiv \eta \pmod 3$ (so $q \equiv \epsilon \pmod 3$), then $y \in \mathrm{Inndiag}(E_6^\eta(q_0)) \setminus E_6^\eta(q_0)$ and $y^3 \in E_6^\eta(q_0)$, so Lemma 7.2 implies that $x \in G = \langle G_0, g \rangle$ once again. Finally, suppose that $q \equiv \epsilon \pmod 3$ and $q \not\equiv \eta \pmod 3$. Here the notes $\star$ and $\dagger$ in Remark 3.16 imply that we only need to consider one automorphism from $\{\varphi^i, \delta\varphi^i, \delta^2\varphi^i\}$, so the fact that $x \in \langle \mathrm{Inndiag}(E_6^\epsilon(q)), \varphi^i \rangle$ is enough to ensure that $x \in \langle G_0, g \rangle$ for a suitable choice of g.

By Lemma 3.20, we note that

$$|x| = \begin{cases} e|y^3| & \text{in cases (i) and (ii)} \\ e|y| & \text{in cases (iii) and (iv).} \end{cases}$$

Let us also note that if $\eta = +$, then $|y^3| = 73$ for $q_0 = 2$, $|y^3| = 757$ for $q_0 = 3$, $|y^3| = 1387$ for $q_0 = 4$ and $|y^3| \geqslant 15751$ for $q_0 \geqslant 5$, so $|y^3|$ is prime in the first two cases. Similarly, if $\eta = -$ then $|y^3| = 19$ for $q_0 = 2$, $|y^3| = 703 = 19 \cdot 37$ for $q_0 = 3$ and $|y^3| \geqslant 4033$ for $q_0 \geqslant 4$.

Proposition 7.3. *Let $H \in \mathcal{M}(x)$. Then $H \in \mathcal{M}_1$ and H is non-parabolic.*

Proof. Let us begin by noting that y^3 is not contained in a maximal parabolic subgroup of $E_6^\eta(q_0)$ (in fact, y^3 is contained in a unique maximal subgroup of $E_6^\eta(q_0)$; see [68, Sections (g) and (h)]), so Corollary 3.24 implies that H is non-parabolic.

Seeking a contradiction suppose that $H \in \mathcal{M}_2 \cup \mathcal{M}_3$ with socle S. First assume that $H \in \mathcal{M}_3$. Then the bound on $\mathrm{meo}(H)$ in Proposition 3.7 implies that $\eta = -$ and $q_0 = 2$. Here $|y| = 19$ and by inspecting each candidate for S in [50], it is easy to check that $\mathrm{Aut}(S) \setminus S$ does not contain an element of order divisible by 19.

Now suppose $H \in \mathcal{M}_2$. First assume that $\eta = +$. If $S = \mathrm{L}_3^{\epsilon'}(16)$, then $|S|$ is indivisible by 73, so $q_0 \geqslant 3$ and Proposition 3.5 implies that $\mathrm{meo}(H) < |x|$. If $S = \mathrm{L}_2(t)$ with $t \leqslant 124\,(2, t-1)$, then $\mathrm{meo}(H) \leqslant t^2/(t-1) < |x|$. If $S = {}^2B_2(t)$ with $t = 2^{2k+1}$ then $k \leqslant 2$ and $\mathrm{meo}(H) \leqslant 205$, so $q_0 = 2$ is the only option, but in both cases we find that $|S|$ is indivisible by 73. If $S = {}^2G_2(t)'$, then Proposition 3.5 implies that $\mathrm{meo}(H) < |x|$.

Next assume that $\mathrm{rk}(S) = 3$ and $t \leqslant 9$ (we continue to assume that $\eta = +$). Here the bound on $\mathrm{meo}(H)$ from Proposition 3.5 gives an immediate reduction to the case $t = 8$ with $q_0 = 2$. The cases $S = \mathrm{L}_4(8)$ and $\mathrm{PSp}_6(8)$ are ruled out by Proposition 3.8 and one checks that $|\mathrm{U}_4(8)|$ is indivisible by 73. Finally, suppose $\mathrm{rk}(S) = 2$. For classical S, the bound in Proposition 3.5 is sufficient. Similarly, if $S = G_2(t)'$ then by applying Proposition 3.5 we reduce to the cases where (t, q_0) is one of $(4, 2)$, $(8, 2)$ or $(9, 3)$. Here $|G_2(4)|$ and $|G_2(9)|$ are indivisible by 73 and 757 respectively, and the case $S = G_2(8)$ is ruled out by Proposition 3.8.

Finally, let us assume $\eta = -$. We proceed as before, first noting that the cases where S is one of $\mathrm{L}_3^{\epsilon'}(16)$, $\mathrm{L}_2(t)$, ${}^2B_2(t)$ and ${}^2G_2(t)'$ present no difficulties. Suppose $\mathrm{rk}(S) = 3$ and $t \leqslant 9$. Here S is classical and by applying the bound on $\mathrm{meo}(H)$ in Proposition 3.5, we reduce to the case $q_0 = 2$ with $t \in \{4, 8\}$. One checks that $|\mathrm{L}_4^{\epsilon'}(4)|$ and $|\mathrm{L}_4(8)|$ are indivisible by 19, so

these options are ruled out. For $S = \mathrm{U}_4(8)$, with the aid of Magma [7], we find that there are no elements in $\mathrm{Aut}(S) \setminus S$ of order divisible by 19 and so this possibility is also eliminated.

Now assume that $\mathrm{rk}(S) = 2$. If $S = \mathrm{L}_3(t)$, then Proposition 3.5 implies that $\mathrm{meo}(H) < |x|$ unless $t = 8$ and $q_0 = 2$, but this case does not arise since $|\mathrm{L}_3(8)|$ is indivisible by 19. Similar reasoning handles the case $S = \mathrm{PSp}_4(t)$. For $S = G_2(t)'$, the bound coming from Proposition 3.5 is effective unless (t, q_0) is one of $(4, 2)$, $(8, 2)$ or $(9, 3)$. We can rule out the latter case since $|G_2(9)|$ is indivisible by 37. Similarly, $|G_2(4)|$ is indivisible by 19 and the case $S = G_2(8)$ is eliminated by applying Proposition 3.8.

Finally, suppose that $S = \mathrm{U}_3(t)$. As before, by applying Proposition 3.5 we reduce to the case $t = 8$ with $q_0 = 2$. Using Magma, we find that there are elements in $\mathrm{Aut}(S) \setminus S$ of order $19m$ for some positive integer m if and only if $m = 3$, so we must have $G_0 = {}^2E_6(8)$ and $g = \varphi$ (so $e = 3$ and $|x| = e|y^3| = 3(2^6 - 2^3 + 1)/(2 + 1, 3) = 57$). To resolve this case, we appeal to [25, Theorem 1.2], which states that S is *strongly imprimitive* in the ambient simple algebraic group $\bar{G} = E_6$ (also see [25, Proposition 10.2]). In the context of Theorem 3.2, this means that every almost simple subgroup of G with socle $\mathrm{U}_3(8)$ is contained in a type (I) maximal subgroup of G, so this case does not arise. □

Proposition 7.4. *The conclusion to Theorem 8 holds in case (b) of Table 7.*

Proof. Let $H \in \mathcal{M}(x)$ and let $z \in G$ be nontrivial. By Proposition 7.3, $H \in \mathcal{M}_1$ and H is non-parabolic, so [47, Theorem 2] gives $\mathrm{fpr}(z, G/H) \leqslant 2q^{-6}$. Since

$$|C_{\mathrm{Inndiag}(E_6^\eta(q_0))}(y^3)| = |y| = q_0^6 + \eta q_0^3 + 1,$$

we see that Proposition 3.3 and Lemma 3.25 imply that

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < (19 + \log\log q) \cdot (q_0^6 + \eta q_0^3 + 1) \cdot 2q^{-6}.$$

If $q > 7$, then the upper bound is at most q^{-1}, and for $q > 4$ it is less than $\frac{1}{2}$. Finally, if $q = 4$ then we find that there are at most 14 conjugacy classes of subgroups in $\mathcal{M}(x)$ (for example, there are no exotic locals). Replacing the $19 + \log\log q$ factor by 14 in the above bound shows that $P(z, x) < \frac{1}{2}$, which completes the proof. □

7.3. **Case (c): Shintani descent over F_4.** We now turn to case (c) in Table 7, which involves two subcases labelled (i) and (ii). Here we can apply Shintani descent in the indirect manner encapsulated in Lemma 3.26 (compare with the method adopted in [38, Sections 5.4.2 and 6.4.2]).

