ON THE PROBABILITY OF GENERATING INVARIABLY A
FINITE SIMPLE GROUP

DANIELE GARZONI AND EILIDH MCKEMMIE

Abstract. Let $G$ be a finite simple group. In this paper we consider the
existence of small subsets $A$ of $G$ with the property that, if $y \in G$ is cho-
sen uniformly at random, then with high probability $y$ invariably generates $G$
together with some element of $A$. We prove various results in this direction,
both positive and negative. As a corollary, we prove that two randomly chosen
elements of a finite simple group of Lie type of bounded rank invariably gen-
erate with probability bounded away from zero. Our method is based on the
positive solution of the Boston–Shalev conjecture by Fulman and Guralnick, as
well as on certain connections between the properties of invariable generation
of a group of Lie type and the structure of its Weyl group.

1. Introduction

Let $G$ be a finite group. Given a subset $A = \{x_1, \ldots, x_t\} \subseteq G$, we say that $A$
invariably generates $G$ if $\langle x_{g_1}, \ldots, x_{g_t} \rangle = G$ for every choice of
$g_1, \ldots, g_t \in G$. We write in this case $\langle x_1, \ldots, x_t \rangle_I = G$. This concept was introduced by Dixon with
motivations from computational Galois theory; see [Dix92] for details.

For a subset $A$ of $G$, denote by $P_{\text{inv}}(G, A)$ the probability that, if
$y \in G$ is chosen uniformly at random, there exists $x \in A$ such that
$\langle x, y \rangle_I = G$. In case $A = \{x\}$, we will write $P_{\text{inv}}(G, x)$ instead of $P_{\text{inv}}(G, \{x\})$.

We state our first result, which in most cases will be asymptotically su-
pered by subsequent theorems. In Subsection 1.2 we will provide more context for these
theorems, also in relation to “classical” generation.

Theorem 1.1. There exists an absolute constant $\epsilon > 0$ such that every nonabelian
finite simple group $G$ contains an element $x \in G$ satisfying $P_{\text{inv}}(G, x) \geq \epsilon$.

Guralnick–Malle [GM12b] and Kantor–Lubotzky–Shalev [KLS11] independently
proved that every finite simple group is invariably generated by two elements. The-
orem 1.1 is a strengthening of this result.

In light of Theorem 1.1, one would like to find many elements $x \in G$ with the
property that $P_{\text{inv}}(G, x)$ is bounded away from zero uniformly. For groups of Lie
type of bounded rank different from $G_2(3^a)$, one can take almost all elements. In
the following statement, the untwisted rank of $G$ denotes the rank of the ambient
simple algebraic group.

The first author was partially supported by a grant of the Israel Science Foundation No.
702/19, and has received funding from the European Research Council (ERC) under the European
Union’s Horizon 2020 research and innovation programme (grant agreement No. 850956). The
second author was partially supported by the NSF grant DMS 1901506.
Theorem 1.2. Let $G$ be a finite simple group of Lie type of untwisted rank $r$ defined over $\mathbb{F}_q$, or over $\mathbb{F}_{q^2}$ if $G$ is a Suzuki or Ree group, and assume $G \not\cong G_2(q)$ when $3 \mid q$. Then,

$$P_{\text{inv}}(G, x) \geq c/r + O(r^r/q)$$

for an absolute constant $c > 0$ and for a proportion of elements $x \in G$ of the form $1 - O(r^r/q^a)$, where $a = 1/2$ if $G \cong \text{PSL}_2(q)$ and $a = 1$ otherwise.

In order to avoid confusion, we point out that with $u = O(z)$ we mean that $|u| \leq Cz$ for some constant $C$ (so there is no assertion on the sign of $u$).

Remark 1.3. The parameter “$q$” of Theorem 1.2 is the one appearing in Table 1. In fact, this parameter admits a conceptual definition in terms of algebraic groups and Steinberg endomorphisms; see Section 3 for details. We stress that $q$ is an integer, except for Suzuki and Ree groups, where $q$ is not an integer but $q^2$ is an integer. See Remark 1.6(iii) for further comments regarding our notation for Suzuki and Ree groups.

In Theorem 6.1 we will give an explicit value for the constant $c$ appearing in Theorem 1.2. The groups $G = G_2(3^a)$ are genuine exceptions; we will see that $P_{\text{inv}}(G, x) = 0$ for roughly half of the elements $x \in G$, but we can show that $P_{\text{inv}}(G, x) \geq 1/6 + O(1/q)$ for the remaining elements (see Theorem 4.1). By considering separately the error term in the case $G \cong \text{PSL}_2(q)$, we get the following immediate consequence.

Theorem 1.4. Let $G$ be a finite simple group of Lie type of untwisted rank $r$ defined over $\mathbb{F}_q$, or over $\mathbb{F}_{q^2}$ if $G$ is a Suzuki or Ree group. Let $x_1, x_2 \in G$ be chosen uniformly at random. Then,

$$P((x_1, x_2)_I = G) \geq c/r + O(r^r/q)$$

for an absolute constant $c > 0$.

Of course, in the previous two theorems we are thinking of $r$ fixed, and $q \to \infty$. We will review the history of Theorem 1.4 in Subsection 1.1. An interesting goal is to seek sharp bounds in Theorem 1.3. Although in this paper we do not pursue this goal, in Theorem 6.3 we will obtain a formula of the type

$$P((x_1, x_2)_I = G) = f(r) + d(r)/q.$$ 

The main term $f(r)$ is very explicit, depending only on the Weyl group of $G$, and can be computed essentially in an algorithmic way; it should be possible to compute it precisely for all exceptional groups.

Eberhard–Ford–Green [EFG17] and the second author [McK21] showed that, for alternating groups of large degree and for groups of Lie type of large rank over large fields, $P((x_1, x_2, x_3)_I = G)$ tends to zero. (Conjecturally, in groups of Lie type there should be no restriction on the field size.) Therefore, it is not possible to extend Theorem 1.2 to the other families of finite simple groups – not even for a proportion of elements bounded away from zero.

