University of Bristol - Explore Bristol Research
General rights

Shintani descent, simple groups and spread

Scott Harper

The spread of a group G, written $s(G)$, is the largest k such that for any nontrivial elements $x_1, \ldots, x_k \in G$ there exists $y \in G$ such that $G = \langle x_i, y \rangle$ for all i. Burness, Guralnick and Harper recently classified the finite groups G such that $s(G) > 0$, which involved a reduction to almost simple groups. In this paper, we prove an asymptotic result that determines exactly when $s(G_n) \to \infty$ for a sequence of almost simple groups (G_n). We apply probabilistic and geometric ideas, but the key tool is Shintani descent, a technique from the theory of algebraic groups that provides a bijection, the Shintani map, between conjugacy classes of almost simple groups. We provide a self-contained presentation of a general version of Shintani descent, and we prove that the Shintani map preserves information about maximal overgroups. This is suited to further applications. Indeed, we also use it to study $\mu(G)$, the minimal number of maximal overgroups of an element of G. We show that if G is almost simple, then $\mu(G) \leqslant 3$ when G has an alternating or sporadic socle, but in general, unlike when G is simple, $\mu(G)$ can be arbitrarily large.

1 Introduction

Generation questions about finite groups, especially finite simple groups, have attracted much attention for many years, and asymptotic behaviour has been an important theme. For example, a landmark result of Liebeck and Shalev [36] asserts that if (G_i) is a sequence of finite simple groups satisfying $|G_i| \to \infty$, then the probability that two randomly chosen elements generate G_i tends to 1, which proves Dixon's conjecture of 1969 [18].

A recent programme of research [3, 4, 9, 10, 24, 27, 28, 29] has focussed on *spread*, a notion that captures how generating pairs are distributed across a 2-generated group (this notion is related to the *generating graph* and the *product replacement graph*, both of which have been the subject of recent research, see the discussion before [10, Corollaries 6 and 7].)

Definition. Let G be a finite noncyclic 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 that C witnesses $u(G) \geqslant k$.

Observe that $s(G) > 0$ if and only if every nontrivial element of G is contained in a generating pair (a property known as $\frac{3}{2}$-*generation*). It is easy to see that if $s(G) > 0$ then every proper quotient of G is cyclic. Recently, Burness, Guralnick and Harper [10] settled a conjecture of Breuer, Guralnick and Kantor [4], by proving that the converse is true. In fact, they proved that if every proper quotient of G is cyclic, then $s(G) \geqslant 2$. The proof involves reducing to almost simple groups. If G is simple, then $s(G) \geqslant 2$ was proved in [4], but the almost simple groups pose further challenges and the series of papers [9, 10, 28, 29] are dedicated to proving $s(G) \geqslant 2$ in this case.

In [27], Guralnick and Shalev determined exactly when a sequence of simple groups (G_i) satisfies $s(G_i) \to \infty$. However, the asymptotic behaviour of the spread of almost simple groups is not yet known. By [10, Corollary 9], the unsettled case involves sequences of groups of Lie type defined over a field of fixed size. We settle this in our first main theorem. Here, and in Corollary 3, we use the term *graph automorphism* in the sense of [22, Definition 2.5.13].

Theorem 1. *Fix a prime power q. Let (G_i) be a sequence of almost simple groups of Lie type defined over $\mathbb{F}_q$ such that $G_i / \operatorname{soc}(G_i)$ is cyclic and $|G_i| \to \infty$. Write $G_i = \langle \operatorname{soc}(G_i), x_i \rangle$. Then the following are equivalent*

(i) $s(G_i) \to \infty$

(ii) $u(G_i) \to \infty$

(iii) (G_i) *has no infinite subsequence where one of the following holds*

    (a) $\operatorname{soc}(G_i) \in \{\operatorname{Sp}_{2m_i}(q) \text{ (q even)}, \Omega_{2m_i+1}(q)\}$

    (b) $\operatorname{soc}(G_i) \in \{\operatorname{PSL}_{2m_i+1}^{\pm}(q), \operatorname{P\Omega}_{2m_i}^{\pm}(q)\}$ *and a power of x_i is a graph automorphism.*

Remark 2. There is a geometric characterisation of the exceptions in Theorem 1(iii). Roughly, if $G = \langle T, x \rangle$ is an almost simple classical group, then the exceptions in Theorem 1 are the groups where every element of Tx fixes a 1-dimensional subspace of the natural module for T (or a closely related module), see Theorem 5.8 and Remark 5.12 for precise statements.

Combining Theorem 1 with [10, Corollary 9] gives a complete characterisation of when the spread or uniform spread of a sequence of almost simple groups diverges to infinity.

Corollary 3. *Let (G_i) be a sequence of almost simple groups such that $G / \operatorname{soc}(G_i)$ is cyclic and $|G_i| \to \infty$. Write $G_i = \langle \operatorname{soc}(G_i), x_i \rangle$. Then the following are equivalent*

(i) $s(G_i) \to \infty$

(ii) $u(G_i) \to \infty$

(iii) (G_i) *has no infinite subsequence where one of the following holds*

    (a) $G_i = A_{n_i}$ *where n_i is divisible by a fixed prime*

    (b) $G_i = S_{n_i}$

    (c) $\operatorname{soc}(G_i) \in \{\operatorname{Sp}_{2m_i}(q) \text{ (q even)}, \Omega_{2m_i+1}(q)\}$ *for fixed q*

    (d) $\operatorname{soc}(G_i) \in \{\operatorname{PSL}_{2m_i+1}^{\pm}(q), \operatorname{P\Omega}_{2m_i}^{\pm}(q)\}$ *for fixed q, and x_i powers to a graph automorphism.*

The key tool in the proof of Theorem 1 is a general form of *Shintani descent*. This technique from algebraic groups has played an important role in the character theory of almost simple groups over several decades, beginning with the work of Shintani and Kawanaka (see [13, 16, 17, 31, 37] for example). More recently, Shintani descent has been useful in studying the almost simple groups themselves, especially in the context of spread [9, 10, 28, 29].

Let us introduce the key idea of Shintani descent. Let X be a connected algebraic group and let σ_1 and σ_2 be commuting Steinberg endomorphisms of X. Then there exists a bijection F, called the *Shintani map* of (X, σ_1, σ_2), between the conjugacy classes in the cosets $X_{\sigma_1}\sigma_2$ and $X_{\sigma_2}\sigma_1$, where X_{σ_i} is set of fixed points of X under σ_i.

Previous applications of Shintani descent to group theoretic problems have assumed that $\sigma_1 = \sigma_2^e$, and, as we explain in Remark 2.21, this makes some almost simple groups not amenable to this technique. Therefore, we take the opportunity in Section 3 to demonstrate how all almost simple groups can be studied in a uniform manner using this more general version of Shintani descent.

To use Shintani descent effectively, we must understand what is preserved by the Shintani map F, and for our applications, we are particularly interested in how the maximal overgroups of g in $\langle X_{\sigma_1}, \sigma_2 \rangle$ relate to the maximal overgroups of g_0 in $\langle X_{\sigma_2}, \sigma_1 \rangle$ if $F(g^{X_{\sigma_1}}) = g_0^{X_{\sigma_2}}$. When $\sigma_1 = \sigma_2^e$, partial information is given by [29, Lemma 3.3.2], namely if $Y \leqslant X$ is a closed connected $\langle \sigma_1, \sigma_2 \rangle$-stable subgroup such that $N_{X_{\sigma_i}}(Y_{\sigma_i}) = Y_{\sigma_i}$, then the $\langle X_{\sigma_1}, \sigma_2 \rangle$-conjugates of $\langle Y_{\sigma_1}, \sigma_2 \rangle$ that contain g correspond to the $\langle X_{\sigma_2}, \sigma_1 \rangle$-conjugates of $\langle Y_{\sigma_2}, \sigma_1 \rangle$ that contain g_0.

To prove Theorem 1, we need to be able to study maximal overgroups that arise from disconnected subgroups $Y \leqslant X$. Our next main result allows us to do this. Here for a closed σ_i-stable subgroup $Y \leqslant X$, we fix a set $R_i(Y) \subseteq X$ such that for all $x \in X$ the subgroup $(Y^x)_{\sigma_i}$ is X_{σ_i}-conjugate to $(Y^r)_{\sigma_i}$ for exactly one $r \in R_i(Y)$ (see Remark 2.7 for details).

Theorem 4. *Let X be connected, let σ_1 and σ_2 be commuting Steinberg endomorphisms of X and let F be the Shintani map of (X, σ_1, σ_2). Let $Y \leqslant X$ be a closed $\langle \sigma_1, \sigma_2 \rangle$-stable subgroup satisfying $N_{X_{s\sigma_i}}(Y_{s\sigma_i}^\circ) = N_X(Y^\circ)_{s\sigma_i}$ for all $s \in N_X(Y^\circ)$. If $F(g^{X_{\sigma_1}}) = g_0^{X_{\sigma_2}}$, then the overgroups of g in*

$$\{ (\langle Y, \sigma_2 \rangle^r)_{\sigma_1}^x \mid r \in R_1(Y) \text{ and } x \in \langle X_{\sigma_1}, \sigma_2 \rangle \}$$

are in bijection with the overgroups of g_0 in

$$\{ (\langle Y, \sigma_1 \rangle^r)_{\sigma_2}^x \mid r \in R_2(Y) \text{ and } x \in \langle X_{\sigma_2}, \sigma_1 \rangle \}.$$

To prove Theorem 4 we require the more general version of Shintani descent in Section 2, which is based on Deshpande's approach [16] that does not assume that X is connected. In fact, our version is even more general since we do not assume that σ_1 and σ_2 commute.

Let us now highlight the important roles that Theorem 4 plays in our proof of Theorem 1. Let $G = \langle T, x \rangle$ be an almost simple classical group with socle T.

As suggested by Remark 2, upper bounds on the spread of classical groups G featured in part (iii) will arise from studying the subspaces of the natural module for T that are stabilised by elements of G (see Corollary 5.5). To do this, we will apply Theorem 4 in the case where X is a simple classical group and Y is a subspace stabiliser (which may be disconnected).

To obtain lower bounds on uniform spread, we apply the probabilistic method introduced by Guralnick and Kantor [24]. Here, the idea is to identify an element $s \in G$ such that the set $\mathcal{M}(G, s)$ of maximal subgroups of G that contain s is small, because if

$$\sum_{H \in \mathcal{M}(G,s)} \frac{|x^G \cap H|}{|x^G|} < \frac{1}{k}$$

then s^G witnesses $u(G) \geqslant k$ (see Lemma 5.11). Without loss of generality, if s^G witnesses $u(G) \geqslant k > 0$, then $s \in Tx$. Shintani descent is then the crucial tool for understanding the conjugacy classes in Tx. Roughly, we find a Shintani map F that puts the classes in Tx in bijection with the classes in another coset $T_0 x_0$ that is easier to understand. We choose an element $s \in Tx$ by specifying its image $s_0 \in T_0 x_0$ under F, and we use Theorem 4 to deduce $\mathcal{M}(G, s)$ from information about s_0.

Shintani descent has had applications to other problems in group theory (for example, in [21, 23]) and we anticipate the general version in this paper will be useful in future. Indeed, in Section 4, we give some additional applications of Theorem 4, which we now discuss.

Motivated by the *uniform domination number* (an invariant related to uniform spread), Burness and Harper [11], defined $\mu(G)$ as the minimal number of maximal overgroups

of an element of G. They showed $\mu(G) \leqslant 3$ if G is simple, with four exceptions where $4 \leqslant \mu(G) \leqslant 7$, and they determined $\mu(G)$ exactly when G is alternating or sporadic.

The following theorem summarises our results on $\mu(G)$ for almost simple groups G.

Theorem 5. *The following hold.*

 (i) *If G is an almost simple group with alternating or sporadic socle, then $\mu(G) \leqslant 3$.*

 (ii) *There is no constant c such that for all almost simple groups G we have $\mu(G) \leqslant c$.*

 (iii) *There are infinitely many nonsimple almost simple groups of Lie type G such that $\mu(G) = 1$.*

Remark 6. Let us comment on Theorem 5.

 (i) Proposition 4.1 gives the value of $\mu(G)$ when $\mathrm{soc}(G)$ is alternating or sporadic, so we determine when these groups contain an element with a unique maximal overgroup.

 (ii) In Proposition 4.2, we fix $k \geqslant 1$ and give an almost simple group G with socle $\mathrm{PSL}_2(2^f)$ such that $|\mathcal{M}(G,g)| \geqslant k$ for each $g \in G$ (we choose f so it has c distinct prime factors). Therefore, $\mu(G)$ is even unbounded for almost simple groups G of bounded rank.

 (iii) In Proposition 4.5, we will see that for all $m \geqslant 8$, there exists $f > 1$ such that $\Omega_{2m}^+(2^f).f$ has an element with a unique maximal overgroup (of type $\mathrm{O}_{2k}^+(2^f) \times \mathrm{O}_{2m-2k}^+(2^f)$).

Organisation. Section 2 introduces a general version of Shintani descent and features a proof of Theorem 4. In Section 3, we apply Shintani descent systematically to all almost simple groups of Lie type, and we use this to study their maximal subgroups in Section 4, thus proving Theorem 5. Section 5 sees the proof of Theorem 1.

Notation. Our notation for algebraic groups and groups of Lie type follows [22, 32]. Let us highlight that $\mathrm{SL}_n^+(q) = \mathrm{SL}_n(q)$ and $\mathrm{SL}_n^-(q) = \mathrm{SU}_n(q)$, and that $\Omega_n(\overline{\mathbb{F}}_p)$ is the connected component $\mathrm{O}_n(\overline{\mathbb{F}}_p)^\circ$. For a group G and a prime p, we write $O^{p'}(G)$ for the subgroup generated by the p-elements of G. We write (a,b) for the greatest common divisor of a and b.

2 Shintani descent

2.1 Introduction

Let us introduce the general version of Shintani descent that is at the heart of the remainder of the paper. Throughout Section 2, let p be prime and X be a linear algebraic group over $\overline{\mathbb{F}}_p$, which from now on we simply refer to as an *algebraic group*.

We fix some notation. For a Steinberg endomorphism σ of X, write $X_\sigma = \{x \in X \mid x^\sigma = x\}$. For an automorphism α of a group G, we say that $g, h \in G$ are *α-conjugate* if $g\alpha$ and $h\alpha$ are conjugate in the semidirect product $G{:}\langle \alpha \rangle$, and we call the α-conjugacy classes *α-classes*.

In our first main theorem, we introduce a general version of Shintani descent. In the proof we argue as Deshpande does in [16], but our setup is slightly more general since we define a Shintani map for an arbitrary pair of Steinberg endomorphisms, which need not commute.

Theorem 2.1. *Let X be an algebraic group and let σ_1 and σ_2 be Steinberg endomorphisms of X. Let X_i be a set of σ_i-class representatives of X. Then the* Shintani map *of (X, σ_1, σ_2)*

$$F \colon \bigcup_{s \in X_1} \{ g^{X_{s\sigma_1}} \mid g \in (X\sigma_2)_{s\sigma_1} \} \to \bigcup_{t \in X_2} \{ h^{X_{t\sigma_2}} \mid h \in (X\sigma_1)_{t\sigma_2} \}$$

defined as $F(g^{X_{s\sigma_1}}) = h^{X_{t\sigma_2}}$ if and only if $(g, s\sigma_1)^X = (t\sigma_2, h)^X$ is a well-defined bijection. Moreover, if $F(g^{X_{s\sigma_1}}) = h^{X_{t\sigma_2}}$, then $C_{X_{s\sigma_1}}(g) \cong C_{X_{t\sigma_2}}(h)$.

Proof. Write $R = \{ (g, h) \in X\sigma_2 \times X\sigma_1 \mid [g, h] = 1 \}$ and let R/X be the set of orbits of the conjugation action of X on R. If $h \in X\sigma_1$, then h is X-conjugate to $xs\sigma_1$ for some $x \in X^\circ$ and $s \in X_1$, and by the Lang–Steinberg theorem, $xs\sigma_1$ is X°-conjugate to $s\sigma_1$, so

$$R/X = \bigcup_{s \in X_1} \{ (g, s\sigma_1)^X \mid g \in (X\sigma_2)_{s\sigma_1} \}.$$

Observe that the distinct elements of $\{ (g, s\sigma_1)^X \mid g \in (X\sigma_2)_{s\sigma_1} \}$ correspond to the distinct $X_{s\sigma_1}$-class representatives g in $(X\sigma_2)_{s\sigma_1}$. Similarly, we deduce that

$$R/X = \bigcup_{t \in X_2} \{ (t\sigma_2, h)^X \mid h \in (X\sigma_1)_{t\sigma_2} \},$$

with distinct elements of $\{ (t\sigma_2, h)^X \mid h \in (X\sigma_1)_{t\sigma_2} \}$ corresponding to distinct $X_{t\sigma_2}$-class representatives h in $(X\sigma_1)_{t\sigma_2}$. Therefore,

$$\bigcup_{s \in X_1} \{ (g, s\sigma_1)^X \mid g \in (X\sigma_2)_{s\sigma_1} \} = R/X = \bigcup_{t \in X_2} \{ (t\sigma_2, h)^X \mid h \in (X\sigma_1)_{t\sigma_2} \},$$

and we obtain the bijection F in the statement.

If we fix $g \in (X^\circ t\sigma_2)_{s\sigma_1}$ and $h \in (X^\circ s\sigma_1)_{t\sigma_2}$ such that $F(g^{X_{s\sigma_1}}) = h^{X_{t\sigma_2}}$, then we may write $(g, s\sigma_1) = (t\sigma_2, h)^a$ for some $a \in X$, whence

$$C_{X_{s\sigma_1}}(g) = \{ x \in X \mid (g, s\sigma_1)^x = (g, s\sigma_1) \} = \{ x \in X \mid (t\sigma_2, h)^x = (t\sigma_2, h) \}^a = C_{X_{t\sigma_2}}(h)^a.$$

This completes the proof. $\qquad\square$

We can give an explicit definition of the Shintani map.

Lemma 2.2. *Let F be the Shintani map of (X, σ_1, σ_2), and let $s, t \in X$ with $[s\sigma_1, t\sigma_2] = 1$. If $F(g^{X_{s\sigma_1}}) = h^{X_{t\sigma_2}}$, then there exists $a \in X^\circ$ such that $g = aa^{-(t\sigma_2)^{-1}} t\sigma_2$ and $h = a^{-1} a^{(s\sigma_1)^{-1}} s\sigma_1$.*

Proof. If $F(g^{X_{s\sigma_1}}) = h^{X_{t\sigma_2}}$, then $(g, s\sigma_1) = (t\sigma_2, h)^a$ for some $a \in X^\circ$, which implies that $g = aa^{-(t\sigma_2)^{-1}} t\sigma_2$ and $h = a^{-1} a^{(s\sigma_1)^{-1}} s\sigma_1$, as required. $\qquad\square$

Remark 2.3. For our applications to finite groups, we will be interested in not the infinite order Steinberg endomorphisms σ_1 and σ_2, but their finite order restrictions to finite fixed point subgroups; however, this makes no substantive change to the claims made in this section. In particular, if X is connected and $[\sigma_1, \sigma_2] = 1$, then for the restrictions $\widetilde{\sigma}_1 = \sigma_1|_{X_{\sigma_2}}$ and $\widetilde{\sigma}_2 = \sigma_2|_{X_{\sigma_1}}$, the Shintani map F of (X, σ_1, σ_2) gives a well-defined bijection

$$\{ (x\widetilde{\sigma}_2)^{X_{\sigma_1}} \mid x \in X_{\sigma_1} \} \to \{ (y\widetilde{\sigma}_1)^{X_{\sigma_2}} \mid y \in X_{\sigma_2} \}$$

$$(x\widetilde{\sigma}_2)^{X_{\sigma_1}} \mapsto (y\widetilde{\sigma}_1)^{X_{\sigma_2}} \iff (x\sigma_2, \sigma_1)^X = (\sigma_2, y\sigma_1)^X.$$

We will harmlessly identify this bijection with F, but we will adopt the notation $\widetilde{\sigma}_1 = \sigma_1|_{X_{\sigma_2}}$ and $\widetilde{\sigma}_2 = \sigma_2|_{X_{\sigma_1}}$ when convenient.