Fix a proper divisor i of f and write $e = f/i$ and $q = q_0^e$. Recall that in case (ii) we have $\epsilon = +$ and e is odd, whereas $\epsilon = -$ in case (i) (and there is no parity condition on e). Let $\bar{G}$ be the adjoint algebraic group E_6 over $\bar{\mathbb{F}}_p$ and let σ be the Steinberg endomorphism φ^i in case (i) and $\gamma\varphi^i$ in case (ii). Observe that $\bar{G}_{\gamma\sigma^e} = \mathrm{Inndiag}(G_0)$ in both cases. Let $\bar{K} = C_{\bar{G}}(\gamma) = F_4$ and note that $\bar{K}$ is σ-stable. Choose $y \in \bar{K}_\sigma = F_4(q_0) \leqslant E_6^{-\epsilon}(q_0)$ such that

$$|y| = q_0^4 - q_0^2 + 1$$

and $C_{\bar{K}_\sigma}(y) = \langle y \rangle$. Here γ is an algebraic automorphism of $\bar{G}$ of order 2, so by Lemma 3.26(i), there exists $x \in \bar{K}_{\sigma^e}\sigma = F_4(q)g \subseteq E_6^\epsilon(q)g$ such x^e is $\bar{G}$-conjugate to $y\gamma$. In addition, since $|y^2|$ is odd, we note that $|x| = 2e|y|$ (see Remark 3.27).

Proposition 7.5. *Let $H \in \mathcal{M}(x)$. Then $H \in \mathcal{M}_1$ and H is non-parabolic.*

Proof. By considering the order of y^2, we observe that y^2 is not contained in a maximal parabolic subgroup of $E_6^{-\epsilon}(q_0)$. Therefore, Lemma 3.26(ii)(b) implies that there are no parabolic subgroups in $\mathcal{M}(x)$.

For the remainder, let us assume $H \in \mathcal{M}_2 \cup \mathcal{M}_3$ has socle S. First assume $H \in \mathcal{M}_2$, noting that the possibilities for S are described in Theorem 3.4. Suppose $S = \mathrm{L}_3(16)$. Here $p = 2$

and $\mathrm{meo}(H) \leqslant 273$, so $q_0 = 2$ is the only possibility and thus $|x| = 26e$, but one checks that there are no elements of order $26e$ (with $e \geqslant 2$) in $\mathrm{Aut}(S) \setminus S$, so this case does not arise. A very similar argument rules out $S = \mathrm{U}_3(16)$. Next assume $S = \mathrm{L}_2(t)$ with $t \leqslant 124\,(2, t-1)$. By applying Proposition 3.5 we reduce to $q_0 \in \{2, 3\}$, but we find that there are no elements of order $2e|y|$ in $\mathrm{Aut}(S) \setminus S$. Very similar reasoning eliminates the cases where S is either ${}^2B_2(t)$ or ${}^2G_2(t)'$.

To complete the analysis of the candidates in $\mathcal{M}_2$, we may assume S is a simple group of Lie type over $\mathbb{F}_t$ with $\mathrm{rk}(S) \in \{2, 3\}$ and $t \leqslant 9$. Suppose $\mathrm{rk}(S) = 3$, so Proposition 3.5 gives $\mathrm{meo}(H) \leqslant t^4/(t-1)$. This bound reduces the problem to a handful of possibilities with $q_0 \in \{2, 3\}$, and apart from the cases where S is one of $\mathrm{L}_4(8)$, $\mathrm{U}_4(8)$ and $\mathrm{U}_4(9)$, one checks that there are no elements in $\mathrm{Aut}(S) \setminus S$ with order divisible by $|y|$.

To handle the three special cases, we proceed as follows. First assume $S = \mathrm{L}_4^{\epsilon'}(8)$, so $q_0 = 2$, $|y| = 13$ and one checks that there are elements in $\mathrm{Aut}(S) \setminus S$ of order $26e$ if and only if $e = 5$, so $q = 2^5$ and $\epsilon = +$. Now 13 is a primitive prime divisor of $q^{12} - 1$ and by inspecting [54] we see that $C_{G_0}(y)$ is either $C_{q^4-q^2+1} \times C_{q^2+q+1}$ or ${}^3D_4(q) \times C_{q^2+q+1}$. In particular, $|C_{G_0}(y)|$ is not divisible by 5. However, the centraliser of any element in S of order 13 has order $65m$, where $m = 9$ if $\epsilon' = +$ and $m = 7$ if $\epsilon' = -$. This is clearly a contradiction since $|C_S(y)|$ must divide $|C_{G_0}(y)|$. A very similar argument rules out the case $S = \mathrm{U}_4(9)$; here $q_0 = 3$, $e = 5$ and $\epsilon = +$. Moreover, $|y| = 73$ is a primitive prime divisor of $q^{12} - 1$. Therefore, the possibilities for $C_{G_0}(y)$ are as described above and in both cases we see that $|C_{G_0}(y)|$ is indivisible by 5. However, this is incompatible with the fact that every element in S of order 73 is centralised by an element of order 5.

Next assume that $\mathrm{rk}(S) = 2$. If S is classical, then Proposition 3.5 gives $\mathrm{meo}(H) \leqslant t^3/(t-1)$ and this reduces the problem to $t = 8$ with $q_0 = 2$, but in each case, one checks that there are no elements in $\mathrm{Aut}(S) \setminus S$ of order $26e$. Similarly, if $S = G_2(t)'$, then the bound in Proposition 3.5 is sufficient unless (t, q_0) is $(4, 2)$ or $(9, 3)$, or if $t = 8$ and $q_0 \in \{2, 4\}$. For the cases with $q_0 = 2$, it is easy to see that there are no elements in $\mathrm{Aut}(S) \setminus S$ of order $26e$. We can rule out $S = G_2(9)$ since Proposition 3.8 gives $\mathrm{meo}(\mathrm{Aut}(S) \setminus S) = 36$. Similarly, if $S = G_2(8)$ and $q_0 = 4$, then $|y| = 241$ and we note that $|\mathrm{Aut}(S)|$ is indivisible by 241.

Finally, let us assume $H \in \mathcal{M}_3$. By Proposition 3.7 we have $\mathrm{meo}(H) \leqslant 60$, so we immediately reduce to the case $q_0 = e = 2$. Here $|x| = 52$ and by inspecting the possibilities for S recorded in [50], it is straightforward to check that there are no elements in $\mathrm{Aut}(S) \setminus S$ of order 52. □

Lemma 7.6. *We have* $C_{\mathrm{Inndiag}(E_6^{-\epsilon}(q_0))}(y) = C_{q_0^4-q_0^2+1} \times C_{q_0^2-\epsilon q_0+1}$.

Proof. The centralisers of semisimple elements in $\mathrm{Inndiag}(E_6^{-\epsilon}(q_0))$ are listed in [54]. For a contradiction, suppose that the centraliser is not the one given in the statement. In terms of divisibility, we see that the only other possibility is ${}^3D_4(q_0) \times C_{q_0^2-\epsilon q_0+1}$. In this case, if $\bar{G} = E_6$ and $\bar{H} = F_4$ are the corresponding algebraic groups, then $C_{\bar{G}}(y) = D_4T_2$ and, as explained in the proof of [47, Lemma 5.4], this implies that $C_{\bar{H}}(y) = B_3T_1$. But y is a regular semisimple element of $\bar{H}$, so this is a contradiction. □

Proposition 7.7. *The conclusion to Theorem 8 holds in case (c) of Table 7.*

Proof. Let us first observe that since $\langle y^2 \rangle = \langle y \rangle$, Lemma 7.6 implies that

$$C_{\mathrm{Inndiag}(E_6^{-\epsilon}(q_0))}(y^2) = C_{q_0^4-q_0^2+1} \times C_{q_0^2-\epsilon q_0+1}.$$

Now let $H \in \mathcal{M}(x)$ and let $z \in G$ be nontrivial. Let $a(q)$ be the upper bound on $\mathrm{fpr}(z, G/H)$ given in (18). Then by combining Propositions 3.3 and 7.5, noting that there are no parabolic subgroups in $\mathcal{M}(x)$, and using Lemma 3.26(b)(i), we deduce that

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (19 + \log\log q) \cdot (q_0^4 - q_0^2 + 1)(q_0^2 + q_0 + 1) \cdot a(q).$$

Recalling that $e \geqslant 3$ if $\epsilon = +$, one checks that this bound is always less than $\frac{1}{2}$ and also less than q^{-1} for $q > 27$. □

7.4. **Case (d): involutory graph automorphisms.** To complete the proof of Theorem 8 for $G_0 = E_6^\epsilon(q)$, we may assume that $G = \langle G_0, g\rangle$, where g is the graph automorphism γ in Definition 3.9(iii). In particular, since g does not arise from a Steinberg endomorphism of the ambient algebraic group $\bar{G}$, we cannot use Shintani descent in this case and a different approach is required.

Choose $y \in C_{G_0}(g) = F_4(q)$ such that

$$|y| = q^4 - q^2 + 1$$

and $C_{F_4(q)}(y) = \langle y\rangle$. Set $x = yg \in G$ and note that $x^2 = y^2 \in G_0$ and $|x| = 2|y|$ since $|y| = q^4 - q^2 + 1$ is odd. In addition, $|y| \equiv 1 \pmod 3$ and we note that $|y|$ is divisible by a primitive prime divisor of $q^{12} - 1$, so $|y|$ divides $q^i - 1$ if and only if i is divisible by 12. It will also be useful to observe that $|y|$ is 13, 73, 241, 601 (all of which are prime) when q is 2, 3, 4, 5, respectively, and $|y| \geqslant 2353$ when $q \geqslant 7$.

