Harper, S. (2017). On the uniform spread of almost simple symplectic and orthogonal groups. *Journal of Algebra*, *490*, 330-371. https://doi.org/10.1016/j.jalgebra.2017.07.008

ON THE UNIFORM SPREAD OF ALMOST SIMPLE SYMPLECTIC AND ORTHOGONAL GROUPS

SCOTT HARPER

ABSTRACT. A group is $\frac{3}{2}$-generated if every non-identity element is contained in a generating pair. A conjecture of Breuer, Guralnick and Kantor from 2008 asserts that a finite group is $\frac{3}{2}$-generated if and only if every proper quotient of the group is cyclic, and recent work of Guralnick reduces this conjecture to almost simple groups. In this paper, we prove a stronger form of the conjecture for almost simple symplectic and odd-dimensional orthogonal groups. More generally, we study the uniform spread of these groups, obtaining lower bounds and related asymptotics. This builds on earlier work of Burness and Guest, who established the conjecture for almost simple linear groups.

1. INTRODUCTION

Let G be a finite group. We say that G is *d-generated* if G has a generating set of size d. It is well-known that every finite simple group is 2-generated [39, 2]. In fact, almost surely, any two elements of a finite simple group G generate the group, in the sense that the probability that two randomly chosen elements form a generating pair tends to one as $|G|$ tends to infinity [31, 35]. Therefore, generating pairs are abundant in finite simple groups, and it is natural to ask how they are distributed across the group. With this in mind, we say that G is *$\frac{3}{2}$-generated* if every non-identity element of G is contained in a generating pair. By a theorem of Guralnick and Kantor [27] (also see Stein [38]), every finite simple group is $\frac{3}{2}$-generated, resolving a question of Steinberg [39] in the affirmative.

It is straightforward to see that every proper quotient of a $\frac{3}{2}$-generated group is cyclic. In [9], Breuer, Guralnick and Kantor make the following remarkable conjecture.

Conjecture. *A finite group is $\frac{3}{2}$-generated if and only if every proper quotient is cyclic.*

This conjecture has recently been reduced by Guralnick [26] to almost simple groups G. By the main theorem of [21], these groups are 3-generated and, in fact, 2-generated if $G/\mathrm{soc}(G)$ is cyclic, where $\mathrm{soc}(G)$ denotes the (simple) socle of G. In the case where $\mathrm{soc}(G)$ is alternating the conjecture was established in [6], and the sporadic groups are handled in [9] using computational methods. Therefore, it remains to consider the almost simple groups of Lie type. In [17], Burness and Guest establish a stronger version of the conjecture for almost simple linear groups. The aim of this paper is to extend this result to almost simple symplectic and odd-dimensional orthogonal groups. We will handle the remaining groups of Lie type in a forthcoming paper.

Following Brenner and Wiegold [7], a finite group G has *spread k* if for any k non-identity elements $x_1, \ldots, x_k \in G$ there exists $g \in G$ such that, for all i, $\langle x_i, g\rangle = G$. Moreover, G is said to have *uniform spread k* if the element g can be chosen from a fixed conjugacy class of G. We write $s(G)$ (respectively $u(G)$) for the greatest k such that G has spread k (respectively uniform spread k). (If G is cyclic, then write $s(G) = u(G) = \infty$.)

Date: July 7, 2017.

2010 *Mathematics Subject Classification.* Primary 20D06; Secondary 20E28, 20F05, 20P05.

Key words and phrases. Classical groups; Maximal subgroups; Uniform spread.

In [9], using probabilistic methods, it was proved that $u(G) \geq 2$ for all finite simple groups G, with equality if and only if

$$G \in \{A_5, A_6, \Omega_8^+(2)\} \cup \{\mathrm{Sp}_{2m}(2) \mid m \geq 3\}.$$

This was extended by Burness and Guest in [17], where they prove that $u(G) \geq 2$ for $G = \langle \mathrm{PSL}_n(q), g\rangle$ with $g \in \mathrm{Aut}(\mathrm{PSL}_n(q))$ unless $G = \mathrm{PSL}_2(9).2 \cong S_6$, for which $u(G) = 0$ and $s(G) = 2$. In particular, this demonstrates that $\langle \mathrm{PSL}_n(q), g\rangle$ is $\frac{3}{2}$-generated.

Let us now introduce the groups which will be the focus of this paper. Write

$$\mathcal{T} = \{\mathrm{PSp}_{2m}(q)' \mid m \geq 2\} \cup \{\Omega_{2m+1}(q) \mid q \text{ odd}, m \geq 3\} \tag{1.1}$$

$$\mathcal{A} = \{\langle T, \theta\rangle \mid T \in \mathcal{T}, \theta \in \mathrm{Aut}(T)\} \tag{1.2}$$

The restrictions on m in the definition of $\mathcal{T}$ account for the familiar low-rank isomorphisms $\mathrm{PSp}_2(q) \cong \Omega_3(q) \cong \mathrm{PSL}_2(q)$ and $\Omega_5(q) \cong \mathrm{PSp}_4(q)$ (see [32, Prop. 2.9.1]).

We can now present the main result of the paper.

Theorem 1. *Let $G \in \mathcal{A}$. Then $u(G) \geq 2$ unless $G = \mathrm{PSp}_4(2)'.2 \cong S_6$, in which case $u(G) = 0$ and $s(G) = 2$.*

As an immediate consequence of Theorem 1, all groups in $\mathcal{A}$ are $\frac{3}{2}$-generated. Therefore, this establishes the main conjecture for all almost simple groups whose socle is a symplectic group or odd-dimensional orthogonal group.

Remark 1. In the definition of $\mathcal{T}$, we take the derived subgroup of $\mathrm{PSp}_{2m}(q)$ since $\mathrm{PSp}_4(2) \cong S_6$ is not perfect. Accordingly, $A_6 \in \mathcal{T}$ and $\mathcal{A}$ includes A_6 together with the three cyclic extensions: S_6, $\mathrm{PGL}_2(9)$ and M_{10}. It is well-known that $u(A_6) = 2$ and $u(S_6) = 0$ but $s(S_6) = 2$. Moreover, using Magma [4], we can show that $u(\mathrm{PGL}_2(9)) = 5$ and $u(M_{10}) \geq 8$. (See Section 2.3 for a brief discussion of our computational methods.)

If we exclude some cases, we can strengthen the lower bound in Theorem 1.

Theorem 2. *Let $G \in \mathcal{A}$. Assume that q is odd and $m \geq 3$. If $\mathrm{soc}(G) = \Omega_{2m+1}(q)$ then $u(G) \geq 3$, and if $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ then $u(G) \geq 4$.*

By [30, Theorem 1.1], if (G_i) is a sequence of finite simple groups of Lie type such that $|G_i| \to \infty$, then $s(G_i) \to \infty$ if and only if (G_i) does not have a subsequence of symplectic groups in even characteristic or odd-dimensional orthogonal groups, over a field of fixed size. We wish to establish similar results for sequences (G_i) of almost simple groups of Lie type for which $G_i/\mathrm{soc}(G_i)$ is cyclic. (See [17, Theorem 4] for an asymptotic result for almost simple linear groups.) To this end, we prove the following result.

Theorem 3. *Let (G_i) be a sequence of groups in $\mathcal{A}$ with $|G_i| \to \infty$. Then $u(G_i) \to \infty$ if and only if there is no subsequence (G_{i_k}) of groups over a field of fixed size such that either*

(i) $\mathrm{soc}(G_{i_k})$ *are symplectic groups in even characteristic; or*
(ii) $\mathrm{soc}(G_{i_k})$ *are odd-dimensional orthogonal groups.*

We can find explicit bounds for the groups in Theorem 3 with bounded uniform spread.

Theorem 4. *Let $G \in \mathcal{A}$. If q is even, $\mathrm{soc}(G) = \mathrm{PSp}_{2m}(q)$ and θ is not a graph-field automorphism, then $s(G) \leq q$. If $\mathrm{soc}(G) = \Omega_{2m+1}(q)$, then $s(G) < \frac{q^2+q}{2}$.*

Remark 2. Let q be even. Write $G = \langle T, \theta\rangle$ where $T = \mathrm{PSp}_4(q)'$ and $\theta \in \mathrm{Aut}(T)$.

(i) If $q = 4$ and θ is an involutory field automorphism, then it can be shown computationally that $u(G) = 4$ (see Table 4). Therefore, the bound for symplectic groups in Theorem 4 is sharp.

(ii) By [30, Prop. 2.5], $s(T) \leq q$. Theorem 4 extends this result by establishing that if θ is a field automorphism then $s(G) \leq q$. However, this upper bound does *not* apply when θ is a graph-field automorphism. Indeed, in this case, if $q = 4$ then $u(G) \geq 10$, and, strikingly, if $q = 8$ and θ has order two then $u(G) \geq 76$. This behaviour is captured by Proposition 4.22(iii), which establishes that if θ is an involutory graph-field automorphism then $u(G) \geq q^2/C$ for a constant C. (The proof of Proposition 4.22(iii) shows that we may choose $C = 18$.) In particular, this gives infinitely many examples where $u(G) > u(\mathrm{soc}(G))$.

Remark 3. Let q be even. Write $G = \langle T, \theta \rangle$ where $T = \mathrm{PSp}_{2m}(q)$ and $\theta \in \mathrm{Aut}(T)$. By Proposition 4.20(iv), if $m \geq 16$, then $q - 1 \leq u(G) \leq s(G) \leq q$, so the upper bound for symplectic groups in Theorem 4 is certainly close to best possible in large rank.

Remark 4. The above results can be recast combinatorially by way of the *generating graph*. For a finite group G, let $\Gamma(G)$ be the graph whose vertices are the non-identity elements of G and in which two vertices g and h are adjacent if and only if $\langle g, h \rangle = G$. This graph encodes many interesting generation properties of the group. For example, $\Gamma(G)$ has no isolated vertices if and only if G is $\frac{3}{2}$-generated. Further, if $s(G) \geq 2$, then $\Gamma(G)$ is connected with diameter at most 2. Therefore, by [9, Theorem 1.2], the diameter of the generating graph of any non-abelian finite simple group is two. Moreover, Theorem 1 shows that the same conclusion holds for the groups in $\mathcal{A}$.

Many other natural questions about generating graphs have been investigated in recent years. For example, in [10, Theorem 1.2], it is shown that for all sufficiently large simple groups G, the graph $\Gamma(G)$ has a Hamiltonian cycle. Indeed, it is conjectured that for all finite groups G of order at least four, the generating graph $\Gamma(G)$ has a Hamiltonian cycle if and only if every proper quotient of G is cyclic. This is a significant strengthening of the aforementioned conjecture of Breuer, Guralnick and Kantor, which asserts that the generating graph $\Gamma(G)$ has no isolated vertices if and only if every proper quotient of G is cyclic. This stronger conjecture has been verified for soluble groups [10, Prop. 1.1].

In the remainder of this introductory section, we will briefly discuss the main tools used in the proofs of Theorems 1–4. As in [17], the main ingredient is the probabilistic method used by Guralnick and Kantor in [27]. Fix $G = \langle T, \theta \rangle \in \mathcal{A}$ and $s \in G$. Write $\mathcal{M}(G, s)$ for the set of maximal subgroups of G which contain s. For $x \in G$, let $P(x, s)$ be the probability that x and a random conjugate of s do not generate G; that is,

$$P(x, s) = 1 - \frac{|\{z \in s^G \mid G = \langle x, z \rangle\}|}{|s^G|}.$$

By [17, Lemma 2.1], G has uniform spread k if for all k-tuples $(x_1, \ldots, x_k)$ of prime order elements in G,

$$\sum_{i=1}^{k} P(x_i, s) < 1.$$

To estimate $P(x, s)$ we use fixed point ratios. For a G-set Ω, let $\mathrm{fix}(x, \Omega)$ be the number of fixed points of x on Ω and let $\mathrm{fpr}(x, \Omega) = \mathrm{fix}(x, \Omega)/|\Omega|$ be the corresponding *fixed point ratio*. For $x \in G$, by [17, Lemma 2.2],

$$P(x, s) \leq \sum_{H \in \mathcal{M}(G,s)} \mathrm{fpr}(x, G/H). \tag{1.3}$$

Therefore, our probabilistic method has three steps: select an appropriate element $s \in G$, determine $\mathcal{M}(G, s)$ and use fixed point ratio estimates to bound $P(x, s)$ for each $x \in G$ of prime order. In the case where θ is a field automorphism, we will use the theory of *Shintani descent* to choose s and control its maximal overgroups (see Section 2.2).

$\mathcal{C}_1$	stabilisers of subspaces, or pairs of subspaces, of V
$\mathcal{C}_2$	stabilisers of decompositions $V = \bigoplus_{i=1}^t V_i$ where $\dim V_i = a$
$\mathcal{C}_3$	stabilisers of prime degree field extensions of $\mathbb{F}_q$
$\mathcal{C}_4$	stabilisers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathcal{C}_5$	stabilisers of prime index subfields of $\mathbb{F}_q$
$\mathcal{C}_6$	normalisers of symplectic-type r-groups in absolutely irreducible representations
$\mathcal{C}_7$	stabilisers of decompositions $V = \bigotimes_{i=1}^t V_i$ where $\dim V_i = a$
$\mathcal{C}_8$	stabilisers of non-degenerate forms on V

TABLE 1. The collections of geometric subgroups

Our framework for understanding $\mathcal{M}(G, s)$ is provided by Aschbacher's subgroup structure theorem for finite classical groups [1]. Roughly, this theorem states that if G is an almost simple classical group, then any maximal subgroup of G not containing $\mathrm{soc}(G)$ belongs to one of eight collections $\mathcal{C}_1, \ldots, \mathcal{C}_8$ of so-called geometric subgroups, or it is contained in $\mathcal{S}$, a collection of absolutely irreducible almost simple subgroups. The geometric subgroups preserve certain geometric structures on the natural module (see Table 1), and we refer the reader to [32] for further details regarding these subgroups. A complete description of the maximal subgroups of classical groups of dimension at most 12 is given in [5]. For a maximal subgroup H of G, the *type* of H is a rough indication of the structure of H. In addition to determining the types of subgroups in $\mathcal{M}(G, s)$, we need to calculate the multiplicity with which each type occurs.

Finally, in view of (1.3), we use fixed point ratio estimates to bound $P(x, s)$. There is a vast literature on fixed point ratios for primitive actions of almost simple groups. If G is a finite almost simple classical group, then the *subspace subgroups* of G are roughly the maximal subgroups which act reducibly on the natural module for G; that is, they are roughly the $\mathcal{C}_1$ subgroups. (For the precise definition see [11, Definition 1].) In [11, 12, 13, 14], Burness establishes close to best possible upper bounds on $\mathrm{fpr}(x, G/H)$ when G is an almost simple classical group, H is a maximal non-subspace subgroup and $x \in G$ has prime order. In particular, if n is the dimension of the natural module for G, then

$$\mathrm{fpr}(x, G/H) \leq |x^G|^{-\frac{1}{2}+o(1)},$$

where $o(1) \to 0$ as $n \to \infty$. An explicit exponent is given in [11, Theorem 1]. For subspace subgroups we will use the bounds of Guralnick and Kantor in [27, §3], together with some new bounds we establish in Section 3.

For some low-dimensional groups over small fields, our probabilistic approach is complemented by computational methods implemented in MAGMA [4]. We refer the reader to Section 2.3 for the details.

Acknowledgements. The author would like to thank his PhD supervisor Dr Tim Burness for bringing this problem to his attention, and he acknowledges the financial support of EPSRC and the Heilbronn Institute for Mathematical Research. He also thanks Prof Robert Guralnick for helpful advice.

2. PRELIMINARIES

In this section, we record preliminary results and fix notation.

2.1. **Symplectic and orthogonal groups.** Let us begin by discussing the almost simple groups which will be the focus of this paper. Let $q = p^f$ where p is prime and let $V = \mathbb{F}_q^n$. For finite classical groups we will use the notation and terminology adopted by Kleidman and Liebeck in [32] and Burness and Giudici in [16].

Case	T	n	Forms on $V = \mathbb{F}_q^n$	Conditions on q
S	$\mathrm{PSp}_{2m}(q)$	$2m \geq 6$	symplectic form $(\ ,\ )$	none
$\mathbf{S_4}$	$\mathrm{PSp}_4(q)$	4	symplectic form $(\ ,\ )$	$q > 2$
O	$\Omega_{2m+1}(q)$	$2m+1 \geq 7$	non-degenerate quadratic form Q with symmetric form $(\ ,\ )$	q odd

TABLE 2. The three cases for groups in $\mathcal{A}$

Let $(\ ,\ )$ be a bilinear form on V. The corresponding similarity group $\Delta(V)$ is the subgroup of $\mathrm{GL}(V)$ containing the elements g for which there exists $\tau(g) \in \mathbb{F}_q$ such that $(ug, vg) = \tau(g)(u, v)$ for all $u, v \in V$. We refer to $\tau\colon \Delta(V) \to \mathbb{F}_q^\times$ as the *similarity map*.

Write $\mathrm{Sp}(V), \mathrm{GSp}(V), \Gamma\mathrm{Sp}(V)$ for the groups of isometries, similarities and semisimilarities of V with respect to a symplectic (i.e. non-degenerate alternating) form, and respectively $\mathrm{O}(V), \mathrm{GO}(V), \Gamma\mathrm{O}(V)$ for an odd-dimensional space V with a non-degenerate symmetric form (over a field of odd characteristic). Let $\mathrm{SO}(V)$ be the index two subgroup of $\mathrm{O}(V)$ of maps with determinant one. The kernel of the spinor norm $\eta\colon \mathrm{SO}(V) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ (see [32, pp. 29–30]) is the unique index two subgroup $\Omega(V)$ of $\mathrm{SO}(V)$.

The sets $\mathcal{T}$ and $\mathcal{A}$ were introduced in (1.1) and (1.2). In Table 2, we partition $\mathcal{A}$ into three subsets. (We omit groups with socle $\mathrm{PSp}_4(2)' \cong A_6$; see Remark 1.) In each case, we define a formed space $V = \mathbb{F}_q^n$, which is the natural module for T.

Let $T \in \mathcal{T}$. We will now determine the possible groups $\langle T, \theta\rangle$ where $\theta \in \mathrm{Aut}(T)$. To do this, it suffices to consider, for the choice of θ, the representatives of the outer automorphisms of T. By [40, Theorem 30], $\mathrm{Out}(T)$ is generated by *diagonal*, *field*, *graph* and *graph-field automorphisms*. (We adopt the terminology of [25, Definition 2.5.13].) The structure of $\mathrm{Out}(T)$ is easily determined, and we can identify the possibilities for θ (see Table 3).