Remark 2.4. We often abuse notation and write the Shintani map of (X, σ_1, σ_2) as

$$F \colon \bigcup_{s \in X_1} (X\sigma_2)_{s\sigma_1} \to \bigcup_{t \in X_2} (X\sigma_1)_{t\sigma_2} \quad \text{where} \quad (x\sigma_2, s\sigma_1)^X = (t\sigma_2, F(x\sigma_2))^X.$$

In particular, if X is connected and $[\sigma_1, \sigma_2] = 1$, we simply write $F \colon X_{\sigma_2}\sigma_1 \to X_{\sigma_1}\sigma_2$.

Example 2.5. Let $X = \mathrm{GL}_m \wr S_2 \leqslant \mathrm{GL}_{2m}$. Let $\varphi \colon X \to X$ be the standard Frobenius endomorphism of X defined as $(x_{ij}) \mapsto (x_{ij}^p)$, and let $\gamma \colon X \to X$ be the restriction of the graph automorphism of GL_{2m} defined as $x \mapsto x^{-\mathsf{T}}$. Observe that φ and γ commute.

Write $X = X^\circ {:} \langle s \rangle$, where $s \in \mathrm{GL}_{2m}$ is an involution interchanging the two factors of $X^\circ = \mathrm{GL}_m \times \mathrm{GL}_m$. We choose s such that it commutes with φ and γ. Here, $X_1 = X_2 = \{1, s\}$.

Write $q = p^f$ and let F be the Shintani map of $(X, \gamma\varphi^f, \varphi)$. In the notation of Remark 2.4,

$$F \colon (\mathrm{GU}_m(q) \wr S_2)\varphi \cup (\mathrm{GL}_m(q^2){:}C_2)\varphi \to (\mathrm{GL}_m(p) \wr S_2)\gamma\varphi^f \cup (\mathrm{GL}_m(p^2){:}C_2)\gamma\varphi^f,$$

where, for example, $\mathrm{GL}_m(q^2){:}C_2$-classes in $\mathrm{GL}_m(q^2)\varphi = X^\circ_{s\gamma\varphi^f}\varphi$ correspond to $\mathrm{GL}_m(p) \wr S_2$-classes in $\mathrm{GL}_m(p)^2 s\gamma\varphi^f = X^\circ_\varphi s\gamma\varphi^f$ via a centraliser order preserving bijection.

2.2 Shintani descent and subgroups

For the remainder of Section 2, let X be a connected algebraic group and let σ_1 and σ_2 be commuting Steinberg endomorphisms of X. For $\{i, j\} = \{1, 2\}$, write $\widetilde{\sigma}_i = \sigma_i|_{X_{\sigma_j}}$ and assume that $\langle \widetilde{\sigma}_i \rangle \cap X_{\sigma_j} = 1$. Let $F \colon X_{\sigma_1}\widetilde{\sigma}_2 \to X_{\sigma_2}\widetilde{\sigma}_1$ be the Shintani map of (X, σ_1, σ_2).

Let us fix some notation.

Notation 2.6. Let Y be a closed σ_i-stable subgroup of X.

(i) Fix $S_i = S_i(Y)$ as a set of σ_i-class representatives of $N_X(Y^\circ)$.

(ii) For each $s \in X$, by the Lang–Steinberg theorem (see [22, Theorem 2.1.1] for example), fix $s_i \in X$ such that $[s_i^{-1}, \sigma_i^{-1}] = s$.

Remark 2.7. Note that the set $R_i(Y)$ defined before Theorem 4 is $\{s_i \mid s \in S_i(Y)\}$.

We will now give a strong version of Theorem 4, which is our main result on Shintani descent and it captures how overgroups are preserved under the Shintani map.

Theorem 2.8. *Let $Y \leqslant X$ be a closed $\langle \sigma_1, \sigma_2 \rangle$-stable subgroup satisfying $N_{X_{s\sigma_i}}(Y^\circ_{s\sigma_i}) = N_X(Y^\circ)_{s\sigma_i}$ for all $s \in N_X(Y^\circ)$. Let $g \in X_{\sigma_1}\widetilde{\sigma}_2$.*

(i) *The total number of $\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$-conjugates of $(\langle Y, \widetilde{\sigma}_2 \rangle^{s_1})_{\sigma_1}$, as s ranges across $S_1(Y)$, that contain g equals the total number of $\langle X_{\sigma_2}, \widetilde{\sigma}_1 \rangle$-conjugates of $(\langle Y, \widetilde{\sigma}_1 \rangle^{s_2})_{\sigma_2}$, as s ranges across $S_2(Y)$, that contain $F(g)$.*

(ii) *For $s, t \in N_X(Y^\circ)$ satisfying $[s\sigma_1, t\sigma_2] = 1$, the number of $\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$-conjugates of $((Y^\circ t\widetilde{\sigma}_2)^{s_1})_{\sigma_1}$ that contain g equals the number of $\langle X_{\sigma_2}, \widetilde{\sigma}_1 \rangle$-conjugates of $((Y^\circ s\widetilde{\sigma}_1)^{t_2})_{\sigma_2}$ that contain $F(g)$.*

Proof. For $s, t \in Y$ satisfying $[s\sigma_1, t\sigma_2] = 1$, let $m_{(s,t)}$ be the number of $\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$-conjugates of the coset $((Y^\circ t\widetilde{\sigma}_2)^{s_1})_{\sigma_1} = (Y^\circ_{s\sigma_1} t\widetilde{\sigma}_2)^{s_1}$ that contain g and let $n_{(t,s)}$ be the number of $\langle X_{\sigma_2}, \widetilde{\sigma}_1 \rangle$-conjugates of the coset $((Y^\circ s\widetilde{\sigma}_1)^{t_2})_{\sigma_2} = (Y^\circ_{t\sigma_2} s\widetilde{\sigma}_1)^{t_2}$ that contain $F(g)$.

Let us show that (i) is a consequence of (ii). Observe that $Y^\circ s\sigma_i$ for $s \in S_i$ are representatives of the $N_X(Y^\circ)$-classes in $N_X(Y^\circ)\sigma_i/Y^\circ$. For $t \in Y$, fix $S_{i,t}$ such that $Y^\circ s\sigma_i$ for $s \in S_{i,t}$ are representatives of the $C_{N_X(Y^\circ)/Y^\circ}(Y^\circ t\sigma_j)$-classes in $C_{N_X(Y^\circ)\sigma_i/Y^\circ}(Y^\circ t\sigma_j)$ where $\{i, j\} = \{1, 2\}$.

For $s \in N_X(Y)$, let m_s be the number of $\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$-conjugates of $(\langle Y, \widetilde{\sigma}_2 \rangle^{s_1})_{\sigma_1} = (\langle Y, \widetilde{\sigma}_2 \rangle_{s\sigma_1})^{s_1}$ that contain g, and for $t \in Y$, let n_t be the number of $\langle X_{\sigma_2}, \widetilde{\sigma}_1 \rangle$-conjugates of $(\langle Y, \widetilde{\sigma}_1 \rangle^{t_2})_{\sigma_2} = (\langle Y, \widetilde{\sigma}_2 \rangle_{t\sigma_2})^{t_2}$ that contain $F(g)$. Then

$$m_s = \sum_{t \in S_{2,s}} m_{(s,t)} \text{ and } n_t = \sum_{s \in S_{1,t}} n_{(t,s)}. \tag{2.1}$$

Notice that both $\bigcup_{s \in S_1} \{(Y^\circ s\sigma_1, Y^\circ t\sigma_2) \mid t \in S_{2,s}\}$ and $\bigcup_{t \in S_2} \{(Y^\circ s\sigma_1, Y^\circ t\sigma_2) \mid s \in S_{1,t}\}$ are sets of orbit representatives for

$$\{(Y^\circ s\sigma_1, Y^\circ t\sigma_2) \in N_X(Y^\circ)\sigma_1/Y^\circ \times N_X(Y^\circ)\sigma_2/Y^\circ \mid [Y^\circ s\sigma_1, Y^\circ t\sigma_2] = Y^\circ\}$$

under the conjugation action of $N_X(Y^\circ)/Y^\circ$. For $s, x \in X$ we can, and will, assume that $(s^x)_i = s_i^x$. Thus, for all $x \in X$, we have $(Y_{(t\sigma_2)^x}^\circ (s\widetilde{\sigma}_1)^x)^{(t^x)_2} = (Y_{t\sigma_2}^\circ s\widetilde{\sigma}_1)^{t_2 x}$, so $n_{(t',s')} = n_{(t,s)}$ if $(s'\sigma_1, t'\sigma_2) = (s\sigma_1, t\sigma_2)^x$. Therefore,

$$\sum_{s \in S_1} \sum_{t \in S_{2,s}} n_{(t,s)} = \sum_{t \in S_2} \sum_{s \in S_{1,t}} n_{(t,s)} \tag{2.2}$$

The conclusion of part (ii) is that $m_{(s,t)} = n_{(t,s)}$ for all $s, t \in Y$ such that $[s\sigma_1, t\sigma_2]$, and, in light of (2.1) and (2.2), this implies that

$$\sum_{s \in S_1} m_s = \sum_{s \in S_1} \sum_{t \in S_{2,s}} m_{(s,t)} = \sum_{s \in S_1} \sum_{t \in S_{2,s}} n_{(t,s)} = \sum_{t \in S_2} \sum_{s \in S_{1,t}} n_{(t,s)} = \sum_{t \in S_2} n_t.$$

which is the conclusion of part (i).

It remains to prove part (ii). Let $s, t \in N_X(Y^\circ)$ such that $[s\sigma_1, t\sigma_2] = 1$. We have

$$
\begin{aligned}
m_{(s,t)} &= \frac{|\{x \in \langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle \mid g \in (Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)^{s_1 x}\}|}{|N_{\langle X_{\sigma_1}, \widetilde{\sigma}_1 \rangle}((Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)^{s_1})|} = \frac{|g^{X_{\sigma_1}} \cap (Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)^{s_1}||C_{\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle}(g)|}{|N_{\langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle}((Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)^{s_1})|} \\
&= \frac{|(g^{s_1^{-1}})^{X_{s\sigma_1}} \cap Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2||C_{\langle X_{s\sigma_1}, \widetilde{\sigma}_2 \rangle}(g)|}{|N_{\langle X_{s\sigma_1}, \widetilde{\sigma}_2 \rangle}(Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)|} = \frac{|(g^{s_1^{-1}})^{X_{s\sigma_1}} \cap Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2||C_{X_{s\sigma_1}}(g)|}{|N_{X_{s\sigma_1}}(Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2)|}.
\end{aligned} \tag{2.3}
$$

Similarly,

$$n_{(t,s)} = \frac{|(F(g)^{t_2^{-1}})^{X_{t\sigma_2}} \cap Y_{t\sigma_2}^\circ s\widetilde{\sigma}_1||C_{X_{\sigma_2}}(F(g))|}{|N_{X_{t\sigma_2}}(Y_{t\sigma_2}^\circ s\widetilde{\sigma}_1)|}. \tag{2.4}$$

Let $y_1, \ldots, y_k$ represent the $Y_{s\sigma_1}^\circ$-classes in $Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2$, and let $I = \{i \mid y_i \in (g^{s_1^{-1}})^{X_{s\sigma_1}}\}$. Then

$$|(g^{s_1^{-1}})^{X_{s\sigma_1}} \cap Y_{s\sigma_1}^\circ t\widetilde{\sigma}_2| = \sum_{i \in I} |y_i^{Y_{s\sigma_1}^\circ}| = \sum_{i \in I} \frac{|Y_{s\sigma_1}^\circ|}{|C_{Y_{s\sigma_1}^\circ}(y_i)|}. \tag{2.5}$$

Observe that

$$I = \{i \mid y_i \in (g^{s_1^{-1}})^{X_{s\sigma_1}}\} = \{i \mid (y_i, s\sigma_1)^X = (g^{s_1^{-1}}, s\sigma_1)^X\}.$$

Applying the Shintani map F, we see

$$(g^{s_1^{-1}}, s\sigma_1)^X = (g, \sigma_1)^X = (\sigma_2, F(g))^X = (t\sigma_2, F(g)^{t_2^{-1}})^X.$$

Let $E_{(s,t)}$ be the Shintani map of $(Y^\circ, s\sigma_1, t\sigma_2)$. Then $E_{(s,t)}(y_1), \ldots, E_{(s,t)}(y_k)$ represent the $Y_{t\sigma_2}^\circ$-classes in $Y_{t\sigma_2}^\circ s\widetilde{\sigma}_1$, and $(y_i, s\sigma_1)^{Y^\circ} = (t\sigma_2, E_{(s,t)}(y_i))^{Y^\circ}$, so $(y_i, s\sigma_1)^X = (t\sigma_2, E_{(s,t)}(y_i))^X$. Therefore,

$$I = \{i \mid (t\sigma_2, E_{(s,t)}(y_i))^X = (t\sigma_2, F(g)^{t_2^{-1}})^X\} = \{i \mid E_{(s,t)}(y_i) \in (F(g)^{t_2^{-1}})^{X_{t\sigma_2}}\}.$$

7

This implies that

$$|(F(g)^{t_2^{-1}})^{X_{t\sigma_2}} \cap Y^\circ_{t\sigma_2} s\widetilde{\sigma}_1| = \sum_{i \in I} |y_i^{Y^\circ_{t\sigma_2}}| = \sum_{i \in I} \frac{|Y^\circ_{t\sigma_2}|}{|C_{Y^\circ_{t\sigma_2}}(E_{(s,t)}(y_i))|}. \tag{2.6}$$

By Theorem 2.1, $|C_{X_{\sigma_1}}(g)| = |C_{X_{\sigma_2}}(F(g))|$ and $|C_{Y^\circ_{s\sigma_1}}(y_i)| = |C_{Y^\circ_{t\sigma_2}}(E_{(s,t)}(y_i))|$. Therefore, by combining (2.3)–(2.6), we obtain

$$\frac{m_{(s,t)}}{n_{(t,s)}} = \frac{|N_{X_{t\sigma_2}}(Y^\circ_{t\sigma_2} s\widetilde{\sigma}_1) : Y^\circ_{t\sigma_2}|}{|N_{X_{s\sigma_1}}(Y^\circ_{s\sigma_1} t\widetilde{\sigma}_2) : Y^\circ_{s\sigma_1}|} = \frac{|C_{N_{X_{t\sigma_2}}(Y^\circ_{t\sigma_2})/Y^\circ_{t\sigma_2}}(s\sigma_1)|}{|C_{N_{Y_{s\sigma_1}}(Y^\circ_{s\sigma_1})/Y^\circ_{s\sigma_1}}(t\sigma_2)|} = \frac{|C_{(N_X(Y^\circ)/Y^\circ)_{t\sigma_2}}(s\sigma_1)|}{|C_{(N_X(Y^\circ)/Y^\circ)_{s\sigma_1}}(t\sigma_2)|}.$$

We conclude that $m_{(s,t)} = n_{(t,s)}$ since

$$|C_{(N_X(Y^\circ)/Y^\circ)_{t\sigma_2}}(s\sigma_1)| = |C_{(N_X(Y^\circ)/Y^\circ)}(s\sigma_1) \cap C_{(N_X(Y^\circ)/Y^\circ)}(t\sigma_2)| = |C_{(N_X(Y^\circ)/Y^\circ)_{s\sigma_1}}(t\sigma_2)|.$$

This completes the proof. $\qquad\square$

The following example not only highlights how we apply Theorem 2.8, but also introduces an embedding that we will return to at the end of the paper.

Example 2.9. Let $q = 2^f$. Let $T = \mathrm{Sp}_{2m}(q)$ and $g = \varphi^i$ where i divides f. Let X be the simple algebraic group Sp_{2m} and let φ be the standard Frobenius endomorphism $(x_{ij}) \mapsto (x_{ij}^2)$. Fix $\sigma = \varphi^i$, and write $\sigma_1 = \sigma^e$ and $\sigma_2 = \sigma$, where $e = f/i$. Then the Shintani map of (X, σ_1, σ_2) is $F \colon \mathrm{Sp}_{2m}(q)g \to \mathrm{Sp}_{2m}(q_0)$, where $q_0 = 2^i$ and $q = q_0^e = 2^f$.

Let $Y = \mathrm{O}_{2m}$, a maximal closed σ-stable subgroup of X. Now $Y^\circ = \Omega_{2m}$ and $Y = Y^\circ{:}\langle s \rangle$ where s is a transvection. Then $\{1, s\}$ is a transversal of Y° in $Y = N_X(Y^\circ)$. Fix $s_1, s_2 \in X$ such that $[s_i^{-1}, \sigma_i^{-1}] = s$.

Both $Y_{\sigma^e} = \mathrm{O}^+_{2m}(q)$ and $(Y^{s_1})_{\sigma^e} = Y^{s_1}_{s\sigma^e} = \mathrm{O}^-_{2m}(q)$ are maximal subgroups of $X_{\sigma^e} = \mathrm{Sp}_{2m}(q)$, and $Y_\sigma = \mathrm{O}^+_{2m}(q_0)$ and $(Y^{s_2})_\sigma = Y^{s_2}_{s\sigma} = \mathrm{O}^-_{2m}(q_0)$ are maximal subgroups of $X_\sigma = \mathrm{Sp}_{2m}(q_0)$.

We now apply Theorem 2.8.

(i) For all $x \in \mathrm{Sp}_{2m}(q)$, the total number of maximal subgroups of $G = \langle \mathrm{Sp}_{2m}(q), \widetilde{\varphi}^i \rangle$ of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ that contain $x\widetilde{\varphi}^i$ equals the total number of maximal subgroups of $G_0 = \mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^+_{2m}(q_0)$ or $\mathrm{O}^-_{2m}(q_0)$ that contain $F(x\widetilde{\varphi}^i)$.

(ii) In fact, we have the following more detailed correspondences

$$\{A \in (\Omega^+_{2m}(q)\varphi^i)^G \mid x \in A\} \longleftrightarrow \{B \in \Omega^+_{2m}(q_0)^{G_0} \mid F(x) \in B\}$$
$$\{A \in (\Omega^-_{2m}(q)\varphi^i)^G \mid x \in A\} \longleftrightarrow \{B \in (\Omega^+_{2m}(q_0)s)^{G_0} \mid F(x) \in B\}$$
$$\{A \in (\Omega^+_{2m}(q)s\varphi^i)^G \mid x \in A\} \longleftrightarrow \{B \in (\Omega^-_{2m}(q_0)s^e)^{G_0} \mid F(x) \in B\}$$
$$\{A \in (\Omega^-_{2m}(q)s\varphi^i)^G \mid x \in A\} \longleftrightarrow \{B \in (\Omega^-_{2m}(q_0)s^{e+1})^{G_0} \mid F(x) \in B\}.$$

Remark 2.10. Example 2.9(i) was given by more indirect means in [28, Section 2.2.3] relying on the isogeny $\mathrm{SO}_{n+1} \to \mathrm{Sp}_n$ in characteristic two and a bespoke geometric argument, but the more detailed information given in Example 2.9(ii) was not available in that context.