In Theorems 1.1 and 1.2 we have bounded $P_{\text{inv}}(G, x)$ away from zero. Next, we would like to get probabilities approaching 1. With this purpose, we consider more elements simultaneously. In most cases, only a few elements are needed, which is in stark contrast to the remaining cases, where the asymptotic statement does not hold even if we take the whole group.
Theorem 1.5. Let $G$ be a nonabelian finite simple group.

1. Assume $G$ is of Lie type and $G \not\cong G_2(q)$ when $3 \mid q$. Then, there exists a subset $A_b$ of $G$ such that $|A_b|$ and $P_{inv}(G, A_b)$ satisfy the bounds in Table 1.

2. Assume $G$ is alternating or classical. Then, there exists a subset $A_\ell$ of $G$ such that $|A_\ell|$ and $P_{inv}(G, A_\ell)$ satisfy the bounds in Table 1.

3. Assume $G = G_2(q)$ with $3 \mid q$, or $G = \text{PSp}_{2m}(q)$ with $q$ even and $m$ sufficiently large, or $G = \text{PO}_{2m+1}(q)$ with $q$ odd and $m$ sufficiently large. Then $P_{inv}(G, G)$ satisfies the bounds in Table 1.

We make some remarks on the statement of Theorem 1.5 and on the notation and conventions in Table 1.

Remark 1.6. (i) In Table 1 “r” denotes the untwisted rank of $G$. Moreover, it is understood that every nonempty entry in the fourth column of the table applies to all subsequent empty lines.

(ii) If $G = \text{PSU}_n(q)$ we assume $n \geq 3$; if $G = \text{PSp}_{2m}(q)$ we assume $m \geq 2$; if $G = \text{PO}_{2m}^+(q)$ we assume $m \geq 4$; if $G = \text{PO}_{2m+1}(q)$ we assume $m \geq 3$. These assumptions are valid due to the existence of exceptional isomorphisms between certain low rank classical groups. Moreover, in Table 1 for each $G$ we further exclude the finitely many values of $(n, q)$ or $(m, q)$ for which $G$ is not simple; see, e.g. [KL90, Proposition 2.9.1] (this is not crucial, since the statements have no content for bounded $|G|$).

(iii) If $G = 2B_2(q^2)$ or $G = 2D_4(q^2)$ then $q^2 = 2^{2a+1}$ with $a \geq 1$. If $G = 2G_2(q^2)$ then $q^2 = 3^{2a+1}$ with $a \geq 1$. A common notation in the literature is $2B_2(q)$ with $q = 2^{2a+1}$ and $a \geq 1$, etc. Of course, one notation is obtained from the other by performing a change of variables, and $2B_2(8)$, say, denotes the same group in both cases. Our choice is convenient since groups of Lie type behave uniformly with respect to the parameter “$q$”, which is not an integer for Suzuki and Ree groups; see Section 3 for more details. We note that the same convention is adopted, for instance, in [MT11]; see [MT11, Table 22.1, p. 193].

(iv) In $A_b$, “b” stands for “bounded”, and in $A_\ell$, “ell” stands for “large”. This refers to the rank of the groups; the reason of this choice should be clarified by looking at the bounds in Table 1.

Theorem 1.5 presents a strong dichotomy; it is worth stating this separately.

Consider the following groups:

$$G = \begin{cases} 
G_2(q) & \text{with } 3 \mid q \\
\text{PSp}_{2m}(q) & \text{with } q \text{ even} \\
\text{PO}_{2m+1}(q) & \text{with } q \text{ odd}.
\end{cases}$$

(1)

Corollary 1.7. Let $G$ be a nonabelian finite simple group with $|G| \to \infty$.

(i) Assume $G \not\cong G_2(q)$ when $3 \mid q$, and assume that if $G = \text{PSp}_{2m}(q)$ with $q$ even or $G = \text{PO}_{2m+1}(q)$ with $q$ odd then $q \to \infty$. Then, there exists $A \subseteq G$ of size at most 6 such that $P_{inv}(G, A)$ tends to 1 as $|G| \to \infty$.

(ii) Assume $G$ is as in (i), and assume that if $G = \text{PSp}_{2m}(q)$ with $q$ even or $G = \text{PO}_{2m+1}(q)$ with $q$ odd then $q$ is bounded. Then, $P_{inv}(G, G)$ remains bounded away from 1 as $|G| \to \infty$. (Equivalently, $P_{inv}(G, y) = 0$ for a proportion of elements $y \in G$ bounded away from zero.)
Table 1. Bounds given in the statement of Theorem 1.5. See Remark 1.6 for notation and conventions used in the table.

| $G$            | Conditions | Size of $A_b$ or $A_\ell$ | Bounds                  |
|----------------|------------|---------------------------|-------------------------|
| $2B_2(q^2)$    |            | 2                         | $\mathbf{P}_{\text{inv}}(G, A_b) \geq 1 - O(r^* / q)$ |
| $G_2(q)$       |            | 2                         |                         |
| $3D_4(q)$      |            | 2                         |                         |
| $^2G_2(q^{2r})$|            | 2                         |                         |
| $F_4(q)$       | $q$ odd   | 2                         |                         |
| $E_6(q)$       |            | 2                         |                         |
| $^2E_6(q)$     |            | 2                         |                         |
| $E_7(q)$       |            | 2                         |                         |
| $E_8(q)$       |            | 2                         |                         |
| $PSL_n(q)$     |            | 2                         |                         |
| $PSU_n(q)$     |            | 2                         |                         |
| $PSp_{2m}(q)$  | $m$ even, $q$ odd | 2                        |                         |
| $PSp_{2m}(q)$  | $m$ odd, $q$ odd | 3                        |                         |
| $PSp_{2m}(q)$  | $q$ even   | 4                         |                         |
| $P\Omega_{2m+1}(q)$ | $q$ odd | 2                         |                         |
| $P\Omega_{2m}(q)$ |            | 2                         |                         |
| $P\Omega_{2m}(q)$ | $m$ odd   | 2                         |                         |
| $P\Omega_{2m}(q)$ | $m$ even   | 4                         |                         |
| $A_n$          |            | 1                         | $\mathbf{P}_{\text{inv}}(G, A_\ell) \geq 1 - O(n^{-0.08})$ |
| $PSL_n(q)$     |            | 1                         | $\mathbf{P}_{\text{inv}}(G, A_\ell) \geq 1 - O(r^{-0.005})$ |
| $PSU_n(q)$     |            | 1                         |                         |
| $PSp_{2m}(q)$  | $q$ odd   | 1                         |                         |
| $P\Omega_{2m}(q)$ |            | 1                         |                         |
| $P\Omega_{2m}(q)$ | $q$ even | 2                         | $\mathbf{P}_{\text{inv}}(G, A_\ell) \geq 1 - 6/q + O(r^{-0.005})$ |
| $P\Omega_{2m+1}(q)$ | $q$ odd | 2                         |                         |
| $G_2(q)$       | $3 | q$   |                           | $\mathbf{P}_{\text{inv}}(G, G) = 1/2 + O(1/q)$ |
| $PSp_{2m}(q)$  | $q$ even, $m$ large |                     | $\mathbf{P}_{\text{inv}}(G, G) \leq 1 - 1/4q^3$ |
| $P\Omega_{2m+1}(q)$ | $q$ odd, $m$ large |                     | $\mathbf{P}_{\text{inv}}(G, G) \leq 1 - 1/6q$ |