Since $\mathcal{M}(x) \subseteq \mathcal{M}(y)$, we will focus on determining the subgroups in $\mathcal{M}(y)$ and we proceed by considering the cases arising in Theorem 3.2. It will be convenient to handle the cases $q = 2$ and $q > 2$ separately.

Proposition 7.8. *Assume that $q = 2$ and let $H \in \mathcal{M}(x)$.*

(i) *If $\epsilon = +$, then H has type $F_4(2)$ or ${}^3D_4(2) \times 7$.*
(ii) *If $\epsilon = -$, then H has type $F_4(2)$ or $\mathrm{SO}_7(3)$.*

Proof. First note that $|y| = 13$ and $|x| = 26$. Suppose $\epsilon = +$, so $G = \mathrm{Aut}(E_6(2)) = E_6(2).2$. In [44], the maximal subgroups of G are determined up to conjugacy and it is easy to read off the subgroups with order divisible by 13, giving the two cases recorded in part (i). Similar reasoning applies when $\epsilon = -$ and $G = {}^2E_6(2).2$, using the list of maximal subgroups presented in the Atlas [21] (also see [70]). In the latter case, note that $|\mathrm{Fi}_{22}|$ is divisible by 13, but Fi_{22}:2 does not contain any elements of order 26. □

Proposition 7.9. *If $q > 2$ and $H \in \mathcal{M}(x)$, then H has type $F_4(q)$ or ${}^3D_4(q) \times (q^2 + \epsilon q + 1)$.*

Proof. First assume $H \in \mathcal{M}_1$. Suppose H is of type (I) in Theorem 3.2, so $H = N_G(\bar{H}_\sigma)$ for some σ-stable closed subgroup $\bar{H}$ of $\bar{G}$. If $\bar{H}$ is parabolic, then H is of type $P_{1,6}$, P_2, $P_{3,5}$ or P_4 (since H is normalised by a graph automorphism) and in each case it is straightforward to check that $|H|$ is indivisible by $|y| = q^4 - q^2 + 1$. In the same way, by carefully inspecting [48], we deduce that the only candidate maximal rank subgroups in $\mathcal{M}(x)$ are of type ${}^3D_4(q) \times (q^2 + \epsilon q + 1)$. In addition, if the rank of $\bar{H}$ is less than 6, then $H \cap G_0 = F_4(q)$ is the only option and it is easy to see that there are no subgroups in $\mathcal{M}(x)$ of type (II) or (III).

To complete the proof, let us suppose that $H \in \mathcal{M}_2 \cup \mathcal{M}_3$ with socle S. If $H \in \mathcal{M}_3$, then Proposition 3.7 implies that $\mathrm{meo}(H) \leqslant 60$, which is a contradiction since $|x| \geqslant 146$. Now assume $H \in \mathcal{M}_2$, so the possibilities for S are described in Theorem 3.4. Here we use the bound on $\mathrm{meo}(H)$ from Proposition 3.5 to reduce the problem to a handful of cases with $q \in \{3, 4\}$. In each of these cases, one checks that $\mathrm{Aut}(S)$ contains an element of order $|x|$ if and only if $q = 3$ and S is either $\mathrm{U}_4(9)$ or $G_2(9)$. The latter case is ruled out by Proposition 3.8 since $\mathrm{meo}(\mathrm{Aut}(S) \setminus S) = 36 < |x|$, so let us assume $S = \mathrm{U}_4(9)$. Here $|y| = 73$ and $\mathrm{Aut}(S) \setminus S$ does contain elements of order $|x| = 146$, but we can eliminate this case by arguing as follows. By Lemma 7.6, we have $C_{G_0}(y) = C_{73m}$, where $m = 13$ if $\epsilon = +$ and $m = 7$ if $\epsilon = -$. However, every element in S of order 73 commutes with an element of order 5, which is a contradiction since $|C_S(y)|$ must divide $|C_{G_0}(y)|$. □

We will need the next two lemmas, which, in some special cases of interest, give slightly stronger fixed point ratio estimates than the relevant bounds presented in [47].

Lemma 7.10. *Let H be a maximal subgroup of G of type ${}^3D_4(q) \times (q^2 + \epsilon q + 1)$ and let $z \in G$ be nontrivial. Then*

$$\mathrm{fpr}(z, G/H) \leqslant 2q^{-6}.$$

Proof. In view of [47, Theorem 2], we may assume that $\epsilon = +$ and $z \in G$ is a graph automorphism (here [47] only gives $\mathrm{fpr}(z, G/H) \leqslant (q^4 - q^2 + 1)^{-1}$). By inspecting the proof of [12, Lemma 3.10], we see that $\mathrm{fpr}(z, G/H) < q^{-6}$ if $q \geqslant 3$. Finally, if $q = 2$, then $G = G_0.2 = \mathrm{Aut}(G_0)$,

$$H = ({}^3D_4(2) \times D_{14}){:}3, \quad H \cap G_0 = ({}^3D_4(2) \times 7){:}3$$

(see [44, Table 1], for example) and

$$|z^G \cap H| \leqslant i_2(H \setminus H \cap G_0) = 487312, \quad |z^G| \geqslant |E_6(2) : F_4(2)| = 64884736.$$

The result follows. □

Lemma 7.11. *Let K be a maximal subgroup of G of type $F_4(q)$ and let $z \in G$ be nontrivial. Then*

$$\mathrm{fpr}(z, G/K) \leqslant (q^6 - q^3 + 1)^{-1}.$$

Proof. Here $K = C_G(g) = F_4(q) \times \langle g \rangle$ and as in the previous lemma, we may assume $\epsilon = +$ and z is an involutory graph automorphism. Note that each element in $z^G \cap K$ is of the form sg, where $s \in F_4(q)$ satisfies $s^2 = 1$.

First assume that $C_{G_0}(z) = F_4(q)$. As explained in the proof of [47, Lemma 5.4], if $p \neq 2$, then

$$|z^G \cap K| = 1 + |x_1^{F_4(q)}| = 1 + q^8(q^8 + q^4 + 1)$$

and $x_1 \in F_4(q)$ is an involution with $C_{F_4}(x_1) = B_4$. Similarly, if $p = 2$, then

$$|z^G \cap K| = 1 + |x_2^{F_4(q)}| = 1 + (q^4 + 1)(q^{12} - 1),$$

where $x_2 \in F_4(q)$ is a short root element.

Now assume that $C_{G_0}(z) \neq F_4(q)$. Suppose $p \neq 2$, so $|C_{G_0}(z)| = |\mathrm{Sp}_8(q)|$. The group $F_4(q)$ has two classes of involutions and from the previous paragraph we deduce that $z^G \cap K$ is the set of involutions in K of the form sg with $C_{F_4}(s) = A_1C_3$. Therefore,

$$|z^G \cap K| = \frac{|F_4(q)|}{|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|} = q^{14}(q^6 + 1)(q^4 + q^2 + 1)(q^4 + 1).$$

For $p = 2$, we have

$$|C_{G_0}(z)| = |C_{F_4(q)}(t)| = q^{24}(q^2 - 1)(q^4 - 1)(q^6 - 1),$$

where $t \in F_4(q)$ is a long root element, and the proof of [47, Lemma 5.4] gives

$$|z^G \cap K| = (q^4 + 1)(q^{12} - 1) + (q^4 + 1)(q^6 - 1)(q^{12} - 1) + q^4(q^4 + q^2 + 1)(q^8 - 1)(q^{12} - 1).$$

In every case, the desired bound holds. □

We can now handle the case $q > 2$.

Proposition 7.12. *The conclusion to Theorem 8 holds in case (d) of Table 7 if $q > 2$.*

Proof. Let H and K be maximal subgroups of G of type ${}^3D_4(q) \times (q^2 + \epsilon q + 1)$ and $F_4(q)$, respectively, and note that there is a unique $\mathrm{Inndiag}(G_0)$-class of each type of subgroup. By Proposition 7.9, each subgroup in $\mathcal{M}(x)$ is conjugate to either H or K.

For any maximal subgroup $M \leqslant G$, let $n(M)$ be the number of conjugates of M that contain y, and note that

$$n(M) = \frac{|y^G \cap M|}{|y^G|} \cdot \frac{|G|}{|M|}.$$

First consider $n(H)$. Given the structure of H, we see that every element in H of order q^4-q^2+1 is contained in the subgroup $L = {}^3D_4(q)$ (indeed, note that q^4-q^2+1 and $q^2+\epsilon q+1$ are coprime for all q). Each $z \in L$ of order q^4-q^2+1 is self-centralising and by inspecting [26, Table 4.4] we deduce that L has $\frac{1}{4}q^2(q^2-1)$ distinct classes of semisimple elements with centraliser a cyclic maximal torus of order q^4-q^2+1. Therefore,

$$|y^G \cap H| \leqslant \frac{1}{4}q^2(q^2-1) \cdot \frac{|{}^3D_4(q)|}{q^4-q^2+1}$$

and this yields $n(H) \leqslant \frac{1}{12}q^2(q^2-1)$.