Let us define the notation used in Table 3. For $f > 1$, let $\varphi \in \mathrm{Aut}(T)$ be the field automorphism of order f defined as $\overline{(a_{ij})} \mapsto \overline{(a_{ij}^p)}$, for each $\overline{(a_{ij})} \in T$. (Here we write linear maps on V as matrices with respect to a standard basis for V (see [32, Prop 2.5.3]), and we use overlines to denote reduction modulo scalars.) Moreover, in case $\mathbf{S_4}$, if q is even, let ρ be a graph-field automorphism of order $2f$ such that $\rho^2 = \varphi$ (see [19, Prop. 12.3.3]). Finally, in cases **S** and $\mathbf{S_4}$ (respectively case **O**), if q is odd, let δ be a diagonal automorphism of order 2 induced by an element of $\mathrm{GSp}_{2m}(q) \setminus \mathrm{Sp}_{2m}(q)$ (respectively $\mathrm{SO}_{2m+1}(q) \setminus \Omega_{2m+1}(q)$). We write $\mathrm{Inndiag}(T)$ for the subgroup of $\mathrm{Aut}(T)$ generated by inner and diagonal automorphisms.

Now consider the elements of G. The conjugacy classes of elements of prime order in G are described in [16, §3.4–3.5], and we will refer to the relevant results when they are required. By [16, Lemmas 3.4.2, 3.5.3], the conjugacy class of an odd order semisimple element g of $\mathrm{GSp}_n(q)$ or $\mathrm{SO}_n(q)$ is determined by the eigenvalues of g over $\overline{\mathbb{F}}_q$. Therefore, up to conjugacy, we will write $[\lambda_1, \ldots, \lambda_n]$ for g, where $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{F}}_q$ are the eigenvalues of g.

Case	q	$\mathrm{Aut}(T)$	$\mathrm{Out}(T)$	θ
S	even	$\langle T, \varphi\rangle$	C_f	$1, \varphi^i$
$\mathbf{S_4}$	even	$\langle T, \rho\rangle$	C_{2f}	$1, \rho^j, \varphi^i$
S, $\mathbf{S_4}$, **O**	odd	$\langle T, \delta, \varphi\rangle$	$C_2 \times C_f$	$1, \delta, \varphi^i, \delta\varphi^i$

TABLE 3. The possibilities for θ
($1 \leq i < f$ and $1 \leq j < 2f$ with j odd)

2.2. **Shintani descent.** Let $G = \langle T, \theta \rangle \in \mathcal{A}$ (see (1.1) and (1.2)). The first step of our probabilistic method is to select a G-class s^G, with respect to which we will analyse the uniform spread of G. It is straightforward to see that we must choose $s \in G \setminus T$, so we will choose $s \in T\theta$. We need to control the maximal subgroups of G which contain s, and the technique of Shintani descent from the theory of algebraic groups will allow us to do this.

Following [17, §2.6], let X be a connected linear algebraic group over an algebraically closed field and let $\sigma\colon X \to X$ be a Steinberg morphism. Write X_σ for the (necessarily finite) fixed point subgroup of X under σ. Let $e > 1$ and observe that X_{σ^e} is σ-stable. Therefore, σ restricts to an automorphism of X_{σ^e} and, with a slight abuse of notation, we may consider the semidirect product $G_1 = X_{\sigma^e}{:}\langle\sigma\rangle$.

Remark 2.1. Let us clarify our use of the symbol σ. Fix $g \in X_{\sigma^e}$. In one sense, σ is a Steinberg morphism of X which restricts to an automorphism of X_{σ^e}. Therefore, $\sigma(g)$ denotes the image of g under the map σ. In a second sense, σ is an element of the semidirect product $G_1 = X_{\sigma^e}{:}\langle\sigma\rangle$, so by $g\sigma$ we mean the product of g and σ in G_1 and by g^σ we mean $\sigma^{-1}g\sigma$. By the definition of the semidirect product G_1, $g^\sigma = \sigma(g)$, so g^σ will be our preferred way of referring to $\sigma(g)$.

Let $g \in X_{\sigma^e}$. By the Lang-Steinberg Theorem [37, Theorem 21.7], there exists $a \in X$ such that $g = aa^{-\sigma^{-1}}$. Define the *Shintani map* as

$$f\colon \{(g\sigma)^{G_1} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\} \quad g\sigma \mapsto a^{-1}(g\sigma)^e a,$$

for $a \in X$ such that $g = aa^{-\sigma^{-1}}$. We abuse notation by writing $f(g\sigma)$ for a representative of the class given by $f(g\sigma)$. The following combines [17, Lemma 2.13, Theorem 2.14].

Theorem 2.2. *Let X be the algebraic group, σ be the Steinberg morphism and f be the Shintani map as above.*

(i) *The Shintani map f is a well-defined bijection.*
(ii) *For all $g \in X_{\sigma^e}$, $C_{X_{\sigma^e}}(g\sigma) \cong aC_{X_\sigma}(f(g\sigma))a^{-1}$.*
(iii) *Let Y be a closed connected σ-stable subgroup of X. Then for all $g \in X_{\sigma^e}$,*

$$\mathrm{fix}(g\sigma, X_{\sigma^e}/Y_{\sigma^e}) = \mathrm{fix}(f(g\sigma), X_\sigma/Y_\sigma).$$

Remark 2.3.

(i) In [17, §2.6], it is verified that $(g\sigma)^{G_1} = (g\sigma)^{X_{\sigma^e}}$, for all $g \in X_{\sigma^e}$. Consequently, f is a bijection from $\{(g\sigma)^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\}$ to $\{x^{X_\sigma} \mid x \in X_\sigma\}$.
(ii) The hypothesis that σ is a Steinberg morphism is used (via the Lang-Steinberg Theorem) to guarantee the existence of the element $a \in X$ required to define the map f. However, the rest of the proof of Theorem 2.2 holds whenever σ is an automorphism of X as an abstract group with a finite fixed point subgroup. Therefore, we may define a Shintani map for any abstract automorphism σ of X which has a finite fixed point subgroup and such that for all $g \in X_{\sigma^e}$ there exists $a \in X$ for which $aa^{-\sigma^{-1}} = g$.

We will now demonstrate how we will apply this general theory to our specific settings. Let $T \in \mathcal{T}$ and $\theta \in \mathrm{Aut}(T)$. Assume that $\theta \notin \mathrm{Inndiag}(T)$. Let $K = \overline{\mathbb{F}}_q$ and define

$$X = \begin{cases} \mathrm{PGSp}_{2m}(K) & \text{if } T = \mathrm{PSp}_{2m}(q) \\ \mathrm{SO}_{2m+1}(K) & \text{if } T = \Omega_{2m+1}(q) \end{cases} \tag{2.1}$$

Abusing notation, as explained in Remark 2.1, let $\varphi\colon X \to X$ be defined as $\overline{(a_{ij})} \mapsto \overline{(a_{ij}^p)}$. Observe that $\varphi|_T$ is the automorphism φ from Table 3. We will split into two cases depending on whether θ is a graph-field automorphism.

2.2.1. *Automorphisms other than graph-field automorphisms.* Assume that θ is not a graph-field automorphism. Then, from Table 3, $\theta = \varphi^i$ or $\theta = \delta\varphi^i$ for some $1 \leq i < f$. Let e be the order of φ^i and write $q = q_0^e$. Then define the Frobenius morphism $\sigma\colon X \to X$ as

$$\sigma = \varphi^i. \tag{2.2}$$

That is, σ is defined as $\overline{(a_{ij})} \mapsto \overline{(a_{ij}^{q_0})}$. Therefore, if $T = \mathrm{Sp}_{2m}(q)$ and q is even, then $\theta = \varphi^i$, and we obtain the Shintani map

$$f\colon \{(t\theta)^{\mathrm{Sp}_{2m}(q)} \mid t \in \mathrm{Sp}_{2m}(q)\} \to \{x^{\mathrm{Sp}_{2m}(q_0)} \mid x \in \mathrm{Sp}_{2m}(q_0)\}. \tag{2.3}$$

Additionally, if q is odd (and $T = \mathrm{PSp}_{2m}(q)$ or $T = \Omega_{2m+1}(q)$), then we obtain the maps

$$f\colon \{(g\varphi^i)^{\mathrm{PGSp}_{2m}(q)} \mid g \in \mathrm{PGSp}_{2m}(q)\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PGSp}_{2m}(q_0)\}; \tag{2.4}$$

$$f\colon \{(g\varphi^i)^{\mathrm{SO}_{2m+1}(q)} \mid g \in \mathrm{SO}_{2m+1}(q)\} \to \{x^{\mathrm{SO}_{2m+1}(q_0)} \mid x \in \mathrm{SO}_{2m+1}(q_0)\}. \tag{2.5}$$

However, for our application, we need to study cosets of T rather than of $\mathrm{Inndiag}(T)$. The following propositions allow us to do this.

Proposition 2.4. *Let q be odd and let $T = \mathrm{PSp}_{2m}(q)$. The Shintani map f restricts to bijections*

(i) $f_1\colon \{(t\varphi^i)^{\mathrm{PGSp}_{2m}(q)} \mid t \in T\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PSp}_{2m}(q_0)\}$;
(ii) $f_2\colon \{(t\delta\varphi^i)^{\mathrm{PGSp}_{2m}(q)} \mid t \in T\} \to \{x^{\mathrm{PGSp}_{2m}(q_0)} \mid x \in \mathrm{PGSp}_{2m}(q_0) \setminus \mathrm{PSp}_{2m}(q_0)\}$.

Proposition 2.5. *Let $T = \Omega_{2m+1}(q)$. The Shintani map f restricts to bijections*

(i) $f_1\colon \{(t\varphi^i)^{\mathrm{SO}_{2m+1}(q)} \mid t \in T\} \to \{x^{\mathrm{SO}_{2m+1}(q_0)} \mid x \in \Omega_{2m+1}(q_0)\}$;
(ii) $f_2\colon \{(t\delta\varphi^i)^{\mathrm{SO}_{2m+1}(q)} \mid t \in T\} \to \{x^{\mathrm{SO}_{2m+1}(q_0)} \mid x \in \mathrm{SO}_{2m+1}(q_0) \setminus \Omega_{2m+1}(q_0)\}$.

We will prove Proposition 2.4; the proof of Proposition 2.5 is analogous, replacing the similarity map τ with the spinor norm η.

For all k, there are natural embeddings $\mathrm{PSp}_{2m}(p^k) \hookrightarrow \mathrm{PGSp}_{2m}(p^k) \hookrightarrow \mathrm{PSp}_{2m}(K)$. Thus, we will identify each of the symplectic groups in the following proof with suitable subgroups of $\mathrm{PSp}_{2m}(K)$ and write $Z = Z(\mathrm{Sp}_{2m}(K))$. Let $N\colon \mathbb{F}_q \to \mathbb{F}_{q_0}$ be the norm map.

Proof of Proposition 2.4. Fix $g \in \mathrm{PGSp}_{2m}(q)$ and let $y \in \mathrm{PGSp}_{2m}(q_0)$ be a representative of the conjugacy class $f(g\sigma)$. Write $\sigma = \varphi^i$ and let $a \in \mathrm{PSp}_{2m}(K)$ be such that $g = aa^{-\sigma^{-1}}$. We will now take suitable lifts of elements. Write $a = \hat{a}Z$ and $\hat{g} = \hat{a}\hat{a}^{-\sigma^{-1}} \in \mathrm{GSp}_{2m}(q)$. So $g = \hat{g}Z$. Therefore, $y = f(g\sigma) = \hat{a}^{-1}(\hat{g}\sigma)^e\hat{a}Z$, and, accordingly, write $\hat{y} = \hat{a}^{-1}(\hat{g}\sigma)^e\hat{a}$.

Now we wish to connect $\tau(\hat{y})$ and $\tau(\hat{g})$. Observe that

$$\tau(\hat{y}) = \tau(\hat{a}^{-1}(\hat{g}\sigma)^e\hat{a}) = \tau((\hat{g}\sigma)^e) = \tau(\hat{g})\tau(\hat{g}^{\sigma^{e-1}})\cdots\tau(\hat{g}^{\sigma}) = N(\tau(\hat{g})),$$

since $\tau(\hat{g}^{\sigma^k}) = \tau(\hat{g})^{\sigma^k}$ for all k. In particular, $\tau(\hat{g})$ is a square in $\mathbb{F}_q$ if and only if $\tau(\hat{y})$ is a square in $\mathbb{F}_{q_0}$. That is, $g \in \mathrm{PSp}_{2m}(q)$ if and only if $f(g\sigma) = y \in \mathrm{PSp}_{2m}(q_0)$. Therefore, restricting f to $\mathrm{PGSp}_{2m}(q)$-classes of $T\sigma$ and $T\delta\sigma$ gives the required bijections. □

2.2.2. *Graph-field automorphisms.* Now assume that q is even and $T = \mathrm{Sp}_4(q)$. Let θ be the graph-field automorphism ρ^j where j is an odd integer such that $1 \leq j < 2f$ (see Table 3). Then $(\rho^j)^2 = \varphi^j$ since, by definition, $\rho^2 = \varphi$. Let e be the order of φ^j and write $q = q_0^e$. Therefore, $q_0 = 2^j$. Abusing notation as above, let $\rho\colon X \to X$ be a Steinberg morphism such that $\rho^2 = \varphi$. Define the Steinberg morphism $\sigma\colon X \to X$ as

$$\sigma = \rho^j. \tag{2.6}$$

The following proposition describes the Shintani map given by the above setup. (In this result, $Sz(q_0)$ is the Suzuki group over the field $\mathbb{F}_{q_0}$.)

Proposition 2.6. *Let $T = \mathrm{Sp}_4(q)$ with $q > 2$ even and let $\theta = \rho^j$. Then there is a Shintani map*

$$f\colon \{(t\theta)^T \mid t \in T\} \to \{x^{Sz(q_0)} \mid x \in Sz(q_0)\} \quad t\theta \mapsto a^{-1}(t\theta)^{2e}a.$$

Proof. By Theorem 2.2, there is a Shintani map f from the $X_{(\rho^j)^{2e}}$-classes in $X_{(\rho^j)^{2e}}\rho^j$ to the X_{ρ^j}-classes in X_{ρ^j}. Since $2^{je} = q_0^e = q$, $X_{(\rho^j)^{2e}} = \mathrm{Sp}_4(q) = T$ and the restriction of ρ^j to $X_{(\rho^j)^{2e}}$ is the automorphism θ. Similarly, $X_{\rho^j} = C_{X_{\rho^{2j}}}(\rho^j) = C_{\mathrm{Sp}_4(q_0)}(\rho^j)$. Since ρ^j is an involutory graph-field automorphism of $\mathrm{Sp}_4(q_0)$, by [3, (19.4)], $C_{\mathrm{Sp}_4(q_0)}(\rho^j) \cong Sz(q_0)$. This proves the result. □

2.2.3. *Applications.* Let us now record several applications of Shintani descent to the problem of studying the maximal overgroups of particular elements, a crucial component of our probabilistic approach. For the remainder of this section, let $G = \langle T, \theta\rangle \in \mathcal{A}$ and recall the formed space $V = \mathbb{F}_q^n$ from Table 2. Moreover, let X be the algebraic group defined in (2.1), let σ be the Steinberg morphism defined in (2.2) or (2.6) and let f be the Shintani map defined in (2.3)–(2.5) or Proposition 2.6. Recall that we write $G_1 = X_{\sigma^e}{:}\langle\sigma\rangle$.

Our first result, which is [17, Prop. 2.16(i)], provides a general bound.

Proposition 2.7. *Let H be a maximal subgroup of G and let $g\sigma \in G$. Then $g\sigma$ is contained in at most $|C_{X_\sigma}(f(g\sigma))|$ G_1-conjugates of H.*

Proposition 2.7 is notable for both its effectiveness and its generality. However, for some particular subgroups we require a tighter bound for our probabilistic estimates. For instance, the following result is modelled on [17, Corollary 2.15] and the proof is similar.

Proposition 2.8. *Let Y be the stabiliser in X of a totally isotropic k-space, or, in the case where $T = \mathrm{PSp}_{2m}(q)$, the stabiliser of a non-degenerate k-space with $k < m$. Assume that Y is σ-stable. For all $g \in X_{\sigma^e}$, the number of X_{σ^e}-conjugates of Y_{σ^e} which are normalised by $g\sigma$ is equal to the number of X_σ-conjugates of Y_σ which contain $f(g\sigma)$.*

In even characteristic, we can also use Shintani descent to determine the number of orthogonal subgroups of a symplectic group which contain a given element. Let q be even and recall that $K = \overline{\mathbb{F}}_q$. Let $X = \mathrm{Sp}_{2m}(K)$ and $Y = \mathrm{O}_{2m+1}(K)$, the isometry group of a non-singular quadratic form on K^{2m+1} (see [42, pp. 143–144]). By [42, Theorem 11.9], there exists an isomorphism $\psi\colon X \to Y$ of abstract groups.

Let $\sigma\colon X \to X$ be a Frobenius morphism, and define $\tau\colon Y \to Y$ as $\tau = \psi \circ \sigma \circ \psi^{-1}$. It is straightforward to verify that ψ extends to an isomorphism $\psi\colon X{:}\langle\sigma\rangle \to Y{:}\langle\tau\rangle$ by defining $\psi(\sigma) = \tau$. By Theorem 2.2, for $e > 1$, we have a Shintani map

$$f\colon \{(g\sigma)^{X_{\sigma^e}} \mid g \in X_{\sigma^e}\} \to \{x^{X_\sigma} \mid x \in X_\sigma\}.$$

Since Y_{τ^e} is τ-stable and ψ restricts to an isomorphism $\psi\colon X_{\sigma^e}{:}\langle\sigma\rangle \to Y_{\tau^e}{:}\langle\tau\rangle$, define

$$f'\colon \{(h\tau)^{Y_{\tau^e}} \mid h \in Y_{\tau^e}\} \to \{y^{Y_\tau} \mid y \in Y_\tau\}$$

as $f' = \psi \circ f \circ \psi^{-1}$. (Recall the notation for automorphisms explained in Remark 2.1.)

Lemma 2.9. *With the notation above, for all $h \in Y_{\tau^e}$ there exists $b \in Y$ such that $bb^{-\tau^{-1}} = h$ and $f'(h\tau) = b^{-1}(h\tau)^e b$.*

Proof. Let $g \in X_{\sigma^e}$ such that $\psi(g) = h$, and let $a \in X$ such that $aa^{-\sigma^{-1}} = g$. Then

$$f'(h\tau) = \psi(f(\psi^{-1}(h\tau))) = \psi(f(g\sigma)) = \psi(a^{-1}(g\sigma)^e a) = \psi(a)^{-1}(h\tau)^e\psi(a)$$

where

$$\psi(a)\psi(a)^{-\tau^{-1}} = \psi(a)\tau^{-1}(\psi(a^{-1})) = \psi(a)\psi(\sigma^{-1}(a^{-1})) = \psi(aa^{-\sigma^{-1}}) = \psi(g) = h. \quad \square$$

Although τ need not be a Frobenius morphism of Y, by Remark 2.3(ii), the conclusion of Theorem 2.2 holds for f' as Lemma 2.9 guarantees that the required $b \in Y$ exists.