By [19, Theorem 2], when $p = 2$, every element of $\mathrm{Sp}_{2m}(q)$ is contained in a maximal subgroup of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$. Therefore, Example 2.9 implies the following.

Proposition 2.11. *Let $p = 2$ and let $\mathrm{PSp}_{2m}(q) \leqslant G \leqslant \mathrm{P\Gamma Sp}_{2m}(q)$. Then every element of G is contained in a maximal subgroup of the form $N_G(H)$ where H is a maximal subgroup of $\mathrm{PSp}_{2m}(q)$ isomorphic to $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$.*

2.3 Further properties

Continue to assume that X is a connected algebraic group, σ_1 and σ_2 are commuting Steinberg endomorphisms of X and F is the Shintani map of (X, σ_1, σ_2).

We now present properties of Shintani descent, beginning with a general version of [29, Lemma 3.2.2]. If an isogeny $\pi\colon X \to Y$ has a $\langle \sigma_1, \sigma_2 \rangle$-stable kernel, then σ_i induces a Steinberg endomorphism $\sigma_{i,Y}$ on Y such that $\sigma_{i,Y} \circ \pi = \pi \circ \sigma_i$ and, by mapping $\sigma_i \mapsto \sigma_{i,Y}$, π extends to an abstract group homomorphism $\pi\colon \langle X, \sigma_1, \sigma_2 \rangle \to \langle Y, \sigma_{1,Y}, \sigma_{2,Y} \rangle$. We simply write σ_i for $\sigma_{i,Y}$.

Lemma 2.12. *Let $\pi\colon X \to Y$ be an isogeny with a $\langle \sigma_1, \sigma_2 \rangle$-stable kernel. Let E be the Shintani map of (Y, σ_1, σ_2). Then $E \circ \pi = \pi \circ F$ and $E^{-1} \circ \pi = \pi \circ F^{-1}$*

Proof. If $(x\sigma_2, \sigma_1)^X = (\sigma_2, y\sigma_1)^X$ then $(\pi(x)\sigma_2, \sigma_1)^Y = (\sigma_2, \pi(y)\sigma_1)^Y$, so

$$E(\pi(x\sigma_2)^{Y_{\sigma_1}}) = E((\pi(x)\sigma_2)^{Y_{\sigma_1}}) = (\pi(y)\sigma_1)^{Y_{\sigma_2}} = \pi((y\sigma_1)^{X_{\sigma_2}}) = \pi(F(x\sigma_2)),$$
$$E^{-1}(\pi(y\sigma_1)^{Y_{\sigma_2}}) = E^{-1}((\pi(y)\sigma_1)^{Y_{\sigma_2}}) = (\pi(x)\sigma_2)^{Y_{\sigma_1}} = \pi((x\sigma_2)^{X_{\sigma_1}}) = \pi(F^{-1}(y\sigma_1)),$$

which proves the result. $\qquad\square$

Corollary 2.13. *Let $\pi\colon X \to Y$ be a bijective isogeny with a $\langle \sigma_1, \sigma_2 \rangle$-stable kernel. Then $\pi \circ F \circ \pi^{-1}$. is the Shintani map of (Y, σ_1, σ_2).*

Corollary 2.14. *Let $\pi\colon X \to Y$ be an isogeny with a $\langle \sigma_1, \sigma_2 \rangle$-stable kernel. Let E be the Shintani map of (Y, σ_1, σ_2). Then E restricts to a bijection*

$$\{(x\widetilde{\sigma}_2)^{Y_{\sigma_1}} \mid x \in \pi(X_{\sigma_1})\} \to \{(y\widetilde{\sigma}_1)^{Y_{\sigma_2}} \mid y \in \pi(X_{\sigma_2})\}.$$

Example 2.15. Let $Y = \mathrm{PSL}_n$, let $\varphi\colon Y \to Y$ be Frobenius endomorphism $(y_{ij}) \mapsto (y_{ij}^p)$ and let $\gamma\colon Y \to Y$ be the standard involutory graph automorphism $y \mapsto (y^{-\mathsf{T}})^J$ where J is the antidiagonal matrix with antidiagonal entries $1, -1, 1, -1, \dots, (-1)^{n+1}$. Write $q = p^f$ and let $E\colon \mathrm{PGL}_n(q)\gamma\widetilde{\varphi} \to \mathrm{PGU}_n(p)\gamma^f$ be the Shintani map of $(Y, \varphi^f, \gamma\varphi)$, noting that $\widetilde{\varphi}^f|_{Y_{\gamma\varphi}} = \gamma^f|_{Y_{\gamma\varphi}}$. For many applications, we will want to focus on the coset $\mathrm{PSL}_n(q)\gamma\widetilde{\varphi}$. Does this coset correspond to $\mathrm{PSU}_n(p)\gamma^f$ under F? Yes. To see this, let $\pi\colon \mathrm{SL}_n \to \mathrm{PSL}_n$ be isogeny given by taking the quotient of SL_n by its centre. As $\pi(Y_{\varphi^f}) = \pi(\mathrm{SL}_n(q)) = \mathrm{PSL}_n(q)$ and $\pi(Y_{\gamma\varphi}) = \pi(\mathrm{SU}_n(p)) = \mathrm{PSU}_n(p)$, Corollary 2.14 implies that E restricts to the bijection

$$\{(x\widetilde{\varphi})^{\mathrm{PGL}_n(q)} \mid x \in \mathrm{PSL}_n(q)\} \to \{(y\gamma^f)^{\mathrm{PGU}_n(p)} \mid y \in \mathrm{PSU}_n(p)\}.$$

When f is even this can also be proved via determinants, as in [9, Lemma 5.3], but this more concrete approach does not apply when f is odd.

The application of Corollary 2.14 in Example 2.15 will be vastly generalised by the concept of *outer Shintani descent*, which we introduce in Section 3.5.

The next lemma captures how powers and element orders behave under Shintani descent.

Lemma 2.16. *Assume that there exist $d, e \geqslant 1$ such that d divides $|\widetilde{\sigma}_1|$, de divides $|\widetilde{\sigma}_2|$ and $\widetilde{\sigma}_2^{de} = \widetilde{\sigma}_1^d$. For all $x \in X_{\sigma_1}$, the following hold*

(i) $F(x\widetilde{\sigma}_2)^d = E((x\widetilde{\sigma}_2)^d)$, *where E is the Shintani map of $(X, \sigma_2^{de}, \sigma_2^d)$*

(ii) $|x\widetilde{\sigma}_2| = de|F(x\widetilde{\sigma}_2)|$.

Proof. Let $\sigma = \sigma_2^d$ and let E be the Shintani map of (X, σ^e, σ). Fix $a \in X$ such that $x = aa^{-\sigma_2^{-1}}$. Then $F(x\widetilde{\sigma}_2) = a^{-1}a^{\sigma_1^{-1}}\widetilde{\sigma}_2$. Now $(x\widetilde{\sigma}_2)^d = aa^{-\sigma^{-1}}\widetilde{\sigma}$ and $F(x\widetilde{\sigma}_2)^d = a^{-1}a^{\sigma^{-e}}\widetilde{\sigma}^e$, so $F(x\widetilde{\sigma}_2)^d = E((x\widetilde{\sigma}_2)^d)$. In particular, $|(x\widetilde{\sigma}_2)^d| = e|E((x\widetilde{\sigma}_2)^d)| = |F(x\widetilde{\sigma})^d|$. Since d divides $|\widetilde{\sigma}_2|$, which divides $|x\widetilde{\sigma}_2|$, we conclude that $|x\widetilde{\sigma}_2| = d|(x\widetilde{\sigma}_2)^d| = de|F(x\widetilde{\sigma})^d|$. $\qquad\square$

The following observation [10, Lemma 3.20] is an immediate consequence of Lemma 2.16.

Corollary 2.17. *Let σ be a Steinberg endomorphism of X, let e be a positive integer and let F be the Shintani map of (X, σ^e, σ). Then $|x\widetilde{\sigma}| = e|F(x\widetilde{\sigma})|$ for all $x \in X_\sigma$.*

We use Corollary 2.17 to obtain the following result, which is important to Section 4.

Lemma 2.18. *Let X be connected, let σ be a Steinberg endomorphism of X and let $e > 1$. Let F be the Shintani map of (X, σ^e, σ). Let $x \in X_{\sigma^e}$ and $y \in X_\sigma$ satisfy $F(x\widetilde{\sigma}) = y$. Write $G = \langle X_{\sigma^e}, \widetilde{\sigma} \rangle$.*

  (i) *Assume that e is a prime divisor of $|y|$ and $|y|$ does not properly divide the order of any element of X_σ. Then $x\widetilde{\sigma}$ is not contained in any G-conjugate of $\langle X_\sigma, \widetilde{\sigma} \rangle$.*

  (ii) *Assume that e is coprime to $|y|$ and $y^X \cap X_\sigma = y^{X_\sigma}$. Then $x\widetilde{\sigma}$ is contained in a G-conjugate of $\langle X_{\sigma^{e/k}}, \widetilde{\sigma} \rangle$ for every prime divisor k of e.*

Proof. For part (i), suppose that $x\widetilde{\sigma} \in \langle X_\sigma, \widetilde{\sigma} \rangle^g$ for some $g \in X_{\sigma^e}$. Then $(x\widetilde{\sigma})^g = h\widetilde{\sigma} \in \langle X_\sigma, \widetilde{\sigma} \rangle$, that is, $h \in X_\sigma$. By Corollary 2.17, $e|y| = |h\widetilde{\sigma}| = e|h|/(e, |h|) = |h|$, which is a contradiction since we assumed that $|y|$ does not properly divide the order of any element of X_σ.

For part (ii), fix d such that $ed \equiv -1 \pmod{|y|}$. Then $y^d \in X_\sigma \leqslant X_{\sigma^e}$ and $F((y^d\widetilde{\sigma})^{X_{\sigma^e}}) = (a^{-1}(y^d\widetilde{\sigma})^{-e}a)^{X_\sigma} = (a^{-1}ya)^{X_\sigma}$ for some $a \in X$. Since $y^X \cap X_\sigma = y^{X_\sigma}$, we know that $a^{-1}ya$ is X_σ-conjugate to y, so $F((y^d\widetilde{\sigma})^{X_{\sigma^e}}) = y^{X_\sigma}$ and $x\widetilde{\sigma} = (y^d\widetilde{\sigma})^g$ for some $g \in X_{\sigma^e}$. Now $y^d\widetilde{\sigma} \in \langle X_\sigma, \widetilde{\sigma} \rangle \leqslant \langle X_{\sigma^{e/k}}, \widetilde{\sigma} \rangle$ for every prime divisor k of e, so $x\widetilde{\sigma} \in \langle X_{\sigma^{e/k}}, \widetilde{\sigma} \rangle^g$, as claimed. $\square$

Our next result is a direct generalisation of [29, Lemma 3.3.4].

Lemma 2.19. *Let $x \in X_{\sigma_1}$ and let $H \leqslant G = \langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$. Then x is contained in at most $|C_{X_{\sigma_2}}(F(x\widetilde{\sigma}_2))|$ distinct G-conjugates of H.*

Proof. By [29, Lemma 2.1.2] for example, the number of G-conjugates of H that contain $x\widetilde{\sigma}_2$ is

$$\frac{|G|}{|N_G(H)|} \cdot \frac{|(x\widetilde{\sigma}_2)^G \cap H|}{|(x\widetilde{\sigma}_2)^G|} = \frac{|(x\widetilde{\sigma}_2)^G \cap H||C_G(x\widetilde{\sigma}_2)|}{|N_G(H)|} = \frac{|(x\widetilde{\sigma}_2)^G \cap H||\widetilde{\sigma}_2||C_{X_{\sigma_1}}(x\widetilde{\sigma}_2)|}{|N_G(H)|}$$

$$= \frac{|(x\widetilde{\sigma}_2)^G \cap H||\widetilde{\sigma}_2||C_{X_{\sigma_2}}(F(x\widetilde{\sigma}_2))|}{|N_G(H)|} \leqslant \frac{|H|}{|N_G(H)|} \cdot |C_{X_{\sigma_2}}(F(x\widetilde{\sigma}_2))| \leqslant |C_{X_{\sigma_2}}(F(x\widetilde{\sigma}_2))|,$$

where the penultimate inequality holds since $|(x\widetilde{\sigma}_2)^G \cap H| \leqslant |H|/|\widetilde{\sigma}_2|$. $\square$

Let us comment on the special case of Shintani descent that has previously been applied to group theoretic problems (see [29, Chapter 3] for a general reference). The key is the following immediate consequence of Lemma 2.2.

Lemma 2.20. *Let X be connected, let σ be a Frobenius endomorphism of X and let $e > 1$. Let F be the Shintani map of (X, σ^e, σ). Then $F((x\widetilde{\sigma})^{X_{\sigma^e}}) = (a^{-1}(x\widetilde{\sigma})^{-e}a)^{X_\sigma}$ for $a \in X$ such that $x = aa^{-\sigma^{-1}}$.*

Hence, what is referred to in the literature as the Shintani map of (X, σ, e) is the map

$$F' \colon \{(x\widetilde{\sigma})^{X_{\sigma^e}} \mid x \in X_{\sigma^e}\} \to \{y^{X_\sigma} \mid y \in X_\sigma\} \qquad F'((x\widetilde{\sigma})^{X_{\sigma^e}}) = (F(x\widetilde{\sigma})^{-1})^{X_\sigma},$$

where F is the Shintani map of (X, σ^e, σ). Therefore, previous applications of Shintani descent are essentially the special case where X is connected and $\sigma_1 = \sigma_2^e$. Here, up to X-conjugacy, the Shintani map F simply involves raising to the power $-e$, which is often useful.

Remark 2.21. Our main application is to almost simple groups, where we have a finite simple group of Lie type T and an automorphism $g \in \text{Aut}(T)$, which we study by writing $T = O^{p'}(X_{\sigma_1})$ and $g \in X_{\sigma_1}\widetilde{\sigma}_2$ for a simple algebraic group X and two commuting Steinberg endomorphisms σ_1 and σ_2. However, we cannot always insist that $\sigma_1 = \sigma_2^e$. For example, if $T = \text{PSL}_n(p^f)$ for odd f and $g = \gamma\widetilde{\varphi}$, then we choose $(X, \sigma_1, \sigma_2) = (\text{PSL}_n, \varphi^f, \gamma\varphi)$, but σ_1 is not a power of σ_2 (see Example 2.5 for the definitions of φ and γ). A partial solution was found in [28, Lemma 3.4.1], which allows us to work with some elements of Tg but does not allow us to prove results about all elements of Tg, which we need to be able to do in order to prove Theorem 1. The unified approach of this paper allows us to do this.

3 Shintani descent and finite groups of Lie type

In this section, we systematically apply Shintani descent to almost simple groups of Lie type, and we begin by recalling some information about these groups in Sections 3.1–3.3.

3.1 Finite groups of Lie type

Let $\mathcal{L}$ be the set of finite groups T such that $T = O^{p'}(X_\sigma)$ for a simple algebraic group X of adjoint type and a Steinberg endomorphism σ of X. Every group in $\mathcal{L}$ other than

$$\text{PSL}_2(2) \cong 3{:}2, \quad \text{PSL}_2(3) \cong 2^2{:}3, \quad \text{PSU}_3(2) \cong 3^2{:}Q_8, \quad {}^2B_2(2) \cong 5{:}4$$

$$\text{PSp}_4(2) \cong S_6, \quad G_2(2) \cong \text{P}\Gamma\text{L}_3(3), \quad {}^2G_2(3) \cong \text{P}\Gamma\text{L}_2(8), \quad {}^2F_4(2)$$

is a nonabelian simple group, and we will refer to these as the *finite simple groups of Lie type*. (Note that by this definition, the Tits group ${}^2F_4(2)'$ is not a finite simple group of Lie type.)

Let X be a simple algebraic group of adjoint type. Let us fix some notation:

φ is the Frobenius endomorphism of X fixing $\mathbb{F}_p$

γ is the standard involutory graph automorphism of $X \in \{\text{PSL}_n, \text{P}\Omega_{2m}, E_6\}$

τ is the standard triality graph automorphism of $X = \text{P}\Omega_8$

ρ is the graph-field endomorphism of X fixing $\mathbb{F}_p$ if $(X, p) \in \{(\text{PSp}_4, 2), (F_4, 2), (G_2, 3)\}$.

Write $\Sigma(X)$ for the group generated by $\varphi, \gamma, \tau, \rho$ when they are defined. Note that

$$|\gamma| = 2, \quad [\gamma, \varphi] = 1, \quad |\tau| = 3, \quad \tau^\gamma = \tau^{-1}, \quad [\tau, \varphi] = 1, \quad \rho^2 = \varphi.$$

For $T = O^{p'}(X_\sigma) \in \mathcal{L}$, note that $\text{Aut}(T) \cong \text{Inndiag}(T){:}\Sigma(T)$, where $\text{Inndiag}(T) = X_\sigma$ and $\Sigma(T) = \{g|_{X_\sigma} \mid g \in \Sigma(X) \text{ and } g^\sigma = g\}$ (see [22, Theorem 2.5.4]).

3.2 Classical groups

We say that a simple algebraic group is a *classical group* with natural module $\overline{\mathbb{F}}_p^n$ if it is one of

$$\text{PSL}_n \ (n \geqslant 2), \quad \text{PSp}_n \ (n \geqslant 4), \quad \text{P}\Omega_n \ (n \geqslant 7),$$

where we omit reference to the field. Similarly, $T \in \mathcal{L}$ is a *classical group* if it is one of

$$\text{PSL}_n(q) \ (n \geqslant 2), \quad \text{PSU}_n(q) \ (n \geqslant 3), \quad \text{PSp}_n(q) \ (n \geqslant 4), \quad \text{P}\Omega_n^\varepsilon(q) \ (n \geqslant 7),$$

and the natural module for T is $\mathbb{F}_{q^u}^n$ where $u = 2$ if $T = \text{PSU}_n(q)$ and $u = 1$ otherwise.

If X is a simple classical algebraic group, then define $\text{Aut}^*(X) = X{:}\Sigma^*(X)$ where

$$\Sigma^*(X) = \begin{cases} \langle \varphi, \gamma \rangle \cong C_2 \times C_\infty & \text{if } X \in \{\text{PSL}_n \ (n \geqslant 3), \ \text{P}\Omega_{2m}\} \\ \langle \varphi \rangle \cong C_\infty & \text{if } X \in \{\text{PSL}_2, \ \text{PSp}_{2m}, \ \text{P}\Omega_{2m+1}\}. \end{cases}$$

Similarly, for classical $T = O^{p'}(X_\sigma) \in \mathcal{L}$, define $\Sigma^*(T) = \{g|_{X_\sigma} \mid g \in \Sigma^*(X) \text{ and } g^\sigma = g\}$ and $\mathrm{Aut}^*(T) = \mathrm{Inndiag}(T){:}\Sigma^*(T)$, so $\mathrm{Aut}^*(T) = \mathrm{Aut}(T)$ unless T is $\mathrm{PSp}_4(2^f)$ or $\mathrm{P\Omega}_8^+(q)$.

For $T \in \mathcal{L}$ and $g \in \Sigma(T)$, say that (T, g) is *classical* if T is a classical group and $g \in \Sigma^*(T)$.

3.3 Automorphisms

Let us now give a concrete description of the automorphism group of T.