Now let us turn to $n(K)$. By inspecting [60, 63], we see that there are precisely $\frac{1}{12}q^2(q^2-1)$ regular semisimple classes in $F_4(q)$ with centraliser a torus of order q^4-q^2+1. Therefore,

$$|y^G \cap K| \leqslant \frac{1}{12}q^2(q^2-1) \cdot \frac{|F_4(q)|}{q^4-q^2+1}$$

and we deduce that

$$n(K) \leqslant \frac{1}{12}q^2(q^2-1)(q^2+\epsilon q+1).$$

Alternatively, we can bound $|y^G \cap K|$ by arguing as in the proof of [47, Lemma 4.5], noting that $|W(E_6) : W(F_4)| = 45$ (where $W(X)$ denotes the Weyl group of X). Indeed, it follows that $y^G \cap K$ is a union of at most 45 distinct K-classes, so

$$|y^G \cap K| \leqslant 45 \cdot \frac{|F_4(q)|}{q^4-q^2+1}$$

and subsequently $n(K) \leqslant 45(q^2+\epsilon q+1)$, which is a better bound for $q \geqslant 5$.

Finally, using the bounds in Lemmas 7.10 and 7.11, we deduce that

$$\sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant \frac{1}{12}q^2(q^2-1) \cdot 2q^{-6} + a(q) \cdot (q^2+\epsilon q+1) \cdot (q^6-q^3+1)^{-1}$$

for all nontrivial $z \in G$, where $a(q) = \frac{1}{12}q^2(q^2-1)$ if $q \leqslant 4$ and $a(q) = 45$ for $q \geqslant 5$. One checks that this upper bound is less than q^{-1} for all q. □

Finally, we deal with the special case $q = 2$.

Proposition 7.13. *The conclusion to Theorem 8 holds in case (d) of Table 7.*

Proof. In view of Proposition 7.12, we may assume $G_0 = E_6^{\epsilon}(2)$, so $|y| = 13$ and we note that G has a unique conjugacy class of elements of order 13 (see [16, Table 9], for example).

First assume $\epsilon = +$, so each subgroup in $\mathcal{M}(x)$ has type ${}^3D_4(2) \times 7$ or $F_4(2)$ (see Proposition 7.8(i)). Note that $|C_{G_0}(y)| = 91$ by Lemma 7.6. By repeating the argument in the proof of Proposition 7.12, we see that y is contained in a unique subgroup of type ${}^3D_4(2) \times 7$ and 7 subgroups of type $F_4(2)$. Therefore, by applying the fixed point ratio bounds in Lemmas 7.10 and 7.11, we deduce that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant 1 \cdot \frac{1}{2^5} + 7 \cdot \frac{1}{2^6-2^3+1} < \frac{1}{2}$$

for all nontrivial $z \in G$ and the result follows.

Now assume $\epsilon = -$, so Proposition 7.8(ii) informs us that the subgroups in $\mathcal{M}(x)$ are of type $F_4(2)$ or $\mathrm{SO}_7(3)$. Note that $C_{G_0}(y) = \langle y \rangle$. If $H \in \mathcal{M}(x)$ has type $F_4(2)$, then $|y^G \cap H| = i_{13}(F_4(2)) = |F_4(2)|/13$ and we deduce that y is contained in a unique conjugate of H. Similarly, if H has type $\mathrm{SO}_7(3)$, then $|y^G \cap H| = i_{13}(H) = |\mathrm{SO}_7(3)|/13$ and thus y is

TABLE 8. The relevant groups $G = \langle G_0, g\rangle$ for $G_0 = F_4(q)$

Case	g	Conditions
(a)	φ^i	i is a proper divisor of f
(b)	ρ^i	i is an odd divisor of f & $p = 2$

contained in 2 conjugates of H. Therefore, x is contained in at most 3 maximal subgroups of G and the bound in (18) implies that

$$P(z,x) \leqslant \sum_{H\in\mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant 3 \cdot \frac{1}{2^6 - 2^3 + 1} < \frac{1}{2}$$

for all nontrivial $z \in G$, as required. □

By combining Propositions 7.1, 7.4, 7.7 and 7.13, we obtain the following.

Theorem 7.14. *The conclusion to Theorem 8 holds when $G_0 = E_6^\epsilon(q)$.*

8. Proof of Theorem 8: $G_0 = F_4(q)$

We now turn to the groups with socle $G_0 = F_4(q)$. By Proposition 3.15, in order to prove Theorem 8 we may assume that $G = \langle G_0, g\rangle$, where g is recorded in Table 8. We will analyse cases (a) and (b) in Sections 8.1 and 8.2, respectively. It will be useful to observe that for all $H \in \mathcal{M}$ and all nontrivial $z \in G$, [47, Theorem 1] gives

$$\mathrm{fpr}(z, G/H) \leqslant (q^4 - q^2 + 1)^{-1}. \tag{19}$$

8.1. **Case (a): field automorphisms.** Fix a proper divisor i of f and write $e = f/i$ and $q = q_0^e$. Let $\bar{G}$ be the algebraic group F_4 and let σ be the Steinberg endomorphism φ^i of $\bar{G}$. Let $F\colon F_4(q)g \to F_4(q_0)$ be the Shintani map of $(\bar{G}, \sigma, e)$. Fix an element $y \in F_4(q_0)$ such that

$$|y| = \begin{cases} q_0^4 - q_0^2 + 1 & \text{if } q_0 > 2 \\ 17 & \text{if } q_0 = 2 \end{cases}$$

and $C_{F_4(q_0)}(y) = \langle y\rangle$ (see [54]). Choose $x \in G$ with $F(x) = y$ and note that $|x| = e|y|$ (see Lemma 3.20). In addition, note that $|y|$ is 7, 73, 241, 601 (all of which are prime) when q_0 is 2, 3, 4, 5, respectively, and that $|y| \geqslant 2353$ for $q_0 \geqslant 7$.

Proposition 8.1. *Let $H \in \mathcal{M}(x)$. Then $H \in \mathcal{M}_1$ and H is non-parabolic.*

Proof. First observe that the order of each maximal parabolic subgroup of $F_4(q_0)$ is indivisible by $|y|$, so Corollary 3.24 implies that there are no parabolic subgroups in $\mathcal{M}(x)$. For the remainder, let us assume $H \in \mathcal{M}_2 \cup \mathcal{M}_3$ has socle S.

Suppose $H \in \mathcal{M}_3$. By inspecting the possibilities for S given in [50], it is easy to see that $\mathrm{Aut}(S) \setminus S$ does not contain an element of order divisible by $|y|$. For the remainder, let us assume $H \in \mathcal{M}_2$.

Suppose $S = \mathrm{L}_3^\epsilon(16)$, so $p = 2$ and Proposition 3.5 gives $\mathrm{meo}(H) \leqslant 273$. Therefore, $q_0 = 2$ is the only possibility and we find that $\mathrm{Aut}(S) \setminus S$ contains elements of order 34 (and there are also elements of order $3 \cdot 17$ and $15 \cdot 17$ when $\epsilon = +$). This implies that $e \in \{2, 3, 15\}$. However, if $e \in \{2, 3\}$, then [17, Lemma 8.5] states that G does not have a maximal subgroup with socle $\mathrm{L}_3^\epsilon(16)$ and it is easy to see that the same proof also applies when $e = 15$.

Next assume $S = \mathrm{L}_2(t)$ with $t \leqslant 68\,(2, t-1)$. By applying the bound on $\mathrm{meo}(H)$ from Proposition 3.5, we quickly reduce to the case $q_0 = 2$ with $t = 2^6$, but $|\mathrm{L}_2(64)|$ is indivisible by $|y| = 17$, so this case does not arise. The cases $S = {}^2B_2(t)$ and ${}^2G_2(t)'$ are handled in the same way.

To complete the proof, we may assume that $\mathrm{rk}(S) = 2$ and $t \leqslant 9$. If S is classical, then by applying Proposition 3.5 we may assume $q_0 = 2$ and $t = 8$, but in each case one checks that $|S|$ is indivisible by 17. Finally, suppose $S = G_2(t)'$. Here the bound from Proposition 3.5 is sufficient unless $q_0 \in \{2, 3\}$. For $t \in \{2, 4, 8\}$, it is easy to check that $|S|$ is indivisible by 17. Similarly, $|G_2(3)|$ is indivisible by 73 and the case $S = G_2(9)$ is ruled out by Proposition 3.8. □

Proposition 8.2. *The conclusion to Theorem 8 holds in case (a) of Table 8.*

Proof. Let $H \in \mathcal{M}(x)$ and let $z \in G$ be nontrivial. By combining Propositions 3.3 and 8.1 with Lemma 3.25, we deduce that

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < (25 + \log\log q) \cdot |y| \cdot (q^4 - q^2 + 1)^{-1}.$$

If $q_0 \geqslant 3$, then this bound is always less than $\frac{1}{2}$ and it is less than q^{-1} for $q > 25$. If $q_0 = 2$, then $|y| = 7$ and again this bound is sufficient unless $q = 4$.