Let σ be the standard Frobenius morphism with fixed field $\mathbb{F}_{q_0}$ and write $q = q_0^e$. Then $X_{\sigma^e} = \mathrm{Sp}_{2m}(q)$ and $X_\sigma = \mathrm{Sp}_{2m}(q_0)$. The author thanks Prof Robert Guralnick for helpful comments on the proof of the following proposition.

Proposition 2.10. *With the notation above, for all $g\sigma \in \mathrm{Sp}_{2m}(q){:}\langle\sigma\rangle$ the total number of maximal subgroups of $\mathrm{Sp}_{2m}(q){:}\langle\sigma\rangle$ of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ which contain $g\sigma$ equals the total number of subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^+_{2m}(q_0)$ or $\mathrm{O}^-_{2m}(q_0)$ which contain $f(g\sigma)$.*

Proof. The maximal subgroups of $\mathrm{Sp}_{2m}(q){:}\langle\sigma\rangle$ of type $\mathrm{O}^\pm_{2m}(q)$ which contain $g\sigma$ correspond to the maximal subgroups of $\mathrm{O}_{2m+1}(q)$ of type $\mathrm{O}^\pm_{2m}(q)$ which are normalised by $\psi(g\sigma)$, and these are exactly the stabilisers of non-degenerate hyperplanes of $W = \mathbb{F}_q^{2m+1}$.

If a hyperplane U is non-degenerate, then U does not contain the radical $W \cap W^\perp = \langle v\rangle$. We claim that the converse also holds. To see this, assume $v \notin U$ and suppose that $x \in U \cap U^\perp$ is non-zero. Since $v \notin U$, we know that $x \notin \mathrm{rad}(W)$. Hence, there exists $w \in W$ such that $(x, w) \neq 0$. Therefore, $w \notin U$ and, hence, $W = \langle U, w\rangle$. In particular, $v = u + \lambda w$ for some $u \in U$ and $\lambda \neq 0$. Then $(x, v) = (x, u) + \lambda(x, w) = 0 + \lambda(x, w) \neq 0$ since $\lambda \neq 0$ and $(x, w) \neq 0$. However, $(x, v) = 0$ since $v \in W \cap W^\perp$, which is a contradiction. Therefore, $U \cap U^\perp = 0$, so U is non-degenerate. To summarise, the maximal subgroups of $\mathrm{O}_{2m+1}(q)$ of type $\mathrm{O}^\pm_{2m}(q)$ are exactly the stabilisers of hyperplanes not containing v.

Therefore, the maximal subgroups of $\mathrm{Sp}_{2m}(q){:}\langle\sigma\rangle$ of type $\mathrm{O}^\pm_{2m}(q)$ which contain $g\sigma$ correspond to the stabilisers in $\mathrm{O}_{2m+1}(q)$ of hyperplanes not containing v which are normalised by $\psi(g\sigma)$. By lifting to $\mathrm{SL}_{2m+1}(q)$ and applying [17, Corollary 2.15] (a consequence of Theorem 2.2(iii) which is the analogue of Proposition 2.8 in the linear case), the stabilisers in $\mathrm{SL}_{2m+1}(q)$ of hyperplanes not containing v which are normalised by $\psi(g\sigma)$ correspond to the stabilisers in $\mathrm{SL}_{2m+1}(q_0)$ of hyperplanes not containing the radical of $\mathbb{F}_{q_0}^{2m+1}$ which contain $f'(\psi(g\sigma))$. By the argument of the previous paragraph, the intersections of these subgroups with $\mathrm{O}_{2m+1}(q_0)$ are exactly the maximal subgroups of $\mathrm{O}_{2m+1}(q_0)$ of type $\mathrm{O}^\pm_{2m}(q_0)$ which contain $f'(\psi(g\sigma))$. These subgroups correspond to the maximal subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^\pm_{2m}(q_0)$ which contain $\psi^{-1}(f'(\psi(g\sigma))) = f(g\sigma)$. □

Let us record a consequence of Proposition 2.10.

Corollary 2.11. *Let q be even and let $G = \mathrm{Sp}_{2m}(q){:}\langle\phi\rangle$, where ϕ is a field automorphism of $\mathrm{Sp}_{2m}(q)$. Then every element of G is contained in at least one maximal subgroup of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$.*

Proof. If $x \in \mathrm{Sp}_{2m}(q)$, then, by [22, Theorem 2], x is contained in at least one subgroup H of type $\mathrm{O}^\pm_{2m}(q)$. Hence, $x \in N_G(H)$, a maximal subgroup of G of type $\mathrm{O}^\pm_{2m}(q)$. If $x \in G \setminus \mathrm{Sp}_{2m}(q)$, then $x = g\sigma$ where σ is a power of ϕ. Therefore, by Proposition 2.10, the number of subgroups of G of type $\mathrm{O}^\pm_{2m}(q)$ containing $g\sigma$ equals the number of subgroups of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^\pm_{2m}(q_0)$ containing $f(g\sigma)$, which is at least one. □

2.3. **Computational methods.** In addition to the probabilistic method described in the introduction, we carry out computations in Magma [4] to determine lower bounds on the uniform spread of some particular groups. In this way, for each group $G = \langle T, \theta\rangle$ in Table 4, we verify that $u(G) \geq k$. (Here we use the notation from Table 3.)

In each case, the group G can be accessed directly, constructed using the command `AutomorphismGroup` or found as a subgroup of $\langle \mathrm{PSp}_n(q), \varphi, \delta\rangle$, which is obtained from $\mathrm{P\Sigma L}_n(q)$ by repeatedly using `MaximalSubgroups`. We have implemented an algorithm in Magma which takes as input a finite group `G`, positive integers `k`, `N` and an element `s` in G whose conjugacy class we wish to show witnesses the uniform spread k of G.

T	θ	k
$\mathrm{PSp}_4(3)$	δ	2
$\mathrm{PSp}_6(3)$	$1, \delta$	4
$\Omega_7(3)$	δ	3
$\mathrm{PSp}_4(4)$	φ	4
$\mathrm{PSp}_4(4)$	ρ	10
$\mathrm{PSp}_4(8)$	φ, ρ	2
$\mathrm{PSp}_4(8)$	ρ^3	76
$\mathrm{PSp}_4(16)$	φ, φ^2, ρ	2
$\mathrm{PSp}_4(9)$	$\varphi, \delta\varphi$	4
$\mathrm{PSp}_4(25)$	$\varphi, \delta\varphi$	2
$\mathrm{PSp}_4(27)$	$\varphi, \delta\varphi$	2

TABLE 4. Computational results: $u(\langle T, \theta\rangle) \geq k$

First, we follow the probabilistic method described in the introduction. To determine $\mathcal{M}(G, s)$ we use `MaximalSubgroups`. For each conjugacy class x^G, we need to compute $\mathrm{fpr}(x, G/H)$ for each $H \in \mathcal{M}(G, s)$; we do this by calculating $|x^G \cap H|$ using `IsConjugate`, noting that $\mathrm{fpr}(x, G/H) = \frac{|x^G \cap H|}{|x^G|}$. If for all k-tuples of classes $(x_1^G, \ldots, x_k^G)$ we establish that $P(x_1, s) + \cdots + P(x_k, s) < 1$, then we have verified that $u(G) \geq k$ with respect to s^G.

Otherwise, for each k-tuple of classes $(C_1, \ldots, C_k)$, we apply a randomised method (parameterised by N) to explicitly construct an element $z \in s^G$ such that for all $c_i \in C_i$, $\langle c_1, z\rangle = \cdots = \langle c_k, z\rangle = G$. This randomised approach is based on the GAP calculations in [9, §4], which are described by Breuer in [8, §3.3]. Observe that it suffices to show that for all representatives $(x_1, \ldots, x_k)$ of the orbits of $C_1 \times \cdots \times C_k$ under the diagonal conjugation action of G, there exists $z \in s^G$ such that $\langle x_1, z\rangle = \cdots = \langle x_k, z\rangle = G$. An algorithm of [8, pp. 18–19] to construct these orbit representatives is the crucial ingredient. Given these representatives, we test at most N random conjugates of s for each list of representatives, and we return any k-tuples of conjugacy classes for which no suitable conjugate of s is found. If no k-tuples fail, then the bound $u(G) \geq k$ holds.

3. Fixed point ratios

This section serves to provide the fixed point ratio bounds we require in order to apply the probabilistic method in Section 4. There is a vast literature on fixed point ratios for primitive actions of almost simple groups. In addition to the essential role they play in random generation, these bounds have many other applications, such as to the study of base sizes (e.g. see [15]) and monodromy groups (e.g. see [24]).

The most general bound in this area is [34, Theorem 1] of Liebeck and Saxl, which establishes that $\mathrm{fpr}(x, G/H) \leq 4/3q$, for any almost simple group of Lie type over $\mathbb{F}_q$, maximal subgroup $H \leq G$ and non-identity element $x \in G$, with a known list of exceptions. However, a theorem of Burness [11, Theorem 1] gives a stronger result when G is a finite almost simple classical group, H is a non-subspace subgroup and $x \in G$ has prime order. (Recall that, roughly, a subgroup of G is *non-subspace* if it acts irreducibly on the natural module for G; see [11, Definition 1].) Namely, if n is the dimension of the natural module for G, then

$$\mathrm{fpr}(x, G/H) \leq |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota}$$

where ι is given in [11, Table 1].

For remainder of this section, let G be an almost simple group with socle $T \in \mathcal{T}$, where

$$\mathcal{T} = \{\mathrm{PSp}_{2m}(q)' \mid m \geq 2\} \cup \{\Omega_{2m+1}(q) \mid q \text{ odd}, m \geq 3\}.$$

Assume that $T \neq \mathrm{PSp}_4(2)' \cong A_6$.

Let us introduce some notation.

Notation 3.1. Let $V = \mathbb{F}_q^n$ and let $x \in \mathrm{PGL}(V)$. Let $\hat{x}$ be a preimage of x in $\mathrm{GL}(V)$. Define $\nu(x)$ to be the codimension of the largest eigenspace of $\hat{x}$ on $\overline{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$.

We begin by recording a consequence of [11, Theorem 1].

Proposition 3.2. *Let $x \in G$ have prime order and assume that $m \geq 3$. Suppose that H is a maximal non-subspace subgroup of G. Let $\ell = 1$ unless specified otherwise in Table 5.*

(i) *If $T = \Omega_{2m+1}(q)$, then*

$$\mathrm{fpr}(x, G/H) < \frac{(4q+4)^{1/2}}{q^{m-\ell+\varepsilon}},$$

where $\varepsilon = 1/2$ unless $x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$, in which case $\varepsilon = 0$.

(ii) *If $T = \mathrm{PSp}_{2m}(q)$, then*

$$\mathrm{fpr}(x, G/H) < \frac{(2q+2)^{1/2}}{q^{m-\ell}}.$$

(iii) *If $T = \mathrm{PSp}_{2m}(q)$, then $\mathrm{fpr}(x, G/H) < F(x, G/H)$ as given in Table 6.*

Proof. First suppose that $x \in \mathrm{PGL}(V)$. If $T = \mathrm{PSp}_{2m}(q)$ and $s = \nu(x) = 1$, then $\max(s(2m-s), sm) = 2m-1$. Therefore, by [12, Prop. 3.22, 3.36],

$$|x^G| \geq |x^{\mathrm{PSp}_{2m}(q)}| > \frac{q^{2m}}{2q+2}.$$

By [11, Theorem 1], letting $\ell = 1 + 2m\iota$,

$$\mathrm{fpr}(x, G/H) < \frac{1}{|x^G|^{1/2-1/2m-\iota}} < \frac{(2q+2)^{1/2-1/2m-\iota}}{q^{m-1-2m\iota}} = \frac{(2q+2)^{1/2-\ell/2m}}{q^{m-\ell}}.$$

The remaining cases are similar.

Now assume that $x \notin \mathrm{PGL}(V)$. Therefore, x is a field automorphism, and

$$|x^G| \geq |x^T| \geq \frac{|\mathrm{PSp}_{2m}(q)|}{|\mathrm{PGSp}_{2m}(q^{\frac{1}{2}})|} > \frac{1}{2} q^{m^2+m/2}$$

since $|\mathrm{PSp}_{2m}(q)| = |\Omega_{2m+1}(q)|$. Then, by [11, Theorem 1],

$$\mathrm{fpr}(x, G/H) < \frac{1}{|x^G|^{1/2-\ell/2m}} < \frac{2}{q^m}. \qquad \square$$

T	Type of H	ℓ
$\mathrm{PSp}_{2m}(q)$	$\mathrm{Sp}_m(q) \wr S_2$	2
$\mathrm{PSp}_{2m}(q)$	$\mathrm{Sp}_m(q^2)$	2
$\Omega_7(q)$	$G_2(q)$	1.76
$\mathrm{PSp}_8(2)$	A_{10}	1.50
$\Omega_7(3)$	$\mathrm{Sp}_6(2)$	1.46
$\mathrm{PSp}_6(2)$	$\mathrm{PSU}_3(3)$	1.33

TABLE 5. Values of ℓ

Condition on x	$F(x, G/H)$
$x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$	$\dfrac{(2q+2)^{1/2-\ell/2m}}{q^{m-\ell}}$
$x \in \mathrm{PGL}(V)$ and $\nu(x) \geq 2$	$\dfrac{(2q+2)^{1/2-\ell/2m}}{q^{2(m-\ell)-3/2+3/2m}}$
$x \notin \mathrm{PGL}(V)$	$\dfrac{2}{q^m}$

TABLE 6. Bounds for Proposition 3.2(iii)

In a special case of interest, we can provide a stronger result for subfield subgroups.

Proposition 3.3. *Let $x \in G \cap \mathrm{PGL}(V)$ have prime order and assume that $\nu(x) = 1$. Let H be a maximal subfield subgroup of G. Then*

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

Proof. By [16, §3.4–3.5], a prime order element with $\nu(x) = 1$ is G-conjugate to the block diagonal matrix $[-I_{2m}, 1]$ in case **O**, and $[J_2, I_{2m-2}]$ in cases **S** and $\mathbf{S_4}$. (Here we use J_i to denote a Jordan block of size i.) Therefore, in each case, $x^G \cap H = x^H$. The result follows from the centraliser orders in [16, Appendix B]. □

Since [11, Theorem 1] excludes subspace subgroups, we use the bounds in [27, §3] in these cases. For convenience we record the relevant bounds below. (Recall that the *Witt index* of an orthogonal space is the largest dimension of a totally singular subspace. Thus, the Witt index of a non-degenerate $(2m+1)$-space is m, and the Witt index of a non-degenerate $2m$-space is m if the space is plus-type, and $m-1$ if the space is minus-type.)

Proposition 3.4. *Let $x \in G$ have prime order and assume that $m \geq 3$.*

(i) *Let H be the stabiliser of a totally isotropic k-space, where $1 \leq k \leq m$. Then*

$$\mathrm{fpr}(x, G/H) < 2q^{-(m-1)} + q^{-m} + q^{-k}.$$

(ii) *Let $T = \Omega_{2m+1}(q)$ and let H be the stabiliser of a non-degenerate k-space of Witt index l, where $1 \leq k \leq 2m$. Then*

$$\mathrm{fpr}(x, G/H) < 2q^{-(m-1)} + q^{-m} + q^{-l} + q^{-(2m+1-k)}.$$

(iii) *Let $T = \mathrm{PSp}_{2m}(q)$ and let H be the stabiliser of a non-degenerate k-space, where $1 \leq k \leq 2m-1$. Then*

$$\mathrm{fpr}(x, G/H) < 2q^{-(m-\alpha)} + q^{-m} + q^{-k/2} + q^{-(2m-k)},$$

where $\alpha = 1$ if q is even, and $\alpha = 2$ if q is odd.

(iv) *Let q be even, let $T = \mathrm{Sp}_{2m}(q)$ and let H be a subgroup of G of type $\mathrm{O}^{\pm}_{2m}(q)$. Then*

$$\mathrm{fpr}(x, G/H) < q^{-\beta} + q^{-m},$$

where $\beta = 1$ if $x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$, and $\beta = 2$ otherwise.

Proof. See [27, Prop. 3.15, 3.16, Lemma 3.18]. □

Notice that the bounds in Proposition 3.4(i)–(iii) do not depend on x. In contrast, [23, Theorems 1–6] provide upper and lower bounds for the fixed point ratio of an element x of an almost simple classical group on an appropriate set of k-spaces which depend not only on q, n and k, but also $\nu(x)$ when $x \in G \cap \mathrm{PGL}(V)$. However, for our application, the constants in these bounds are not sufficient. Therefore, we present bounds which are similar to those in [23], but with sharper constants in the special case that we are interested in.

Proposition 3.5. *Let $T = \mathrm{PSp}_{2m}(q)$ with $m \geq 3$. Let $x \in G$ have prime order. If $x \in \mathrm{PGL}(V)$, then write $s = \nu(x)$. Let H be the stabiliser in G of a non-degenerate 2-space. Then*

$$\mathrm{fpr}(x, G/H) \leq \begin{cases} q^{-2s} + q^{-(2s+2)} + q^{-(2m-2)} + q^{-(2m-1)} & \text{if } x \in \mathrm{PGL}(V) \\ 2q^{-(2m-1)} & \text{if } x \notin \mathrm{PGL}(V) \end{cases}$$

Proof. If x is not contained in a G-conjugate of H, then $\mathrm{fpr}(x, G/H) = 0$. Therefore, let us assume that $x \in H$. Write $L = G \cap \mathrm{PGL}(V)$ and $H_0 = H \cap L$. Hence, H_0 is a subgroup of $\mathrm{GSp}_2(q) \times \mathrm{GSp}_{2m-2}(q)$, modulo scalars.

Case 1: $x \in L$

We will adopt the notation of [16, §3.4] for elements of prime order in L. Let x have order r. Consider the case when r is odd. If x is semisimple, then x^L is determined by the eigenvalues of x on V whereas if x is unipotent, then x^L is described in terms of (but not uniquely determined by) the Jordan form of x on V. If x is an involution, then we use the notation of [25, Table 4.5.1] if x is semisimple and of Aschbacher and Seitz [3] if x is unipotent.