Corollary 1.7 follows from Theorem 1.5 by setting $A = A_\ell$ for alternating groups, $A = A_b$ for exceptional groups, and $A = A_b \cup A_\ell$ for classical groups.

Of course, every case in which the size of $A_\ell$ is equal to 1 represents a strengthening of Theorem 1.1. Combining this with Theorem 1.2, we see that in most cases asymptotically we can do better than Theorem 1.1. The improvement is complementary: while there is no sensible analogue of Theorem 1.2 in large rank, here we cannot have $|A_b| = 1$ in bounded rank (see Lemma 7.2). We note finally that the size of $|A_\ell|$ is sharp in every case (Lemmas 8.10 and 8.17), and that there are cases in which we need $|A_b| \geq 4$ (see Lemma 7.1 note that $|A_b| \leq 4$ unless $G = F_4(2^n)$). Here, with “sharp” we mean that if we choose a set $Y$ of smaller size, then $\mathbf{P}_{\text{inv}}(G, Y)$ remains bounded away from 1 as the relevant parameters grow.
1.1. Context: Theorem 1.4. The first result of the flavour of Theorem 1.4 was obtained by Dixon [Dix92]. Dixon showed that $O((\log n)^{1/2})$ random elements of $S_n$ invariably generate $S_n$ with probability tending to 1 as $n \to \infty$. Luczak–Pyber [LP93] showed that $O(1)$ random elements of $S_n$ invariably generate with probability bounded away from zero. (One cannot approach 1 with a bounded number of elements, since a random permutation has a fixed point with probability approaching $1 - 1/e$.) The exact value of $O(1)$ turned out to be four: Pemantle–Peres–Rivin [PPR16] proved that four elements are enough, while Eberhard–Ford–Green [EFG17] showed that three are not. The same results hold for alternating groups. The second author [McK21] extended these results to classical groups of large rank, proving that four random elements of a finite simple classical group of rank $r$ defined over $F_q$ invariably generate with probability bounded away from zero if $r$ and $q$ are large enough, and three random elements invariably generate with probability tending to zero as $r, q \to \infty$.

Theorem 1.4 addresses the case of groups of Lie type of bounded rank, which therefore nearly finishes the problem of invariable generation of finite simple groups by randomly chosen elements – only the case of classical groups of large rank over small fields remains open. (As in the case of symmetric groups, using a bounded number of elements the probability cannot approach 1; this follows from results by Fulman–Guralnick [FG03], and it is summarized for instance in [KLS11, Corollary 5.7].)

Probabilistic invariable generation has been studied also for general finite groups. Confirming a conjecture of Kowalski and Zywina [KZ12], Lucchini [Luc18] proved that, for every finite group $G$, picking $O(|G|^{1/2})$ random elements is sufficient, on average, in order to generate $G$ invariably. Lucchini–Tracey [LT17] showed that the above bound can be improved to $(1 + \epsilon)|G|^{1/2 + O(\epsilon)}$ for every $\epsilon > 0$.

1.2. Context: Theorems 1.1, 1.2 and 1.5. It is convenient to visualize things as follows. The generating graph $\Gamma(G)$ of $G$ is the graph whose vertices are the nonidentity elements of $G$, with $x$ and $y$ adjacent if $\langle x, y \rangle = G$. The first author [Gar20, Subsection 1.3] defined a similar graph $\Lambda_e(G)$: the vertex set is the same, and $x$ and $y$ are adjacent if $\langle x, y \rangle_I = G$. In this language, Theorem 1.1 says that $\Lambda_e(G)$ contains large stars when $G$ is simple.

For $x \in G$, let $P(G, x)$ denote the probability that, if $y \in G$ is random, then $\langle x, y \rangle = G$: this is the “classical” version of our $P_{\text{inv}}(G, x)$. Set then $P^-(G) = \min\{P(G, x) : 1 \neq x \in G\}$. Guralnick and Kantor [GK00] showed that $P^-(G) > 0$ for every finite simple group $G$, i.e., $\Gamma(G)$ has no isolated vertices. Moreover, in [GLSS99], following results from [GKS94] and [LS99], the behaviour of $P^-(G)$, where $G$ is simple and $|G| \to \infty$, was determined.

It is easy to see that the Guralnick–Kantor result fails for invariable generation: $\Lambda_e(G)$ can have isolated vertices (for instance, a 3-cycle in $A_n$ with $n$ even). It seems to us that Theorems 1.1, 1.2 and 1.5 are essentially the best one can hope for in the invariable setting. Moreover, our results are among the first probabilistic statements concerning invariable generation of finite simple groups by two elements. We are aware only of Shalev [Sha98, Theorem 4.2], which is Theorem 1.5 in case $G = \text{PSL}_n(q)$ and $n$ large.

Corollary 1.7 can be clearly stated in terms of $\Lambda_e(G)$ as follows.