Therefore, for the remainder of the proof, we may assume that $q = 4$. In this case, $|x| = 34$. By Proposition 8.1, we know that $H \in \mathcal{M}_1$ is non-parabolic. Moreover, by carefully considering the subgroups of type (I) to (IV) in Theorem 3.2, noting that $|H \cap \bar{G}_\sigma|$ is divisible by 17, we deduce that there are at most 5 G_0-classes of subgroups in $\mathcal{M}(x)$, namely

$$\begin{aligned} &\mathrm{Aut}(\mathrm{Sp}_8(4)) = \mathrm{Sp}_8(4).2 \text{ (two classes)} \\ &\mathrm{Aut}(\Omega_8^+(4)) = \Omega_8^+(4).\mathrm{Sym}_3.2 \text{ (two classes)} \\ &F_4(2) \times 2 \end{aligned}$$

Now y is contained in exactly two maximal subgroups of $F_4(2)$, both of type $\mathrm{Sp}_8(2)$ (see [35, Table IV]). Since B_4 and C_4 are closed connected maximal subgroups of $\bar{G}$, Lemma 3.23 implies that x is contained in exactly two maximal subgroups of G of type $\mathrm{Sp}_8(4).2$. Therefore

$$P(z, x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < \frac{2 + 3 \cdot 17}{4^4 - 4^2 + 1} = \frac{53}{241} < \frac{1}{2}$$

for all nontrivial $z \in G$ and we have proved the result. □

8.2. **Case (b): graph-field automorphisms.** Now let us turn to case (b) in Table 8. Here $q = 2^f$ and i is an odd divisor of f. As usual, write $e = f/i$ and $q = q_0^e$, where $e \geqslant 1$. Let σ be the graph-field Steinberg endomorphism ρ^i of $\bar{G} = F_4$ and let $F\colon F_4(q)g \to {}^2F_4(q_0)$ be the Shintani map of $(\bar{G}, \sigma, 2e)$. Let $y \in {}^2F_4(q_0)$ be a regular semisimple element such that

$$|y| = q_0^2 + \sqrt{2q_0^3} + q_0 + \sqrt{2q_0} + 1$$

and $C_{{}^2F_4(q_0)}(y) = \langle y \rangle$ (see [61, Table IV]). Let $x \in G$ be a Shintani correspondent of y and note that $|x| = 2e|y|$ by Lemma 3.20. In addition, observe that $|y|$ is 13, 109, 1321 (all of which are prime) when q_0 is 2, 8, 32, respectively, and $|y| \geqslant 18577$ if $q > 32$.

First we settle the case $q = 2$.

Proposition 8.3. *The conclusion to Theorem 8 holds in case (b) of Table 8 with $q = 2$.*

Proof. Here $G = \mathrm{Aut}(G_0) = G_0.2$ and the maximal subgroups of G are determined up to conjugacy by Norton and Wilson in [57]. By inspecting [57, Table 1], we see that the only maximal subgroups of G containing y (other than G_0) are of the form $H = {}^2F_4(2) \times 2$ and $K = \mathrm{L}_4(3){:}2^2$ (the latter is in $\mathcal{M}_3$) and there is a unique conjugacy class of each type of subgroup. As before, we write $n(H)$ and $n(K)$ for the number of conjugates of H and K, respectively, that contain y. Now $F_4(2)$ has a unique class of elements of order 13, so $C_{G_0}(y) = \langle y \rangle$ and

we deduce that $|y^G \cap H| = i_{13}(H) = |{}^2F_4(2)|/13$ and $|y^G \cap K| = i_{13}(\mathrm{L}_4(3)) = 4|\mathrm{L}_4(3)|/13$. Therefore, $n(H) = 1$ and $n(K) = 2$. Finally, by applying the bound in (19), we see that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant \frac{3}{13}$$

for all nontrivial $z \in G$ and the result follows. □

Proposition 8.4. *If $e = 1$ and $q \geqslant 8$, then each $H \in \mathcal{M}(x)$ is of type ${}^2F_4(q)$ or $C_{q^4-q^2+1}{:}C_{12}$.*

Proof. Let $H \in \mathcal{M}(x)$ and observe that $|H|$ is divisible by $|y|$. Then just by considering the orders of the maximal parabolic subgroups $P_{1,4}$ and $P_{2,3}$, we immediately deduce that H is non-parabolic. As in previous cases, the bound on $\mathrm{meo}(H)$ in Proposition 3.7 eliminates the subgroups in $\mathcal{M}_3$. Similarly, if $H \in \mathcal{M}_2$ has socle S, then Proposition 3.5 reduces the analysis to a handful of cases with $q \in \{8, 32\}$ and in each one it is clear that there are no elements in $\mathrm{Aut}(S) \setminus S$ of order $|x|$. Finally, if $H \in \mathcal{M}_1$ then the fact that $|H|$ is divisible by $|y|$ is highly restrictive and by inspecting the subgroups of type (I), (II) and (III) in Theorem 3.2 it is easy to check that the only possibilities are those of type ${}^2F_4(q)$ and $C_{q^4-q^2+1}{:}C_{12}$ (here we note that the maximal rank subgroups of type ${}^3D_4(q).3$ are non-maximal since G contains graph-field automorphisms). This completes the proof and we note that there is a unique G_0-class of subgroups of each type. □

Proposition 8.5. *If $e > 1$ then each $H \in \mathcal{M}(x)$ is non-parabolic and contained in $\mathcal{M}_1$.*

Proof. To see this, let us first observe that $|x| \geqslant 52$, so subgroups in $\mathcal{M}_3$ are ruled out by Proposition 3.7. Now assume $H \in \mathcal{M}_2$. By applying the bound on $\mathrm{meo}(H)$ in Proposition 3.5, we quickly reduce to a handful of cases with $q_0 \in \{2, 8\}$. In each of these, one checks that $\mathrm{Aut}(S) \setminus S$ has an element of order divisible by $|y|$ if and only if $S = \mathrm{L}_3(16)$ or $\mathrm{PSp}_4(8)$ (both with $q_0 = 2$, so $|y| = 13$). However, in both cases, there are no elements in $\mathrm{Aut}(S) \setminus S$ of order $26e$ with $e \geqslant 2$. Finally, observe that the order of y is not compatible with the containment of y in a maximal parabolic subgroup of ${}^2F_4(q_0)$, so Corollary 3.24 implies that there are no maximal parabolic subgroups in $\mathcal{M}(x)$. □

Proposition 8.6. *The conclusion to Theorem 8 holds in case (b) of Table 8.*

Proof. In view of Proposition 8.3, we may assume $q > 2$. Let $H \in \mathcal{M}(x)$ and let $z \in G$ be nontrivial. Recall that $C_{2_{F_4(q_0)}}(y) = \langle y \rangle$. If $e = 1$, then by combining Lemma 3.25 with Proposition 8.4 and the bound in (19), we deduce that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < 2 \cdot |y| \cdot (q^4 - q^2 + 1)^{-1} < \frac{1}{q}$$

for all nontrivial $z \in G$. Similarly, if $e > 1$ then by applying Propositions 3.3 and 8.5 we get

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) < (21 + \log\log q) \cdot |y| \cdot (q^4 - q^2 + 1)^{-1}.$$

One checks that this upper bound is less than q^{-1} for $q > 4$, but the case $q = 4$ requires further attention (even for the desired $\frac{1}{2}$ bound).

Assume that $q = 4$ with $q_0 = 2$ and $e = 2$, so $|x| = 52$. By Proposition 8.5, we know that each $H \in \mathcal{M}(x)$ is non-parabolic and is contained in $\mathcal{M}_1$. There are no exotic local subgroups (see [20]) and so it remains to consider the maximal rank subgroups in $\mathcal{M}(x)$, together with the subfield subgroup $F_4(2)$. By inspecting [48], using the fact that $H \cap G_0$ must contain elements of order 13 and G contains graph-field automorphisms, we deduce that the only possible maximal rank subgroups in $\mathcal{M}(x)$ are of type $\mathrm{U}_3(4)^2.2$ and $13^2{:}(3 \times \mathrm{SL}_2(3))$. In particular, we may replace the leading factor $21 + \log\log q$ in the above bound by 3 and the result follows. □

TABLE 9. The relevant groups $G = \langle G_0, g\rangle$ for $G_0 = {}^3D_4(q)$

Case	g	Conditions
(a)	$\tau\varphi^i$	$i \in \Delta(f)$ & $f/i \not\equiv 0 \pmod 3$
(b)	φ^i	$i \in \Delta(f)$
(c)	τ	

By combining Propositions 8.2 and 8.6, we have now proved the following theorem.

Theorem 8.7. *The conclusion to Theorem 8 holds when $G_0 = F_4(q)$.*

9. Proof of Theorem 8: $G_0 = {}^3D_4(q)$

In this final section, we complete the proof of Theorem 8 by handling the almost simple groups G with socle $G_0 = {}^3D_4(q)$. In [41], Kleidman determines the maximal subgroups of G and we note that G has at most $10 + \log\log q$ conjugacy classes of maximal subgroups. In addition, [47, Theorem 1] gives the bound

$$\mathrm{fpr}(z, G/H) \leqslant (q^4 - q^2 + 1)^{-1} \tag{20}$$

for all $H \in \mathcal{M}$ and all nontrivial $z \in G$.

By considering Proposition 3.15, we see that it suffices to assume $G = \langle G_0, g\rangle$, where g is recorded in Table 9. In this table, we write $\Delta(f)$ for the set of positive proper divisors of f and τ is the triality graph automorphism of G_0 in Definition 3.9(iii).