For $x \in \mathrm{Aut}(T)$, write $\ddot{x} = Tx$, so

$$\mathrm{Out}(T) = \{\ddot{x} \mid x \in \mathrm{Aut}(T)\} \quad \text{and} \quad \mathrm{Outdiag}(T) = \{\ddot{x} \mid x \in \mathrm{Inndiag}(T)\}.$$

The group $\mathrm{Out}(T)$ is described in [22, Theorem 2.5.12]. If $T \neq \mathrm{P\Omega}_{2m}^\varepsilon(q)$, then $\mathrm{Outdiag}(T)$ is cyclic and we write $\mathrm{Inndiag}(T) = \langle T, \delta \rangle$ if it is nontrivial. If $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$, then we adopt the notation from [32, Chapter 2] (see also [29, Section 5.2]) but we write z for $r_\square r_\boxtimes$.

The following result gives a complete description of the conjugacy classes in $\mathrm{Out}(T)$.

Theorem 3.1. *Let* $T = O^{p'}(X_{\sigma_1}) \in \mathcal{L}$ *defined over* $\mathbb{F}_q$ *where* $q = p^f$.

(i) *Let* $x \in \mathrm{Aut}(T)$. *Then* $\langle \ddot{x} \rangle$ *is* $\mathrm{Out}(T)$-*conjugate to* $\langle \ddot{h}\ddot{g} \rangle$ *for a unique* $g = \sigma_2|_{\mathrm{Inndiag}(T)}$ *from Table 1 and some* $h \in \mathrm{Inndiag}(T)$.

(ii) *Let* $g = \sigma_2|_{\mathrm{Inndiag}(T)}$ *for some* σ_2 *in Table 1. Then* $\mathrm{Outdiag}(T)$ *is trivial or the* $\mathrm{Out}(T)$-*classes in* $\mathrm{Outdiag}(T)\ddot{g}$ *are* $\ddot{S}\ddot{g}$ *where* S *is a set given in Table 2.*

Proof. If T is classical, then this is a combination of [29, Proposition 5.2.15, Remark 5.2.17, Proposition 6.2.6 and Remark 6.2.7]. If T is exceptional, then this is [10, Proposition 3.15]. $\square$

3.4 Standard Shintani setups

We can now explain how to study the almost simple groups of Lie type via Shintani descent.

Let $T \in \mathcal{L}$ and $g \in \Sigma(T)$. A *Shintani setup* for (T, g) is a triple (X, σ_1, σ_2), where X is a simple algebraic group of adjoint type and where σ_1 and σ_2 are commuting Steinberg endomorphisms of X such that $T = O^{p'}(X_{\sigma_1})$ and $\langle g \rangle = \langle \sigma_2|_{X_{\sigma_1}} \rangle$.

If $T = O^{p'}(X_{\sigma_1})$ and $g = \sigma_2|_{X_{\sigma_1}}$ for (X, σ_1, σ_2) in Table 1, then (T, g) is a *standard pair*, (X, σ_1, σ_2) is *the* Shintani setup of (T, g) and the Shintani map F of (X, σ_1, σ_2) is *the* Shintani map of (T, g). Note that $F\colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ where $T_0 \in \mathcal{L}$ and $g_0 \in \mathrm{Aut}(T_0)$ are given in Table 1. In particular, (T, g) is classical if and only if $\mathrm{Inndiag}(T_0)$ is classical.

3.5 Outer Shintani descent

In this section, we explain how to restrict a Shintani map $F\colon X_{\sigma_1}\widetilde{\sigma}_2 \to X_{\sigma_2}\widetilde{\sigma}_1$ to particular cosets of $O^{p'}(X_{\sigma_i})$. To do this we introduce an auxiliary bijection. This generalises the observation in Example 2.15 to all almost simple groups of Lie type.

For a standard pair (T, g) with Shintani map F, define the *outer Shintani map* of (T, g) as

$$\ddot{F}\colon \{(Txg)^{\mathrm{Out}(T)} \mid x \in \mathrm{Inndiag}(T)\} \to \{(T_0 x_0 g_0)^{\mathrm{Out}(T_0)} \mid x_0 \in \mathrm{Inndiag}(T_0)\}$$

$$\ddot{F}((Txg)^{\mathrm{Out}(T)}) = (T_0 x_0 g_0)^{\mathrm{Out}(T_0)} \iff F((xg)^{\mathrm{Inndiag}(T)}) = (x_0 g_0)^{\mathrm{Inndiag}(T_0)}.$$

Theorem 3.2. *The outer Shintani map* $\ddot{F}$ *is a well-defined bijection, and if* $\ddot{F}((Txg)^{\mathrm{Outdiag}(T)}) = (T_0 x_0 g_0)^{\mathrm{Outdiag}(T_0)}$, *then* $C_{\mathrm{Outdiag}(T)}(Txg) \cong C_{\mathrm{Outdiag}(T_0)}(T_0 x_0 g_0)$.

Table 1: Standard Shintani setups (i divides f and $q_0 = p^i$)

X	σ_1	T	σ_2	f/i	T_0	g_0	conditions
PSL_n	φ^f	$\mathrm{PSL}_n(q)$	φ^i	any	$\mathrm{PSL}_n(q_0)$	1	
			$\gamma\varphi^i$	even	$\mathrm{PSU}_n(q_0)$	1	
			$\gamma\varphi^i$	odd	$\mathrm{PSU}_n(q_0)$	γ	
	$\gamma\varphi^f$	$\mathrm{PSU}_n(q)$	$\gamma\varphi^i$	odd	$\mathrm{PSU}_n(q_0)$	1	
			φ^i	any	$\mathrm{PSL}_n(q_0)$	γ	
$\mathrm{P}\Omega_{2m+1}$	φ^f	$\Omega_{2m+1}(q)$	φ^i	any	$\Omega_{2m+1}(q_0)$	1	
PSp_{2m}	φ^f	$\mathrm{PSp}_{2m}(q)$	φ^i	any	$\mathrm{PSp}_{2m}(q_0)$	1	
			ρ^i	any	$^2B_2(q_0)$	1	$m = p = 2$ & i odd
	ρ^f	$^2B_2(q)$	ρ^i	any	$^2B_2(q_0)$	1	$m = p = 2$ & f odd
$\mathrm{P}\Omega_{2m}$	φ^f	$\mathrm{P}\Omega_{2m}^+(q)$	φ^i	any	$\mathrm{P}\Omega_{2m}^+(q_0)$	1	
			$\gamma\varphi^i$	even	$\mathrm{P}\Omega_{2m}^-(q_0)$	1	
			$\gamma\varphi^i$	odd	$\mathrm{P}\Omega_{2m}^-(q_0)$	γ	
			$\tau\varphi^i$	$3 \mid e$	$^3D_4(q_0)$	1	$m = 4$
			$\tau\varphi^i$	$3 \nmid e$	$^3D_4(q_0)$	τ^{-1}	$m = 4$
	$\gamma\varphi^f$	$\mathrm{P}\Omega_{2m}^-(q)$	$\gamma\varphi^i$	odd	$\mathrm{P}\Omega_{2m}^-(q_0)$	1	
			φ^i	any	$\mathrm{P}\Omega_{2m}^+(q_0)$	γ	
	$\tau\varphi^f$	$^3D_4(q)$	$\tau\varphi^i$	$3 \nmid e$	$^3D_4(q_0)$	1	$m = 4$
			φ^i	any	$\mathrm{P}\Omega_8^+(q_0)$	τ^{-1}	$m = 4$
E_6	φ^f	$E_6(q)$	φ^i	any	$E_6(q_0)$	1	
			$\gamma\varphi^i$	even	$^2E_6(q_0)$	1	
			$\gamma\varphi^i$	odd	$^2E_6(q_0)$	γ	
	$\gamma\varphi^f$	$^2E_6(q)$	$\gamma\varphi^i$	odd	$^2E_6(q_0)$	1	
			φ^i	any	$E_6(q_0)$	γ	
E_7	φ^f	$E_7(q)$	φ^i	any	$E_7(q_0)$	1	
E_8	φ^f	$E_8(q)$	φ^i	any	$E_8(q_0)$	1	
F_4	φ^f	$F_4(q)$	φ^i	any	$F_4(q_0)$	1	
			ρ^i	any	$^2F_4(q_0)$	1	$p = 2$ & i odd
	ρ^f	$^2F_4(q)$	ρ^i	any	$^2F_4(q_0)$	1	$p = 2$ & f odd
G_2	φ^f	$G_2(q)$	φ^i	any	$G_2(q_0)$	1	
			ρ^i	any	$^2G_2(q_0)$	1	$p = 3$ & i odd
	ρ^f	$^2G_2(q)$	ρ^i	any	$^2G_2(q_0)$	1	$p = 3$ & f odd

Table 2: Out(T)-classes in Outdiag(T)g

T	σ_2	f/i	the sets S	conditions
$\mathrm{PSL}_n(q)$	φ^i	any	$\{\delta^j, \delta^{-j}, \ldots, \delta^{jp^{f-1}}, \delta^{-jp^{f-1}}\}\langle\delta^{p^i-1}\rangle$	
	$\gamma\varphi^i$	even	$\{\delta^j, \delta^{-j}, \ldots, \delta^{jp^{f-1}}, \delta^{-jp^{f-1}}\}\langle\delta^{p^i+1}\rangle$	
	$\gamma\varphi^i$	odd	$\langle\delta\rangle$	$(n, q-1)$ odd
			$\langle\delta^2\rangle,\ \delta\langle\delta^2\rangle$	$(n, q-1)$ even
$\mathrm{PSU}_n(q)$	$\gamma\varphi^i$	odd	$\{\delta^j, \ldots, \delta^{jp^{f-1}}\}\langle\delta^{p^i+1}\rangle$	
	φ^i	any	$\langle\delta\rangle$	$(n, q+1)$ odd
			$\langle\delta^2\rangle,\ \delta\langle\delta^2\rangle$	$(n, q+1)$ even
$\Omega_{2m+1}(q)$	φ^i	any	$\{1\}, \{\delta\}$	q odd
$\mathrm{PSp}_{2m}(q)$	φ^i	any	$\{1\}, \{\delta\}$	q odd
$\mathrm{P\Omega}_{2m}^+(q)$	φ^i	any	$\{1\}, \{\delta\}$	$q^m \equiv 3 \pmod 4$
			$\{1\}, \{z\}, \{\delta, z\delta\}$	$p^{im} \equiv 1 \pmod 4$
			$\{1, z\}, \{\delta, z\delta\}$	$p^{im} \equiv 3 \pmod 4\ \&\ f/i$ even
	$\gamma\varphi^i$	even	$\{1\}, \{\delta\}$	$q^m \equiv 3 \pmod 4$
			$\{1\}, \{z\}, \{\delta, z\delta\}$	$p^{im} \equiv 3 \pmod 4$
			$\{1, z\}, \{\delta, z\delta\}$	$p^{im} \equiv 1 \pmod 4$
	$\gamma\varphi^i$	odd	$\{1\}, \{\delta\}$	$q^m \equiv 3 \pmod 4$
			$\{1, z\}, \{\delta, z\delta\}$	$q^m \equiv 1 \pmod 4$
	$\tau\varphi^i$	$3 \mid e$	$\{1, \delta, z, z\delta\}$	$m = 4\ \&\ q$ odd
$\mathrm{P\Omega}_{2m}^-(q)$	$\gamma\varphi^i$	odd	$\{1\}, \{\delta\}$	$q^m \equiv 1 \pmod 4$
			$\{1\}, \{z\}, \{\delta, z\delta\}$	$p^m \equiv 3 \pmod 4$
	φ^i	any	$\{1\}, \{\delta\}$	$q^m \equiv 1 \pmod 4$
			$\{1, z\}, \{\delta, z\delta\}$	$q^m \equiv 3 \pmod 4$
$E_6(q)$	φ^i	any	$\{1\}, \{\delta, \delta^2\}$	$p^i \equiv 1 \pmod 3$
			$\{1, \delta, \delta^2\}$	$p^i \equiv 2 \pmod 3\ \&\ f/i$ even
	$\gamma\varphi^i$	even	$\{1\}, \{\delta, \delta^2\}$	$p^i \equiv 2 \pmod 3$
			$\{1, \delta, \delta^2\}$	$p^i \equiv 1 \pmod 3$
	$\gamma\varphi^i$	odd	$\{1, \delta, \delta^2\}$	$q \equiv 1 \pmod 3$
$^2E_6(q)$	$\gamma\varphi^i$	odd	$\{1\}, \{\delta, \delta^2\}$	$q \equiv 2 \pmod 3$
	φ^i	any	$\{1, \delta, \delta^2\}$	$q \equiv 2 \pmod 3$
$E_7(q)$	φ^i	any	$\{1\}, \{\delta\}$	q odd

Before proving Theorem 3.2, let us recall some convenient notation for orthogonal groups that was introduced in [29]. For a field K of characteristic $p > 0$, write

$$\mathrm{DO}_{2m}^{\varepsilon}(K) = \begin{cases} \Omega_{2m}^{\varepsilon}(K) & \text{if } p = 2 \\ \{g \in \mathrm{GO}_{2m}^{\varepsilon}(K) \mid \det(g) = \tau(g)^m\} & \text{otherwise.} \end{cases}$$

Here $\tau \colon \mathrm{DO}_{2m}^{\varepsilon}(K) \to K$ is the similarity map and $\det(g) = \pm\tau(g)^m$ for all $g \in \mathrm{GO}_{2m}^{\varepsilon}(K)$ (see [32, Lemmas 2.1.2 and 2.8.4]). As recorded in [29, (2.12)],

$$\mathrm{PDO}_{2m}^{\varepsilon}(q) = \mathrm{DO}_{2m}^{\varepsilon}(q)/Z(\mathrm{DO}_{2m}^{\varepsilon}(q)) = \mathrm{Inndiag}(\mathrm{P}\Omega_{2m}^{\varepsilon}(q)).$$

Proof of Theorem 3.2. We assume that $\mathrm{Inndiag}(T) > T$ or $\mathrm{Inndiag}(T_0) > T_0$ since otherwise $\mathrm{Outdiag}(T)$ and $\mathrm{Outdiag}(T_0)$ are trivial and $\ddot{F} \colon \{\{\ddot{g}\}\} \to \{\{\ddot{g}\}\}$. We consider each nontrivial case in turn, explicitly describing $\ddot{F}$ and showing that it is a bijection, but leaving the reader to verify the claim about centralisers, which is not difficult.

First assume that $p \neq 2$ and $T \in \{\mathrm{PSp}_{2m}(q), \Omega_{2m+1}(q), E_7(q)\}$, so $|\mathrm{Inndiag}(T) : T| = 2$. Let $X \in \{\mathrm{PSp}_{2m}, \mathrm{P}\Omega_{2m+1}, E_7\}$ be the corresponding simple algebraic group of adjoint type. In this case, $g = \widetilde{\varphi}^i$ for some i dividing f, $g_0 = 1$ and $|\mathrm{Inndiag}(T_0) : T_0| = 2$. Now the two distinct $\mathrm{Out}(T)$-classes in $\mathrm{Outdiag}(T)\ddot{\varphi}^i$ are $\{\ddot{\varphi}^i\}$ and $\{\ddot{\delta}\ddot{\varphi}^i\}$ and the two distinct $\mathrm{Out}(T_0)$-classes in $\mathrm{Outdiag}(T_0)$ are $\{\ddot{1}\}$ and $\{\ddot{\delta}_0\}$. Let X^{sc} be the simply connected version of X and let $\pi \colon X^{\mathrm{sc}} \to X$ be the isogeny defined by taking the quotient of X^{sc} by $Z(X^{\mathrm{sc}}) \cong C_2$. Applying Corollary 2.14 to π establishes that

$$F \colon \{(x\widetilde{\varphi}^i)^{\mathrm{Inndiag}(T)} \mid x \in \mathrm{Inndiag}(T)\} \to \{x_0^{\mathrm{Inndiag}(T_0)} \mid x_0 \in \mathrm{Inndiag}(T_0)\}$$

restricts to

$$\{(x\widetilde{\varphi}^i)^{\mathrm{Inndiag}(T)} \mid x \in T\} \to \{x_0^{\mathrm{Inndiag}(T_0)} \mid x_0 \in T_0\}$$

This proves that $\ddot{F}(\{\ddot{\varphi}^i\}) = \{\ddot{1}\}$ and $\ddot{F}(\{\ddot{\delta}\ddot{\varphi}^i\}) = \{\ddot{\delta}_0\}$. In particular, $\ddot{F}$ is a bijection.

Next assume that $p \neq 3$ and $T = E_6^{\varepsilon}(q)$. Write $F \colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ with $T_0 = E_6^{\varepsilon_0}(q_0)$. Note that $|\mathrm{Inndiag}(T) : T| = (3, q - \varepsilon)$ and $|\mathrm{Inndiag}(T_0) : T_0| = (3, q_0 - \varepsilon_0)$. If $\mathrm{Outdiag}(T)$ and $\mathrm{Outdiag}(T_0)$ both consist of a unique $\mathrm{Out}(T)$-class, then there is nothing to prove. From Table 2, we note that $\mathrm{Outdiag}(T)$ has multiple $\mathrm{Out}(T)$-classes (necessarily $\{\ddot{g}\}$ and $\{\ddot{\delta}\ddot{g}, \delta^2\ddot{g}\}$) if and only if $\mathrm{Outdiag}(T_0)$ has multiple $\mathrm{Out}(T_0)$-classes (necessarily $\{\ddot{g}_0\}$ and $\{\ddot{\delta}_0\ddot{g}_0, \ddot{\delta}_0^2\ddot{g}_0\}$) if and only if $g_0 = 1$ and $q_0 \equiv \varepsilon_0 \pmod 3$ (which implies that $q \equiv \varepsilon \pmod 3$). Therefore, assume that $g_0 = 1$ and $q_0 \equiv \varepsilon_0 \pmod 3$. Then applying Corollary 2.14 to the isogeny $E_6^{\mathrm{sc}} \to E_6$ with kernel $Z(E_6^{\mathrm{sc}}) \cong C_3$, shows that F restricts to

$$\{(xg)^{\mathrm{Inndiag}(E_6(q))} \mid x \in E_6(q)\} \to \{(x_0g_0)^{\mathrm{Inndiag}(E_6(q_0))} \mid x_0 \in E_6(q_0)\},$$

establishing that $\ddot{F}(\{\ddot{g}\}) = \{\ddot{g}_0\}$ and $\ddot{F}(\{\ddot{\delta}\ddot{g}, \delta^2\ddot{g}\}) = \{\ddot{\delta}_0\ddot{g}_0, \ddot{\delta}_0^2\ddot{g}_0\}$, so $\ddot{F}$ is bijective.