**Corollary 1.8.** Let $G$ be a nonabelian finite simple group with $|G| \to \infty$. 

(i) Assume $G \not\cong G_2(q)$ when $3|q$, and assume that if $G = \text{PSp}_{2n}(q)$ with $q$ even or $G = \text{PSp}_{2m+1}(q)$ with $q$ odd then $q \to \infty$. Then, the proportion of isolated vertices of $\Lambda_e(G)$ tends to zero as $|G| \to \infty$. More precisely, if we remove an asymptotically negligible proportion of vertices from $\Lambda_e(G)$, and if we remove some further edges, we obtain a graph which is the union of at most $6$ stars.

(ii) Assume $G$ is as in (i), and assume that if $G = \text{PSp}_{2n}(q)$ with $q$ even or $G = \text{PSp}_{2m+1}(q)$ with $q$ odd then $q$ is bounded. Then, the proportion of isolated vertices of $\Lambda_e(G)$ remains bounded away from zero as $|G| \to \infty$.

Corollary 1.8(ii) reveals a surprising and sharp contrast with respect to the case of classical generation. Theorem 1.5 and Corollary 1.7 can also be seen as a sort of “invariable” version of a concept introduced recently by Burness and Harper. In [BH19], the total domination number of a finite simple group $G$ is defined as the total domination number of $\Gamma(G)$, i.e., the minimal size of a subset $A$ of $G$ such that, if $1 \neq y \in G$, there exists $x \in A$ such that $\langle x, y \rangle = G$. Corollary 1.7 can be thought of as an analogue for invariable generation – although again it is necessary to ignore a small proportion of elements.

1.3. Methods. Here we briefly outline some of the methods we use in the proofs of our main results.

Let $G$ be a finite group, and let $x \in G$. We define $\mathcal{M}(x)$ as the union of all conjugates of maximal subgroups of $G$ containing $x$. Equivalently, $\mathcal{M}(x)$ coincides with the union of all conjugacy classes of elements intersecting some maximal overgroup of $x$.

**Lemma 1.9.** Let $A$ be a subset of $G$. Then,

$$1 - P_{\text{inv}}(G, A) = \frac{|\bigcap_{x \in A} \mathcal{M}(x)|}{|G|}.$$ 

**Proof.** Given $y \in G$, $\{x, y\}$ invariably generates $G$ if and only if $y \notin \mathcal{M}(x)$. The statement follows. 

Therefore our business is to find elements $x$ such that $\mathcal{M}(x)$ is small. This depends on two facts:

(I) existence of elements lying in few maximal subgroups, and

(II) existence of maximal subgroups $M$ of $G$ such that $\bigcup_{g \in G} M^g$ is small.

We must note that, in fact, (I) and (II) perform only part of the job. Indeed, taking the intersection of the sets $\mathcal{M}(x)$ is rather more delicate, and will require much more work. Moreover, of course the proof of the upper bound on $P_{\text{inv}}(G, G)$ in Theorem 1.5 goes in the opposite direction.

Item (I) is a well studied topic (see, e.g., [GK00, Wei92, BH19]). Often, for us, applying results from these papers will be convenient, rather than essential. One reason is that, in our probabilistic approach, we can ignore the overgroups which are small (e.g., certain almost simple subgroups in groups of Lie type).

For what concerns item (II), we will make essential use of deep results. We will use results of Luczak–Pyber [LP93] for alternating groups (subsequently improved in Eberhard–Ford–Green [EFG16] and Eberhard–Ford–Koukoulopoulos [EFK16]), and results of Fulman–Guralnick [FG03, FG12, FG17, FG18] for groups of Lie type. In these four papers, Fulman and Guralnick completed the proof of the so-called
Boston–Shalev conjecture, which asserts that for every finite simple group $G$ and for every proper subgroup $M$ of $G$, the proportion of elements belonging to $\bigcup_{g \in G} M^g$ is bounded away from 1 absolutely (equivalently, the proportion of derangements in the action of $G$ on the cosets of $M$ is bounded away from zero absolutely). They proved much stronger asymptotic results in many cases.

One of our main tools is the intimate connection between the properties of invariably generation of a group of Lie type and the structure of its Weyl group. We will make this precise in Section 3. In bounded rank, this will allow us to translate the main theorems in terms of maximal tori (see e.g. Theorem 3.10). We will exploit the connection also in large rank, where the asymptotic properties of the Weyl groups will be relevant.

We remark again that it is enough to prove Theorem 1.1 for sufficiently large finite simple groups, since in [GM12b] and [KLS11] it was proved that every finite simple group is invariably generated by two elements. What is more, for groups of Lie type we can divide the proof of Theorem 1.1 in two steps: first produce an element $x_1$ for groups of sufficiently large rank, and then produce an element $x_2$ for groups of bounded rank and sufficiently large fields.

Finally, we note that we are free to define the subsets $A_b$ and $A_\ell$ from Theorem 1.5 only for sufficiently large finite simple groups. In fact, in groups of Lie type, for the set $A_b$ we may assume that $r$ is sufficiently large, and for the set $A_\ell$ we may assume (say) that $q \geq C r^r$ for some large constant $C$. Clearly, the proof of Theorem 1.5 also splits naturally into the bounded rank and large rank cases.

2. Alternating groups

In this section we prove Theorems 1.1 and 1.5 for alternating groups. Conceptually, the proof follows from [LP93]. We will make use of [EFG16] and [EFK16] in order to obtain better bounds.

**Theorem 2.1.** The conclusions to Theorems 1.1 and 1.5 hold in the case $G = A_n$.

**Proof.** If $n$ is odd, choose $x \in G = A_n$ to be an $n$-cycle. If $n$ is even, choose $x \in G$ to have cycle type $(n/2, n/2)$. Then set $A_\ell = \{x\}$. In the first case, the overgroups of $x$ are transitive subgroups, while in the second case the overgroups of $x$ are either transitive, or fix a set of size $n/2$.