In each case, the description of elements in [16, Chapter 3] allows the splitting of $x^L \cap H_0$ into H_0-classes to be easily determined and we verify the bound using the centraliser orders in [16, Appendix B]. For example, if $r = p = 2$ and $x = b_s$, then $x^L \cap H_0$ is the union of $x_1^{H_0}$, $x_2^{H_0}$, and $x_3^{H_0}$ where x_1, x_2 and x_3 are the elements (I_2, b_s), (b_1, a_{s-1}) and (b_1, c_{s-1}) of $\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$. So

$$\mathrm{fpr}(x, G/H) = \mathrm{fpr}(x, L/H_0) = \frac{|H_0|}{|L|} \sum_{i=1}^{3} \frac{|C_L(x_i)|}{|C_{H_0}(x_i)|} \leq \frac{1}{q^{2s}} + \frac{1}{q^{2m-1}} + \frac{1}{q^{2m+s-1}}.$$

For another example, suppose that $r \notin \{p, 2\}$, so x is a semisimple element of odd order. By [16, Prop. 3.4.3], a lift of x is L-conjugate to the block diagonal matrix $[M_1, \ldots, M_d, I_\ell]$ where, for some even k, the matrices $M_1, \ldots, M_d$ either each act irreducibly on a non-degenerate k-space U_i, or preserve the decomposition of a non-degenerate k-space U_i into two totally isotropic $\frac{k}{2}$-spaces, acting irreducibly on both. Now let $h \in H$ be G-conjugate to x. Then h lifts to $(M, N) \in \mathrm{GSp}_2(q) \times \mathrm{GSp}_{2m-2}(q)$. If $M = I_2$, then $\ell \geq 2$ and h is H_0-conjugate to x_0, an element lifting to $(I_2, [M_1, \ldots, M_d, I_{\ell-2}])$. If $M \neq I_2$, then let $\lambda \in \overline{\mathbb{F}}_q$ be a non-trivial eigenvalue of M. Hence, λ is an eigenvalue of M_i for some i. Since the set of eigenvalues of M is closed under the map $\mu \mapsto \mu^q$, it must be that $k = 2$ and $M = M_i$. Therefore, h is H_0-conjugate to x_i, an element lifting to $(M_i, [M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_d, I_\ell])$. So, if $\ell = 0$ and $k > 2$, then $x^L \cap H_0 = \emptyset$; if $\ell \geq 2$ and $k > 2$, then $x^L \cap H_0 = x_0^{H_0}$; and if $k = 2$, then $x^L \cap H_0 = x_a^{H_0} \cup \cdots \cup x_d^{H_0}$ where $a = 0$ if $\ell \geq 2$ and $a = 1$ if $\ell = 0$. The result follows from the centralisers in [16, Appendix B].

Case 2: x **is a field automorphism**

In this case, $|x^G|$ is at most the number of elements of order r in Tx. So $|x^G \cap H|$ is at most the number of elements of order r in $Tx \cap H = H_0 x$. By [25, Prop. 4.9.1(d)], this is at most $2|x^H|$. So $|x^G \cap H| \leq 2|x^H|$ and

$$\mathrm{fpr}(x, G/H) = \frac{2|H||C_G(x)|}{|G||C_H(x)|} \leq \frac{2|\mathrm{Sp}_2(q)||\mathrm{Sp}_{2m-2}(q)|e|\mathrm{Sp}_{2m}(q^{1/r})|e}{|\mathrm{Sp}_{2m}(q)|e|\mathrm{Sp}_2(q^{1/r})||\mathrm{Sp}_{2m-2}(q^{1/r})|e} \leq \frac{2}{q^{2m-2}}. \qquad \square$$

The four-dimensional symplectic groups require special attention and we will provide a close to best possible fixed point ratio bound for these groups.

Proposition 3.6. *Let $q = p^f$ where $f > 1$ and let G be an almost simple group with socle $\mathrm{PSp}_4(q)$. For a maximal non-subspace subgroup H of G and $x \in G$ of prime order*

$$\mathrm{fpr}(x, G/H) \leq \frac{4}{q(q-1)},$$

unless H has type $\mathrm{Sp}_2(q) \wr S_2$ or $\mathrm{Sp}_2(q^2)$ and x is an a_2 or t_2 involution, in which case,

$$\mathrm{fpr}(x, G/H) \leq \frac{q}{q^2-1}.$$

Moreover, we have the following stronger bounds when q is even.

(i) *If H has type $Sz(q)$, then $\mathrm{fpr}(x, G/H) \leq 1/q^2$.*
(ii) *If H has type $\mathrm{O}_2^-(q^2)$, then $\mathrm{fpr}(x, G/H) \leq 8/q^2(q-1)$.*

Proof. Let x have prime order r. We may assume that $x \in H$. By [5, Tables 8.12–8.14], the possibilities for the type of H are the following. (Here l is a prime divisor of e.)

- in all cases:

Type	$\mathrm{Sp}_4(q^{1/l})$	$Sz(q)$	$\mathrm{PSL}_2(q)$
Condition		q even & f odd	q odd

- if G does not contain a graph-field automorphism:

Type	$\mathrm{Sp}_2(q) \wr S_2$	$\mathrm{GL}_2(q).2$	$\mathrm{Sp}_2(q^2)$	$\mathrm{GU}_2(q)$
Condition		q odd		q odd

- if G contains a graph-field automorphism:

Type	$\mathrm{O}_2^+(q) \wr S_2$	$\mathrm{O}_2^-(q) \wr S_2$	$\mathrm{O}_2^-(q^2)$

Write $T = \mathrm{PSp}_4(q)$, $L = G \cap \mathrm{PGL}(V)$ and $H_0 = H \cap L$. Assume that H does not have type $\mathrm{PSL}_2(q)$ since the calculation for this case is in [14, Prop. 2.22].

Case 1: $x \in L$

Suppose for now that H does not have type $Sz(q)$. We proceed as in the proof of Proposition 3.5. The splitting of x^L into H_0-classes is straightforward to determine, except for involutions when q is odd. For these elements the arguments are often more subtle. We present the example where q is odd, x is an involution and H has type $\mathrm{GU}_2(q)$.

Write $H_0 = B{:}\langle\psi\rangle$ where B is the image of $\mathrm{GU}_2(q)$ in $\mathrm{Sp}_4(q)$ modulo scalars, and ψ induces the inverse-transpose map on B. As explained in Section 2.1, we will denote semisimple elements of $\mathrm{GL}_4(q)$, up to conjugacy, as $[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$. By [16, Lemma 5.3.11], the image of $\mathrm{GU}_2(q)$, modulo scalars, is given as $[\lambda, \mu] \mapsto [\lambda, \lambda^q, \mu, \mu^q]$. First suppose that $x \in B$. Following [25], there are two classes of involutions in B. The t_1 class is represented by an element which lifts to $[-1, 1]$ and so embeds in L as $[-I_2, I_2]$, a t_1 involution of L. If $q \equiv 1 \pmod 4$, then the second class is represented by t_1', which lifts to $[\xi, \xi^{-q}]$, where ξ has order 4 in $\mathbb{F}_{q^2}^\times$. In this case, $\xi \in \mathbb{F}_q$ and so $[\xi, \xi^{-q}] = [\xi, \xi^{-1}]$ embeds in L as $[\xi I_2, \xi^{-1} I_2] \in L$, a t_2 involution of L. If $q \equiv 3 \pmod 4$, then the second class arises from central involutions z which lift to $[\lambda, \lambda]$, where $\lambda \in \mathbb{F}_{q^2}^\times$ has order 4. Since $\lambda \notin \mathbb{F}_q$, z embeds in L as a t_2' involution. Now suppose that $x \in H_0 \setminus B$. Then x lifts to $A\psi$ such that $(A\psi)^2 \in \{I, -I\}$. That is, A is either symmetric or skew-symmetric. Moreover, x has a 1-eigenvector, and hence embeds as $t_1 \in L$, if and only if A is skew-symmetric. So we have determined how $x^L \cap H_0$ splits into H_0 classes, and the result follows as in the proof of Proposition 3.5. For example, if x is a t_1 involution and $L = \mathrm{PSp}_4(q)$ then, since there are $q+1$ skew-symmetric matrices in $\mathrm{GU}_2(q)$,

$$\mathrm{fpr}(x, G/H) = \frac{|x^L \cap H_0|}{|x^L|} = \frac{|\mathrm{Sp}_2(q)|^2}{|\mathrm{PSp}_4(q)|} \left(\frac{|\mathrm{GU}_2(q)|}{2|\mathrm{GU}_1(q)|^2} + \frac{q+1}{2} \right) = \frac{1}{q^2}.$$

Now consider the case where H has type $Sz(q)$. By [12, Prop. 3.52], either $x = c_2$ or $x = [\lambda_1, \lambda_1^{-1}, \lambda_2, \lambda_2^{-1}]$ for $\lambda_1 \neq \lambda_2$. For the former case, we use the fact that $|x^T \cap H_0|$ is at most $(q-1)(q^2+1)$, the number of involutions in $Sz(q)$. In the latter case, the bound $|x^T \cap H_0| \leq |H_0|$ suffices.

The stronger bound for the subgroup of type $\mathrm{O}_2^-(q^2)$ is obtained by observing that, in this case, H_0 does not contain any involutions of type a_2 or b_1 (see [16, Prop. 5.9.2], for example).

Case 2: x is a field automorphism

Assume that if H has type $\mathrm{Sp}_4(q^{1/l})$ then $r \neq l$ and if $H \in \mathcal{C}_2$ or $H \in \mathcal{C}_3$ then $r \neq 2$ (see Table 1). The calculations in these cases are similar and we will present an example below. If these conditions are not satisfied, then the situation is slightly more complicated. We will demonstrate how to handle this when $r = 2$ and $H \in \mathcal{C}_2$ then outline the other cases.

Consider the case where H has type $\mathrm{Sp}_2(q) \wr S_2$. Let $H_0 = B{:}\langle\pi\rangle$ where $B \leq H_0$ is the index two subgroup of type $\mathrm{Sp}_2(q) \times \mathrm{Sp}_2(q)$. By [16, Prop. 3.4.15], we may assume that x is a power of the standard field automorphism. Moreover, we may choose π such that π and x commute. Since $|x^G|$ is at most the number of elements of order r in Tx, $|x^G \cap H|$ is at most the number of elements of order r in $Tx \cap H = H_0x = Bx \cup B\pi x$. If $r \neq 2$, then, since π has order two and commutes with x, no element of $B\pi x$ has order r. In this case, $|x^G \cap H|$ is at most the number of elements of order r in Bx which, by [25, Prop. 4.9.1(d)], is at most $2|x^H|$. If $r = 2$, then the previous argument gives the number of involutions in Bx, so it remains to determine the number of involutions in $B\pi x$. Let $g\pi x \in B\pi x$ be an involution. Suppose that g lifts to $[M, N] \in \mathrm{GSp}_2(q) \times \mathrm{GSp}_2(q)$. Then for $\lambda \in \mathbb{F}_q$,

$$\lambda[I, I] = ([M, N]\pi x)^2 = [M, N][M, N]^{\pi x} = [MN^x, NM^x].$$

Hence, $\lambda \in \{1, -1\}$ and $N = \lambda M^{-x}$. So there are at most $2|\mathrm{Sp}_2(q)| = 2q(q^2-1)$ involutions in $B\pi x$. The bound follows.

Let us now remark on the remaining subtleties. First, if $r = 2$ and H has type $\mathrm{Sp}_2(q^2)$ or $\mathrm{GU}_2(q)$, then $\mathrm{fpr}(x, G/H) = 0$. To see this, suppose that $G = \mathrm{PSp}_4(q){:}\langle\sigma\rangle$ and that $H = \mathrm{PSp}_2(q^2){:}\langle\tau\rangle$ where σ is a field automorphism of $\mathrm{PSp}_4(q)$ of order e and τ is a field automorphism of $\mathrm{PSp}_2(q^2)$ of order $2e$; the other cases are similar. If $x \notin \mathrm{PSp}_2(q^2)$ is an involution, then $x = g\tau^e$ for some $g \in \mathrm{PSp}_2(q^2)$. However, $g\tau^e \in \mathrm{PSp}_2(q^2){:}\langle\tau^e\rangle = H \cap L$ and so $x \in L$: a contradiction. Second, let H have type $\mathrm{Sp}_{2m}(q^{1/l})$ with $r = l$. For $S \subseteq G$, let $i_r(S)$ be the number of elements of S of order r. Although $|x^G \cap H| = i_r(H_0x)$, we cannot argue that $i_r(H_0x) = |x^H|$, as we did above, since x commutes with H_0. Therefore, we need to explicitly bound $i_r(H_0x) \leq 1 + i_r(H_0)$. If $r \geq 5$ then the bound $i_r(H_0) \leq |H_0|$ suffices, and if $r \in \{2, 3\}$ then we use the bounds from [33, Prop. 1.3].

Case 3: x is a graph-field automorphism

In this case $r = p = 2$. First, if $H_0 = \mathrm{Sp}_4(q^{1/l})$, then we argue as for field automorphisms. Second, if $H_0 = Sz(q)$, then, as above, x commutes with H_0 and we need the result that $i_2(Sz(q)) = (q-1)(q^2+1)$. Finally, if H has type $\mathrm{O}_2^\varepsilon(q) \wr S_2$ or $\mathrm{O}_2^-(q^2)$, then, since H is a split extension of H_0 by a cyclic group of order $2e = |H : H_0|$, there are at most $|H|/e = 2|H_0|$ elements of order 2 in H. The bound $|x^G \cap H| \leq 2|H_0|$ suffices. □

4. Proof of the Main Results

In this final section we will prove Theorems 1–4. Recall the definitions of $\mathcal{T}$ and $\mathcal{A}$ from (1.1) and (1.2). For this entire section, fix $G = \langle T, \theta\rangle \in \mathcal{A}$ and assume that $T \neq \mathrm{PSp}_4(2)' \cong A_6$ (see Remark 1). Let $V = \mathbb{F}_q^n$ be the formed space defined in Table 2. Moreover, let X be the algebraic group defined in (2.1), let σ be the Steinberg morphism defined in (2.2) or (2.6), let f be the Shintani map defined in (2.3)–(2.5) or Proposition 2.6 and let $q = q_0^e$.

We will follow the probabilistic approach outlined in the introduction. Let us recall two pieces of notation which are central to this approach. For $x, s \in G$, write $\mathcal{M}(G, s)$ for the set of maximal subgroups of G which contain s, and write

$$P(x, s) = 1 - \frac{|\{z \in s^G \mid G = \langle x, z\rangle\}|}{|s^G|}.$$

4.1. **Diagonal automorphisms.** We will begin by proving Theorems 1, 2 and the reverse direction of Theorem 3, in the case where $\theta \in \mathrm{Inndiag}(T)$. We need the following lemma.

Lemma 4.1. *Let $d \geq 1$, let q be odd and let $\langle \zeta \rangle = \mathbb{F}_q^\times$.*

(i) *Let $A \in \mathrm{Sp}_{2d}(q)$ generate a subgroup $\mathrm{GU}_1(q^d)$. Then there exists $C \in \mathrm{GSp}_{2d}(q)$ such that $C^{q-1} = A$ and $\tau(C) = \zeta$. In particular, $C \notin \mathrm{Sp}_{2d}(q)$.*
(ii) *Let $A \in \mathrm{SO}^-_{2d}(q) \leq \mathrm{SO}_{2d+1}(q)$ generate a subgroup $\mathrm{GU}_1(q^d)$. Then $A \notin \Omega_{2d+1}(q)$.*

Proof. First consider (i). Recall that $\Delta\mathrm{U}_1(q^d)$ is the similarity group of a 1-dimensional unitary space over $\mathbb{F}_{q^d}$ with similarity map $\tau\colon \Delta\mathrm{U}_1(q^d) \to \mathbb{F}_{q^d}$ (see Section 2.1). The group

$$H = \{h \in \Delta\mathrm{U}_1(q^d) \mid \tau(h) \in \mathbb{F}_q\}$$

is naturally a subgroup of $\mathrm{GSp}_{2d}(q)$. Moreover, $\langle A \rangle$ is the index $q-1$ subgroup of H containing the isometries in H. Hence, there is a generator C for H such that $C^{q-1} = A$. Since C generates H, we may assume that $\tau(C) = \zeta$. Now consider (ii). By [18, Theorem 4], $\Omega_{2d+1}(q_0)$ does not have a maximal torus of order $|\langle A \rangle| = q^d + 1$, so $A \notin \Omega_{2d+1}(q_0)$. □

Proposition 4.2. *Let $T \in \mathcal{T}$, let $\theta \in \mathrm{Inndiag}(T)$ and let $G = \langle T, \theta \rangle$.*

(i) *In all cases, $u(G) \geq 2$*
(ii) *If $T = \Omega_{2m+1}(q)$, then $u(G) \geq 3$.*
(iii) *If $T = \mathrm{PSp}_{2m}(q)$, q is odd and $m \geq 3$, then $u(G) \geq 4$.*
(iv) *In all cases, $u(G) \to \infty$ as $q \to \infty$.*
(v) *If $T = \mathrm{PSp}_{2m}(q)$ and q is odd, then $u(G) \to \infty$ as $m \to \infty$.*

Proof. By [9, Corollary 1.3], (i) and (ii) hold if $\theta = 1$. In particular, (i) holds if q is even. Therefore, let us suppose that q is odd to prove parts (i)–(iii). We may exclude the cases covered by the Magma computations listed in Table 4.

For now, let us assume that m is odd if $T = \Omega_{2m+1}(3)$. In the proofs of [9, Prop. 5.10, 5.12, 5.19, 5.20], by separating into several cases depending on T and m, it is shown that for all prime order elements $x \in T$, $P(x, s) < 1/3$, for a suitable choice of semisimple element $s \in T$. In each case, by Lemma 4.1, there exists $g \in G \setminus T$ such that $g^2 = s$. The proofs that $P(x, s) < 1/3$ each comprise two steps: determining $\mathcal{M}(T, s)$ and computing the fixed point ratios $\mathrm{fpr}(x, T/H_0)$ for all $H_0 \in \mathcal{M}(T, s)$. To determine $\mathcal{M}(T, s)$, the main result of [28] is applied and the properties of T and s which are used to eliminate subgroups hold also for G and g. Hence, the subgroups in $\mathcal{M}(G, g)$ have the same type and multiplicities as those in $\mathcal{M}(T, s)$. Moreover, the bounds on $\mathrm{fpr}(x, T/H_0)$ for $H_0 \in \mathcal{M}(T, s)$ apply also to $\mathrm{fpr}(x, G/H)$ for $H \in \mathcal{M}(G, s)$ and $x \in G$. Therefore, $P(x, g) < 1/3$ and so $u(G) \geq 3$. In fact, if $m \geq 3$ and $T = \mathrm{PSp}_{2m}(q)$, then, by using the bounds from Proposition 3.2 instead of the bounds in [9], we obtain $P(x, s) < 1/4$ and $P(x, g) < 1/4$. As a result, $u(G) \geq 4$.