Now assume that $p \neq 2$ and $T = \mathrm{P}\Omega_{2m}^{\varepsilon}(q)$. Write $F \colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ with $T_0 = \mathrm{P}\Omega_{2m}^{\varepsilon_0}(q_0)$. Now $|\mathrm{Inndiag}(T) : T| = (4, q^m - \varepsilon)$ and $\{\ddot{\delta}\ddot{g}, \ddot{z}\ddot{\delta}\ddot{g}\}$ is an $\mathrm{Out}(T)$-class (possibly of size one) in $\mathrm{Outdiag}(T)\ddot{g}$, and similarly, $|\mathrm{Inndiag}(T_0) : T_0| = (4, q_0^m - \varepsilon_0)$ and $\{\ddot{\delta}_0\ddot{g}_0, \ddot{z}_0\ddot{\delta}_0\ddot{g}_0\}$ is an $\mathrm{Out}(T_0)$-class in $\mathrm{Outdiag}(T_0)\ddot{g}_0$. Applying Corollary 2.14 to the isogeny $\mathrm{SO}_{2m} \to \mathrm{PSO}_{2m}$ with kernel $Z(\mathrm{SO}_{2m})$ shows that F restricts to

$$\{(xg)^{\mathrm{PDO}_{2m}^{\varepsilon}(q)} \mid x \in \mathrm{PSO}_{2m}^{\varepsilon}(q)\} \to \{(x_0g_0)^{\mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)} \mid x_0 \in \mathrm{PSO}_{2m}^{\varepsilon_0}(q_0)\}$$

and consequently that $\ddot{F}(\{\ddot{g}, \ddot{z}\ddot{g}\}) = \{\ddot{g}_0, \ddot{z}_0\ddot{g}_0\}$ and $\ddot{F}(\{\ddot{\delta}\ddot{g}, \ddot{z}\ddot{\delta}\ddot{g}\}) = \{\ddot{\delta}_0\ddot{g}_0, \ddot{z}_0\ddot{\delta}_0\ddot{g}_0\}$. Now if $\ddot{g}$ and $\ddot{z}\ddot{g}$ are $\mathrm{Out}(T)$-conjugate (perhaps even equal) and $\ddot{g}_0$ are $\ddot{z}_0\ddot{g}_0$ are $\mathrm{Out}(T_0)$-conjugate, then the proof that $\ddot{F}$ is bijective is complete. Table 2 allows us to deduce that $\ddot{g}$ and $\ddot{z}\ddot{g}$ are not

Out(T)-conjugate if and only if $\ddot{g}_0$ are $\ddot{z}_0\ddot{g}_0$ are not Out(T_0)-conjugate if and only if $g_0 = 1$ and $q_0^m \equiv \varepsilon_0 \pmod 4$ (which implies that $q^m \equiv \varepsilon \pmod 4$). Therefore, assume that $g_0 = 1$ and $q_0^m \equiv \varepsilon_0 \pmod 4$. Applying Corollary 2.14 to the isogeny $\mathrm{Spin}_{2m} \to \mathrm{PSO}_{2m}$ with kernel $Z(\mathrm{Spin}_{2m})$ shows that F restricts to the bijection

$$\{(xg)^{\mathrm{PDO}_{2m}^{\varepsilon}(q)} \mid x \in \mathrm{P\Omega}_{2m}^{\varepsilon}(q)\} \to \{(x_0 g_0)^{\mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)} \mid x_0 \in \mathrm{P\Omega}_{2m}^{\varepsilon_0}(q_0)\},$$

which implies that $\ddot{F}(\{\ddot{g}\}) = \{\ddot{g}_0\}$ and $\ddot{F}(\{\ddot{z}\ddot{g}\}) = \{\ddot{z}_0\ddot{g}_0\}$. Therefore, $\ddot{F}$ is a bijection.

Finally assume that $T = \mathrm{PSL}_n^{\varepsilon}(q)$. Write $F\colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ with $T_0 = \mathrm{PSL}_n^{\varepsilon_0}(q_0)$. Note that $|\mathrm{Inndiag}(T) : T| = |\ddot{\delta}| = (n, q - \varepsilon)$ and $|\mathrm{Inndiag}(T_0) : T| = |\ddot{\delta}_0| = (n, q_0 - \varepsilon_0)$. For now assume that $g_0 = 1$, so $\ddot{F}\colon \langle\ddot{\delta}\rangle\ddot{g} \to \langle\ddot{\delta}_0\rangle$. Let $x \in \mathrm{PGL}_n^{\varepsilon}(q)$. Then

$$\det(F(xg)) = \det((xg)^{-e}) = \det(x)^{-\frac{q-\varepsilon}{q_0-\varepsilon_0}},$$

so $\ddot{F}(\ddot{\delta}^j\ddot{\varphi}^i) = \ddot{\delta}_0^{-j}$ and $\ddot{F}$ is bijective (this is an easy calculation, but see also [9, Lemmas 4.2 and 5.3] and [29, Lemma 6.4.2]). It remains to assume that $g_0 = \gamma$. From Table 2, we note that Outdiag(T) has multiple Out(T)-classes (necessarily $\langle\ddot{\delta}^2\rangle\ddot{g}$ and $\delta\langle\ddot{\delta}^2\rangle\ddot{g}$) if and only if Outdiag(T_0) has multiple Out(T_0)-classes (necessarily $\langle\ddot{\delta}_0^2\rangle\ddot{g}_0$ and $\delta_0\langle\ddot{\delta}_0^2\rangle\ddot{g}_0$) if and only if n is even and q is odd. If n is even and q is odd, then applying Corollary 2.14 to the isogeny $2.\mathrm{PSL}_n \to \mathrm{PSL}_n$ with kernel $Z(2.\mathrm{PSL}_n) \cong C_2$ shows that F restricts to

$$\{(xg)^{\mathrm{PGL}_n^{\varepsilon}(q)} \mid x \in \tfrac{1}{2}\mathrm{PGL}_n^{\varepsilon}(q)\} \to \{(x_0 g_0)^{\mathrm{PGL}_n^{\varepsilon_0}(q_0)} \mid x_0 \in \tfrac{1}{2}\mathrm{PGL}_n^{\varepsilon_0}(q_0)\},$$

so $\ddot{F}(\langle\ddot{\delta}^2\rangle\ddot{g}) = \langle\ddot{\delta}_0^2\rangle\ddot{g}_0$ and $\ddot{F}(\delta\langle\ddot{\delta}^2\rangle\ddot{g}) = \delta_0\langle\ddot{\delta}_0^2\rangle\ddot{g}_0$, as required. $\square$

We will apply the following corollary of Theorem 3.2 in Proposition 5.6.

Corollary 3.3. *Let $F\colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ be the Shintani map of a standard pair (T, g). Let P and P_0 be properties of elements of $\mathrm{Aut}(T)$ and $\mathrm{Aut}(T_0)$, respectively, that are preserved by conjugation. Assume that $h \in \mathrm{Inndiag}(T)g$ has P if and only if $F(h) \in \mathrm{Inndiag}(T_0)g_0$ has P_0. Then Tx contains an element with property P for all $x \in \mathrm{Inndiag}(T)g$ if and only if T_0x_0 contains an element with property P_0 for all $x_0 \in \mathrm{Inndiag}(T_0)g_0$.*

Proof. We prove the forward implication; the reverse is very similar. Let $x \in \mathrm{Inndiag}(T_0)g$. By hypothesis, $T_0F(x^{\mathrm{Inndiag}(T)})$ contains an element y_0 with property P_0. Let $y \in \mathrm{Inndiag}(T)g$ such that $F(y^{\mathrm{Inndiag}(T)}) = y_0^{\mathrm{Inndiag}(T)}$. By Theorem 3.2, $\ddot{F}(\ddot{y}^{\mathrm{Out}(T)}) = \ddot{y}_0^{\mathrm{Out}(T_0)} = \ddot{F}(\ddot{x}^{\mathrm{Out}(T)})$, that is, $y \in Tx^{\mathrm{Inndiag}(T)}$, so there exists an element in Tx with property P, as required. $\square$

3.6 Maximal subgroups

We conclude this section, with a fundamental theorem, combining [34, Theorem 2] and [35, Theorem 2], that describes the maximal subgroups of the almost simple groups of Lie type.

Theorem 3.4. *Let G be an almost simple group of Lie type with socle T. Write $T = O^{p'}(X_\sigma)$ for a simple algebraic group X of adjoint type and a Steinberg endomorphism σ of X. Let H be a maximal subgroup of G not containing T. Then H is one of*

(I) *$N_G(Y_\sigma \cap T)$ for a maximal closed σ-stable positive-dimensional subgroup Y of X*

(II) *$N_G(X_\alpha \cap T)$ for a Steinberg endomorphism α of X such that $\alpha^k = \sigma$ for a prime k*

(III) *a local subgroup not in (I)*

(IV) *an almost simple group not in (I) or (II)*

(V) *the Borovik subgroup: $H \cap T = (A_5 \times A_6).2^2$ with $T = E_8(q)$ and $p \geqslant 7$.*

Table 3: Geometrically defined subgroups of classical algebraic groups

	structure stabilised	rough description in GL_n
$\mathcal{C}_1$	subspace	maximal parabolic
$\mathcal{C}_1'$	pair of subspaces	$P_{a,b}$ or $\mathrm{GL}_a \times \mathrm{GL}_b$ with $n = a + b$
$\mathcal{C}_2$	$V = \bigoplus_{i=1}^k V_i$ where $\dim V_i = a$	$\mathrm{GL}_a \wr S_k$ with $n = ak$
$\mathcal{C}_3$	tensor product $V = V_1 \otimes V_2$	$\mathrm{GL}_a \circ \mathrm{GL}_b$ with $n = ab$
$\mathcal{C}_4$	$V = \bigotimes_{i=1}^k V_i$ where $\dim V_i = a$	$(\mathrm{GL}_a \circ \cdots \circ \mathrm{GL}_a){:}S_k$ with $n = a^k$
$\mathcal{C}_6$	nondegenerate classical form	GSp_n or GO_n

Remark 3.5. Let us comment on the subgroups arising in Theorem 3.4.

(i) Assume that X is classical with natural module $\overline{\mathbb{F}}_p^n$, $\sigma \in \mathrm{Aut}^*(X)$ and $G \leqslant \mathrm{Aut}^*(T)$.

   (I) The subgroups $Y < X$ are those in the union $\mathcal{C}_1 \cup \mathcal{C}_1' \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4 \cup \mathcal{C}_6$ of classes from [35] defined as stabilisers of geometric structures on $\overline{\mathbb{F}}_p^n$, see Table 3. (Be warned that $\mathcal{C}_i$ notation is inconsistent with the notation for classes of geometric subgroups of *finite* classical groups in [32], which we will not use in this paper.)

  (III) The local subgroups are the symplectic-type normalisers from [32, Section 4.6].

  (IV) Since H is not in (I) or (II), H is a member of the class $\mathcal{S}$ defined in [32, p.3]. In particular, the action of H on the natural module for T is absolutely irreducible, not realisable over a proper subfield and preserves no nondefining classical forms. The subgroups $H \in \mathcal{S}$ are not known in general, but they are given in [2] when $n \leqslant 12$.

Thus, in this case, Theorem 3.4 returns Aschbacher's subgroup structure theorem [1]. The structure, conjugacy and maximality of the subgroups in (I)–(III) is given in [32] when $n > 12$ (complete information on all maximal subgroups is in [2] when $n \leqslant 12$).

(ii) Assume that X is exceptional.

   (I) Here either Y has maximal rank (see [33]) or Y is given in [34, Table II].

  (III) The subgroups in this case are the exotic local subgroups [14].

  (IV) To date, the almost simple subgroups that arise have been completely determined when $T \in \{{}^2F_4(q), {}^2G_2(q), G_2(q)\}$ (see [2] and the references therein).

(iii) Assume that X is $\mathrm{PSp}_4(\overline{\mathbb{F}}_2)$ or $\mathrm{P\Omega}_8(\overline{\mathbb{F}}_p)$ and either $\sigma \notin \mathrm{Aut}^*(X)$ or $G \nleqslant \mathrm{Aut}^*(T)$. Here, T is $\mathrm{PSp}_4(2^f)$ or $\mathrm{P\Omega}_8^+(q)$ and G contains a graph-field or triality automorphism, or T is ${}^2B_2(2^f)$ or ${}^3D_4(q)$. In each case, the maximal subgroups of G are in [2] (where original references are given) and one sees that these subgroups fall into the classes (I)–(IV).

Theorem 3.4 gives the following for the groups that are the main focus of this paper (recall the definition of $\Sigma(X)$ from Section 3.1).

Theorem 3.6. *Let (T, g) be a standard classical pair with Shintani setup (X, σ_1, σ_2). Write $G = \langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$. Let H be a maximal subgroup of G not containing T. Then H is G-conjugate to one of*

(I) *$(\langle Y, \widetilde{\sigma}_2 \rangle^x)_{\sigma_1}$ for some $\langle \sigma_1, \sigma_2 \rangle$-stable subgroup*

$$Y \in \mathcal{C}_1 \cup \mathcal{C}_1' \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4 \cup \mathcal{C}_6$$

and $x \in X$ such that $[x^{-1}, \sigma_1^{-1}] \in Y$

(II) *$\langle X_\alpha, \widetilde{\sigma}_2 \rangle$ for a Steinberg endomorphism $\alpha \in C_{\Sigma(X)}(\sigma_2)$ such that $\alpha^k = \sigma_1$ for some prime k*

(III) *a symplectic-type normaliser*

(IV) *an almost simple group in $\mathcal{S}$.*

4 Applications of Shintani descent to maximal subgroups

In this section, we apply Shintani descent to study the question of which almost simple groups contain elements with few maximal overgroups, motivated by the work on simple groups by Burness and Harper [11]. Our aim is not to comprehensively study this question but to shed light on what Shintani descent does, and does not, allow us to quickly deduce about almost simple groups from existing information on simple groups. In particular, we will prove Theorem 5.

For almost simple groups G, there are two natural pursuits: seeking elements contained in few maximal subgroups and elements contained in few maximal subgroups, all of which are core-free. For $s \in G$, write

$$\mathcal{M}(G,s) = \{H < G \mid H \text{ is maximal in } G \text{ and } s \in H\}.$$

Then we are interested in the following two invariants

$$\mu(G) = \min_{s \in G} |\mathcal{M}(G,s)| \text{ and } \mu^*(G) = \min_{s \in G^*} |\mathcal{M}(G,s)|$$

where G^* is the set of elements of G that are not contained in any proper normal subgroup. A specific motivation for $\mu^*(G)$ is that applications to generation often require core-free maximal overgroups (see [11, Corollary 2.2] on uniform domination, for example).

If G is a nonabelian simple group, then $\mu(G) = \mu^*(G)$, and in [11, Theorem 5], Burness and Harper proved that $\mu(G) \leqslant 3$, except for four groups of Lie type where $4 \leqslant \mu(G) \leqslant 7$. Moreover, they determined $\mu(G)$ for alternating and sporadic G [11, Theorems 3.1 and 4.1].

Before we study the almost simple groups of Lie type via Shintani descent, let us first observe that the methods in [11] are sufficient to completely determine $\mu(G)$ and $\mu^*(G)$ for almost simple groups G with alternating and sporadic socles; this will be of a different flavour to the rest of the paper. It will be convenient to write

$$\mathcal{H} = \left\{n \in \mathbb{N} \mid n = \frac{q^d - 1}{q - 1} \text{ for some prime power } q \text{ and integer } d \geqslant 2\right\}.$$

Proposition 4.1. *Let G be an almost simple group whose socle is alternating, sporadic or $^2F_4(2)'$. Then $\mu(G) \leqslant \mu^*(G) \leqslant 3$. Moreover, if G is not simple, then the following hold.*

(i) *If $G = S_{2m+1}$, then $\mu(G) = \mu^*(G) = 1$ witnessed by an element of shape $[m, m+1]$.*

(ii) *If $G = S_n$ for $n = 2m \geqslant 8$, then $\mu(G) = 2$ witnessed by an element of shape $[m - k, m + k]$, where $k = (m - 1, 2)$. In addition, $\mu^*(G) = 3$ witnessed by an element of shape*

$$\begin{cases} [l - 1, l, l + 1] & \text{if } n = 3l \\ [l - 2, l + 1, l + 2] & \text{if } n = 3l + 1 \\ [l - 1, l + 1, l + 2] & \text{if } n = 3l + 2 \end{cases}$$

unless m is prime and $n \notin \mathcal{H}$, in which case $\mu^*(G) = 2$ witnessed by an n-cycle.

(iii) *Otherwise, G appears in Table 4 and $\mu(G) = \mu^*(G) = k$ witnessed by s.*

Proof. Part (iii) can easily be obtained by employing the computational methods from [11] that are documented in [12], where we describe s using ATLAS notation [15]. From now on we will assume that $G = S_n$ (with $n \neq 6$) and we argue as in the proof of [11, Theorem 3.1].

First assume that $n = 2m + 1$ is odd and $s \in G$ has shape $[m, m+1]$. Then s is contained in a unique maximal intransitive subgroup $H \cong S_m \times S_{m+1}$ and no transitive imprimitive

Table 4: The data for Proposition 4.1(iii), where $\mu(G) = \mu^*(G) = |\mathcal{M}(G,s)| = k$

G	S_6	M_{10}	$\mathrm{PGL}_2(9)$	$M_{12}.2$	$M_{22}.2$	$J_2.2$	$J_3.2$	HS.2
k	3	1	1	3	2	1	1	2
s	6A	8A	10A	12B	14A	14A	34A	20D

Suz.2	McL.2	He.2	O'N.2	$\mathrm{Fi}_{22}.2$	$\mathrm{Fi}'_{24}.2$	HN.2	$^2F_4(2)$
1	1	2	1	2	2	1	2
28A	22A	24A	22A	42A	46A	42A	16E

subgroups (see [11, Lemma 3.4], for example). Moreover, since a power of s is an m-cycle, a theorem of Marggraf (see [40, Theorem 13.5]) implies that no proper primitive subgroup of S_n contains s, noting that s is odd. Therefore, $\mathcal{M}(G,s) = \{H\}$ and $\mu(G) = \mu^*(G) = 1$.

Now assume that $n \geqslant 8$ is even. We begin with upper bounds on $\mu(G)$ and $\mu^*(G)$. Arguing as above, if s has shape $[m-k, m+k]$, then $\mathcal{M}(G,s) = \{A_n, S_{m-k} \times S_{m+k}\}$, and if s has shape $[a,b,c]$ as displayed in the statement, then $\mathcal{M}(G,s) = \{S_a \times S_{n-a}, S_b \times S_{n-b}, S_c \times S_{n-c}\}$, except when $n = 10$ where $\mathcal{M}(G,s) = \{S_9, S_4 \times S_6, S_5 \wr S_2\}$, so $\mu(G) \leqslant 2$ and $\mu^*(G) \leqslant 3$.

We now obtain lower bounds. Let $s \in G$. If s has at least three cycles, then $|\mathcal{M}(G,s)| \geqslant 3$, and if s has shape $[a,b]$, then $s \in A_n$ and s is contained in at least one maximal core-free subgroup of G (of type $S_a \times S_b$ if $a \neq b$ and $S_a \wr S_2$ if $a = b$) so $|\mathcal{M}(G,s)| \geqslant 2$. Now assume that s is an n-cycle. In this case, s is contained in $S_2 \wr S_m$ and $S_m \wr S_2$. If m is composite, say $m = ab$, then s is also contained in $S_a \wr S_{2b}$, and if $n \in \mathcal{H}$, say $n = (q^d - 1)/(q - 1)$, then s is contained in $\mathrm{P\Gamma L}_d(q)$. Therefore, $|\mathcal{M}(G,s)| \geqslant 3$, unless m is prime and $n \notin \mathcal{H}$, in which case, [30, Theorem 3] implies that $|\mathcal{M}(G,s)| = 2$. We may now conclude that $\mu(G) \geqslant 2$ and $\mu^*(G) \geqslant 3$ unless m is prime and $n \notin \mathcal{H}$, in which case $\mu^*(G) = 2$, witnessed by an n-cycle. This completes the proof. $\qquad\square$

We now turn to almost simple groups of Lie type. We begin with a proposition highlighting that, unlike for simple groups, there is no constant upper bound on $\mu(G)$.

Proposition 4.2. *There is no constant c such that for all almost simple groups G we have $\mu(G) \leqslant c$.*

Before proving Proposition 4.2, let us record the following number theoretic result (the author thanks Dan Fretwell for this).