9.1. **Case (a): Shintani descent.** Here i is a proper divisor of f and $e = f/i$ is indivisible by 3. Set $q = q_0^e$ and let $\bar{G}$ be the adjoint algebraic group D_4 over $\bar{\mathbb{F}}_p$. Let σ be the Steinberg endomorphism $\tau\varphi^i$ of $\bar{G}$ and let $F\colon {}^3D_4(q)g \to {}^3D_4(q_0)$ be the Shintani map of $(\bar{G}, \sigma, e)$. Choose $y \in {}^3D_4(q_0)$ such that $|y| = q_0^4 - q_0^2 + 1$ and $C_{{}^3D_4(q_0)}(y) = \langle y\rangle$. Let $x \in G$ be a Shintani correspondent, so $|x| = e|y|$.

Proposition 9.1. *The conclusion to Theorem 8 holds in case (a) of Table 9.*

Proof. First observe that y is not contained in a maximal parabolic subgroup of ${}^3D_4(q_0)$, since $|y|$ does not divide the order of any such group, whence x is not contained in a maximal parabolic subgroup of G by Corollary 3.24. Therefore, in view of Lemma 3.25 and the bound in (20), we deduce that

$$\sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (8 + \log\log q) \cdot |y| \cdot (q^4 - q^2 + 1)^{-1}$$

for all nontrivial $z \in G$. One checks that this bound is always sufficient (in particular, the bound is less than q^{-1} for $q > 4$). □

9.2. **Case (b): Shintani descent over G_2.** In this case, we can proceed as in Section 7.4, using Lemma 3.26. Fix a proper divisor i of f and write $e = f/i$ and $q = q_0^e$. Set $\bar{G} = D_4$ and let σ be the Steinberg endomorphism φ^i. In addition, let τ be a triality graph automorphism of $\bar{G}$ such that $\bar{K} = C_{\bar{G}}(\tau) = G_2$ and note that $\bar{K}$ is σ-stable and $\bar{G}_{\tau\sigma^e} = {}^3D_4(q)$. Fix an element $y \in \bar{K}_\sigma = G_2(q_0)$ of order

$$|y| = \begin{cases} q_0^2 - q_0 + 1 & \text{if } q_0 > 2 \\ 7 & \text{if } q_0 = 2. \end{cases}$$

By Lemma 3.26(i), there exists $x \in \bar{K}_{\sigma^e}\sigma = G_2(q)g \subseteq {}^3D_4(q)g$ such that x^e is $\bar{G}$-conjugate to $y\tau^2$. In particular, x^{3e} is $\bar{G}$-conjugate to y^3. By Remark 3.27, $|x| = 3e|y^3|$ and we note that $|y^3| = (q_0^2 - q_0 + 1)/(3, q_0 + 1)$ if $q_0 > 2$.

Proposition 9.2. *The conclusion to Theorem 8 holds in case (b) of Table 9.*

Proof. Here $\bar{G}_\sigma = \mathrm{Inndiag}(\mathrm{P}\Omega_8^+(q_0))$ and $y^3 \in G_2(q_0) \leqslant \bar{G}_\sigma$. From [54], we see that the order of y implies that

$$|C_{\bar{G}_\sigma}(y^3)| = c(q_0) = \begin{cases} (q_0^3+1)(q_0+1) & \text{if } q_0 > 2 \\ 7 & \text{if } q_0 = 2. \end{cases}$$

Therefore, by applying Lemma 3.26(ii)(a) and the bound in (20) we deduce that

$$P(z,x) \leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \leqslant (10 + \log\log q) \cdot c(q_0) \cdot (q^4 - q^2 + 1)^{-1}$$

for all nontrivial $z \in G$. The result follows (in particular, the upper bound is less than q^{-1} if $q > 9$). □

9.3. **Case (c): triality graph automorphisms.** We have reached the final case. Here we may assume that $G = \langle G_0, g \rangle$, where g is the standard triality graph automorphism of G_0. As in Section 7.3, we cannot apply Shintani descent in this case.

First we handle the case $q = 2$.

Proposition 9.3. *The conclusion to Theorem 8 holds in case (c) of Table 9 with $q = 2$.*

Proof. As in the proof of Proposition 4.1, it is straightforward to use Magma to handle this case. In particular, we find that the class labelled `24A` in the Atlas [21] witnesses $u(G) \geqslant 4$. □

For the remainder, we will assume $q \geqslant 3$. Choose $y \in C_{G_0}(g) = G_2(q)$ such that

$$|y| = q^2 - q + 1$$

and $C_{G_2(q)}(y) = \langle y \rangle$. Set $x = yg \in G$ and note that $x^3 = y^3 \in G_0$ and $|x| = 3|y|/(3, q+1)$. Write

$$r = |y^3| = (q^2 - q + 1)/(q+1, 3),$$

which is divisible by a primitive prime divisor of $q^6 - 1$.

Lemma 9.4. *We have $C_{G_0}(y) = C_{q^2-q+1} \times C_{q^2-q+1}$.*

Proof. We may choose $y \in \mathrm{SU}_3(q) < G_2(q)$, so $y \in \bar{L} < \bar{H} < \bar{G}$, where $\bar{L} = A_2$, $\bar{H} = G_2$ and $\bar{G} = D_4$ are the corresponding algebraic groups. Let V and U be the natural modules for $\bar{G}$ and $\bar{L}$, respectively, and observe that $V|_{\bar{L}} = U \oplus U^* \oplus 0^2$, where 0 is the trivial module and U^* is the dual of U. By first considering the eigenvalues of y on U, and then on V via the given decomposition, we deduce that the connected component of $C_{\bar{G}}(y)$ is a maximal torus. In particular, y is a regular semisimple element of G_0 and by inspecting [41, Table II] we deduce that $C_{G_0}(y)$ is either $C_{q^2-q+1} \times C_{q^2-q+1}$ or $C_{q^3+1} \times C_{q+1}$. Finally, we observe that the $\mathrm{SU}_3(q)$ subgroup of $G_2(q)$ containing y is centralised in ${}^3D_4(q)$ by a torus of order $q^2 - q + 1$ and this rules out the latter possibility. □

Proposition 9.5. *If $q > 2$ then each $H \in \mathcal{M}(x)$ is of one of the following types:*

$$G_2(q),\ \mathrm{PGU}_3(q)\ (q \equiv 2 \pmod 3),\ \mathrm{SU}_3(q) \times C_{q^2-q+1},\ C_{q^2-q+1} \times C_{q^2-q+1}.$$

Proof. Since $\mathcal{M}(x) \subseteq \mathcal{M}(y^3)$, we proceed by considering the maximal overgroups H_0 of y^3 in G_0, referring to the main theorem of [41] (also see [69, Theorem 4.3]).

By inspection, the only parabolic subgroup with order divisible by r is of the form

$$H_0 = q^{1+8}{:}\mathrm{SL}_2(q^3).C_{q-1}.$$

However, the maximal tori of $\mathrm{SL}_2(q^3)$ have order $q^3 \pm 1$, so there are no elements in H_0 with the appropriate centraliser in G_0. Therefore, there are no parabolic subgroups in $\mathcal{M}(x)$.

Plainly, we will find subgroups of type $G_2(q)$ in $\mathcal{M}(y^3)$, and there may also be subgroups of type $\mathrm{PGU}_3(q)$ when $q \equiv 2 \pmod 3$. If $p = 2$ and $H_0 = \mathrm{L}_2(q^3) \times \mathrm{L}_2(q)$, then $C_{H_0}(z)$ has a cyclic subgroup of order $q^3 + 1$ (a maximal torus in the first factor) for each $z \in H_0$ of order r, so these subgroups do not arise. Since y^3 does not commute with an involution, we can also exclude the involution centraliser when p is odd. Subfield subgroups can be ruled out by Lagrange's theorem. Similarly, just by considering divisibility, we see that the only other possibilities are subgroups of type $\mathrm{SU}_3(q) \times C_{q^2-q+1}$ and $C_{q^2-q+1} \times C_{q^2-q+1}$ (the latter is the centraliser of y^3 in G_0). The result follows. □

Let $H \in \mathcal{M}(x)$. If H is of type $G_2(q)$, then [47] gives $\mathrm{fpr}(z, G/H) \leqslant (q^4 - q^2 + 1)^{-1}$ for all nontrivial $z \in G$ and this bound is best possible. Indeed, equality holds if z is a long root element in G (see the proof of [47, Lemma 6.3]). For the other subgroups arising in Proposition 9.5, we need to sharpen the bound on $\mathrm{fpr}(z, G/H)$ in [47]. To do this, it will be helpful to observe that if $z \in G$ has prime order, but is not a long root element, then $|z^G| > q^{14}$. In addition, if $1 \neq z \in G_0$ is not a long root element, then $|z^G| > q^{16}$. For both of these claims, see [26].