For $T = \Omega_{2m+1}(3)$ with m even, for suitable $s \in T$, it is shown in [9, Prop. 5.7] that $P(x, s) \leq 1/3$ with equality if and only if x is an involution with $\nu(x) = 1$. By Lemma 4.1, we can choose $g \in G \setminus T$ and, by arguing as above, we show that $P(x, g) \leq 1/3$ with equality if and only if x is an involution with $\nu(x) = 1$. By the argument in [9, Prop. 5.7], for all involutions $x_1, x_2, x_3 \in T$ such that $\nu(x_1) = \nu(x_2) = \nu(x_3) = 1$, there exists a G-conjugate z of g for which $\langle x_1, z \rangle = \langle x_2, z \rangle = \langle x_3, z \rangle = G$. Therefore, $u(G) \geq 3$.

Now consider parts (iv) and (v). By [30, Theorem 1.1], these parts holds when $\theta = 1$. In the proof of [27, Prop. 4.1], it is shown that $P(x, s) \to 0$ as $m \to \infty$ or $q \to \infty$, for suitable $s \in \mathrm{PSp}_{2m}(q)$. By Lemma 4.1, there exists $g \in \mathrm{PGSp}_{2m}(q) \setminus \mathrm{PSp}_{2m}(q)$ such that $P(x, g) \to 0$ as $m \to \infty$ or $q \to \infty$. Very similarly, by the proof of [27, Prop. 4.1], we can find $g \in \mathrm{SO}_{2m+1}(q) \setminus \Omega_{2m+1}(q)$ such that $P(x, g) \to 0$ as $q \to \infty$. □

Therefore, if $\theta \in \mathrm{Inndiag}(T)$, then it remains to prove only Theorem 4 (which implies the forward direction of Theorem 3). This will be done in Section 4.5. Therefore, in Sections 4.2–4.4 we will assume that $\theta \notin \mathrm{Inndiag}(T)$.

4.2. **Element selection.** Let $G = \langle T, \theta \rangle \in \mathcal{A}$ with $T \neq \mathrm{PSp}_4(2)'$ and $\theta \notin \mathrm{Inndiag}(T)$. Maintain the notation introduced at the opening of Section 4. In particular, recall that $q = q_0^e$. The goal of this section is to identify an element $t\theta \in G$ to represent the conjugacy class with respect to which we will study the uniform spread of G.

We will introduce notation for the elements which we will use repeatedly.

Definition 4.3. Let $d \geq 2$, $W = \mathbb{F}_{q_0}^{2d}$ and $\mathbb{F}_{q_0}^\times = \langle \alpha \rangle$.

Cases S and $\mathbf{S_4}$

(i) Let $A_{2d} \in \mathrm{Sp}_{2d}(q_0)$ be a generator of a cyclic subgroup $\mathrm{GU}_1(q_0^d)$.
(ii) Write $W = W_1 \oplus W_2$ where W_1 and W_2 are totally isotropic d-spaces. Let $B_{2d} = [B, B^{-T}] \in \mathrm{Sp}_{2d}(q_0)$ have order $q_0^d - 1$ and stabilise the spaces W_1 and W_2, acting irreducibly on both.
(iii) If q is odd, then let $C_{2d} \in \mathrm{GSp}_{2d}(q_0)$ be such that $C_{2d}^{q_0-1} = A_{2d}$ and $\tau(C_{2d}) = \alpha$ (see Lemma 4.1).
(iv) Let $D_{2d} = [\alpha B, B^{-T}] \in \mathrm{GSp}_{2d}(q_0)$, where B is as in (ii).

Case O

(iv) Assume that W is minus-type. Let $A_{2d} \in \mathrm{SO}^-_{2d}(q_0)$ be a generator of a cyclic subgroup $\mathrm{GU}_1(q_0^d)$.
(v) Assume that W is plus-type and write $W = W_1 \oplus W_2$ where W_1 and W_2 are totally isotropic d-spaces. Let $B_{2d} = [B, B^{-T}] \in \mathrm{SO}^+_{2d}(q_0)$ have order $q_0^d - 1$ and stabilise the spaces W_1 and W_2, acting irreducibly on both.

Let us record some straightforward properties of the elements defined in Definition 4.3.

Lemma 4.4. *Adopt the notation from Definition 4.3.*

(i) A_{2d} *has order* $q_0^d + 1$.
(ii) A_{2d} *acts irreducibly on* W.
(iii) *The eigenvalues of* A_{2d} *over* $\overline{\mathbb{F}}_{q_0}$ *are* $\lambda, \lambda^{q_0}, \ldots, \lambda^{q_0^{2d-1}}$, *for some* $\lambda \in \overline{\mathbb{F}}_{q_0}$ *of order* $q_0^d + 1$. *Moreover, these eigenvalues are distinct.*
(iv) *In cases* **S** *and* $\mathbf{S_4}$, $C_{\mathrm{Sp}_{2d}(q_0)}(A_{2d}) = \langle A_{2d} \rangle$, *and in case* **O**, $C_{\mathrm{SO}^-_{2d}(q_0)}(A_{2d}) = \langle A_{2d} \rangle$.
(v) B_{2d} *has order* $q_0^d - 1$.
(vi) *The eigenvalues of* B_{2d} *over* $\overline{\mathbb{F}}_{q_0}$ *are*

$$\mu, \mu^{-1}, \mu^{q_0}, \mu^{-q_0}, \ldots, \mu^{q_0^{d-1}}, \mu^{-q_0^{d-1}},$$

for some $\mu \in \overline{\mathbb{F}}_{q_0}$ *of order* $q_0^d - 1$. *Moreover, if* d *is odd, then these are distinct.*
(vii) *Assume that* d *is odd. In cases* **S** *and* $\mathbf{S_4}$, $C_{\mathrm{Sp}_{2d}(q_0)}(B_{2d}) = \langle B_{2d} \rangle$, *and in case* **O**, $C_{\mathrm{SO}^+_{2d}(q_0)}(B_{2d}) = \langle B_{2d} \rangle$.

Proof. See [16, Prop. 3.4.3, 3.5.4, Remarks 3.4.4, 3.5.6]. □

Recall that X is the algebraic group defined in (2.1) and σ is the Steinberg morphism defined in (2.2) or (2.6). We will define $t\theta$ as the preimage, under a Shintani map, of an element $\overline{y} \in X_\sigma$. We need to select $t\theta \in G$ in a way which allows us to control the maximal subgroups of G which contain it. Therefore, we will choose $t\theta$ such that it has the following two features, which place significant restrictions on its maximal overgroups. First, $t\theta$ should not be contained in many reducible subgroups, and second, a power of $t\theta$ should have a 1-eigenspace of large dimension in its action on the natural module for G. These two conditions will inform our choice of element $\overline{y} \in X_\sigma$.

Case	q	θ	y	Condition
S	even	φ^i	$[A_2, A_{2m-2}]$	m odd
			$[A_2, B_{2m-2}]$	m even
	odd	φ^i	$[A_2, A_{2m-2}]$	m odd
			$[A_2, B_{2m-2}]$	m even
		$\delta\varphi^i$	$[C_2, C_{2m-2}]$	m odd
			$[C_2, D_{2m-2}]$	m even
O	odd	φ^i	$[A_2, A_{2m-2}, 1]^2$	m odd
			$[A_2, B_{2m-2}, 1]^2$	m even
		$\delta\varphi^i$	$[A_2, A_{2m-2}, 1]$	m odd
			$[A_2, B_{2m-2}, 1]$	m even
$\mathbf{S_4}$	even	φ^i	A_4	
		ρ^j	A_4^ℓ	
	odd	φ^i	A_4	
		$\delta\varphi^i$	C_4	

TABLE 10. The element $t\theta \in G$ satisfies $f(t\theta) = \overline{y}$.

Table 10 partitions the possibilities for G into several cases, and, in each case, an element y is given. We will now define these elements more precisely, and we will verify that in each case $\overline{y}$ (the image of y modulo scalars) is contained in the image of the coset $T\theta$ under the relevant Shintani map.

In case **S**, the element $y \in \mathrm{GSp}_{2m}(q_0)$ is a block diagonal matrix preserving a decomposition $V = U_1 \oplus U_2$, where U_1 and U_2 are non-degenerate subspaces of dimensions 2 and $2m-2$, respectively. If $\theta = \varphi^i$ then $\overline{y} \in \mathrm{PSp}_{2m}(q_0)$, and if $\theta = \delta\varphi^i$ (so q_0 is odd) then $\overline{y} \in \mathrm{PGSp}_{2m}(q_0) \setminus \mathrm{PSp}_{2m}(q_0)$ since, by Lemma 4.1(i), $\tau(y) = \alpha$, a non-square in $\mathbb{F}_{q_0}$. Therefore, in each case, by Proposition 2.4, $\overline{y} \in f(T\theta)$.

In case **O**, the element $y \in \mathrm{SO}_{2m+1}(q_0)$ is a block diagonal matrix preserving a decomposition $V = U_1 \oplus U_2 \oplus U_3$ where U_1, U_2 and U_3 are non-degenerate subspaces of dimensions 2, $2m-2$ and 1, respectively. Moreover, U_1 is plus-type and U_2 is ε-type where $\varepsilon = (-)^m$. If $\theta = \varphi^i$ then $y \in \Omega_{2m+1}(q_0)$ since $[A_2, A_{2m-2}, 1] \in \mathrm{SO}_{2m+1}(q_0)$ and $[A_2, B_{2m-2}, 1] \in \mathrm{SO}_{2m+1}(q_0)$. However, if $\theta = \delta\varphi^i$ then $y \in \mathrm{SO}_{2m+1}(q_0) \setminus \Omega_{2m+1}(q_0)$, by Lemma 4.1. Therefore, by Proposition 2.5, $\overline{y} \in f(T\theta)$.

In case $\mathbf{S_4}$, if $\theta = \varphi^i$ then $y \in \mathrm{PSp}_4(q)$, and if $\theta = \delta\varphi^i$ then $y \in \mathrm{PGSp}_4(q) \setminus \mathrm{PSp}_4(q)$. Before defining the element y when $\theta = \rho^j$, let us record a useful number theoretic notion.

For positive integers a, k, we say that r is a *primitive prime divisor (ppd)* of $a^k - 1$ if r divides $a^k - 1$ but r does not divide $a^i - 1$ for $1 \leq i < k$. The following is a theorem of Zsigmondy [43].

Theorem 4.5. *If $k \geq 2$ and $(a, k) \notin \{(2, 6)\} \cup \{(2^l - 1, 2) \mid l \in \mathbb{N}\}$, then $a^k - 1$ has a primitive prime divisor.*

Let $\theta = \rho^j$. By Lemma 4.4(i), A_4 has order $q_0^4 - 1$. By Theorem 4.5, let r be a ppd of $q_0^4 - 1$ and let ℓ be a positive integer such that A_4^ℓ has order r. Since r divides $|Sz(q_0)| = q_0^2(q_0-1)(q_0^2+1)$, the subgroup $Sz(q_0)$ contains an element of order r. Therefore, we may assume that $y \in Sz(q_0) \leq \mathrm{Sp}_4(q_0)$. Hence, by Proposition 2.6, $\overline{y} \in f(T\theta)$.

To summarise, for each row of Table 10, we have verified that $\overline{y} \in f(T\theta)$. Therefore, we define $t\theta \in G$ as an element such that $f(t\theta) = \overline{y}$.

4.3. **Maximal subgroups.** Let $G = \langle T, \theta \rangle \in \mathcal{A}$ with $T \neq \mathrm{PSp}_4(2)'$ and $\theta \notin \mathrm{Inndiag}(T)$. Maintain the notation introduced at the opening of Section 4. For this section, fix $t\theta$ as the element defined in Table 10. The aim of this section is to study $\mathcal{M}(G, t\theta)$, the set of maximal subgroups of G which contain $t\theta$. The main result is the following.

Proposition 4.6. *The maximal subgroups of G which contain $t\theta$ are listed in Table 11, where $m(H)$ is an upper bound on the multiplicity of the subgroups of type H in $\mathcal{M}(G, t\theta)$.*

Before proving Proposition 4.6, we will first prove two results on the multiplicities of subgroups in $\mathcal{M}(G, t\theta)$. Recall that $G_1 = X_{\sigma^e}{:}\langle\sigma\rangle$.

Proposition 4.7. *Maximal geometric subgroups of G of the same type are G-conjugate except for subfield subgroups over $\mathbb{F}_{q^{1/2}}$, in which case there are at most two G-classes but exactly one G_1-class.*

Proof. Note that q is not prime since $\theta \notin \mathrm{Inndiag}(T)$. If $n \leq 12$, then the result follows from the tables in [5, Chapter 8]. Now suppose that $n \geq 13$. Let H be a maximal geometric subgroup of G. By [32, Theorem 3.1.1], the subgroups of the same type as H are $\mathrm{Aut}(T)$-conjugate to H. Moreover, the group $\mathrm{Aut}(T)/T$ acts on $\{H_1, \ldots, H_c\}$, a set of representatives of the T-classes of subgroups of $\mathrm{Aut}(T)$ of the same type as H. Let $\pi\colon \mathrm{Aut}(T)/T \to S_c$ be the permutation representation of this action. By [32, Tables 3.5C & 3.5D], $c = 1$ and the G-classes of subgroups are precisely the $\mathrm{Aut}(T)$-classes, except for the exceptional case in the statement. In this case, by [32, Tables 3.5C & 3.5D], $c = 2$ and the $\mathrm{Aut}(T)$-class splits into two T-classes. By [32, Table 3.5G], δ is not contained in the kernel of π. Therefore, δ permutes the two T-classes. Since $\delta \in G_1$, all subfield subgroups over $\mathbb{F}_{q^{1/2}}$ are G_1-conjugate. □

We will now present a consequence of Proposition 2.7 which provides a general bound on the multiplicities of subgroups in $\mathcal{M}(G, t\theta)$.

Corollary 4.8. *Let H be a maximal subgroup of G and let $t\theta \in G$ be the element defined in Table 10. Then there are at most N subgroups of type H in $\mathcal{M}(G, t\theta)$, where*

$$N = \begin{cases} (q_0+1)(q_0^{m-1}+1) & \text{in case } \mathbf{S} \\ q_0(q_0+1)(q_0^{m-1}+1) & \text{in case } \mathbf{O} \\ q_0^2+1 & \text{in case } \mathbf{S_4} \text{ and } \theta \text{ is a field automorphism} \\ q_0+\sqrt{2q_0}+1 & \text{in case } \mathbf{S_4} \text{ and } \theta \text{ is a graph-field automorphism} \end{cases}$$

Proof. By Proposition 4.7, the subgroups of type H are G_1-conjugate. Therefore, the number of subgroups of type H in $\mathcal{M}(G, t\theta)$ is at most $|C_{X_\sigma}(f(t\theta))|$, by Proposition 2.7.

First consider case **O**, and cases **S** and $\mathbf{S_4}$ when q is even. Here, X_σ is a matrix group and $f(t\theta)$ is X-conjugate to y. Therefore, by Lemma 4.4,

$$|C_{X_\sigma}(f(t\theta))| = |C_{X_\sigma}(y)| \leq N.$$

Now consider cases **S** and $\mathbf{S_4}$ when q is odd. Thus, $T = \mathrm{PSp}_{2m}(q_0)$, $X_\sigma = \mathrm{PGSp}_{2m}(q_0)$ and $y \in \mathrm{Sp}_{2m}(q_0)$ with $|C_{\mathrm{Sp}_{2m}(q_0)}(y)| \leq N$. By considering the eigenvalues of y, we see that y is not T-conjugate to $-y$. Hence, $|C_{\mathrm{Sp}_{2m}(q_0)}(y)| = 2|C_T(\overline{y})|$. Therefore,

$$|C_{X_\sigma}(f(t\theta))| \leq |C_{X_\sigma}(y)| \leq 2|C_T(\overline{y})| = |C_{\mathrm{Sp}_{2m}(q_0)}(y)| \leq N. \qquad \square$$

We will now prove Proposition 4.6. Let $H \in \mathcal{M}(G, t\theta)$. If $T \leq H$, then $\theta \in H$, since $t\theta \in H$. Thus $H = G$: a contradiction. Hence, $T \not\leq H$, so, by [32, Main Theorem], H lies in one of the geometric families $\mathcal{C}_1, \ldots, \mathcal{C}_8$ or is an almost simple irreducible group in the $\mathcal{S}$ collection. We will prove Proposition 4.6 in three parts, considering reducible, imprimitive and primitive subgroups in turn. We begin with the reducible subgroups.

Case	θ	Type of H	$m(H)$	Conditions
S	any	$\mathrm{Sp}_2(q) \times \mathrm{Sp}_{2m-2}(q)$	1	
		P_{m-1}	2	m even
		$\mathrm{Sp}_2(q) \wr S_m$	1	
		$\mathrm{GL}_m(q).2$	$2^{(m-1,e)}$	q odd & *
		$\mathrm{Sp}_m(q) \wr S_2$	$\frac{1}{2}\binom{m}{\frac{m}{2}}$	m even
		$\mathrm{Sp}_{2m}(q^{1/l})$	$\begin{cases} e^2 & \text{if } l = e \\ q_0^m + q_0^{m-1} + q_0 + 1 & \text{if } l \neq e \end{cases}$	
		$\mathrm{O}^{\varepsilon}_{2m}(q)$	1	q even
O	any	$\mathrm{O}^{\varepsilon}_{2m}(q)$	1	
		$\mathrm{O}^{\varepsilon}_2(q) \times \mathrm{O}_{2m-1}(q)$	1	
		$\mathrm{O}_3(q) \times \mathrm{O}^{\varepsilon}_{2m-2}(q)$	1	
		P_{m-1}	2	m even
		$\mathrm{O}_{2m+1}(q^{1/l})$	$\begin{cases} e^3 & \text{if } l = e \\ q_0^{m+1} + q_0^m + q_0^2 + q_0 & \text{if } l \neq e \end{cases}$	
$\mathbf{S_4}$	not g-f	$\mathrm{Sp}_2(q) \wr S_2$	1	e even
		$\mathrm{GL}_2(q).2$	$q_0^2 + 1$	q odd
		$\mathrm{Sp}_2(q^2)$	1	e odd
		$\mathrm{GU}_2(q)$	$q_0^2 + 1$	q odd
		$\mathrm{Sp}_4(q^{1/l})$	$\begin{cases} e & \text{if } l = e \\ q_0^2 + 1 & \text{if } l \neq e \end{cases}$	
		$\mathrm{O}^{\varepsilon}_4(q)$	1	q even
		$Sz(q)$	$q_0^2 + 1$	q even
		$\mathrm{SL}_2(q)$	$q_0^2 + 1$	q odd
$\mathbf{S_4}$	g-f	$\mathrm{O}^+_2(q) \wr S_2$	$q_0 + \sqrt{2q_0} + 1$	$e \neq 1$
		$\mathrm{O}^-_2(q) \wr S_2$	$q_0 + \sqrt{2q_0} + 1$	$e \neq 1$
		$\mathrm{O}^-_2(q^2)$	$q_0 + \sqrt{2q_0} + 1$	
		$\mathrm{Sp}_4(q^{1/l})$	$\begin{cases} e & \text{if } l = e \\ q_0 + \sqrt{2q_0} + 1 & \text{if } l \neq e \end{cases}$	
		$Sz(q)$	$\begin{cases} 1 & \text{if } e = 1 \\ q_0 + \sqrt{2q_0} + 1 & \text{if } e \neq 1 \end{cases}$	

TABLE 11. Description of $\mathcal{M}(G, t\theta)$
(g-f = graph-field; l is a prime divisor of e; $\varepsilon \in \{+, -\}$; * for odd m, $\frac{2m-2}{(2m-2,e)}$ is odd)

Proposition 4.9. *Proposition 4.6 is true for reducible subgroups.*

Proof. First consider parabolic subgroups and, for cases **S** and $\mathbf{S_4}$, the stabilisers of non-degenerate subspaces. (That is, let us postpone the study of stabilisers of non-degenerate subspaces in case **O**.) By Proposition 2.8, the maximal reducible subgroups of G which contain $t\theta$ correspond to the maximal reducible subgroups of X_σ which contain $f(t\theta)$. Since $f(t\theta)$ is X-conjugate to $\overline{y}$, the result follows by inspecting the maximal reducible overgroups of $\overline{y}$ in X_σ.