By [EFK16, Theorem 1.1], the proportion of elements of $A_n$ lying in proper transitive subgroups of $A_n$ is $O(n^{-0.08})$. By [EFG16, Theorem 1.1], the same bound holds for the proportion of elements fixing a set of size $n/2$. Therefore

$$\frac{|\mathcal{M}(x)|}{|G|} = O(n^{-0.08}).$$

Then $P_{mv}(G, A_\ell) = 1 - O(n^{-0.08})$ by Lemma 1.9 (We mention that, in [EFK16] and [EFG16], much more precise estimates are proved than those used here.)

We have proved Theorem 1.5 for alternating groups, and since $|A_\ell| = 1$, this implies Theorem 1.1 in this case. □

3. Groups of Lie type of bounded rank: preliminaries

In this section we introduce all the machinery that will lead us to the proof of the main theorems for groups of Lie type of bounded rank. We will prove Theorem
As well as Theorem 1.5(3) for $G = G_2(3^a)$, in Sections 4 and 5. We will deduce Theorems 1.2 and 1.4 in Section 6.

We single out a special case.

**Theorem 3.1.** Theorems 1.2, 1.4, 1.5 hold in case $G \cong PSL_2(q)$.

The subgroup structure of $PSL_2(q)$ is very well known and it is easy to prove Theorem 3.1. We will do this at the beginning of Section 5.

The reason why we separate out this case is minor. Indeed, we will give an argument which works in general, but which gives error terms in $q$ of type $O(1/q^{1/2})$ if $G \cong PSL_2(q)$, and of type $O(1/q)$ otherwise (see Remark 3.7). We then prefer to consider $PSL_2(q)$ separately, and deal with the other cases uniformly.

Let $X$ be a simple linear algebraic group (of any isogeny type) over an algebraic closure $\mathbb{k}$ of a finite field of characteristic $p$ (for all this theory, our reference is [MT11]). Let $\sigma$ be an endomorphism of $X$ such that the set $X_\sigma$ of fixed points of $\sigma$ is a finite group, and such that the derived subgroup $[X_\sigma, X_\sigma] = (X_\sigma)'$ is a perfect group. Let $T$ be a $\sigma$-stable maximal torus of $X$. Then $\sigma$ acts naturally on the character group $\text{Hom}(T, GL_1)$. It turns out that the eigenvalues of $\sigma$ on $\text{Hom}(T, GL_1) \otimes \mathbb{Z}[C]$ have all the same absolute value, which we denote by $q$, and which is a fractional power of $p$ (see [MT11] Lemma 22.1 and Proposition 22.2). We will write $X_\sigma = X_q$.

**Remark 3.2.** The notation $X_q$ does not determine uniquely a finite group, since $q$ does not determine uniquely $\sigma$. For instance, both the groups $SL_n(q)$ and $SU_n(q)$ can be written as $X_q$ with $X = SL_n$.

Recall, moreover, that $q$ is an integer, except for Suzuki and Ree groups, where $q$ is not an integer but $q^2$ is an integer (cf. Remark 1.6(iii)).

In Sections 3–7 we fix $X$, and we let $\sigma$ vary – concretely, for classical groups we are fixing the rank and we are letting $q$ go to infinity, and moreover we are dealing with the exceptional groups.

### 3.1. Subgroups of maximal rank

We begin by recalling a well known fact.

**Lemma 3.3.** Assume $H \leq X$ is closed, connected and $\sigma$-stable, and assume $s \in H_\sigma$ is semisimple. Then, $s$ belongs to a $\sigma$-stable maximal torus of $H$.

**Proof.** We have that $s$ is contained in a maximal torus $S$ of $H$. Then $s \in S \leq C_H(s)^\circ$. Since $s$ is central in $C_H(s)^\circ$, $s$ is contained in every maximal torus of $C_H(s)^\circ$ (this is also a maximal torus of $H$). Now $C_H(s)^\circ$ is $\sigma$-stable and connected, hence by Lang–Steinberg it contains a $\sigma$-stable maximal torus $L$ (see [MT11] Theorem 21.11). We have $s \in L$ and we are done. □

A proper closed subgroup $K$ of $X$ is said to be of maximal rank if it contains a maximal torus of $X$. A subgroup of $X_\sigma$ is said to be of maximal rank if it is of the form $K_\sigma$, where $K$ is a $\sigma$-stable subgroup of maximal rank (by Lang–Steinberg, $K$ contains a $\sigma$-stable maximal torus).

We list some notation that we will keep throughout Sections 3–7. We advise the reader to consult this list whenever they find an unknown symbol, rather than to read all the items now. We prefer to amass this notation here, since we will use it several times in several different places.

**Notation 3.4.**

(i) We write $X_\sigma = X_q$, where “$q$” was defined in the paragraph preceding Remark 3.2.
(ii) For a subgroup $H$ of $X_{\sigma}$, set
\[ \tilde{H} = \bigcup_{g \in X_{\sigma}} H^g. \]

(iii) $p$ denotes the characteristic of the field $k$.

(iv) $r$ denotes the rank of $X$ (i.e., the dimension of a maximal torus). By Theorem \ref{thm:3.1} we may assume $r \geq 2$, but we will make the requirement explicit.

(v) $\mathcal{M} = \mathcal{M}(X_{\sigma})$ denotes the set of maximal subgroups of $X_{\sigma}$ of the form $K_{\sigma}$, where $K$ is a maximal $\sigma$-stable subgroup of $X$ of maximal rank.

(vi) $\mathcal{M}_{\mathrm{con}} = \mathcal{M}_{\mathrm{con}}(X_{\sigma})$ denotes the set of subgroups of $X_{\sigma}$ of the form $(K^o)_{\sigma}$, where $K$ is a maximal $\sigma$-stable subgroup of $X$ of maximal rank and $K^o$ denotes its connected component.

(vii) For $x \in X_{\sigma}$, $\mathcal{M}(x)$ denotes the set of all conjugates of overgroups of $x$ belonging to $\mathcal{M}$.

(viii) For $x \in X_{\sigma}$, $T(x)$ denotes the set of maximal tori of $X_{\sigma}$ contained in some $K^o_{\sigma}$, where $K_{\sigma} \in \mathcal{M}(x)$ (note that $K^o_{\sigma}$ need not contain $x$).