Lemma 9.6. *Let H be a maximal subgroup of G of type $\mathrm{PGU}_3(q)$, where $q \equiv 2 \pmod 3$ and $q \geqslant 5$, and let $z \in G$ be nontrivial. Then*

$$\mathrm{fpr}(z, G/H) < 2q^{-6}.$$

Proof. By replacing z by a suitable conjugate, we may as well assume z is contained in H and has prime order. Observe that $H = \mathrm{PGU}_3(q) \times 3 = C_G(g')$, where g' is a certain triality graph automorphism of G_0.

First we claim that z is not a long root element in G_0. To see this, let $\bar{H} = A_2$ and $\bar{G} = D_4$ be the corresponding algebraic groups and observe that the natural module V for $\bar{G}$ is the adjoint module for $\bar{H}$. This allows us to compute the Jordan form of each unipotent element in $\bar{H}$ on V. Indeed, if $p = 2$ then $\bar{H}$ has a unique class of involutions and such an element has Jordan form $[J_2^4]$ on V. Similarly, if $p \geqslant 5$ then each element in $\bar{H}$ of order p has Jordan form $[J_3, J_2^2, J_1]$ or $[J_5, J_3]$ on V. The claim now follows since the long root elements in $\bar{G}$ have Jordan form $[J_2^2, J_1^4]$ on V.

To complete the proof, recall that $|z^G| > q^{14}$ if z is not a long root element, so the result follows from the trivial bound $|z^G \cap H| \leqslant 2|\mathrm{PGU}_3(q)| < 2q^8$. □

Lemma 9.7. *Let H be a maximal subgroup of G of type $C_{q^2-q+1} \times C_{q^2-q+1}$, where $q \geqslant 3$, and let $z \in G$ be nontrivial. Then*

$$\mathrm{fpr}(z, G/H) < q^{-6}.$$

Proof. Here $H = (C_{q^2-q+1} \times C_{q^2-q+1})\!:\!\mathrm{SL}_2(3).3$. Assume that $z \in H$ has prime order. As in the proof of Lemma 9.6, if $z \in G$ is not a long root element, then $|z^G| > q^{14}$ and we get

$$\mathrm{fpr}(z, G/H) \leqslant |H| q^{-14} < q^{-6}.$$

Therefore, we just need to rule out the existence of long root elements in H.

If $p \geqslant 5$, then $|H|$ is indivisible by p, so we may assume $p \in \{2, 3\}$. Seeking a contradiction, suppose $z \in H$ is a long root element. Viewing z as an element of the algebraic group $\bar{G} = D_4$, note that z normalises a maximal torus of $\bar{G}$, so [46, Proposition 1.13(iii)] implies that $p = 2$ and thus z is an involution. In particular, z is in the coset St of $S = C_{q^2-q+1} \times C_{q^2-q+1}$, where t is the unique involution in $\mathrm{SL}_2(3)$. However, all the involutions in St are contained in the largest class of involutions in $\bar{G}$ (see [17, Corollary 4.4], for example), whence all the involutions in H are in the G_0-class labelled $3A_1$. In particular, there are no involutions in the class A_1, which comprises the long root elements in G_0. This is a contradiction and the result follows. □

Lemma 9.8. *Let H be a maximal subgroup of G of type $\mathrm{SU}_3(q) \times C_{q^2-q+1}$ and let $z \in G$ be nontrivial. Then*

$$\mathrm{fpr}(z, G/H) < 2q^{-6}.$$

Proof. Assume that $z \in H$ has prime order. Write $H_0 = H \cap G_0$ and observe that

$$H_0 = (\mathrm{SU}_3(q) \circ C_{q^2-q+1}).(3, q+1).2 = \mathrm{SU}_3(q).C_{q^2-q+1}.2.$$

First assume $z \in G$ is either semisimple or unipotent, but not a long root element. Then $|z^G| > q^{16}$ and the result follows since $|z^G \cap H| \leqslant |H_0| < 2q^{10}$. In addition, the long root elements in H_0 coincide with the long root elements in the $\mathrm{SU}_3(q)$ subgroup, so if z is such an element then

$$|z^G \cap H| = (q-1)(q^3+1),\ |z^G| = (q^2-1)(q^8+q^4+1)$$

and thus $\mathrm{fpr}(z, G/H) < q^{-6}$.

To complete the proof, assume $z \in G$ is a graph automorphism of order 3. If $C_{G_0}(z) \neq G_2(q)$, then $|z^G| > \frac{1}{2}q^{20}$ and the desired bound follows since $|z^G \cap H| \leqslant 2|H_0| < q^{12}$. Finally, suppose $C_{G_0}(z) = G_2(q)$, so $|z^G| > q^{14}$. In terms of algebraic groups, let $\bar{J} = A_2T_2 < \bar{G} = D_4$ and let τ be a graph automorphism of $\bar{G}$ with $C_{\bar{G}}(\tau) = G_2$. By arguing as in the proof of [11, Proposition 3.3], we see that $t\tau \in \bar{J}\tau$ is a G_2-type triality graph automorphism if and only if $t \in Z(\bar{J})$. Therefore, returning to the finite groups, we deduce that

$$|z^G \cap H| = 2|Z(\mathrm{SU}_3(q))| \cdot \frac{q^2-q+1}{(3, q+1)} = 2(q^2-q+1)$$

and the desired bound follows. □

Proposition 9.9. *The conclusion to Theorem 8 holds in case (c) of Table 9.*

Proof. In view of Proposition 9.3, we may assume $q \geqslant 3$. Recall that the maximal overgroups H of x are described in Proposition 9.5. For each type of subgroup, we need to bound the number of conjugates of H containing x. As before, we do this by estimating the number of conjugates containing y, which we denote by $n(H)$.

First assume $H \in \mathcal{M}(x)$ is a subgroup of type $G_2(q)$. By inspecting [19, 28], we see that $G_2(q)$ has at most $\frac{1}{6}q(q-1)$ conjugacy classes of semisimple elements with centraliser C_{q^2-q+1} and thus

$$|y^G \cap H| \leqslant \frac{1}{6}q(q-1) \cdot \frac{|G_2(q)|}{q^2-q+1}.$$

This implies that

$$n(H) \leqslant \frac{1}{6}q(q-1)(q^2-q+1).$$

Alternatively, by arguing as in the proof of [47, Lemma 4.5] we see that $y^G \cap H$ is a union of at most $|W(D_4) : W(G_2)| = 16$ distinct H-classes and this yields $n(H) \leqslant 16(q^2-q+1)$. Notice that the latter bound is better for $q > 9$.

Next assume $q \equiv 2 \pmod 3$ and $H \in \mathcal{M}(x)$ is of type $\mathrm{PGU}_3(q)$. Now $\mathrm{PGU}_3(q)$ has $\frac{1}{3}(q^2-q-2)$ classes of semisimple elements with centraliser C_{q^2-q+1}, so

$$|y^G \cap H| \leqslant \frac{1}{3}(q^2-q-2) \cdot \frac{|\mathrm{PGU}_3(q)|}{q^2-q+1}$$

and we get $n(H) \leqslant \frac{1}{3}(q^2-q-2)(q^2-q+1)$.

Now suppose $H \in \mathcal{M}(x)$ is of type $\mathrm{SU}_3(q) \times C_{q^2-q+1}$. Set $H_0 = H \cap G_0$ and recall that $H_0 = \mathrm{SU}_3(q).C_{q^2-q+1}.2$. Now $\mathrm{SU}_3(q)$ has $\lceil \frac{1}{3}(q^2-q-2) \rceil \leqslant \frac{1}{3}q(q-1)$ conjugacy classes of semisimple elements with centraliser of order q^2-q+1 and this implies that

$$|y^G \cap H| \leqslant \frac{1}{3}q(q-1) \cdot \frac{|\mathrm{SU}_3(q)|}{q^2-q+1} \cdot (q^2-q+1).$$

In turn, this gives $n(H) \leqslant \frac{1}{6}q(q-1)(q^2-q+1)$.

Finally, if $H \in \mathcal{M}(x)$ is of type $C_{q^2-q+1} \times C_{q^2-q+1}$ then $|y^G \cap H| \leqslant (q^2-q+1)^2$ and we deduce that $n(H) \leqslant \frac{1}{24}(q^2-q+1)^2$.

By combining the above bounds with the fixed point ratio estimates in (20) and Lemmas 9.6–9.8, we conclude that

$$\begin{aligned} P(z,x) &\leqslant \sum_{H \in \mathcal{M}(x)} \mathrm{fpr}(z, G/H) \\ &< a(q) \cdot (q^2-q+1) \cdot (q^4-q^2+1)^{-1} + \frac{1}{3}(q^2-q-2)(q^2-q+1) \cdot 2q^{-6} \\ &\quad + \frac{1}{6}q(q-1)(q^2-q+1) \cdot 2q^{-6} + \frac{1}{24}(q^2-q+1)^2 \cdot q^{-6} \end{aligned}$$

for all nontrivial $z \in G$, where $a(q) = \frac{1}{6}q(q-1)$ if $q \leqslant 9$ and $a(q) = 16$ for $q > 9$. One checks that this upper bound is less than $\frac{1}{2}$ for all $q > 2$ and less than q^{-1} for $q > 16$. □

In view of Propositions 9.1, 9.2 and 9.9, we have now proved the following result.

Theorem 9.10. *The conclusion to Theorem 8 holds when* $G_0 = {}^3D_4(q)$.