Now consider stabilisers of non-degenerate subspaces in case **O**. These subgroups are disconnected, so we alter our approach slightly. Let $L = \langle \mathrm{SL}_n(q), \theta \rangle$ and $Y = \mathrm{SL}_n(\overline{\mathbb{F}}_q)$. Observe that $t\theta \in G \leq L$ and $f(t\theta) \in X_\sigma \leq Y_\sigma$. Therefore, by considering the maximal overgroups of $\overline{y}$ in X_σ, [17, Corollary 2.15] (the analogue of Proposition 2.8 in the linear case) demonstrates that $t\theta$ is contained in exactly one subgroup of L of types $\mathrm{SL}_{2m}(q)$, $\mathrm{SL}_2(q) \times \mathrm{SL}_{2m-1}(q)$ and $\mathrm{SL}_3(q) \times \mathrm{SL}_{2m-2}(q)$. In particular, the only possibilities for maximal reducible subgroups of G which contain $t\theta$ are those listed in Table 11. □

Before considering the imprimitive subgroups, we state the following elementary lemma.

Lemma 4.10. *Let G be a finite group and let H be a self-normalising subgroup of G. Then for all $x \in G$, the number of G-conjugates of H which contain x is*

$$\frac{|G|}{|H|}\frac{|x^G \cap H|}{|x^G|}.$$

A subgroup of $\mathrm{GL}_n(q)$ is *imprimitive* if it stabilises a direct sum decomposition

$$\mathbb{F}_q^n = V_1 \oplus \cdots \oplus V_k,$$

for some $k > 1$, possibly permuting the summands. It is *primitive* otherwise.

Proposition 4.11. *Proposition 4.6 is true for irreducible imprimitive subgroups.*

Proof. Consider the cases **S** and **O**. Recall that n is either $2m$ or $2m+1$, depending on the case, and $V = \mathbb{F}_q^n$. Let $H \leq G$ be a maximal imprimitive subgroup of G containing $t\theta$. Then H is the stabiliser in G of the direct sum decomposition

$$V = V_1 \oplus \cdots \oplus V_k \tag{4.1}$$

where $k \geq 2$ divides n and $\dim V_i = n/k$ for all $i \in \{1, \ldots, k\}$. For the maximality of H, we require that either each V_i is non-degenerate or that, in case **S**, $k = 2$ and each V_i is totally isotropic. In either case $\dim V_i \geq 2$ and, consequently, $k \leq m$. (That $\dim V_i \neq 1$ in the case **O** follows by the maximality of H since q is not prime; see [32, Table 3.5D].)

By construction, a suitable power of $t\theta$ lifts to an element x of order r, a ppd of $q_0^\beta - 1$ where $\beta = (2m-2)/(m,2)$. (Since $\beta \notin \{2, 6\}$, a ppd of $q_0^\beta - 1$ exists by Theorem 4.5.) We claim that x stabilises each summand in (4.1). Suppose that x induces a non-trivial permutation π on the summands. Then π is a non-trivial product of r-cycles, so $r \leq k$. However, r is a ppd of $q_0^\beta - 1$, so β divides $r-1$ and so $\beta+1 \leq r$. Hence, $\beta+1 \leq r \leq k \leq m$. If m is odd, then this is a contradiction. If m is even, then $r = k = m$. However, r is odd and m is even: another contradiction. Therefore, x stabilises each summand in (4.1).

For $K = \overline{\mathbb{F}}_q$, let $\overline{V} = \langle u_1, \ldots, u_n \rangle_K$ and extend the semilinear action of G on V to an action on $\overline{V}$ by defining, for each $g \in G \cap \mathrm{GL}(V)$ and $\alpha_1, \ldots, \alpha_n \in K$,

$$(\alpha_1 u_1 + \cdots + \alpha_n u_n) g\sigma = \alpha_1^{q_0}(u_1 g) + \cdots + \alpha_n^{q_0}(u_n g).$$

Then the decomposition in (4.1) gives rise to the corresponding decomposition

$$\overline{V} = \overline{V}_1 \oplus \cdots \oplus \overline{V}_k. \tag{4.2}$$

Recall that $f(t\theta)$ lifts to the element y in Table 10. We will show that y stabilises each summand in (4.1). Suppose that x acts non-trivially on V_i and $1 \neq \mu \in K$ is an eigenvalue of x with μ-eigenvector $v \in \overline{V}_i$. Since x and y commute,

$$(vy)x = (vx)y = (\mu v)y = \mu(vy).$$

That is, vy is a μ-eigenvector of x. However, all non-trivial eigenvalues of x have multiplicity one, so $vy \in \overline{V}_i$. Since y preserves the decomposition (4.2), y stabilises $\overline{V}_i$. However, V is y-stable, so y stabilises $\overline{V}_i \cap V = V_i$. Since the 1-eigenspace of x is at most 3-dimensional and $\dim V_i \geq 2$, x acts non-trivially on at least $k-1$ summands. Therefore, y stabilises at least $k-1$ summands and, hence, all k summands.

Now we will find subspaces which are stabilised by $t\theta$. By Lemma 4.4, the eigenvalue set of y is $\{\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{q_0}, \ldots, \lambda_2^{q_0^{2m-3}}\}$. Let $\overline{V}_i$ contain the λ_1-eigenspace of y and $\overline{V}_j$ contain the $\lambda_1^{q_0}$-eigenspace of y. Since y and $t\theta$ commute, if $v \in \overline{V}_i$ is a λ_1-eigenvector for y, then

$$(vt\theta)y = (vy)(t\theta) = (\lambda_1 v)(t\theta) = \lambda_1^{q_0}(vt\theta),$$

so $vt\theta$ is a $\lambda_1^{q_0}$-eigenvector for y. However, $\lambda_1^{q_0}$ has multiplicity one so $vt\theta \in \overline{V}_j$. Similarly, if $w \in \overline{V}_j$ is a $\lambda_1^{q_0}$-eigenvector, then $w\theta$ is a λ_1-eigenvector, so $wt\theta \in \overline{V}_i$. Thus, since y preserves (4.2), $t\theta$ stabilises $\overline{V}_i + \overline{V}_j$, and, since V is $t\theta$-stable, $t\theta$ stabilises $V_i + V_j$.

First consider case **S**. If $i \neq j$, then $t\theta$ stabilises $V_i \oplus V_j$, so, by Proposition 4.9, $2\dim V_i = 4m/k \in \{2, 2m-2, 2m\}$. However, $m \geq 3$ and $2m/k$ divides $2m$, so $k = 2$. Similarly, if $i = j$ then $t\theta$ stabilises V_i, so $\dim V_i = 2m/k \in \{2, m-1, m+1, 2m-2\}$. Since $2m/k$ divides $2m$, $\dim V_i = 2$. By a similar line of reasoning, in case **O**, we must have that $\dim V_i = 3$. Then y is a block diagonal matrix $[M_1, \ldots, M_k]$ where $M_i \in \mathrm{SO}_3(q)$. Hence, M_i has eigenvalues $\lambda_i, \lambda_i', 1$, contradicting 1 being an eigenvalue of y of multiplicity 1.

To summarise, we have established that in case **O** no imprimitive irreducible subgroups arise, and in case **S** either $k = 2$ or $k = m$. We will now obtain an upper bound on the number of such subgroups in case **S**. To do this, we will use Lemma 4.10.

Let H be the stabiliser in G of the decomposition (4.1) and let B be the subgroup of H stabilising each summand. Recall $\overline{y} \in B$ since y stabilises each summand.

Case 1: $k = m$

With respect to a suitable basis, y is a block diagonal matrix $[M_1, \ldots, M_m]$ where $M_i \in \mathrm{GSp}_2(q)$. Since the eigenvalues of y are distinct, for $\varepsilon_i \in \{+, -\}$,

$$|C_G(\overline{y})| = |\mathrm{GL}_1^{\varepsilon_1}(q)| \cdots |\mathrm{GL}_1^{\varepsilon_m}(q)| = |C_B(\overline{y})| = |C_H(\overline{y})|.$$

Moreover, $\overline{y}^G \cap H$ splits into $m!$ B-classes (corresponding to reordering $M_1, \ldots, M_m$), which are fused in H. So $\overline{y}^G \cap H = \overline{y}^H$, and, by Lemma 4.10, $\overline{y}$ is contained in exactly one G-conjugate of H. Hence, $t\theta$ is contained in at most one G-conjugate of H.

Case 2: $k = 2$ **and** V_1, V_2 **are non-degenerate**

Here m is even. Therefore, $y = [A_2, B_{2m-2}]$. Since $\overline{y} \in B$, with respect to a suitable basis, $y = [M, N]$ where $M, N \in \mathrm{GSp}_m(q)$. By Lemma 4.4, the eigenvalue set of y is $\{\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{-1}, \ldots, \lambda_2^{q_0^{m-2}}, \lambda_2^{-q_0^{m-2}}\}$. Since the eigenvalues of M are closed under taking inverses and since $\lambda_1^{q_0} = \lambda_1^{-1}$, we may assume that λ_1 and $\lambda_1^{q_0}$ are eigenvalues of M.

Let $d = (m-1, e)$ and $b = (m-1)/d$. The eigenvalue set of y is $\Lambda \cup \Lambda_1 \cup \cdots \cup \Lambda_d$, where $\Lambda = \{\lambda_1, \lambda_1^{q_0}\}$ and $\Lambda_i = \{\lambda_2^{q_0^i}, \lambda_2^{-q_0^i}, \ldots, (\lambda_2^{q_0^i})^{q^{b-1}}, (\lambda_2^{q_0^i})^{-q^{b-1}}\}$, for each i. Since the eigenvalue sets of M and N are closed under the map $\alpha \mapsto \alpha^q$, the eigenvalue set of M is $\Lambda \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_l}$ and the eigenvalue set of N is $\Lambda_{a_{l+1}} \cup \cdots \cup \Lambda_{a_d}$ where $l \geq 1$ and $\{a_1, \ldots, a_d\} = \{1, \ldots, d\}$. Therefore, b divides m and $m-2$. Thus, b divides 2, so $\Lambda_i = \{\lambda_2^{q_0^i}, \lambda_2^{-q_0^i}\}$, for each i. In particular, $d = m-1$.

By arguing as in Case 1, we can show that $|C_G(\overline{y})| = |C_H(\overline{y})|$ and that $\overline{y}^G \cap H$ splits into $\binom{m}{\frac{m}{2}}$ B-classes (corresponding to choosing $m/2$ of $\Lambda, \Lambda_1, \ldots, \Lambda_{m-1}$ for M) which fuse to $\frac{1}{2}\binom{m}{\frac{m}{2}}$ H-classes. So $\overline{y}$, and thus $t\theta$, lies in at most $\frac{1}{2}\binom{m}{\frac{m}{2}}$ G-conjugates of H.

Case 3: $k = 2$ and V_1, V_2 are totally isotropic

Assume that m is odd. Then $y = [A_2, A_{2m-2}]$, and, since $\overline{y} \in B$, $y = [M, M^{-T}]$ for $M \in \mathrm{GL}_m(q)$. By Lemma 4.4, y has eigenvalue set $\{\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{q_0}, \ldots, \lambda_2^{q_0^{2m-2}}\}$. Since $\lambda_1^{q_0} = \lambda_1^{-1}$, assume that λ_1 is an eigenvalue of M and $\lambda_1^{q_0}$ is an eigenvalue of M^{-T}.

Let $d = (2m-2, e)$ and $b = (2m-2)/d$. The eigenvalue set of y is $\Lambda \cup \Lambda_1 \cup \cdots \cup \Lambda_d$, where $\Lambda = \{\lambda_1, \lambda_1^{q_0}\}$ and where $\Lambda_0, \ldots, \Lambda_d$ are the orbits of the eigenvalue set of A_{2m-2} under the map $\alpha \mapsto \alpha^q$. Since the eigenvalue set of M is closed under the map $\alpha \mapsto \alpha^q$, the eigenvalue set of M is $\{\lambda_1\} \cup \Lambda_{a_1} \cup \cdots \cup \Lambda_{a_l}$ where $l = \frac{d}{2}$ and where $a_1, \ldots, a_l \in \{1, \ldots, d\}$ are distinct. If b is even, then $\Lambda_i^{-1} = \Lambda_i$, for each i. However, this contradicts the distinctness of the eigenvalues of y. Therefore, b is odd.

As in Case 1, we can show that $|C_G(\overline{y})| = |C_H(\overline{y})|$. Additionally, if $N \in \mathrm{GL}_n(q)$ has eigenvalue set $\{\lambda_1^{\varepsilon}\} \cup \Lambda_1^{\varepsilon_1} \cup \cdots \cup \Lambda_l^{\varepsilon_l}$, then a G-conjugate of y is B-conjugate to $[N, N^{-T}]$ for exactly one choice of $(\varepsilon, \varepsilon_1, \ldots, \varepsilon_l) \in \{+, -\}^{l+1}$. Therefore, y^G splits into 2^{l+1} B-classes, which fuse to 2^l H-classes. So y, and thus $t\theta$, lies in at most $2^l = 2^{(2m-2,e)/2} \leq 2^{(m-1,e)}$ G-conjugates of H. When m is even, the analysis is very similar and we omit the details.

We have now established Proposition 4.6 in cases **S** and **O**. For $\mathbf{S_4}$ the argument is similar but briefer. Let $T = \mathrm{PSp}_4(q)$ and assume that θ is not a graph-field automorphism. The possible types of irreducible imprimitive subgroups are $\mathrm{Sp}_2(q) \wr S_2$ and $\mathrm{GL}_2(q).2$. In order to prove Proposition 4.6, we need to show that if $t\theta$ is contained in a subgroup of type $\mathrm{Sp}_2(q) \wr S_2$, then e is even and $t\theta$ is contained in a unique such subgroup.

Suppose that $t\theta$ preserves a decomposition $V = V_1 \oplus V_2$ where V_1 and V_2 are non-degenerate 2-spaces. Let H be the stabiliser in G of this decomposition, and let B be the index two subgroup of H stabilising each summand. Recall that a suitable power of $t\theta$ lifts to an X-conjugate of an element $g \in \mathrm{Sp}_4(q_0)$ which has distinct eigenvalues and whose order is a ppd of $q_0^4 - 1$. (Note that g is y, y^ℓ or $y^{(q_0-1)\ell}$, depending on θ; see Table 10.) Since $t\theta$ preserves the direct sum decomposition so does g. However, g has odd order, so g stabilises each summand. Therefore, each of the eigenvalues of g is contained in $\mathbb{F}_{q^2}$. In particular, since $q = q_0^e$ and the eigenvalues of g are not contained in a proper subfield of $\mathbb{F}_{q_0^4}$, it must be that e is even. Now, for some $M, N \in \mathrm{Sp}_2(q_0)$, $g = [M, N]$, and

$$|C_G(g)| = |\mathrm{GL}_1^{\varepsilon}(q)||\mathrm{GL}_1^{\varepsilon}(q)| = |C_B(g)| = |C_H(g)|.$$

Moreover, as in Case 1 above, $g^G \cap H = g^H$. Therefore, g, and thus $t\theta$, lies in at most one G-conjugate of H. Together with Corollary 4.8, this completes the proof. □

Before proving Proposition 4.6 for primitive subgroups, we will present further results on the multiplicities of subgroups. The first of these results, which pertains to subfield subgroups, is a generalisation of [17, Prop. 2.16(ii)] and the proof is very similar.

Proposition 4.12. *Let $g\sigma \in G$ be such that $f(g\sigma)$ lifts to $[M_1, \ldots, M_k]$ where for each i, $M_i = A_{d_i}$, $M_i = B_{2d_i}$ or $M_i = I_1$, and $d_1, \ldots, d_k$ are distinct. Let H be a maximal subfield subgroup of G over the field $\mathbb{F}_{q_0}$. Then $g\sigma$ is contained in at most e^k G_1-conjugates of H.*

Corollary 4.13. *Suppose that e is prime and let H be a maximal subfield subgroup of G over the field $\mathbb{F}_{q_0}$. Let $t\theta \in G$ be the element defined in Table 10. Then there are at most e^k subgroups of type H in $\mathcal{M}(G, t\theta)$ where $k = 1$ in $\mathbf{S_4}$, $k = 2$ in $\mathbf{S}$ and $k = 3$ in $\mathbf{O}$.*

Proof. By Proposition 4.7, all maximal subfield subgroups over $\mathbb{F}_{q_0}$ are G_1-conjugate. The result now follows from Proposition 4.12 and the choice of element $f(t\theta)$ in Table 10. □

The following is an application of Proposition 2.10.

Corollary 4.14. *Let q be even, $T = \mathrm{Sp}_{2m}(q)$ and θ a field automorphism. Then the element $t\theta \in G$, defined in Table 10, is contained in exactly one subgroup of G of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$.*

Proof. By Proposition 2.10, it suffices to show that y is contained in exactly one subgroup of $\mathrm{Sp}_{2m}(q_0)$ of type $\mathrm{O}^\varepsilon_{2m}(q_0)$. If $m \geq 3$ is odd, then y has order $(q_0+1)(q_0^{m-1}+1)$ and, hence, is not contained in a subgroup of type $\mathrm{O}^-_{2m}(q_0)$. Since the $\mathrm{Sp}_{2m}(q_0)$- and $\mathrm{O}^+_{2m}(q_0)$-conjugacy of semisimple elements of odd order is determined by eigenvalues, $y^G \cap H = y^H$. Moreover,

$$|C_{\mathrm{Sp}_{2m}(q_0)}(y)| = (q_0+1)(q_0^{m-1}+1) = |C_{\mathrm{O}^+_{2m}(q_0)}(y)|$$

(see [16, Appendix B]). Thus, by Lemma 4.10, y is contained in exactly one subgroup of type $\mathrm{O}^-_{2m}(q_0)$. Similar arguments apply when $m \geq 2$ is even, and we omit the details. □

We are now in a position to complete the proof of Proposition 4.6 in cases **S** and **O**.