(ix) For a subset $A \subseteq X_{\sigma}$, $P_{\mathrm{inv}}(X_{\sigma}, A)$ denotes the probability that, if $y \in X_{\sigma}$ is chosen uniformly at random, there exists $x \in A$ such that for every $g_1, g_2 \in X_{\sigma}$, every maximal overgroup of $(x^{g_1}, y^{g_2})$ in $X_{\sigma}$ contains $(X_{\sigma})'$.

(x) $\Delta = \Delta(X_{\sigma})$ denotes the set of elements $y$ of $X_{\sigma}$ which are regular semisimple, and such that if $y$ belongs to a maximal subgroup $M$ of $X_{\sigma}$, then either $(X_{\sigma})' \leq M$, or $M = K_{\sigma} \in \mathcal{M}$ and $y \in K_{\sigma}^o$.

(xi) For a maximal torus $S$ of $X_{\sigma}$, set $\Delta_S = S \cap \Delta$.

We recall a theorem which is essential for our purposes. Note that the proportion in the statement is independent of $X$, hence the result can be applied to groups of growing Lie rank (indeed we will use it in Section \ref{s:8}).

\textbf{Theorem 3.5.} \cite[Theorem 1.1]{CL01} \textit{The proportion of regular semisimple elements of $X_q$ is $1 - O(1/q)$.}

For Suzuki and Ree groups the proportion is in fact $1 - O(1/q^2)$, but we will not use this. The proof of the following theorem is largely contained in \cite{FG03}, although at various places we need more explicit bounds.

\textbf{Theorem 3.6.} Assume $r \geq 2$. We have
\[ \frac{|\Delta|}{|X_q|} = 1 - \frac{O(r^r)}{q}. \]

\textit{Proof.} Clearly we can assume $r \leq q$, otherwise the statement is empty. Let $A_1$ be the set of elements in $X_q$ which are not regular semisimple. Let $A_2$ be the set of elements which belong to maximal subgroups of $X_q$ which do not contain any maximal torus and which do not contain $(X_q)'$. Let $A_3$ be the set of elements which belong to $K_{\sigma} \setminus K^o$ for some maximal $\sigma$-stable subgroup $K$ of $X$ of maximal rank.

We need to prove $|A_1 \cup A_2 \cup A_3|/|X_q| = O(r^r/q)$.

We have $|A_1|/|X_q| = O(1/q)$ by Theorem \ref{thm:3.5}

Next we deal with $A_2$. Let $\Omega$ be the set of maximal subgroups of $X_q$ which do not contain $(X_q)'$, which do not contain any maximal torus of $X_q$, and which are not subfield subgroups (cf. \cite[Section 3]{FG03}). If $M \in \Omega$ then $M$ has $O(q^{r-1})$ conjugacy classes (see \cite{FG03} and the proof of \cite[Theorem 7.3]{FG12}).
Assume now $x \in X_q$ is regular semisimple. Then the $X_q$-class of $x$ has size $O(|X_q|/(q-1)^r)$. By Theorem 3.35, we see that if $M \in \Omega$ then

$$\frac{|\widetilde{M}|}{|X_q|} = \frac{O(q^{r-1})}{(q-1)^r} + \frac{O(1)}{q} = \frac{O(1)}{q},$$

where in the last equality we used $r \leq q$ (in fact $r = O(q)$ is enough). It is known (cf. [LMS05, Theorem 1.3]) that the number of conjugacy classes of subgroups in $\Omega$ is bounded by a function of $r$. (Note that $X_q$ surjects, with central kernel, onto an almost simple group generated by inner-diagonal automorphisms.) In case $X$ is classical, by [GLT12, Theorem 1.2] we can take this function to be $O(r^6)$.

Next we deal with subfield subgroups. The argument given in [FG03, Lemma 3.7] shows that the proportion of elements belonging to subfield subgroups is $O(r/q) + O(1/q)$, which is $O(r/q)$ since $r \geq 2$. Therefore $|A_2|/|X_q| = O(r^6/q)$.

Finally we deal with $A_3$. Let $K$ be a maximal $\sigma$-stable closed subgroup of $X$ of maximal rank. We claim that

$$\frac{|\bigcup_{g \in X_q} (K_\sigma \setminus K^g)^g|}{|X_q|} = O(|K_\sigma : K_\sigma^g|).$$

We go through the proof of [FG03, Proposition 4.2]: we use the same arguments and the same computations, except that we bound the size of a regular semisimple class by $O(|X_q|/(q-1)^r)$, and moreover we use $r = O(q)$, so that $((q+1)/(q-1))^{r-1}$ is bounded.

At this point we can deduce that $|A_3|/|X_q| = O(r^6/q)$. Indeed, it is known that $|K_\sigma : K_\sigma^g| = O((r+1)!)$, and moreover the number of $X_q$-conjugacy classes of maximal subgroups of maximal rank is linear in $r$, from which $|A_3|/|X_q| = O(r^6/q)$. (These facts are known in a very precise way, cf. [LSS92] and [LS98]. We will recall them in Sections 4 and 5.) The term $(r+1)!$ can occur for stabilizers of direct sum decompositions in classical groups.

Putting together the bounds given for $A_1$, $A_2$ and $A_3$, we get the result. □

Remark 3.7. By the same argument as in the previous proof, the proportion of elements of $SL_2(q)$ belonging to subfield subgroups is $O(1/q^{1/2})$. If $q$ is a square, the proportion of elements inside a conjugate of $SL_2(q^{1/2})$ is indeed of this form. This is the only reason for which we have considered this case separately.

We also note that, in bounded rank, an essential part of our method is to focus on regular semisimple elements. By work of Guralnick–Lübeck [GL01] and Fulman–Neumann–Präger [FNP05], it is known that, except for Suzuki and Ree groups, the proportion of elements of $X_q$ which are not regular semisimple is comparable to $1/q$ (up to constants). Therefore, with our method we cannot get error terms in $q$ which are better than $O(1/q)$.

3.2. Maximal tori and Weyl group. There is a well known and fundamental connection between the maximal tori of $X_\sigma$ and the Weyl group of $X$, which now we recall (see [MT11, Section 25] for the general theory). Together with Theorems 3.5 and 3.6 this will enable us to translate the main theorems in terms of maximal tori.