Moreover, by combining this with Theorems 4.5, 5.2, 6.5, 7.14 and 8.7, we conclude that the proof of Theorem 8 is complete.

References

[1] M. Aschbacher and R. Guralnick, *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446–460.

[2] M. Aschbacher and L.L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.

[3] J. Ballantyne, C. Bates and P. Rowley, *The maximal subgroups of* $E_7(2)$, LMS J. Comput. Math. **18** (2015), 323–371.

[4] G.J. Binder, *The bases of the symmetric group*, Izv. Vyssh. Uchebn. Zaved. Mat. **78** (1968), 19–25.

[5] G.J. Binder, *The two-element bases of the symmetric group*, Izv. Vyssh. Uchebn. Zaved. Mat. **90** (1970), 9–11.

[6] G.J. Binder, *Certain complete sets of complementary elements of the symmetric and the alternating group of the nth degree*, Mat. Zametki **7** (1970), 173–180.

[7] W. Bosma, J. Cannon and C. Playoust, *The* Magma *algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.

[8] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Math. Soc. Lecture Notes Series, vol. 407, Cambridge University Press, 2013. v+438 pp.

[9] J.L. Brenner and J. Wiegold, *Two generator groups, I*, Michigan Math. J. **22** (1975), 53–64.

[10] T. Breuer, R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups II*, J. Algebra **320** (2008), 443–494.

[11] T.C. Burness, *Fixed point ratios in actions of finite classical groups, IV*, J. Algebra **314** (2007), 749–788.

[12] T.C. Burness, *On base sizes for almost simple primitive groups*, J. Algebra **516** (2018), 38–74.

[13] T.C. Burness, *Simple groups, generation and probabilistic methods*, Groups St Andrews 2017 in Birmingham, 200–229, London Math. Soc. Lecture Note Ser., 455, Cambridge Univ. Press, Cambridge, 2019.

[14] T.C. Burness and S. Guest, *On the uniform spread of almost simple linear groups*, Nagoya Math. J. **109** (2013), 35–109.

[15] T.C. Burness and S. Harper, *Finite groups,* 2*-generation and the uniform domination number*, Israel J. Math. **239** (2020), 271–367.

[16] T.C. Burness, M.W. Liebeck and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. **98** (2009), 116–162.

[17] T.C. Burness and A.R. Thomas, *On the involution fixity of exceptional groups of Lie type*, Internat. J. Algebra Comput. **28** (2018), 411–466.

[18] F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer and E.A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), 4931–4948.

[19] B. Chang, *The conjugate classes of Chevalley groups of type* (G_2), J. Algebra **9** (1968), 190–211.

[20] A.M. Cohen, M.W. Liebeck, J. Saxl and G.M. Seitz, *The local maximal subgroups of exceptional groups of Lie type*, Proc. Lond. Math. Soc. **64** (1992), 21–48.
[21] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.
[22] B.N. Cooperstein, *Maximal subgroups of* $G_2(2^n)$, J. Algebra **70** (1981), 23–36.
[23] D.A. Craven, *Alternating subgroups of exceptional groups of Lie type*, Proc. Lond. Math. Soc. **115** (2017), 449–501.
[24] D.A. Craven, *Maximal* PSL_2 *subgroups of exceptional groups of Lie type*, Mem. Amer. Math. Soc., to appear.
[25] D.A. Craven, *On medium-rank Lie primitive and maximal subgroups of exceptional groups of Lie type*, submitted.
[26] 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), 39–70.
[27] C. Donoven and S. Harper, *Infinite* $\frac{3}{2}$*-generated groups*, Bull. London Math. Soc. **52** (2020), 657–673.
[28] H. Enomoto, *The conjugacy classes of Chevalley groups of type* (G_2) *over finite fields of characteristic* 2 *or* 3, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 497–512.
[29] M. Evans, T*-systems of certain finite simple groups*, Math. Proc. Cambridge Philos. Soc. **113** (1993), 9–22.
[30] 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), 2221–2303.
[31] M. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
[32] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple* K*-groups*, Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998. xvi+419 pp.
[33] V.S. Guba, *A finitely generated simple group with free* 2*-generated subgroups*, Sibirsk. Mat. Zh. **27** (1986), 50–67.
[34] S. Guest, J. Morris, C.E. Praeger and P. Spiga, *On the maximum orders of elements of finite almost simple groups and primitive permutation groups*, Trans. Amer. Math. Soc. **367** (2015), 7665–7694.
[35] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.
[36] R.M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.
[37] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **490** (2017), 330–371.
[38] S. Harper, *The spread of almost simple classical groups*, Lecture Notes in Math., Springer, to appear.
[39] W.M. Kantor and Á. Seress, *Large element orders and the characteristic of Lie-type simple groups*, J. Algebra **322** (2009), 802–832.
[40] N. Kawanaka, *On the irreducible characters of the finite unitary groups*, J. Math. Soc. Japan **29** (1977), 425–450.
[41] P.B. Kleidman, *The maximal subgroups of the Steinberg triality groups* ${}^3D_4(q)$ *and of their automorphism groups*, J. Algebra **115** (1988), 182–199.
[42] P.B. Kleidman, *The maximal subgroups of the Chevalley groups* $G_2(q)$ *with* q *odd, the Ree groups* ${}^2G_2(q)$*, and their automorphism groups*, J. Algebra **117** (1988), 30–71.
[43] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[44] P.B. Kleidman and R.A. Wilson, *The maximal subgroups of* $E_6(2)$ *and* $\mathrm{Aut}(E_6(2))$, Proc. Lond. Math. Soc. **60** (1990), 266–294.
[45] R. Lawther, *Sublattices generated by root differences*, J. Algebra **412** (2014), 255–263.
[46] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point spaces in actions of exceptional algebraic groups*, Pacific J. Math. **205** (2002), 339–391.
[47] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.
[48] M.W. Liebeck, J. Saxl and G.M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. Lond. Math. Soc. **65** (1992), 297–325.
[49] M.W. Liebeck and G.M. Seitz, *Maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Geom. Dedicata **35** (1990), 353–387.
[50] M.W. Liebeck and G.M. Seitz, *On finite subgroups of exceptional algebraic groups*, J. reine angew. Math. **515** (1999), 25–72.
[51] M.W. Liebeck and G.M. Seitz, *A survey of of maximal subgroups of exceptional groups of Lie type*, in Groups, combinatorics & geometry (Durham, 2001), 139–146, World Sci. Publ., River Edge, NJ, 2003.
[52] M.W. Liebeck and A. Shalev, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem*, Annals of Math. **144** (1996), 77–125.

[53] A.J. Litterick, *On non-generic finite subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. **253** (2018), no. 1207, v+156 pp.
[54] F. Lübeck, *Centralisers and numbers of semisimple classes in exceptional groups of Lie type*, `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/CentSSClasses`
[55] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Semin. Mat. Univ. Padova **98** (1997), 173–191.
[56] G. Malle, *The maximal subgroups of* ${}^2F_4(q^2)$, J. Algebra **139** (1991), 52–69.
[57] S.P. Norton and R.A. Wilson, *The maximal subgroups of* $F_4(2)$ *and its automorphism group*, Comm. Algebra **17** (1989), 2809–2824.
[58] I. Pak, *What do we know about the product replacement algorithm?*, in Groups and computation, III (Columbus, OH, 1999), 301–347, Ohio State Univ. Math. Res. Inst. Publ., de Gruyter, Berlin, 2001.
[59] S. Piccard, *Sur les bases du groupe symétrique et du groupe alternant*, Math. Ann. **116** (1939), 752–767.
[60] K. Shinoda, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic* 2, J. Fac. Sci. Univ. Tokyo Sect. I A Math. **21** (1974), 133–159.
[61] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), J. Fac. Sci. Univ. Tokyo Sect. I A Math. **22** (1975), 1–15.
[62] T. Shintani, *Two remarks on irreducible characters of finite general linear groups*, J. Math. Soc. Japan **28** (1976), 396–414.
[63] T. Shoji, *The conjugacy classes of Chevalley groups of type* (F_4) *over finite fields of characteristic* $p \neq 2$, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 1–17.
[64] A. Stein, $1\frac{1}{2}$*-generation of finite simple groups*, Beiträge Algebra Geom. **39** (1998), 349–358.
[65] R. Steinberg, *Generators for simple groups*, Canadian J. Math. **14** (1962), 277–283.
[66] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.
[67] H.N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.
[68] T.S. Weigel, *Generation of exceptional groups of Lie-type*, Geom. Dedicata **41** (1992), 63–87.
[69] R.A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251. Springer-Verlag London, Ltd., London, 2009. xvi+298 pp.
[70] R.A. Wilson, *Maximal subgroups of* ${}^2E_6(2)$ *and its automorphism groups*, preprint (arxiv:1801.08374).
[71] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monat. Math. Physik **3** (1892), 265–284.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK

Email address: `t.burness@bristol.ac.uk`

R.M. Guralnick, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA

Email address: `guralnic@usc.edu`

S. Harper, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK, and Heilbronn Institute for Mathematical Research, Bristol, UK

Email address: `scott.harper@bristol.ac.uk`