Lemma 4.3. *Let p be prime and let $k, m \geqslant 1$. Then there exist distinct primes $r_1, \ldots, r_k \geqslant p^m$ such that for $1 \leqslant i \leqslant k$ the prime r_i does not divide $p^{mr_1 \cdots r_{i-1} r_{i+1} \cdots r_k} - 1$.*

Proof. For coprime a and b, let $\mathrm{ord}_b(a)$ be the multiplicative order of a modulo b, and note that b divides $a^c - 1$ if and only if $\mathrm{ord}_b(a)$ divides c. Therefore, we seek distinct primes $r_1, \ldots, r_k \geqslant p^m$ such that $\mathrm{ord}_{r_i}(p)$ does not divide $mr_1 \cdots r_{i-1} r_{i+1} \cdots r_k$ for all i.

We proceed by induction on k. For $k = 1$, simply fix a prime $r_1 \geqslant p^m$. Now assume that $k \geqslant 2$ and that there exist primes $p^m \leqslant r_1 < \cdots < r_{k-1}$ where $\mathrm{ord}_{r_i}(p)$ does not divide the product $mr_1 \cdots r_{i-1} r_{i+1} \cdots r_{k-1}$. We claim that we may fix a prime $r_k > r_{k-1}$ such that $r_k - 1$ is coprime to $r_1 \cdots r_{k-1}$. Indeed, for a positive integer x, we know that $x - 1$ is coprime to $r_1 \ldots r_{k-1}$ if the congruence $x \equiv 2 \pmod{r_i}$ is satisfied for all i, but by the Chinese Remainder Theorem, these congruences are equivalent to $x \equiv a \pmod{r_1 \cdots r_k}$ for some a coprime to $r_1 \cdots r_k$ and by Dirichlet's theorem on arithmetic progression, there are infinitely

19

many prime solutions to this latter congruence, so we may choose r_k as a prime solution greater than r_{k-1}. Now $\mathrm{ord}_{r_k}(p)$ is coprime to $r_1 \cdots r_{k-1}$ since $\mathrm{ord}_{r_k}(p)$ divides $r_k - 1$, and $\mathrm{ord}_{r_k}(p)$ does not divide m since $r_k > p^m - 1$, so we deduce that $\mathrm{ord}_{r_k}(p)$ does not divide $mr_1 \cdots r_{k-1}$. In addition, for $1 \leqslant i \leqslant k-1$, $\mathrm{ord}_{r_i}(p)$ is coprime to r_k since $\mathrm{ord}_{r_i}(p) < r_i < r_k$, and $\mathrm{ord}_{r_i}(p)$ does not divide $mr_1 \cdots r_{i-1}r_{i+1} \cdots r_{k-1}$ by hypothesis, so $\mathrm{ord}_{r_i}(p)$ does not divide $mr_1 \cdots r_{i-1}r_{i+1} \cdots r_k$. Therefore, $\mathrm{ord}_{r_i}(p)$ does not divide $mr_1 \cdots r_{i-1}r_{i+1} \cdots r_k$ for all $1 \leqslant i \leqslant k$, as required. The proof is complete by induction. $\qquad\square$

Proof of Proposition 4.2. Fix a positive integer k. We will exhibit an almost simple group G such that $\mu(G) \geqslant k$. By Lemma 4.3, we may fix k distinct primes $r_1, \ldots, r_k \geqslant 2^2$ such that each r_i does not divide $2^{2r_1 \cdots r_{i-1}r_{i+1} \cdots r_k} - 1$. Write $f = r_1 \cdots r_k$. Let $G = \langle \mathrm{PSL}_2(q), \widetilde{\varphi} \rangle$ where $q = 2^f$. Note that r_i does not divide $|\mathrm{PGL}_2(q^{1/r_i})| = q^{1/r_i}(q^{2/r_i} - 1)$.

Let $s \in G$. We claim that $|\mathcal{M}(G, s)| \geqslant k$. Replacing s by another generator of $\langle s \rangle$ if necessary, we can write $s = x\widetilde{\varphi}^i$ where i divides f. Write $e = f/i$ and $q_0 = 2^i$. Let $X = \mathrm{PSL}_2$ and $\sigma = \varphi^i$, and let $F \colon \mathrm{PGL}_2(q)\widetilde{\varphi}^i \to \mathrm{PGL}_2(q_0)$ be the Shintani map of (X, σ^e, σ). Write $F(s) = y$. Note that $y^{\mathrm{PGL}_2} \cap \mathrm{PGL}_2(q_0) = y^{\mathrm{PGL}_2(q_0)}$. Since each r_i does not divide $|\mathrm{PGL}_2(q^{1/r_i})|$, we deduce that $(e, |\mathrm{PGL}_2(q_0)|) = 1$ and consequently that $(e, |y|) = 1$. Therefore, by Lemma 2.18(ii), s is contained in a maximal subgroup of type $\mathrm{PGL}_2(q^{1/r})$ for every prime divisor r of e. Moreover, $s \in \langle \mathrm{PSL}_2(q), \widetilde{\varphi}^r \rangle$ for every prime divisor r of i. Therefore, s is contained in at least k maximal subgroups, as claimed. $\qquad\square$

Remark 4.4. The proof of Proposition 4.2 shows that there does not even exist a constant c such that $\mu(G) \leqslant c$ for all almost simple groups with socle in $\{\mathrm{PSL}_2(2^f) \mid f \geqslant 1\}$.

Despite the negative result in Proposition 4.2, there do exist nonsimple almost simple groups of Lie type containing an element with a unique maximal overgroup.

Proposition 4.5. *Let $G = \langle \Omega_{2m}^+(2^f), \widetilde{\varphi}^i \rangle$ for $m \geqslant 8$ and a proper divisor i of f. Then there exists $s \in G$ such that $\mathcal{M}(G, s) = \{H\} \cup \mathcal{M}_{(\mathrm{II})}$ where H is the stabiliser of a plus-type subspace and $\mathcal{M}_{(\mathrm{II})}$ consists of subfield subgroups. Moreover, if f is a prime dividing $2^k + 1$ or $2^{m-k} + 1$ for some $1 \leqslant k \leqslant \sqrt{2m}/4$ coprime to m, then $\mathcal{M}_{(\mathrm{II})}$ is empty and $\mu(G) = \mu^*(G) = 1$.*

Proof. Fix an integer $1 \leqslant k \leqslant \sqrt{2m}/4$ coprime to m. Write $g = \widetilde{\varphi}^i$ and $(q_0, q) = (2^i, 2^f)$. Let (X, σ^e, σ) be the Shintani setup for (T, g) and let $F \colon \Omega_{2m}^+(q)g \to \Omega_{2m}^+(q_0)$ be the Shintani map of (T, g). Write $V = \mathbb{F}_q^{2m}$ and $V_0 = \mathbb{F}_{q_0}^{2m}$. In addition, write $V_0 = U_1 \perp U_2$, where U_1 and U_2 are nondegenerate minus-type subspaces of dimensions $2k$ and $2m - 2k$, respectively. With respect to this decomposition, let $y = y_1 \perp y_2 \in \Omega_{2m}^+(q_0)$ where $|y_1| = q_0^k + 1$ and $|y_2| = q_0^{m-k} + 1$. Let $s \in Tg$ satisfy $F(s) = y$.

Let $H \in \mathcal{M}(G, s)$. Observe $T \not\leqslant H$ since $G/T = \langle Ts \rangle$. By Theorem 3.6, H has type (I)–(IV). Since $(|y_1|, |y_2|) = 1$, a power of s has a 1-eigenspace of codimension $2k < \max\{2, \sqrt{2m}/2\}$, so [26, Theorem 7.1] implies that $H \in \mathcal{M}_{(\mathrm{I})} \cup \mathcal{M}_{(\mathrm{II})}$, where $\mathcal{M}_{(\mathrm{I})}$ and $\mathcal{M}_{(\mathrm{II})}$ are the sets of type (I) geometric subgroups and type (II) subfield subgroups in $\mathcal{M}(G, s)$.

For now assume that $H \in \mathcal{M}_{(\mathrm{I})}$. That is, H is G-conjugate to $(\langle Y, \widetilde{\sigma} \rangle^{s_1})_{\sigma^e}$ for a maximal closed σ-stable subgroup $Y \in \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ and $s_1 \in X$ such that $[s_1^{-1}, \sigma^{-f}] \in Y$ (note that $\mathcal{C}_1'$ and $\mathcal{C}_6$ are empty for $X = \Omega_{2m}$). To determine the possibilities for H we will consider the maximal type (I) subgroups of X_σ that contain y and then apply Shintani descent.

Let H_0 be a type (I) subgroup of T_0 that contains y. The order of y is divisible by a primitive prime divisor r of $q_0^{2m-2k} - 1$, so by the main theorem of [25], $H_0 \neq Y_\sigma$ for $Y \in \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$. In addition, by Goursat's lemma (see [29, Lemma 2.3.1] for example), y is contained in a unique reducible subgroup of X_σ, which has type $O_{2k}^-(q_0) \times O_{2m-2k}^-(q_0)$. Therefore, $H_0 = (Y^{t_2})_\sigma$ for a closed σ-stable subgroup Y of X of type $O_{2k} \times O_{2m-2k}$ and an element $t_2 \in X$ such that $[t_2^{-1}, \sigma^{-1}] \in Y \setminus Y^\circ$. Moreover, since y has odd order, $y \in ((Y^\circ)^{s_2})_\sigma$. Therefore, by Theorem 2.8, $\mathcal{M}(G,s) = \{H\} \cup \mathcal{M}_{(\text{II})}$ where $H = \langle Y_{\sigma^e}, \widetilde{\sigma} \rangle$ of type $O_{2k}^+(q) \times O_{2m-2k}^+(q)$ (and s is contained in the coset $(Y_{\sigma^e} \setminus Y_{\sigma^e}^\circ)\widetilde{\sigma}$).

To complete the proof, assume that f is a prime dividing $2^k + 1$ or $2^{m-k} + 1$, so $i = 1$. If $H \in \mathcal{M}_{(\text{II})}$, then H is G-conjugate to $\langle X_\varphi, \widetilde{\varphi} \rangle = \langle \Omega_{2m}^+(2), \widetilde{\varphi} \rangle$, so Lemma 2.18(i) implies that $s \notin H$, noting that f divides $|y|$ and $|y|$ does not properly divide the order of any element of $\Omega_{2m}^+(2)$. Therefore, $\mathcal{M}_{(\text{II})}$ is empty, and $\mu^*(G) = \mu(G) = 1$, as required. $\qquad\square$

Observe that Theorem 5 is a combination of Propositions 4.1, 4.2 and 4.5.

We conclude by discussing exceptional groups. If T is a finite simple exceptional group of Lie type, then apart from a few small exceptions, Weigel [39, Section 3] identifies an element $s \in T$ contained in a unique maximal subgroup, unless T is $F_4(2^f)$ or $G_2(3^f)$, when s has exactly two (isomorphic) maximal overgroups (see [11, Theorem 5.1] for a precise statement). The following example indicates what we can and cannot conclude for almost simple exceptional groups, highlighting that subfield subgroups are the principle obstacle.

Example 4.6. Let G be an almost simple group with socle $T = E_8(q)$. Then $G = \langle T, g \rangle$ where $g = \widetilde{\varphi}^i$ where i divides f. Let (X, σ^e, σ) be a Shintani setup for (T, g) with Shintani map $F \colon E_8(q)g \to E_8(q_0)$. Let $y \in T_0 = E_8(q_0)$ generate a maximal torus of order $q_0^8 + q_0^7 - q_0^5 - q_0^4 - q_0^3 + q_0 + 1$. Then Weigel proves in [39, Section 3(j)] that $N_{T_0}(\langle y \rangle) = \langle y \rangle.C_{30}$ is the unique maximal overgroup of y in T_0.

Let $t \in T$ satisfy $F(tg) = y$ and let $H \in \mathcal{M}(G, tg)$. According to Theorem 3.4, H has type (I)–(V). By [10, Proposition 5.1], H does not have type (IV), and since $|y|$ does not divide the order of the three possible subgroups of types (III) or (V), so $H \in \mathcal{M}_{(\text{I})} \cup \mathcal{M}_{(\text{II})}$, where the subgroups in $\mathcal{M}_{(\text{I})}$ and $\mathcal{M}_{(\text{II})}$ have type (I) and (II), respectively.

First assume that $H \in \mathcal{M}_{(\text{I})}$. Then H is G-conjugate to $(\langle Y, \widetilde{\sigma} \rangle^{s_1})_{\sigma^e}$ for a maximal closed σ-stable positive-dimensional subgroup Y of X and $s_1 \in X$ such that $[s_1^{-1}, \sigma^{-e}] \in Y$. Since $\langle y \rangle.C_{30}$ is the unique maximal overgroup of y, by Theorem 4, $|\mathcal{M}_{(\text{I})}| = 1$.

Therefore, $t\widetilde{\sigma}$ is contained in a unique maximal subgroup if and only if it is contained in no type (II) subgroups, that is, G-conjugates of $N_G(E_8(q^{1/k}))$ for some prime divisor k of f. Let us simply demonstrate that this may or may not be the case, by considering two different possibilities for e. On the one hand, if e is coprime to $|y|$, then since $y^{E_8} \cap E_8(q_0) = y^{E_8(q_0)}$, by Lemma 2.18(ii), $t\widetilde{\sigma}$ is contained in a subgroup of type $E_8(q^{1/k})$ for every prime divisor k of e, so $t\widetilde{\sigma}$ is not contained in a unique maximal subgroup. On the other hand, if $e = f$ is a prime divisor of $|y|$, then the only possibilities for H are subgroups of type $X_\sigma = E_8(p)$, and since $|y|$ does not properly divide the order of any element of $E_8(p)$, by Lemma 2.18(i), $t\widetilde{\sigma}$ is not contained in any such subgroup, so $|\mathcal{M}(G, t\widetilde{\sigma})| = 1$ and $\mu(G) = \mu^*(G) = 1$.

5 Asymptotics of spread and uniform spread

In this final section, we prove Theorem 1 on the asymptotic behaviour of the spread and uniform spread of almost simple groups (recall the definition of these invariants from the introduction).

5.1 Spread and subspace stabilisers

Let T be a finite simple classical group with natural module $V = \mathbb{F}_{q^u}^n$ where $q = p^f$ and where $u = 2$ if $T = \mathrm{PSU}_n(q)$ and $u = 1$ otherwise. Recall the definition of $\mathrm{Aut}^*(T) \leqslant \mathrm{Aut}(T)$ from Section 3.2, noting that $\mathrm{Aut}^*(T) = \mathrm{Aut}(T)$ unless T is $\mathrm{PSp}_4(2^f)$ or $\mathrm{P\Omega}_8^+(q)$. In this section, we highlight a connection between the spread of $T \leqslant G \leqslant \mathrm{Aut}^*(T)$ and the subspaces of V stabilised by elements of G. This is captured by Corollary 5.5.

It is clear what we mean by an element of $\mathrm{Inndiag}(T) \leqslant \mathrm{PGL}(V)$ stabilising a subspace of V, but we will require a more general definition for arbitrary elements of $\mathrm{Aut}^*(T)$.

Definition 5.1. Let $x \in \mathrm{Aut}^*(T)$.

(i) If $x \in \mathrm{P\Gamma L}(V)$, then x *stabilises* a k-space if it normalises the stabiliser of a k-space in T.

(ii) If $T = \mathrm{PSL}_n(q)$ and $x \in \mathrm{Aut}(T) \setminus \mathrm{P\Gamma L}(V)$, then x *stabilises* a k-space if it normalises a subgroup of T of type $P_{k,n-k}$ or $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$.

(iii) We say that x is *irreducible* on V if it stabilises no proper nonzero subspaces of V.

The following geometric observation will be useful.

Lemma 5.2. *Let U and V be two symplectic, orthogonal or unitary spaces. Assume that V is nondegenerate and write $U = U_1 \oplus U_2$ where U_1 is nondegenerate and $U_2 = U \cap U^\perp$. Then U is isometric to a subspace of V if and only if U_1 is isometric to a subspace V, say W_1, and $\dim U_2$ is at most the Witt index of $W_1^\perp$.*

Proof. If U_1 is isometric to a subspace V, say W_1, and $\dim U_2$ is at most the Witt index of $W_1^\perp$, then $W_1 \oplus W_2$ is isometric to U for any totally singular subspace W_2 of $W_1^\perp$ of dimension $\dim U_2$. Conversely, if $U = U_1 \oplus U_2$ is isometric to a subspace $W = W_1 \oplus W_2 \leqslant V$, where W_i is isometric to U_i, then $V = W_1 \oplus W_1^\perp$, since W_1 is nondegenerate, and W_2 is a totally singular subspace of $W_1^\perp$, since $W_2 = W \cap W^\perp$, so the Witt index of $W_1^\perp$ is at least $\dim W_2$. $\square$

A straightforward application of Lemma 5.2 gives this corollary.

Corollary 5.3. *Let U and V be two symplectic, orthogonal or unitary spaces. If V is a nondegenerate $2m$-space, of plus-type if orthogonal, and $\dim U \leqslant m$, then U is isometric to a subspace of V.*

Proposition 5.4. *Let $T \neq \mathrm{PSL}_n(q)$ be a simple classical group with natural module $V = \mathbb{F}_{q^u}^n$ and let $T \leqslant G \leqslant \mathrm{Aut}^*(T)$. Let $1 < d < n/2$. Then there exists a subset $S \subseteq T$ of size $|S| < q^{4ud}$ such that for all elements $y \in G$ that stabilise a k-space of V for some $1 \leqslant k < d$, there exists $x \in S$ such that $\langle x, y \rangle \neq G$.*

Proof. Write $V = U \perp U^\perp$ where $U = U_1 \perp U_2$ for a nondegenerate 2-space U_1 and a nondegenerate $(2d-2)$-space U_2. If T is orthogonal, then assume that U_1 is minus-type and U_2 is plus-type. Let $V_1, \ldots, V_s$ be the subspaces of U isometric to U_1, noting that $s < q^{4ud}$. For each $1 \leqslant i \leqslant s$, let x_i be a nontrivial element of T that centralises $V_i \perp V_i^\perp$, acting trivially on $V_i^\perp$ (for example, let $x_i = [\lambda, \lambda^{-1}] \perp I_{n-2}$ for $\lambda \in \mathbb{F}_{q^2}^\times$ of order $(q+1)/(2, q+1)$).

Let $y \in G$ be an element stabilising a k-space W of V for some $1 \leqslant k < d$. Write $W = \langle w_1, \ldots, w_k \rangle$ and $W_U = \langle u_1, \ldots, u_k \rangle$ where $w_i = u_i + v_i$ with $u_i \in U$ and $v_i \in U^\perp$. Now W_U is a subspace of U of dimension $l \leqslant k < d$. By Corollary 5.3, U_2 contains l-spaces of each isometry type. Therefore, U_1 is orthogonal to an l-space of U of each isometry type, so every l-space of U is orthogonal to a subspace of U isometric to U_1. In particular, we can fix $1 \leqslant i \leqslant s$ such that $W_U \subseteq V_i^\perp$. This implies that $W \subseteq W_U \oplus U^\perp \subseteq V_i^\perp$. Therefore, $\langle x_i, y \rangle$ stabilises W, so $\langle x_i, y \rangle \neq G$, as required. $\qquad \square$

Corollary 5.5. *Let T be a finite simple classical group with natural module $V = K^n$ and let $g \in \mathrm{Aut}^*(T)$. Assume that $T \neq \mathrm{PSL}_n(q)$. If every element of the coset Tg stabilises a k-space for some $1 \leqslant k < d < n/2$, then $s(\langle T, g \rangle) \leqslant |K|^{4d}$.*

5.2 Elements stabilising subspaces

In light of Corollary 5.5, in order to prove Theorem 1, we should study how classical groups act on their natural modules. Here our main result is Theorem 5.8, which may be of independent interest.