Proposition 4.15. *In cases* **S** *and* **O**, *Proposition 4.6 is true for irreducible primitive subgroups.*

Proof. The stated upper bounds on the multiplicities follow from Corollaries 4.8, 4.13 and 4.14. Therefore, we will focus on determining the types of subgroups which arise. Let $H \in \mathcal{M}(G, t\theta)$ be irreducible and primitive. By [32, Main Theorem], H lies in one of the geometric families $\mathcal{C}_3, \ldots, \mathcal{C}_8$ or is an almost simple irreducible group in the $\mathcal{S}$ collection. By construction, a power of $t\theta$ is X-conjugate to $\overline{y}$. Moreover, by the choice of $\overline{y}$, a suitable power of $t\theta$ is X-conjugate to an element z of odd prime order which lifts to a matrix $[M, I_{n-2}]$, where $M \in \mathrm{GL}_2(q_0)$.

Consider $\mathcal{C}_3$ subgroups. By [36, Lemma 4.2], if $g \in G$ is contained in a field extension subgroup of degree k, then $\nu(g) \geq k$ (see Notation 3.1). However, $\nu(z) = 2$, so $k = 2$. Hence, if $H \in \mathcal{C}_3$, then $T = \mathrm{PSp}_{2m}(q)$ and either H has type $\mathrm{Sp}_m(q^2)$, or q is odd and H has type $\mathrm{GU}_m(q)$. We will show that neither of these possibilities occur.

First consider subgroups of type $\mathrm{Sp}_m(q^2)$. A preimage of $z = [\lambda, \lambda^{q_0}, I_{2m-2}]$ in $\mathrm{Sp}_m(q^2)$ has exactly one non-trivial eigenvalue, by [16, Lemma 5.3.11]. However, this is impossible, so z is not contained in a subgroup of type $\mathrm{Sp}_m(q^2)$. Now consider subgroups of type $\mathrm{GU}_m(q)$. If m is even, then over $\mathbb{F}_{q_0}$ a power of y is $[I_2, B_{2m-2}]$, which, by [16, Lemma 5.3.2], is not contained in a subgroup of type $\mathrm{GU}_m(q)$ since $m-1$ is odd. If e is even, then over $\mathbb{F}_{q_0}$ a power of y is $[A_2, I_{2m-2}]$, which over $\mathbb{F}_q$ has the form $[B_2, I_{2m-2}]$, which, as above, is not contained in H. Finally, if m and e are odd, then over $\mathbb{F}_{q_0}$ a power of y is $[I_2, A_{2m-2}]$, which over $\mathbb{F}_q$ has the form $[I_2, A_{2d_1}, \ldots, A_{2d_k}]$, where d_i is even since $m-1$ is even and e is odd. By [16, Lemma 5.3.2], this element is not contained H since d_i is even.

Now let us turn to $\mathcal{C}_4$ subgroups. By [36, Lemma 3.7], if g has prime order and preserves a tensor product decomposition $V = U_1 \otimes U_2$, then $\nu(g) \geq \max\{\dim U_1, \dim U_2\}$. However, $\nu(z) = 2$, so $\dim U_1, \dim U_2 \leq 2$. Hence, $n \leq 4$: a contradiction. Therefore, $H \notin \mathcal{C}_4$.

Write $T = \Sigma_n(q)$ where $\Sigma \in \{\mathrm{PSp}, \Omega\}$. If $H \in \mathcal{C}_5$, then H has type $\Sigma_n(q_1)$ with $q = q_1^l$ for a prime l. Since $f(t\theta)$ has order divisible by a ppd of $q_0^{(2m-2)/(m,2)} - 1$, $f(t\theta) \notin \Sigma_n(F)$ for any proper subfield F of $\mathbb{F}_{q_0}$. However, $f(t\theta) \in \Sigma_n(q_1) \cap \Sigma_n(q_0) \leq \Sigma_n(\mathbb{F}_{q_0} \cap \mathbb{F}_{q_1})$, so $\mathbb{F}_{q_0} \cap \mathbb{F}_{q_1} = \mathbb{F}_{q_0}$. That is, $\mathbb{F}_{q_0} \leq \mathbb{F}_{q_1} \leq \mathbb{F}_q$. So $q_1 = q_0^d$ for some d.

Since q is not prime, $H \notin \mathcal{C}_6$.

We treat $\mathcal{C}_7$ similarly to $\mathcal{C}_4$. By [12, Lemma 7.1], if g has prime order and preserves $V = U_1 \otimes \cdots \otimes U_t$ where $\dim U_1 = \cdots = \dim U_t = a$, then $\nu(g) \geq a^{t/2}$. However, $\nu(z) = 2$, so $a = 1$ or $(a, t) = (2, 2)$. Hence, $n \leq 4$: a contradiction. Therefore, $H \notin \mathcal{C}_7$.

If $H \in \mathcal{C}_8$ then $T = \mathrm{Sp}_{2m}(q)$, q is even and H has type $\mathrm{O}^{\varepsilon}_{2m}(q)$ for $\varepsilon \in \{+,-\}$.

It remains to consider the $\mathcal{S}$ family. By [29, Theorem 7.1], since $n \geq 6$, if $H \in \mathcal{S}$, then $\nu(g) > 2$ for all $g \in H$ or H belongs to a known list of exceptions (see [14, Table 2.3], for a convenient list of the exceptions). Since q is not prime, H is not an alternating or symmetric group acting on the fully deleted permutation module. Therefore, since $\nu(z) = 2$, the possibilities are

(i) $T = \mathrm{PSp}_6(q)$ and q odd: $H = J_2$;
(ii) $T = \mathrm{Sp}_6(q)$ (q even) or $T = \Omega_7(q)$: $H = G_2(q)'$.

First consider case (i). The order of y is $l = \mathrm{lcm}(q_0+1, q_0^2+1)$. If $q_0 \equiv 1 \pmod 4$, then $y^{l/2} = -I_6$ and $\overline{y}$ has order $l/2 \geq \mathrm{lcm}(5+1, 5^2+1)/2 = 39$. Otherwise, $\overline{y}$ has order $l \geq \mathrm{lcm}(3+1, 3^2+1) = 20$. In either case, $\overline{y}$ is not contained in a subgroup of type J_2 since the maximum order of an element of J_2 is 15 (see [20]).

Now consider case (ii). Assume that $T = \Omega_7(q)$; a very similar argument applies to $\mathrm{Sp}_6(q)$. A suitable power of $t\theta$ is an X-conjugate of $g = [\lambda_1, \lambda_1^{q_0}, \lambda_2, \lambda_2^{q_0}, \lambda_2^{q_0^2}, \lambda_2^{q_0^3}, 1]$ where $\lambda_1 \in \mathbb{F}_{q_0^2}$ has order q_0+1 and $\lambda_2 \in \mathbb{F}_{q_0^4}$ has order q_0^2+1. (Either $g = y$ or $g = y^{q-1}$, depending on θ; see Table 10.) It is well-known that $\mathrm{SL}_3(q) \leq G_2(q)$ and that the restriction of V to $\mathrm{SL}_3(q)$ is $U \oplus U^* \oplus 0$ where U is the natural $\mathrm{SL}_3(q)$ module and 0 is the trivial module. Therefore, $g = [\alpha_1, \alpha_2, \alpha_3, \alpha_1^{-1}, \alpha_2^{-1}, \alpha_3^{-1}, 1]$. By the orders of the eigenvalues, without loss of generality, let $\alpha_1 = \lambda_1$ and $\alpha_2 = \lambda_2$. Since $\lambda_2^{-1} = \lambda_2^{q_0^2}$ we must have either: (a) $\alpha_3 = \lambda_2^{q_0}$ or (b) $\alpha_3 = \lambda_2^{q_0^3}$. Since $[\alpha_1, \alpha_2, \alpha_3] \in \mathrm{SL}_3(q)$, $\alpha_1\alpha_2\alpha_3 = 1$. If (a) holds, then

$$\lambda_1^{q_0} = \lambda_1^{-1} = \alpha_1^{-1} = \alpha_2\alpha_3 = \lambda_2\lambda_2^{q_0} = \lambda_2^{1+q_0}$$

$$\lambda_1 = \alpha_1 = (\alpha_2\alpha_3)^{-1} = \lambda_2^{-1}\lambda_2^{-q_0} = \lambda_2^{q_0^2}\lambda_2^{q_0^3} = \lambda_2^{q_0^2+q_0^3}.$$

Therefore, $\lambda_1^{q_0^2} = (\lambda_1^{q_0})^{q_0} = \lambda_2^{q_0+q_0^2}$. Since $\lambda_1 \in \mathbb{F}_{q_0^2}$, $\lambda_1 = \lambda_1^{q_0^2}$, so

$$\lambda_1^{q_0} = (\lambda_1^{q_0^2})^{q_0} = (\lambda_2^{q_0+q_0^2})^{q_0} = \lambda_2^{q_0^2+q_0^3} = \lambda_1.$$

Therefore, $\lambda_1 \in \mathbb{F}_{q_0}$: a contradiction. Case (b) is similar. Hence, H is not $G_2(q)$. This completes the proof. □

For the case $\mathbf{S_4}$ we need two further results on subgroup multiplicities.

Proposition 4.16. *Let q be even, $T = \mathrm{Sp}_4(q)$ and θ an involutory graph-field automorphism. Then the element $t\theta \in G$, defined in Table 10, is contained in exactly one subgroup of G of type $Sz(q)$.*

Proof. By [5, Table 8.14], there is a unique G-class of subgroups of type $Sz(q)$. Let $H = C_G(\theta) = C_T(\theta) \times \langle\theta\rangle \cong Sz(q) \times \langle\theta\rangle$. We need to show that $t\theta$ is contained in exactly one G-conjugate of H. Thus, if we assume that $t\theta \in H$, by Lemma 4.10, it suffices to show that $|C_G(t\theta)| = |C_H(t\theta)|$ and $(t\theta)^G \cap H = (t\theta)^H$.

Let us first show that $|C_G(t\theta)| = |C_H(t\theta)|$. By Proposition 2.6, the Shintani map

$$f\colon \{(g\theta)^T \mid t \in T\} \to \{x^{Sz(q)} \mid x \in Sz(q)\}$$

is defined as $f(g\theta) = a^{-1}(g\theta)^2 a$ where $a^{-\theta^{-1}}a = g$. By Theorem 2.2(ii),

$$|C_G(t\theta)| = 2|C_T(t\theta)| = 2|C_{Sz(q)}(f(t\theta))|.$$

By construction, $f(t\theta) \in Sz(q)$ has order a ppd r of q^4-1. Since r divides $q + \varepsilon\sqrt{2q} + 1$ for some $\varepsilon \in \{1,-1\}$, by [41, Prop. 16],

$$|C_{Sz(q)}(x)| = q + \varepsilon\sqrt{2q} + 1,$$

for every element $x \in Sz(q)$ of order r. Since $t\theta$ has order $2r$, t has order r and

$$2|C_{Sz(q)}(f(t\theta))| = 2(q + \varepsilon\sqrt{2q} + 1) = 2|C_{C_T(\theta)}(t\theta)| = |C_H(t\theta)|.$$

We will now prove that $(t\theta)^G \cap H = (t\theta)^H$. Let $s\theta \in H$ be G-conjugate to $t\theta$. We will first show that s and t are T-conjugate. By Remark 2.3(ii), $s\theta$ and $t\theta$ are T-conjugate. Therefore, $s^2 = (s\theta)^2$ and $t^2 = (t\theta)^2$ are T-conjugate. Record that $s, t \in C_T(\theta) \leq T$ have order r. Since r is odd, the square map on T permutes the T-classes of order r. Therefore, since s^2 and t^2 are T-conjugate, s and t are T-conjugate.

We will now verify that $s\theta$ and $t\theta$ are $C_T(\theta)$-conjugate. Observe that it suffices to show that s and t are $C_T(\theta)$-conjugate. Since s and t are T-conjugate it suffices to show that no two $C_T(\theta)$-classes of elements of order r are fused into one T-class. Since r does not divide $|T : C_T(\theta)| = q^2(q-1)(q^2-1)$, every element of T of order r is T-conjugate to an element of $C_T(\theta)$. Hence, it suffices to verify that there are the same number of classes of elements of order r in $C_T(\theta) \cong Sz(q)$ and $T \cong \mathrm{Sp}_4(q)$.

First consider $Sz(q)$. Let $\mathcal{A}$ be the set of centralisers of elements of order r in $Sz(q)$. By [41, Prop. 16], for all $A \in \mathcal{A}$, $|A| = q + \varepsilon\sqrt{2q} + 1$ and $C_{Sz(q)}(A) = A$. In particular, two members of $\mathcal{A}$ are either equal or intersect trivially. Moreover, by [41, Theorem 9], all members of $\mathcal{A}$ are $Sz(q)$-conjugate. Since $|N_{Sz(q)}(A)| = 4|A|$, for all $x \in A$, $|x^{Sz(q)} \cap A| = 4$. Therefore, there are $(r-1)/4$ conjugacy classes of elements of order r in $Sz(q)$. Now consider $\mathrm{Sp}_4(q)$. The conjugacy classes of elements of order r in $\mathrm{Sp}_4(q)$ are represented by the elements $[\lambda, \lambda^q, \lambda^{q^2}, \lambda^{q^3}]$ where $\lambda \in \mathbb{F}_{q^4}$ is a non-trivial r^{th} root of unity. So there are $(r-1)/4$ conjugacy classes of elements of order r. This establishes that $(t\theta)^G \cap H = (t\theta)^H$ and, thus, proves the result. □

Proposition 4.17. *Let $T = \mathrm{PSp}_4(q)$ and assume that θ is not a graph-field automorphism. Let $t\theta \in G$ be the element defined in Table 10. If $t\theta$ is contained in a subgroup of G of type $\mathrm{Sp}_2(q^2)$, then e is odd and $t\theta$ is contained in at most one such subgroup.*

Proof. Let $H \leq G$ have type $\mathrm{Sp}_2(q^2)$. Write $L = G \cap \mathrm{PGL}(V)$ and let $H_0 = H \cap L = B{:}\langle\psi\rangle$ where $B = \mathrm{PSp}_2(q^2)$ and ψ is an involutory field automorphism of B. Suppose that $t\theta \in H$. By construction, an X-conjugate of a power of $t\theta$ lifts to a prime order element $x = [\lambda, \lambda^{q_0}, \lambda^{q_0^2}, \lambda^{q_0^3}]$ where $\lambda \in \mathbb{F}_{q_0^4}$ is not contained in a proper subfield of $\mathbb{F}_{q_0^4}$.

First suppose that e is even. For $\mu = \lambda^{q_0}$, $x = [\lambda, \lambda^q, \mu, \mu^q]$ if $e \equiv 2 \pmod 4$, and $x = [\lambda, \lambda^{-1}, \mu, \mu^{-1}]$ if $e \equiv 0 \pmod 4$. Since B embeds in L, modulo scalars, as $[\lambda_1, \lambda_2] \mapsto [\lambda_1, \lambda_1^q, \lambda_2, \lambda_2^q]$, neither of these possibilities for x are images of elements of B.

Now suppose that e is odd. Then $x = [\lambda, \lambda^q, \lambda^{q^2}, \lambda^{q^3}]$. Let h be a preimage of x in H. Then $h \in B$ and h lifts to either $[\lambda, \lambda^{q^2}]$ or $[\lambda^q, \lambda^{q^3}]$. However, $[\lambda, \lambda^{q^2}]$ and $[\lambda^q, \lambda^{q^3}]$ are H_0-conjugate (although not B-conjugate). Therefore, $|x^L \cap H_0| = |x^{H_0}|$. Moreover, $|C_L(x)| = q^2+1 = |C_{H_0}(x)|$ (see [16, Appendix B], for example). Hence, by Lemma 4.10, x, and hence $t\theta$, is contained in at most one G-conjugate of H. This completes the proof. □

Proposition 4.18. *In case $\mathbf{S_4}$, Proposition 4.6 is true for irreducible primitive subgroups.*

Proof. By [5, Tables 8.12–8.14], since $q \neq p$, the only types of irreducible primitive maximal subgroups which arise are those given in Table 11. The uniqueness of the subgroups of type $\mathrm{O}_4^\varepsilon(q)$ and $\mathrm{Sp}_2(q^2)$, when they occur, follows from Corollary 4.14 and Proposition 4.17. If q is even, θ is a graph-field automorphism and $e = 1$, then the uniqueness of the subgroup of type $Sz(q)$ follows from Proposition 4.16. Moreover, in this case, no subgroups of type $\mathrm{O}_2^\varepsilon(q) \wr S_2$ occur since the order of $t\theta$ is divisible by a ppd of q^2+1, which does not divide the order of these groups. The remaining multiplicities follow by Corollaries 4.8 and 4.13. □

We have now proved Proposition 4.6.

4.4. **Probabilistic method.** Let $G = \langle T, \theta\rangle \in \mathcal{A}$ with $T \neq \mathrm{PSp}_4(2)'$ and $\theta \notin \mathrm{Inndiag}(T)$. Maintain the notation introduced at the opening of Section 4. Fix $t\theta$ as the element defined in Table 10. In this section, we will use probabilistic techniques to establish our main results on uniform spread. (Some asymptotic results will be proved in Section 4.5.)

Let us begin by recalling the definition

$$P(x,s) = 1 - \frac{|\{z \in s^G \mid G = \langle x, z\rangle\}|}{|s^G|}.$$

We can now state the key lemma, which encapsulates our probabilistic method.

Lemma 4.19. *Let G be a finite group and let $s \in G$.*

(i) *For $x \in G$,*

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

(ii) *If for all k-tuples $(x_1, \ldots, x_k)$ of prime order elements of G*

$$\sum_{i=1}^{k} P(x_i, s) < 1,$$

then G has uniform spread k with respect to the conjugacy class s^G.

Proof. See [17, Lemmas 2.1 & 2.2]. □

Let us introduce a piece of notation. For an integer k, define

$$\pi_k = \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd} \end{cases}$$

We will now consider the cases **S**, **O** and $\mathbf{S_4}$ in turn.