Throughout this subsection, we fix a $\sigma$-stable maximal torus $T$, and let $W = N_X(T)/T$ be the Weyl group of $X$ with respect to $T$. Then $\sigma$ acts on $W$. There is a bijection between $X_\sigma$-conjugacy classes of $\sigma$-stable maximal tori of $X$ and $W$-conjugacy classes contained in the coset $\sigma W$ of the group $\langle \sigma \rangle \ltimes W$ (if $\sigma$ acts trivially...
Theorem 3.8. \(X\) is at most the proportion of elements of \(q\). Despite being trivial, for Remark 3.9. In fact, the previous proof shows that the result can be applied to groups of growing Lie rank. In case \(\Omega = \{w\}\), we will write \(P(W,\sigma,\Omega)\) instead of \(P(W,\sigma,\{w\})\). Using that \(N_{X_\sigma}(T_w) \leq N_{X_\sigma}(\sigma W T_{\sigma})\), by a trivial union bound we get

\[
\frac{|\bigcup_{w \in \Omega} (T_w)_\sigma|}{|X_q|} \leq \sum_{w \in \Omega} \frac{1}{|C_W(\sigma w)|} = P(W,\sigma,\Omega).
\]

(2)

Despite being trivial, for \(q\) large this bound is accurate.

Theorem 3.8.

\[
\frac{|\bigcup_{w \in \Omega} (T_w)_\sigma|}{|X_q|} = P(W,\sigma,\Omega) + \frac{O(1)}{q}.
\]

(3)

Proof. By Lemma 3.3 and Theorem 3.5 we have

\[
\beta := \frac{|\bigcup_{w \in \Omega} (T_w)_\sigma|}{|X_q|} + \frac{|\bigcup_{w \in \Psi \setminus \Omega} (T_w)_\sigma|}{|X_q|} = 1 - \frac{O(1)}{q}.
\]

(Note that \(\beta \leq 1\) by (2).) Moreover

\[
\frac{O(1)}{q} = 1 - \beta = \left( P(W,\sigma,\Omega) - \frac{|\bigcup_{w \in \Omega} (T_w)_\sigma|}{|X_q|} \right) + \left( P(W,\sigma,\Psi \setminus \Omega) - \frac{|\bigcup_{w \in \Psi \setminus \Omega} (T_w)_\sigma|}{|X_q|} \right),
\]

where by (2) both summands are nonnegative. In particular they are both \(O(1/q)\), and the proof is concluded.

Remark 3.9. In fact, the previous proof shows that

\[
P(W,\sigma,\Omega) - \frac{|\bigcup_{w \in \Omega} (T_w)_\sigma|}{|X_q|}
\]

is at most the proportion of elements of \(X_q\) which are not semisimple. Therefore, we are really using that the proportion of \emph{semisimple} elements of \(X_q\) is \(1 - O(1/q)\), rather than Theorem 3.5.

Theorem 3.8 was used in [FG03, FG17] (although we have not found the above proof in the literature). Note, once again, that the error term is independent of \(r\), hence the result can be applied to groups of growing Lie rank.

In this section, the key assumption is that \(X\) is fixed. Then \(W\) is fixed, and if \(\Omega\) is nonempty the expression on the right-hand side of (9) is always bounded away from zero: it is at least \(1/|W| + O(1/q)\).

For a subset \(A\) of \(X_q\), let \(T_1, \ldots, T_t\) be a set of representatives of the \(X_q\)-conjugacy classes of members of \(\cap_{x \in A} T(x)\) (possibly \(t = 0\)). Write \(T_i = (T_{w_i})_\sigma\), where \(T_{w_i}\) is a \(\sigma\)-stable maximal torus of \(X\) and \(w_i \in W = N_X(T)/T\). Set \(\Omega = \{w_1, \ldots, w_t\}\).
Theorem 3.10. Assume \( r \geq 2 \). We have
\[
1 - P_{\text{inv}}^*(X_q, A) = P(W, \sigma, \Omega) + \frac{O(r^r)}{q}.
\] (4)

Proof. Reasoning as in Lemma 1.9 and using Theorem 3.6, we have
\[
1 - P_{\text{inv}}^*(X_q, A) = \frac{\left| \bigcap_{x \in A} \bigcup_{M \in \mathcal{M}(x)} M \right|}{|X_q|} + \frac{O(r^r)}{q}.
\]

Now we look at the right-hand side of the above equation. Assume \( y \in \Delta \). Then \( y \) is regular semisimple; let \( K \) be its maximal torus in \( X \). Assume \( y \in K \) for some \( K \in \mathcal{M}(x) \) and some \( x \in A \) (and \( K \) is \( \sigma \)-stable of maximal rank). By definition of \( \Delta \) we have \( y \in K^\circ \). By Lemma 3.3, \( y \) lies in some \( \sigma \)-stable maximal torus of \( K^\circ \), which is also a maximal torus of \( X \), hence must coincide with \( S \). In particular, if \( y \) lies in some member of \( \mathcal{M}(x) \) for every \( x \in A \), then \( S \) belongs to \( T(x) \) for every \( x \in A \). Using Theorem 3.6, this shows that
\[
1 - P_{\text{inv}}^*(X_q, A) = \frac{\left| \bigcup_{i=1}^{r} (T_{w_i})_\sigma \right|}{|X_q|} + \frac{O(r^r)}{q}.
\] (5)

Finally, the right-hand side of (5) is equal to the right-hand side of (4) by Theorem 3.8.

We record a consequence of the previous proof.

Remark 3.11. Assume \( \cap_{x \in A} T(x) = \emptyset \). Then the set \( \Delta \) contributes to \( P_{\text{inv}}^*(X_q, A) \). In other words, for every \( y \in \Delta \), there exists \( x \in A \) such that, for every \( g_1, g_2 \in X_q \), every maximal overgroup of \( \langle x^{g_1}, y^{g_2} \rangle \) in \( X_{q^2} \) contains \( (X_{q^2})' \).