We begin with the following crucial observation.

Proposition 5.6. *Let X be a simple classical algebraic group, let $\sigma_1, \sigma_2 \in \mathrm{Aut}^*(X)$ be commuting Steinberg endomorphisms of X and let F be the Shintani map of (X, σ_1, σ_2). Then $x\widetilde{\sigma}_2 \in \langle X_{\sigma_1}, \widetilde{\sigma}_2 \rangle$ stabilises a k-space if and only if $F(x\widetilde{\sigma}_1) \in \langle X_{\sigma_2}, \widetilde{\sigma}_1 \rangle$ stabilises a k-space.*

Proof. This is an immediate consequence of Theorem 4 when Y is a $\langle \sigma_1, \sigma_2 \rangle$-stable stabiliser in X of a k-space (or if $X = \mathrm{PSL}_n$, perhaps a subgroup of type $P_{k,n-k}$ or $\mathrm{GL}_k \times \mathrm{GL}_{n-k}$). $\qquad \square$

Corollary 5.7. *Let $F \colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$ be the Shintani map of a standard classical pair (T, g). There exists $y \in Tx$ stabilising a k-space for all $x \in \mathrm{Inndiag}(T)g$ if and only if there exists $y_0 \in T_0 x_0$ stabilising a k-space for all $x_0 \in \mathrm{Inndiag}(T_0)g_0$.*

Proof. This is a combination of Corollary 3.3 and Proposition 5.6. $\qquad \square$

We can now state our main result on irreducible elements of almost simple groups.

Theorem 5.8. *Let T be a finite simple classical group and let $x \in \mathrm{Aut}^*(T)$.*

(i) *Every element of Tx is reducible on V if and only if $x \in \mathrm{Inndiag}(T)g$ for (T, g) in Table 5 or 6.*

(ii) *Assume that $x \in \mathrm{PO}_{2m}^\varepsilon(q)$ if $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$. Then every element of Tx stabilises a 1-space of V if and only if $x \in \mathrm{Inndiag}(T)g$ for (T, g) in Table 5.*

(iii) *If $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$ and $x \in \mathrm{PGO}_{2m}^\varepsilon(q) \setminus \mathrm{PO}_{2m}^\varepsilon(q)$, then every element of Tx stabilises a 1-space or 2-space of V if and only if $x \in \mathrm{Inndiag}(T)g$ for (T, g) in Table 5.*

Before proving Theorem 5.8, we record a consequence of [29, Lemmas 5.3.2–5.3.4 & 6.3.2].

Lemma 5.9. *There exist irreducible elements in*

(i) *every coset of $\mathrm{SL}_n(q)$ in $\mathrm{GL}_n(q)$*

(ii) *every coset of $\mathrm{SU}_{2m+1}(q)$ in $\mathrm{GU}_{2m+1}(q)$*

(iii) *every coset of $\mathrm{Sp}_{2m}(q)$ in $\mathrm{GSp}_{2m}(q)$*

(iv) *every coset of $\Omega_{2m}^-(q)$ in $\mathrm{DO}_{2m}^-(q)$.*

Table 5: The cosets in Theorem 5.8		
T	g	f/i
$\mathrm{PSL}_{2m+1}(q)$ or $\mathrm{P\Omega}^+_{2m}(q)$	$\gamma\widetilde{\varphi}^i$	odd
$\mathrm{PSU}_{2m+1}(q)$ or $\mathrm{P\Omega}^-_{2m}(q)$	$\widetilde{\varphi}^i$	any
$\Omega_{2m+1}(q)$	$\widetilde{\varphi}^i$	any

Table 6: The cosets in Theorem 5.8(i)		
T	g	f/i
$\mathrm{PSL}_{2m+1}(q)$	$\gamma\widetilde{\varphi}^i$	even
$\mathrm{PSU}_{2m+1}(q)$	$\gamma\widetilde{\varphi}^i$	odd
$\mathrm{P\Omega}^+_{2m}(q)$	$\widetilde{\varphi}^i$	any

Proof of Theorem 5.8. Let $x \in \mathrm{Aut}^*(T)$. By Theorem 3.1, we may assume that $x = hg$ where (T, g) is standard and $h \in \mathrm{Inndiag}(T)$. Let (X, σ_1, σ_2) be the Shintani setup for (T, g) with Shintani map $F\colon \mathrm{Inndiag}(T)g \to T_0 g_0$. We consider several cases, where we always assume that i divides f and $q_0 = p^i$.

Case 1. *(T, g) is one of the following:*

T	$\mathrm{PSL}_n(q)$	$\mathrm{PSL}_{2m+1}(q)$	$\mathrm{PSU}_{2m+1}(q)$	$\mathrm{PSp}_{2m}(q)$	$\mathrm{P\Omega}^+_{2m}(q)$	$\mathrm{P\Omega}^-_{2m}(q)$
g	$\widetilde{\varphi}^i$	$\gamma\varphi^i$	$\gamma\widetilde{\varphi}^i$	$\widetilde{\varphi}^i$	$\gamma\widetilde{\varphi}^i$	$\gamma\widetilde{\varphi}^i$
f/i	any	even	odd	any	even	odd

Consulting Table 1, we see that $T_0 \in \{\mathrm{PSL}_n(q_0), \mathrm{PSU}_{2m+1}(q_0), \mathrm{PSp}_{2m}(q_0), \mathrm{P\Omega}^-_{2m}(q_0)\}$ and $g_0 = 1$. Lemma 5.9 implies that every coset of T_0 in $\mathrm{Inndiag}(T_0)$ contains an irreducible element, so by Corollary 5.7, Tx contains an irreducible element for every $x \in \mathrm{Inndiag}(T)g$.

Case 2. *(T, g) is either $(\mathrm{PSL}_{2m}(q), \gamma\widetilde{\varphi}^i)$ for odd f/i or $(\mathrm{PSU}_{2m}(q), \widetilde{\varphi}^i)$.*

For $T = \mathrm{PSL}^\varepsilon_{2m}(q)$, we have $\mathrm{Inndiag}(T_0)g_0 = \mathrm{PGL}^{\varepsilon_0}_{2m}(q_0)\gamma$ with $\varepsilon_0 = -\varepsilon$. By Theorem 3.1, every element of $\mathrm{PGL}^{\varepsilon_0}_{2m}(q_0)\gamma$ is conjugate to an element of $\mathrm{PSL}^{\varepsilon_0}_{2m}(q_0)x_0$ where x_0 is γ or $\delta^\ell_0\gamma$ for $\ell = (n, q_0 - \varepsilon_0)/(n, q_0 - \varepsilon_0)_2$, where p is odd in the latter case. (Note that $\delta^\ell_0\gamma$ is an involution.) Therefore, by Corollary 5.7, it suffices to prove that $T_0 x_0$ contains an irreducible element for these two choices of x_0.

Case 2a. *$x_0 = \gamma$ or m is even or $q_0 \not\equiv 3 \pmod 4$.*

We consider only the case $\varepsilon_0 = +$, since the result for $\varepsilon_0 = -$ follows immediately from the result for $\varepsilon_0 = +$ and Proposition 5.6 via the Shintani map $\mathrm{PGL}_{2m}(q_0)\gamma \to \mathrm{PGU}_{2m}(q_0)\gamma$ of $(\mathrm{PSL}_{2m}(q_0), \gamma)$. If $x_0 = \gamma$, then $C_{\mathrm{PGL}_{2m}(q_0)}(\gamma) \cong \mathrm{PGSp}_{2m}(q_0)$, so we may fix an irreducible element $y \in C_{\mathrm{PGL}_{2m}(q_0)}(\gamma)$ of odd order, but this implies that $(y\gamma)^2 = y^2$ is also irreducible, so $y\gamma \in T_0\gamma$ is irreducible. If p is odd and $x_0 = \delta^\ell_0\gamma$, then $C_{\mathrm{PGL}_{2m}(q_0)}(\delta^\ell_0\gamma) \cong \mathrm{PGO}^-_{2m}(q_0)$ (the assumptions on m and q_0 give the sign), so again there exists $y \in C_{\mathrm{PGL}_{2m}(q_0)}(\delta^\ell_0\gamma)$ such that $y\delta^\ell_0\gamma \in T_0 x_0$ is irreducible.

Case 2b. *$x_0 = \delta^\ell_0\gamma$ and m is odd and $q_0 \equiv 3 \pmod 4$.*

Here we consider only $\varepsilon_0 = -$, since the result for $\varepsilon_0 = +$ will follow by Proposition 5.6. Now $C_{\mathrm{PGU}_{2m}(q_0)}(\delta^\ell_0\gamma) \cong \mathrm{PGO}^-_{2m}(q_0)$ and we fix an element $y \in C_{\mathrm{PGU}_{2m}(q_0)}(\delta^\ell_0\gamma)$ of odd order that acts irreducibly on $\mathbb{F}^{2m}_{q_0}$. Although $y^2 = (y\delta^\ell_0\gamma)^2$ acts irreducibly on $\mathbb{F}^{2m}_{q_0}$, we need to show that it acts irreducibly on $\mathbb{F}^{2m}_{q^2_0}$, the natural module for $\mathrm{PGU}_{2m}(q_0)$. Observe that $y\delta^\ell_0\gamma \in \mathrm{PGU}_{2m}(q_0)\gamma = \mathrm{PGU}_{2m}(q_0)\widetilde{\varphi}^i \subseteq \mathrm{PGL}_{2m}(q^2_0)\widetilde{\varphi}^i$. Let $E\colon \mathrm{PGL}_{2m}(q^2_0)\widetilde{\varphi}^i \to \mathrm{PGL}_{2m}(q_0)$ be the Shintani map of $(\mathrm{PGL}_{2m}, \varphi^{2i}, \varphi^i)$. Then $E(y\delta_2\gamma)$ is PGL_{2m}-conjugate to y^{-2} (see Lemma 2.20), which is irreducible on $\mathbb{F}^{2m}_{q_0}$, so by Proposition 5.6, $y\delta_2\gamma \in T_0 x$ is irreducible on $\mathbb{F}^{2m}_{q^2_0}$.

Case 3. (T, g) *is in Table 6.*

From Table 1, we see that $g_0 = 1$ and $\mathrm{Inndiag}(T_0) \in \{\mathrm{PSU}_{2m}(q), \mathrm{P\Omega}_{2m}^+(q)\}$. It is well known that in this case, $\mathrm{Inndiag}(T_0)$ does not contain any irreducible elements but every coset of T_0 in $\mathrm{Inndiag}(T_0)$ does contain an element that does not stabilise any 1-spaces (nor any 2-spaces if $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$, noting that $2m \geqslant 8$ in this case). Therefore, as in Case 1, applying Corollary 5.7, gives the same conclusion for Tx for every $x \in \mathrm{Inndiag}(T)$.

Case 4. (T, g) *is in Table 5.*

By Corollary 5.7, we need to prove that every element of $\mathrm{Inndiag}(T_0)g_0$ stabilises a 1-space, or if $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$ and $x \in \mathrm{PGO}_{2m}^\varepsilon(q) \setminus \mathrm{PO}_{2m}^\varepsilon(q)$, possibly a 2-space.

Case 4a. $(T, g) = (\Omega_{2m+1}(q), \widetilde{\varphi}^i)$.

In this case, $\mathrm{Inndiag}(T_0)g_0 = \mathrm{SO}_{2m+1}(q)$. Since y is conjugate to $y^{-\mathsf{T}}$, the eigenvalue multiset of y is closed under inversion and therefore must include an odd (and hence positive) number of roots of unity, which implies that y stabilises a 1-space.

Case 4b. (T, g) *is either* $(\mathrm{PSL}_{2m+1}(q), \gamma\widetilde{\varphi}^i)$ *for odd* f/i *or* $(\mathrm{PSU}_{2m+1}(q), \varphi^i)$.

Writing $T = \mathrm{PSL}_{2m+1}^\varepsilon(q)$, we have $\mathrm{Inndiag}(T_0)g_0 = \mathrm{PGL}_{2m+1}^{\varepsilon_0}(q_0)\gamma$ where $\varepsilon_0 = -\varepsilon$. Let $y \in \mathrm{PGL}_{2m+1}^{\varepsilon_0}(q_0)\gamma$. We claim that y fixes a 1-space. The Shintani map of $(\mathrm{PSL}_{2m+1}(q_0), \gamma)$ is $E \colon \mathrm{PGL}_{2m+1}(q_0)\gamma \to \mathrm{PGU}_{2m+1}(q_0)\gamma$, so by Proposition 5.6, it suffices to assume that $\varepsilon = +$. We can now apply the argument from the proofs of [9, Propositions 5.8 and 6.4]. By [20, Theorem 4.2], the eigenvalue multiset of y is closed under inversion, so, as in the previous case, y^2 stabilises a 1-space U of V. Let H be the stabiliser in $\mathrm{PGL}_{2m+1}(q_0)$ of U. Then y normalises $H \cap H^y$. Now H^y is the stabiliser W of a $(n-1)$-space of V. If $U \subseteq W$, then $H \cap H^y$ is a subgroup of type $P_{1,n-1}$; otherwise, $V = U \oplus W$, so $H \cap H^y$ has type $\mathrm{GL}_1(q_0) \times \mathrm{GL}_{n-1}(q_0)$. In either case, by definition, y stabilises a 1-space.

Case 4c. (T, g) *is either* $(\mathrm{P\Omega}_{2m}^+(q), \gamma\widetilde{\varphi}^i)$ *for odd* f/i *or* $(\mathrm{P\Omega}_{2m}^-(q), \gamma\varphi^i)$.

Writing $T = \mathrm{P\Omega}_{2m}^\varepsilon(q)$, we have $\mathrm{Inndiag}(T_0)g_0 = \mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)\gamma$. Let $y \in \mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)\gamma$. We claim that y fixes a 1-space. If $p = 2$, then

$$\mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)\gamma = \Omega_{2m}^{\varepsilon_0}(q_0)\gamma = \mathrm{O}_{2m}^{\varepsilon_0}(q_0) \setminus \Omega_{2m}^{\varepsilon_0}(q_0),$$

and [38, Theorem 11.43] implies that y has an odd-dimensional 1-eigenspace, so it certainly stabilises a 1-space. Now assume that p is odd. Recall that

$$\mathrm{PDO}_{2m}^{\varepsilon_0}(q_0)\gamma = \mathrm{PGO}_{2m}^{\varepsilon_0}(q_0) \setminus \mathrm{PDO}_{2m}^{\varepsilon_0}(q_0) = \{g \in \mathrm{PGO}_{2m}^{\varepsilon_0}(q_0) \mid \tau(g)^m = -\det(g)\}.$$

Write $\alpha = \tau(y)$. Since y is conjugate to $\alpha y^{-\mathsf{T}}$, the eigenvalue multiset Λ of y is closed under the map $\lambda \mapsto \alpha\lambda^{-1}$. Therefore, $\Lambda = \Lambda_1 \cup \Lambda_2$ where $\Lambda_1 = \{\lambda \in \Lambda \mid \lambda^2 = \alpha\}$ and $\Lambda_2 = \{\lambda_1, \alpha\lambda_1^{-1}, \ldots, \lambda_k, \alpha\lambda_k^{-1}\}$. Now $\det(y) = \prod_{\lambda \in \Lambda} \lambda = \alpha^k \prod_{\lambda \in \Lambda_1} \lambda$, which implies that Λ_1 is nonempty. If $y \in \mathrm{PO}_{2m}^{\varepsilon_0}(q_0)$, then $\alpha = 1$ and every eigenvalue in Λ_1 is 1 or -1, so y stabilises a 1-space. Now we may assume that $y \in \mathrm{PGO}_{2m}^{\varepsilon_0}(q_0) \setminus \mathrm{PO}_{2m}^{\varepsilon_0}(q_0)$. Since Λ_1 consists of square roots of α, y has an eigenvalue in $\mathbb{F}_{q_0^2}^\times \setminus \mathbb{F}_{q_0}^\times$, so y stabilises a 2-space.

The proof is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Remark 5.10. Theorem 5.8 implies that there are finite simple classical groups T such that $\mathrm{Inndiag}(T)$ contains no irreducible elements but $\mathrm{Aut}^*(T)$ does. For example, every element of $\mathrm{PGO}_{2m}^+(q)$ acts on $V = \mathbb{F}_q^{2m}$ reducibly, but, by Theorem 5.8, there exist irreducible elements in the coset $\mathrm{P\Omega}_{2m}^+(q)\gamma\widetilde{\varphi}^i$ if f/i is even.

Table 7: The exceptions in Theorem 1(iii)

T	g
$\mathrm{PSL}_{2m+1}(q)$ or $\mathrm{P\Omega}^+_{2m}(q)$	$\gamma\widetilde{\varphi}^i$ (f/i odd)
$\mathrm{PSU}_{2m+1}(q)$ or $\mathrm{P\Omega}^-_{2m}(q)$	$\widetilde{\varphi}^i$
$\mathrm{PSp}_{2m}(q)$ (q even) or $\Omega_{2m+1}(q)$	$\widetilde{\varphi}^i$

5.3 Asymptotics of spread and uniform spread

We now turn to the proof of Theorem 1. To this end, let us outline the probabilistic method for obtaining lower bounds on uniform spread, which was introduced by Guralnick and Kantor in [24] and has been a key tool in the subsequent work of many authors [4, 9, 10, 28, 29].

Let G be a finite group. We fix some notation. For $x, s \in G$, let $P(x, s)$ be the probability that x and a random conjugate of s do not generate G, that is,

$$P(x, s) = \frac{|\{t \in s^G \mid \langle x, t \rangle \neq G\}|}{|s^G|}.$$

For a subgroup $H \leqslant G$, the *fixed point ratio* of $x \in G$ in the action of G on G/H is

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

Recall that $\mathcal{M}(G, s)$ is the set of maximal subgroups of G that contain s. The following key lemma combines [9, Lemmas 2.1 and 2.2].

Lemma 5.11. *Let G be a finite group and let $s \in G$.*

(i) *If $P(z, s) < 1/k$ for all prime order elements $z \in G$, then $u(G) \geqslant k$, witnessed by s^G.*

(ii) *For all $z \in G$,*
$$P(z, s) \leqslant \sum_{H \in \mathcal{M}(G, s)} \mathrm{fpr}(z, G/H).$$

To apply Lemma 5.11 we need upper bounds on fixed point ratios for primitive actions of almost simple groups. There is an extensive literature on these, motivated in part by their use in probabilistic methods across group theory, and we will apply the main theorem of [5, 6, 7, 8] together with bounds in [24]. We are now ready to prove Theorem 1.

Proof of Theorem 1. Observe that for a prime power q, an almost simple group G appears in part (iii) if and only if $G = \langle T, x \rangle$ where $x \in \mathrm{Inndiag}(T)g$ for (T, g) in Table 7 (we ignore $T = \mathrm{PSp}_4(q)$ with a graph-field automorphism g as there are finitely many such groups).