Proposition 4.20. *Let $m \geq 3$ and $G = \langle \mathrm{PSp}_{2m}(q), \theta\rangle$ where $\theta \in \mathrm{Aut}(\mathrm{PSp}_{2m}(q))$.*

(i) *If q is even, then $u(G) \geq 2$.*

(ii) *If q is odd, then $u(G) \geq 4$.*

(iii) *As $q \to \infty$, $u(G) \to \infty$.*

(iv) *If $m \geq 16$, then $u(G) \geq q - 1$.*

Proof. We will apply Lemma 4.19 with $s = t\theta$. Let $x \in G$ have prime order. Proposition 4.6 gives a superset of $\mathcal{M}(G, t\theta)$ and together with the fixed point ratios in Propositions 3.2, 3.4 and 3.5 we obtain

$$P(x,t\theta) < \left(\frac{1}{q^2} + \frac{1}{q^4} + \frac{2}{q^{2m-2}} + \frac{1}{q^{2m-1}}\right) + \pi_m\left(\frac{6}{q^{m-1}} + \frac{2}{q^m}\right) + N\frac{(2q+2)^{1/2}}{q^{m-1}} + \pi_q\left(\frac{1}{q} + \frac{1}{q^m - 1}\right),$$

where

$$N = 1 + N_{nd} \cdot q + N_{ti} + N_s$$

and N_{nd}, N_{ti} and N_s are the numbers of subgroups in $\mathcal{M}(G, t\theta)$ of type $\mathrm{Sp}_m(q) \wr S_2$, $\mathrm{GL}_m(q).2$ and subfield subgroups, respectively. (The factor of q associated with N_{nd} is to account for the fact that, in this case, $\ell = 2$; see Proposition 3.2.)

From Proposition 4.6, Corollary 4.8 and the fact that e has at most $2 + \log\log q$ distinct prime divisors,

$$N \leq 1 + (\pi_m \cdot q + \pi_{q+1} + (2 + \log\log q))(q^{m/2} + q^{(m-1)/2} + q^{1/2} + 1). \tag{4.3}$$

This yields

$$P(x,t\theta) < \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^{m/2-5}} + \left(\frac{1}{q^{m-5}} + \frac{2}{q^{m-3}} + \frac{6}{q^{m-1}} + \frac{1}{q^m - 1} + \frac{2}{q^m} + \frac{3}{q^{2m-2}} \right).$$

Therefore, as $q \to \infty$, $P(x,t\theta) \to 0$ and, consequently, $u(G) \to \infty$. Moreover, if $m \geq 16$, then

$$P(x,t\theta) \leq \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \frac{1}{q^4} < \frac{1}{q-1}$$

and, consequently, $u(G) \geq q-1$. This proves (iii) and (iv).

Let us now prove (i) and (ii). We will consider various cases depending on e, m and q. First suppose that $e \geq 5$. The upper bound in (4.3) decreases with q and m. Therefore, considering $m = 3$ and $q = 2^5$ shows that $P(x,\theta) < 1/2$ for q even, and considering $m = 3$ and $q = 3^5$ shows that $P(x,t\theta) < 1/4$ for q odd.

Now suppose that $e = 4$. Since e has a unique prime divisor, by Proposition 4.6,

$$N \leq 1 + \pi_m \cdot \frac{1}{2} \binom{m}{\frac{m}{2}} \cdot q + \pi_{q+1} \cdot 2^{(m-1,e)} + (q^{m/4} + q^{(m-1)/4} + q^{1/4} + 1)$$

and with this bound the result can be verified.

Finally suppose that $e \in \{2,3\}$. Since e is prime, by Proposition 4.6,

$$N \leq 1 + \pi_m \cdot \frac{1}{2} \binom{m}{\frac{m}{2}} \cdot q + \pi_{q+1} \cdot 2^{(m-1,e)} + e^2.$$

With this bound, the result follows unless $(m,q) \in \{(3,4),(4,4),(3,8),(3,9)\}$.

Let $(m,q) = (3,9)$. Since $\frac{2m-2}{(2m-2,e)} = 2$ is even, $N_{ti} = 0$ (see Table 11). Together with the refined bound from Proposition 3.2 (Table 6), we can verify that $P(x,t\theta) < \frac{1}{4}$.

Now let $(m,q) \in \{(3,8),(4,4)\}$. If $x \notin \mathrm{PGL}(V)$ or $\nu(x) > 1$, then we have improved bounds for the $\mathcal{C}_1$ and $\mathcal{C}_8$ subgroups from Propositions 3.4 and 3.5 and we may use the refined bound in Proposition 3.2. If $x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$, then we have specialised bounds for the subfield subgroups from Proposition 3.3. In both cases, $P(x,t\theta) < \frac{1}{2}$.

Finally, let $(m,q) = (3,4)$. Arguing as above, if $x \notin \mathrm{PGL}(V)$ or $\nu(x) > 1$, then $P(x,t\theta) < 0.254$, and if $x \in \mathrm{PGL}(V)$ and $\nu(x) = 1$, then $P(x,t\theta) < 0.601 < 1 - 0.254$. Therefore, for all $x_1, x_2 \in G$ of prime order there exists $g \in G$ such that $\langle x_1, (t\theta)^g \rangle = \langle x_2, (t\theta)^g \rangle = G$ unless $x_1, x_2 \in \mathrm{PGL}(V)$ and $\nu(x_1) = \nu(x_2) = 1$. In this case, we can verify in Magma that there exists $g \in G$ such that $\langle x_1, (t\theta)^g \rangle = \langle x_2, (t\theta)^g \rangle = G$. □

Proposition 4.21. *Let q be odd, $m \geq 3$ and $G = \langle \Omega_{2m+1}(q), \theta \rangle$ where $\theta \in \mathrm{Aut}(\Omega_{2m+1}(q))$.*

(i) *For all G, $u(G) \geq 3$.*
(ii) *As $q \to \infty$, $u(G) \to \infty$.*
(iii) *If $m \geq 18$, then $u(G) \geq q-1$.*

Proof. Let $x \in G$ have prime order. Proposition 4.6 gives a superset of $\mathcal{M}(G,t\theta)$ and together with the fixed point ratios in Propositions 3.2–3.4 we obtain

$$P(x,t\theta) < \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \frac{1}{q^{m-2}} + \frac{14}{q^{m-1}} + \frac{5}{q^m} + \frac{2}{q^{(m+1)/2}} + N\frac{(4q+4)^{1/2}}{q^{m-1}}$$

where $\mathcal{M}(G,t\theta)$ contains N subfield subgroups. Since e has at most $2 + \log\log q$ distinct prime divisors,

$$N \leq (2 + \log\log q)(q^{(m+1)/2} + q^{m/2} + q + q^{1/2}).$$

Therefore,

$$P(x,t\theta) < \frac{1}{q} + \frac{1}{q^2} + \frac{1}{q^3} + \frac{1}{q^{m/2-5}} + \frac{2}{q^{(m+1)/2}} + \frac{1}{q^{m-5}} + \frac{1}{q^{m-2}} + \frac{14}{q^{m-1}} + \frac{5}{q^m},$$

so $P(x,t\theta) \to 0$, and $u(G) \to \infty$, as $q \to \infty$. Moreover, if $m \geq 18$, then $P(x,t\theta) < \frac{1}{q-1}$, and $u(G) \geq q-1$. Finally, unless $\mathrm{soc}(G) = \Omega_7(9)$, it is straightforward to show that $P(x,t\theta) < \frac{1}{3}$, and $u(G) \geq 3$, by arguing as in the proof of Proposition 4.20. In the case that $\mathrm{soc}(G) = \Omega_7(9)$ we apply the same approach, but for the subspace subgroups we determine the fixed point ratios using Magma. □

Proposition 4.22. *Let $G = \langle \mathrm{PSp}_4(q), \theta \rangle$ where $\theta \in \mathrm{Aut}(\mathrm{PSp}_4(q))$.*

(i) *For all G, $u(G) \geq 2$.*

(ii) *As $q \to \infty$, $u(G) \to \infty$.*

(iii) *If θ is an involutory graph-field automorphism, then $u(G) \geq q^2/18$.*

Proof. For $q \in \{4, 8, 9, 16, 25, 27\}$ the result can be verified computationally in Magma (see Table 4). Therefore, suppose that $q \geq 32$. Let $x \in G$ have prime order.

First suppose that θ is a field automorphism. Proposition 4.6 gives a superset of $\mathcal{M}(G, t\theta)$ and together with the fixed point ratios in Propositions 3.4 and 3.6 we obtain

$$P(x,t\theta) \leq \frac{4(q_0^2+1)(3+2+\log\log q)}{q(q-1)} + \frac{q}{q^2-1} + \frac{1}{q} + \frac{1}{q^2-1} \tag{4.4}$$

$$\leq \frac{4(q+1)(3+2+\log\log q)}{q(q-1)} + \frac{q}{q^2-1} + \frac{1}{q} + \frac{1}{q^2-1}. \tag{4.5}$$

The asymptotic statement in (ii) now follows from (4.5). If $q \geq 64$, then $P(x,t\theta) < \frac{1}{2}$ by (4.4). If $q = 32$, then $q_0 = 2$ and $P(x,t\theta) < \frac{1}{2}$, by (4.4). Therefore, $u(G) \geq 2$.

Now suppose that θ is a graph-field automorphism. Therefore, q is even and has a unique prime divisor. By Propositions 3.6 and 4.6,

$$P(x,t\theta) \leq \frac{4 \cdot 5(q_0 + \sqrt{2q_0} + 1)}{q(q-1)} \leq \frac{20(q + \sqrt{2q} + 1)}{q(q-1)}$$

and (ii) now follows. If θ does not have order two, then $P(x,t\theta) < \frac{1}{2}$ and (i) follows. (If $q = 32$, then we use the observation that $q_0 = 2$ since θ does not have order 2.) If θ is an involutory graph-field automorphism, then, by Proposition 4.6 (with $e = 1$), and the refined bounds in Proposition 3.6,

$$P(x,t\theta) \leq \frac{8(q + \sqrt{2q} + 1)}{q^2(q-1)} + \frac{1}{q^2} \leq \frac{16}{q^2} + \frac{1}{q^2} < \frac{18}{q^2}.$$

Therefore, $u(G) \geq q^2/18$. This proves (i) and (iii), thus completing the proof. □

4.5. **Asymptotic results.** Finally, let us turn to the remaining asymptotic results. Recall the notation for automorphisms which was introduced in Table 3. As intimated in Section 4.1, we now allow $\theta \in \mathrm{Inndiag}(T)$.

Proposition 4.23. *Let q be odd and let $G = \langle T, \theta \rangle$ where $T = \mathrm{PSp}_{2m}(q)$ and $\theta \in \{\varphi^i, \delta\varphi^i\}$. Then $u(G) \to \infty$ as $m \to \infty$.*

Proof. We will follow the probabilistic approach but with a different choice of element $t\theta$. Assume that m is large enough so that $m > 5$ and there exists $d \in \mathbb{N}$ for which $\sqrt{2m}/8 < d < \sqrt{2m}/4$ and $(d, m-d) = 1$. If $\theta = \varphi^i$ then let $y = [A_{2d}, A_{2m-2d}] \in \mathrm{Sp}_{2m}(q_0)$, and if $\theta = \delta\varphi^i$ then let $y = [C_{2d}, C_{2m-2d}] \in \mathrm{GSp}_{2m}(q_0)$. By Proposition 2.4, let $t\theta \in T\theta$ such that $f(t\theta) = \overline{y}$. Therefore, a power of $f(t\theta)$ lifts to an X-conjugate of y.

Let us now consider $\mathcal{M}(G, t\theta)$. By Proposition 2.8, the unique $\mathcal{C}_1$ subgroup of G containing $t\theta$ has type $\mathrm{Sp}_{2d} \times \mathrm{Sp}_{2m-2d}$. There are at most $2m$ types of subgroup in the families $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_7$, and at most e types of $\mathcal{C}_5$ subgroups. In each of these cases, by Proposition 2.7, there are at most $(q_0^d+1)(q_0^{d-m}+1) \leq 2q^{m/2}$ subgroups of each type in $\mathcal{M}(G, t\theta)$. There are no $\mathcal{C}_6$ or $\mathcal{C}_8$ subgroups in $\mathcal{M}(G, t\theta)$. Since $(d, m-d) = 1$, a suitable power of y is $z = [A_{2d}, I_{2m-2d}]$. Observe that z has a 1-eigenspace of codimension $2d < \sqrt{2m}/2$. Therefore, since $2m > 10$, by [29, Theorem 7.1], z, and hence $t\theta$, is not contained in any subgroups in the $\mathcal{S}$ family. (Exceptions involving the fully deleted permutation module do not occur since $p \neq 2$; see [14, Table 2.1], for example.)

Using the bounds from Propositions 3.2 and 3.4, if x has prime order, then

$$P(x, t\theta) \leq \frac{2}{q^{m-2}} + \frac{1}{q^m} + \frac{1}{q^{\sqrt{2m}/8}} + \frac{1}{q^{2m-\sqrt{2m}/2}} + \frac{2(8m+e)(2q+2)^{1/2}}{q^{m/2-1}} \to 0$$

as $m \to \infty$. Therefore, $u(G) \to \infty$ as $m \to \infty$. □

We now turn to upper bounds on spread. In [30, Prop. 2.5], Guralnick and Shalev prove the following.

Theorem 4.24. *Let $m \geq 2$.*

(i) *If q is even and $T = \mathrm{PSp}_{2m}(q)$, then $s(T) \leq q$.*
(ii) *If $T = \Omega_{2m+1}(q)$, then $s(T) < \frac{q^2+q}{2}$.*

We now establish a generalisation of Theorem 4.24.

Proposition 4.25. *Let $G = \langle T, \theta \rangle \in \mathcal{A}$.*

(i) *If q is even, $T = \mathrm{PSp}_{2m}(q)$ and θ is not a graph-field automorphism, then $s(G) \leq q$.*
(ii) *If $T = \Omega_{2m+1}(q)$, then $s(G) < \frac{q^2+q}{2}$.*

Proof. First consider (i). In the proof of [30, Prop. 2.5(ii)], a set $\mathcal{X}$ of $q+1$ transvections in T is constructed with the property that for all subgroups H_0 of T with type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ there exists $x \in \mathcal{X}$ such that $x \in H_0$. Let $g \in G$. By Corollary 2.11, G has at least one subgroup H of type $\mathrm{O}^+_{2m}(q)$ or $\mathrm{O}^-_{2m}(q)$ such that $g \in H$. Therefore, there exists $x \in \mathcal{X}$ such that $x \in H$. As a result, $\langle x, g \rangle \neq G$ and $s(G) \leq q$.

Now consider (ii). Let $V = \mathbb{F}_q^{2m+1}$ and consider the semilinear action of G on V. Write $\ell = (q^2+q)/2$. In the proof of [30, Prop. 2.5(i)], a set $\mathcal{Y}$ of ℓ reflections in T is constructed such that for all vectors $v \in V$ there exists $y \in \mathcal{Y}$ such that $vy = v$. Let $g \in G$. We will show that g fixes a vector $v \in V$. If $g \in \mathrm{Inndiag}(T)$, then the set of eigenvalues of g is closed under taking inverses. Therefore, an odd number of eigenvalues are a square root of unity. If all such eigenvalues are -1, then $\det(g) = -1$, which is a contradiction. So g has a 1-eigenvector. If $g \in G \setminus \mathrm{Inndiag}(T)$, then g is G-conjugate to the standard field automorphism. Therefore, there is a basis for V consisting of vectors fixed by g. Thus g fixes a vector, so there exists $y \in \mathcal{Y}$ such that $\langle g, y \rangle \neq G$. Hence, $s(G) < \ell$. □

4.6. **Proof of main theorems.** We now prove the four main theorems.

Proof of Theorems 1–4. Theorems 1 and 2 follow from Proposition 4.2 (if $\theta \in \mathrm{Inndiag}(T)$) and Propositions 4.20–4.22 (if $\theta \in \mathrm{Aut}(T) \setminus \mathrm{Inndiag}(T)$). Theorem 4, and hence the forward implication of Theorem 3, is a consequence of Proposition 4.25. Therefore, it remains to verify the reverse implication of Theorem 3.

Let (G_i) be a sequence of groups in $\mathcal{A}$ with $|G_i| \to \infty$. Suppose that (G_i) has no subsequence of odd-dimensional orthogonal groups or even characteristic symplectic groups, over a field of fixed size. Then (G_i) is the union of at most three sequences: symplectic groups

in odd characteristic with $q \to \infty$ or $n \to \infty$; symplectic groups in even characteristic with $q \to \infty$; and odd-dimensional orthogonal groups with $q \to \infty$. By Propositions 4.2, 4.20, 4.21 and 4.23, the uniform spread of these sequences, so of the sequence (G_i), diverges to infinity. This completes the proof of Theorem 3. □

References

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

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

[3] M. Aschbacher, G. M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

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

[5] J. N. Bray, D. F. Holt, C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

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

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

[8] T. Breuer, *GAP computations concerning probabilistic generation of finite simple groups*, preprint (arXiv:0710.3267), 2007.

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

[10] T. Breuer, R. M. Guralnick, A. Lucchini, A. Maroti, G. P. Nagy, *Hamiltonian cycles in the generating graphs of finite groups*, Bull. London Math. Soc. **42** (2010), 621-633.

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

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

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

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

[15] T. C. Burness, *On base sizes for actions of finite classical groups*, J. London Math. Soc. **75** (2007), 545–562.

[16] T. C. Burness, M. Giudici, *Classical Groups, Derangements and Primes*, Aust. Math. Soc. Lecture Note Series, vol. 25, Cambridge University Press, 2016.

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

[18] A. A. Buturlakin, M. A. Grechkoseeva, *The cyclic structure of maximal tori of the finite classical groups*, Algebra Logic **46** (2007), 73–89.

[19] R. W. Carter, *Simple Groups of Lie Type*, John Wiley and Sons, 1972.

[20] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[21] F. Dalla Volta, A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), 194–223.

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

[23] D. Frohardt, K. Magaard, *Grassmannian fixed point ratios*, Geom. Dedicata **82** (2000), 21–104.

[24] D. Frohardt, K. Magaard, *Composition factors of monodromy groups*, Ann. of Math. **43** (2001), 327–345.

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

[26] R. M. Guralnick, *The spread of a finite simple group*, preprint.

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

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

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

[30] R. M. Guralnick, A. Shalev, *On the spread of finite simple groups*, Combinatorica **23** (2003), 73–87.
[31] W. M. Kantor, A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), 67–87.
[32] P. B. Kleidman, M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[33] R. Lawther, M. W. Liebeck, G. M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.
[34] M. W. Liebeck, J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.
[35] M. W. Liebeck, A. Shalev, *The probability of generating a finite simple group*, Geom. Dedicata **56** (1995), 103–113.
[36] M. W. Liebeck, A. Shalev, *Simple groups, permutation groups and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.
[37] G. Malle, D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge University Press, 2011.
[38] A. Stein, *$1\frac{1}{2}$-generation of finite simple groups*, Beitr. Algebra Geom. **39** (1998), 349–358.
[39] R. Steinberg, *Generators for simple groups*, Canad. J. Math. **14** (1962), 277–283.
[40] R. Steinberg, *Lectures on Chevalley groups*, Yale University, 1967.
[41] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.
[42] D. E. Taylor, *The Geometry of the Classical Groups*, Helderman Verlag, 1992.
[43] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

S. Harper, School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK
E-mail address: scott.harper@bristol.ac.uk