Clearly (ii) implies (i). We now show that (i) implies (iii). Let G be a group appearing in part (iii), so we can write $G = \langle T, x \rangle$ with $x \in \mathrm{Inndiag}(T)$ and (T, g) in Table 7. Let $V = \mathbb{F}^n_{q^u}$ be the natural module for T. We claim that $s(G)$ is bounded above by a function of q. If $n \leqslant 7$, then $s(G) \leqslant |G| \leqslant q^{150}$, so we will assume that $n \geqslant 8$. For now assume that $T \neq \mathrm{PSp}_{2m}(q)$. By Theorem 5.8, every element of Tx stabilises a 1-space or a 2-space (the latter only occurring if $T = \mathrm{P\Omega}^\varepsilon_{2m}(q)$). Therefore, Corollary 5.5 implies that $s(G) \leqslant q^{16}$, unless $T = \mathrm{PSL}_{2m+1}(q)$, in which case the argument of Guralnick in the proofs of [9, Propositions 5.8 and 6.4] uses the fact that every element of Tx fixes a 1-space to show that $s(G) < (q + 1)^2$. If $T = \mathrm{PSp}_{2m}(q)$, then $s(G) \leqslant q$, by [28, Theorem 4] (the proof of which also relies on every element of G stabilising a 1-space of a particular module, see Remark 5.12 below). Therefore, if (G_i) has

Table 8: Decomposition for Case 1 in the proof of Theorem 1

T_0	decomposition of V_0
$\mathrm{PSL}_n(q_0)$	$k \oplus (n-k)$
$\mathrm{PSU}_n(q_0)$	$k^- \perp (n-k)^{-(-)^n}$
$\mathrm{PSp}_n(q_0)$	$k \perp (n-k)$
$\mathrm{P\Omega}_n^{\varepsilon_0}(q_0)$	$k^- \perp (n-k)^{-\varepsilon_0}$

an infinite subsequence of groups in (iii), then $s(G_i)$ does not diverge to infinity, which gives our desired implication.

It remains to show that (iii) implies (ii). Since $|G_i| \to \infty$, we know that $n_{i_k} \to \infty$, where $\mathbb{F}_{q^u}^{n_i}$ is the natural module for T_i. Fix i and write $G = G_i$ and $n = n_i$. It suffices to show that $u(G) \geqslant f(n)$ for some function f that satisfies $f(n) \to \infty$ as $n \to \infty$.

We may assume that $n > 20$. In particular, by Theorem 3.1, $G = \langle T, x \rangle$ with $x = hg$ where (T, g) is a standard classical pair not in Table 7 and $h \in \mathrm{Inndiag}(T)$. If $g = 1$, then $G \leqslant \mathrm{Inndiag}(T)$ and the result follows as in [24, Proposition 4.1] (compare with the proof of [9, Theorem 3.1]), so we assume that $g \neq 1$. In particular, g is $\widetilde{\varphi}^i$ or $\gamma \widetilde{\varphi}^i$ for a proper divisor i of f, unless $T = \mathrm{PSL}_{2m}^\varepsilon(q)$ and $g = \gamma$.

Case 1. (T, g) is neither $(\mathrm{PSL}_{2m}(q), \gamma \widetilde{\varphi}^i)$ for odd f/i nor $(\mathrm{PSU}_{2m}(q), \widetilde{\varphi}^i)$

Let (X, σ_1, σ_2) be the Shintani setup for (T, g) and let F be the Shintani map of (T, g), so we have $F \colon \mathrm{Inndiag}(T)g \to \mathrm{Inndiag}(T_0)g_0$. Consulting Table 1, we see that $g_0 = 1$ and $T_0 \notin \{\Omega_{2m+1}(q_0), \mathrm{PSp}_{2m}(q_0)\,(q_0 \text{ even})\}$ is a classical group with natural module $V_0 = \mathbb{F}_{q_0^{u_0}}^n$, where $u_0 = 2$ if $T_0 = \mathrm{PSU}_n(q_0)$ and $u_0 = 1$ otherwise.

Fix $1 \leqslant \sqrt{n}/4 < k < \sqrt{n}/2$. Moreover, assume that k is odd if $T_0 = \mathrm{PSL}_n^{\varepsilon_0}(q_0)$ and that k is even and $(n-k)/2$ is odd otherwise. By combining [29, Lemmas 5.3.2–5.36, 6.3.2 and 6.3.4], every coset of T_0 in $\mathrm{Inndiag}(T_0)$ contains an element y whose action on V_0 decomposes according to Table 8. (Here d (or d^-) refers to a nondegenerate (minus-type) d-subspace of V_0 on which y acts irreducibly, and d^+ refers to the direct sum of a dual pair of totally singular $\frac{d}{2}$-spaces which y stabilises, acting irreducibly and nonisomorphically on both $\frac{d}{2}$-spaces.) By Corollary 3.3, there is $t \in T$ such that the action of $F(tx) = y$ decomposes as in Table 8.

Write $\mathcal{M}(G, tg)$ as the disjoint union $\mathcal{M}_1 \cup \mathcal{M}_2$ where $\mathcal{M}_1$ is the set of reducible subgroups in $\mathcal{M}(G, tg)$, and write

$$a = \begin{cases} n & \text{if } T_0 \in \{\mathrm{PSL}_n(q_0), \mathrm{PSU}_n(q_0)\} \\ m & \text{if } T_0 \in \{\mathrm{PSp}_{2m}(q_0), \mathrm{P\Omega}_{2m}^{\varepsilon_0}(q_0)\}. \end{cases}$$

By Goursat's lemma (see [29, Lemma 2.3.1] for example), the proper nonzero subspaces of V_0 stabilised by y are a k-space, an $(n-k)$-space and if $T_0 \in \{\mathrm{PSU}_{2m+1}(q_0), \mathrm{P\Omega}_{2m}^-(q_0)\}$, also two $(n-k)/2$-spaces. Proposition 5.6 gives the analogous statement for tx on V. In particular, $|\mathcal{M}_1| \leqslant 4$ and tx stabilises no nonzero subspace of dimension less than $\sqrt{n}/4$.

Now let $H \in \mathcal{M}_2$. According to Theorem 3.6, H is of type (I)–(IV). Observe that the Shintani setup (X, σ_1, σ_2) for (T, g) satisfies $\sigma_1 = \sigma_2^e$ for some $e > 1$, so in light of Lemma 2.20, $(tx)^{-e}$ is X-conjugate to y. A power of y (and therefore also tx) has 1-eigenspace of codimension $k < \sqrt{n}/2$. Therefore, by [26, Theorem 7.1], H has type (I) with $Y \in \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_6$ (see Remark 3.5(i) and Table 3) or type (II). It is easy to check that this gives $10a + 7$ possible

Table 9: Subcases for Case 2 in the proof of Theorem 1

T	σ_1	x	σ_2	e	ρ	conditions
$\mathrm{PSL}_{2m}(q)$	φ^f	$\gamma\widetilde{\varphi}^i$	$\gamma\varphi^i$	odd	γ	
		$\delta_2\gamma\widetilde{\varphi}^i$	$\delta_2\gamma\varphi^i$	odd	$\delta_2\gamma$	p odd
$\mathrm{PSU}_{2m}(q)$	$\gamma\varphi^f$	$\widetilde{\varphi}^i$	φ^i	any	γ	
		$\delta_2\widetilde{\varphi}^i$	$\delta_2\varphi^i$	even	γ	p odd
				odd	$\delta_2\gamma$	p odd

G-classes of type (I) subgroups and at most $2 + \omega(f) \leqslant 3 + \log_2 f \leqslant 3 + \log_2 \log_2 q$ G-classes of subfield subgroup, where $\omega(f)$ is the number of distinct prime divisors of f (consult the tables in [32, Chapter 3] for example). Therefore, there are at most $10a + 10 + \log_2 \log_2 q$ choices for H up to G-conjugacy. Moreover, by Lemma 2.19, $\mathcal{M}_2$ contains at most $|C_{\mathrm{Inndiag}(T_0)}(y)|$ conjugates of any given $H \in \mathcal{M}_2$. Note that $|C_{\mathrm{Inndiag}(T_0)}(y)| \leqslant 4q_0^a$.

Let $z \in G$ have prime order. From the bounds in [24, Section 3], if $H \leqslant G$ is the stabiliser of a d-space of V, with $d < n/3$, then $\mathrm{fpr}(z, G/H) < 5q^{-d}$. By combining [9, Corollary 2.9], [28, Proposition 3.2] and [29, Propositions 4.2.2 and 4.2.3], which apply the main result of [5], if $H \leqslant G$ is irreducible, then $\mathrm{fpr}(z, G/H) < 2q^{-(a-3)}$. Therefore, by Lemma 5.11(ii), noting that $q_0 \leqslant q^{1/2}$, we obtain

$$
\begin{aligned}
P(z, tx) &< \sum_{H \in \mathcal{M}_1} \mathrm{fpr}(z, G/H) + \sum_{H \in \mathcal{M}_2} \mathrm{fpr}(z, G/H) \\
&< 4 \cdot 5q^{-\sqrt{n}/4} + (10a + 10 + \log_2 \log_2 q) \cdot 4q_0^a \cdot 2q^{-(a-3)} \\
&< 100n \cdot q^{-(n/4-5)}.
\end{aligned}
$$

Lemma 5.11(i) gives $u(G) \geqslant \frac{1}{100n} \cdot q^{n/4-5}$, and $\frac{1}{100n} \cdot q^{n/4-5} \to \infty$ as $n \to \infty$, as required.

Case 2. (T, g) *is either* $(\mathrm{PSL}_{2m}(q), \gamma\widetilde{\varphi}^i)$ *for odd* f/i *or* $(\mathrm{PSU}_{2m}(q), \widetilde{\varphi}^i)$

Let $X = \mathrm{PSL}_{2m}$. By Theorem 3.1, it is sufficient to consider the five cases we define in Table 9 (here $\delta_2 = \delta^\ell$ where $\ell = (n, q - \varepsilon)/(n, q - \varepsilon)_2$). In each case, fix the Steinberg endomorphisms σ_1 and σ_2 and the graph automorphism ρ. Notice that $(X_{\sigma_1}, \widetilde{\sigma}_2) = (\mathrm{Inndiag}(T), x)$ and $\sigma_2^e = \rho\sigma_1$, so $\widetilde{\sigma}_2^e = \widetilde{\sigma}_1 = \rho$. Let $F \colon \mathrm{Inndiag}(T)x \to X_{\sigma_2}\rho$ be the Shintani map of (X, σ_1, σ_2).

Let $Y = C_X(\rho)^\circ$. By [29, Propositions 6.4.7 and 6.6.2], ρ is an involution and commutes with σ_2. Moreover, if $\rho = \gamma$, then $Y_{\sigma_2} \cong \mathrm{PGSp}_{2m}(q_0)$, and if $\rho = \delta_2\gamma$, then $Y_{\sigma_1} \cong \mathrm{PDO}_{2m}^\eta(q_0)$ where $\eta = (-)^{\frac{1}{2}m(q-1)+1}$.

Fix an even integer $1 \leqslant \sqrt{n}/4 < k < \sqrt{n}/2$ such that $(n-k)/2$ is odd. Using the notation for decompositions from Case 1, if $\rho = \gamma$, then fix an odd order element $y \in \mathrm{PSp}_{2m}(q_0) \leqslant Y_{\sigma_2}$ such that the action of y on $\mathbb{F}_{q_0}^{2m}$ decomposes as $k \perp (n-k)$, and if $\rho = \delta_2\gamma$, then fix an odd order element $y \in \mathrm{PSO}_{2m}^\eta(q_0) \leqslant Y_{\sigma_2}$ acting on $\mathbb{F}_{q_0}^{2m}$ as $k^- \perp (n-k)^{-\eta}$.

Let E be the Shintani map of (Y, σ_1, σ_2). Fix $t \in Y_{\sigma_1} \leqslant \mathrm{Inndiag}(T)$ such that $E(t\sigma_2) = y\sigma_1$, so $F(tx) = y\rho$. Since $(\sigma_2|_Y)^e = (\rho\sigma_1)|_Y = \sigma_1|_Y$, by Lemma 2.20, $E(t\sigma_2|_{Y_{\sigma_1}})$ is Y-conjugate to $(t\sigma_2|_{Y_{\sigma_1}})^{-e}$, which implies that $F(tx)$ is Y-conjugate to $(tx)^{-e}$. By applying Theorem 3.2 to E, if $\rho = \gamma$, then $t \in \mathrm{PSp}_{2m}(q)$ since $y \in \mathrm{PSp}_{2m}(q_0)$, and if $\rho = \delta_2\gamma$, then $t \in \mathrm{PSO}_{2m}^\pm(q)$ since $y \in \mathrm{PSO}_{2m}^\eta(q_0)$. In particular, in both cases, $tx \in Tx$.

We now proceed as in Case 1 and write $\mathcal{M}(G, tg)$ as the disjoint union $\mathcal{M}_1 \cup \mathcal{M}_2$ where $\mathcal{M}_1$ is the set of reducible subgroups in $\mathcal{M}(G, tg)$.

We claim that the only possible proper nonzero subspaces of the natural module V_0 of X_{σ_2} stabilised by $y\rho$ are a k-space, an $(n-k)$-space and two $(n-k)/2$-spaces. First assume that $T = \mathrm{PSU}_{2m}(q)$. Then $y \in X_{\rho\gamma\varphi^i} \cong \mathrm{PGL}_{2m}(q_0)$ and $(y\rho)^2 = y^2$ decomposes $\mathbb{F}_{q_0}^{2m}$ as $k \perp (n-k)$ or $k^- \perp (n-k)^{-\eta}$, so the claim is clear in this case. Now assume that $T = \mathrm{PSL}_{2m}(q)$. Here $y \in X_{\rho\varphi^i} \cong \mathrm{PGU}_{2m}(q_0) \leqslant \mathrm{PGL}_{2m}(q_0^2)$ and we need to consider the action on the natural module $\mathbb{F}_{q_0^2}^{2m}$ for $\mathrm{PGU}_{2m}(q_0)$. We proceed as in Case 2b of the proof of Theorem 5.8. Note that $y\rho \in X_{\rho\varphi^i}\gamma = X_{\rho\varphi^i}\widetilde{\varphi}^i \subseteq X_{\varphi^{2i}}\widetilde{\varphi}^i$ and let $D\colon X_{\widetilde{\varphi}^{2i}}\widetilde{\varphi}^i \to X_{\widetilde{\varphi}^i}$ be the Shintani map of $(X, \varphi^i, \varphi^{2i})$. Then $D(y\rho)$ is X-conjugate to y^{-2}, so the claim follows from the previous case by Proposition 5.6 applied to D.

Therefore, by Proposition 5.6, $|\mathcal{M}_1| \leqslant 4$ and every nonzero subspace of V stabilised by tx has dimension at least $\sqrt{n}/4$. Since $(tx)^{-2e}$ is similar to y^2, a power of tx has a 1-eigenspace of dimension $n - k > \sqrt{n}/2$, so [26, Theorem 7.1] implies that there are at most $10n + 10 + \log_2\log_2 q$ choices for $H \in \mathcal{M}_2$ up to G-conjugacy, and by Lemma 2.19, $\mathcal{M}_2$ contains at most $|C_{X_{\sigma_2}}(y\rho)|$ conjugates of any given $H \in \mathcal{M}_2$. Since y has odd order, ρ is an involution and $y \in C_X(\rho)$, we deduce that $|C_{X_{\sigma_2}}(y\rho)| \leqslant |C_{Y_{\sigma_2}}(y)| \leqslant 4q_0^{n/2}$. Therefore, as in Case 1, if $z \in G$ has prime order, then $P(z, tx) < 100n \cdot q^{-(n/4-5)}$ and $u(G) \geqslant \frac{1}{100n} \cdot q^{n/4-5}$. This completes the proof. $\qquad\square$

Remark 5.12. Let q be even. As Lemma 5.9 records, $\mathrm{Sp}_{2m}(q)$ has elements that act irreducibly on $\mathbb{F}_q^{2m}$. However, identifying $\mathrm{Sp}_{2m}(q)$ with $\mathrm{O}_{2m+1}(q)$ gives a natural action of $\mathrm{Sp}_{2m}(q)$ on $\mathbb{F}_q^{2m+1}$ and from this perspective the subgroups of $\mathrm{Sp}_{2m}(q)$ of type $\mathrm{O}_{2m}^+(q)$ and $\mathrm{O}_{2m}^-(q)$ are the stabilisers of particular types of 1-spaces. Therefore, Proposition 2.11 establishes that every element of $\mathrm{P}\Gamma\mathrm{Sp}_{2m}(q)$ stabilises a 1-space of $\mathbb{F}_q^{2m+1}$. In this light, by Theorem 5.8, we see that all of the exceptions in Theorem 1 arise from the fact that every element of Tg stabilises a 1-space (or, in one special case, a 2-space).

References

[1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[2] 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.

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

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

[5] T. C. Burness, *Fixed point ratios in actions of finite classical groups, I*, J. Algebra **309** (2007), 69–79.

[6] T. C. Burness, *Fixed point ratios in actions of finite classical groups, II*, J. Algebra **309** (2007), 80–138.

[7] T. C. Burness, *Fixed point ratios in actions of finite classical groups, III*, J. Algebra **314** (2007), 693–748.

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

[9] T. C. Burness and S. Guest, *On the uniform spread of almost simple linear groups*, Nagoya Math. J. **209** (2013), 35–109.

[10] T. C. Burness, R. M. Guralnick and S. Harper, *The spread of a finite group*, Ann. of Math. **193** (2021), 619–687.

[11] T. C. Burness and S. Harper, *On the uniform domination number of a finite simple group*, Trans. Amer. Math. Soc., **372** (2019), 545–583.

[12] T. C. Burness and S. Harper, *Computations concerning the uniform domination number of a finite simple group* at `http://seis.bristol.ac.uk/~tb13602/udncomp.pdf`.

[13] M. Cabanes and B. Späth, *Descent equalities and the inductive McKay condition for types B and E*, Adv. Math. **356** (2019), 106820.

[14] 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.

[15] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[16] T. Deshpande, *Shintani descent for algebraic groups and almost simple characters of unipotent groups*, Compos. Math. **152** (2016), 1697–1724.

[17] F. Digne and J. Michel, *Groupes réductifs non connexes*, Ann. Sci. École Norm. Sup. (4) **27** (1994), 345–406.

[18] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[19] R. H. Dye, *Interrelations of symplectic and orthogonal groups in characteristic two*, J. Algebra **59** (1979), 202–221.

[20] J. Fulman and R. M. Guralnick, *Conjugacy class properties of the extension of $GL(n,q)$ generated by the inverse transpose involution*, J. Algebra **275** (2004), 356–396.

[21] J. Fulman and R. M. Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), 3023–3070.

[22] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, vol. 40, Amer. Math. Soc., 1998.

[23] 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.

[24] R. M. Guralnick and W. M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[25] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. Lond. Math. Soc. **78** (1997), 167–214.

[26] R. M. Guralnick and J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.

[27] R. M. Guralnick and A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.

[28] S. Harper, *On the uniform spread of almost simple symplectic and orthogonal groups*, J. Algebra **490** (2017), 330–371.

[29] S. Harper, *The spread of almost simple classical groups*, Lecture Notes in Mathematics, vol. 2286, Springer, to appear.

[30] G. A. Jones, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory **5** (2002), 403–407.

[31] N. Kawanaka, *On the irreducible characters of the finite unitary groups*, J. Math. Soc. Japan **29** (1977), 425–450.

[32] 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.

[33] 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.

[34] M. W. Liebeck and G. M. Seitz, *Maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Geom. Dedicata **35** (1990), 353–387.

[35] M. W. Liebeck and G. M. Seitz, *On the subgroup structure of classical groups*, Invent. Math. **134** (1998), 427–453.

[36] M. W. Liebeck and A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.

[37] T. Shintani, *Two remarks on irreducible characters of finite general linear groups*, J. Math. Soc. Japan **28** (1976), 396–414.

[38] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Helderman Verlag, 1992.

[39] T. S. Weigel, *Generation of exceptional groups of Lie-type*, Geom. Dedicata **41** (1992), 63–87.

[40] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964.

Scott Harper

School of Mathematics, University of Bristol, BS8 1UG, UK

Heilbronn Institute for Mathematical Research, Bristol, UK

scott.harper@bristol.ac.uk