3.3. From \( X_{q^2} \) to \( (X_{q^2})' \). All the discussion above is about \( X_{q^2} \), which need not be perfect. Here we establish the connection to the corresponding finite simple groups, which we need in order to prove our main results. In addition, we will show that the isogeny type of \( X \) is not relevant. Let \( X_{q^2} \) be the group of simply connected type, and let \( \pi : X_{q^2} \to X \) be the natural isogeny. Then \( \pi \) lifts to a morphism \( X_{q^2} \to X_{q^2} \) (see [MT11, Proposition 22.7]), which for convenience we still denote by \( \pi \). Write as usual \( X_{q^2} = X_q \) and \( (X_{q^2})_{q^2} = (X_{q^2})_{q^2} \).

Lemma 3.12. Let \( A \) be a subset of \( (X_{q^2})_q \). Then
\[
P_{\text{inv}}((X_q)^r, A^r) = P_{\text{inv}}((X_{q^2})_q, A) = P_{\text{inv}}^*(X_q, A^r) + \frac{O(r^r)}{q}.
\]

Proof. Let \( Z \) be the kernel of \( \pi \). Then \( (X_{q^2})_q / Z_{q^2} \cong ((X_{q^2})_q)^r = (X_q)^r \) (MT11, Proposition 24.21]). Moreover \( Z_{q^2} \) is contained in every maximal subgroup of \( (X_{q^2})_q \), hence the first equality of the statement holds.

Now note that \( P_{\text{inv}}((X_{q^2})_q, A) = P_{\text{inv}}^*(((X_{q^2})_q, A)) \), since \( (X_{q^2})_q \) is perfect. Since \( Z \) is contained in every maximal torus of \( X_{q^2} \), \( \pi \) induces a bijection between \( \sigma \)-stable subgroups of maximal rank of \( X_{q^2} \) and \( X \), which maps overgroups of \( y \in A \) to overgroups of \( y^\sigma \in A^\sigma \). Then the second equality follows from Theorem 3.10.

In order to prove Theorem 1.5(1), in view of Theorem 3.10 and Lemma 3.12 it is sufficient to choose \( X \) of some isogeny type, and prove the following statement.

Theorem 3.13. Assume \( r \geq 2 \) and \( q \geq Cr^r \) for some large constant \( C \), and assume \( X_q \not\cong G_2(q) \) when \( 3 \mid q \). Then, there exists \( A_q \subseteq (X_q)^r \) of size as in Table 7 such that \( \cap_{x \in A_q} T(x) = \emptyset \).
3.4. Reductive subgroups of maximal rank. By the Borel–Tits theorem (see [BT71 Corollaire 3.9]), a maximal $σ$-stable subgroup of $X$ of maximal rank is either parabolic, or its connected component is reductive. In this subsection we make some general observations regarding the second case.

Let $T$ be a $σ$-stable maximal torus of $X$, let $Φ$ be the root system with respect to $T$, and denote by $U_α$, $α ∈ Φ$, the corresponding root subgroups. Let $W = N_X(T)/T$ be the Weyl group of $X$ with respect to $T$.

Assume that $σ$ acts trivially on $Φ$. This is not essential, but it makes the statement of Lemma 3.14 below, easier (and, of course, we will need the lemma only under this assumption).

The following discussion is taken from [LSS92]. Let $K$ be a closed connected reductive subgroup of $X$ containing $T$. Then, $K = (T, U_α, α ∈ Ψ)$ for a $p$-closed subset $Ψ$ of $Φ$ (see [MT11 Section 13] for this notion). Let $W(Ψ)$ be the Weyl group of $K$, i.e., the subgroup of $W$ generated by the reflections in roots of $Ψ$. We have $N_X(K)/K ∼= N_W(W(Ψ))/W(Ψ) =: W_Ψ$. Note that $K$ is $σ$-stable, since $σ$ acts trivially on $Φ$.

Assume now $H$ is a $σ$-stable conjugate of $K$. In particular, there exists $g ∈ X$ such that $H = K^g$ and $T^g$ is $σ$-stable. Then $g^α g^{-1} ∈ N_X(T) ∩ N_X(K)$, which maps to an element of $W_Ψ$ that we denote by $ρ(K^g)$.

Lemma 3.14. Assume that $σ$ acts trivially on $Φ$. The map $ρ$ defined above induces a well-defined bijection between $\{X_σ$-orbits on the $σ$-stable conjugates of $K\}$ and $\{conjugacy classes in $W_Ψ\}$.

Proof. This is [Car78 Propositions 1 and 2] in case $σ$ acts trivially on $Φ$. □

In [Car78 Propositions 1 and 2] the general case, in which $σ$ does not necessarily act trivially, is considered. This is more technical to state.

Next, given a $σ$-stable maximal torus $S$, we want to determine its closed connected reductive overgroups in $X$. We do not need to assume that $σ$ acts trivially, since the argument is the same. Fix $g$ such that $S = T^g$ and let $w$ be the image of $g^α g^{-1}$ in $W$.

The following result appears as [Wei92 Theorem 5], although the language and the proof seem slightly different.

Lemma 3.15. The closed connected $σ$-stable reductive overgroups of $S$ are in bijection with $p$-closed subsets of $Φ$ which are $σw$-stable.

Proof. If $H$ is a closed connected $σ$-stable reductive overgroup of $S$, set $K := H^g$. Then $K = (T, U_α, α ∈ Ψ)$ for some (unique) $p$-closed subset $Ψ$ of $Φ$. Moreover, $σg^αg^{-1}$ normalizes $K$ and $T$, hence $σw$ fixes $Ψ$. Conversely, assume $Ψ$ is $σw$-stable and $p$-closed; then $(T, U_α, α ∈ Ψ)^g$ is a closed connected reductive overgroup of $S$ (see [MT11 Theorem 13.6]). For $α ∈ Ψ$ we have $(U_α^g)^σ = U_α^σg^α = (U_α^σg^αg^{-1})^g = (U_ασw)^g$. Since $Ψ$ is $σw$-stable, we deduce that $(T, U_α, α ∈ Ψ)^g$ is $σ$-stable. □

Of course, if $σ$ acts trivially on $Φ$, then a subset of $Φ$ is $σw$-stable if and only if it is $w$-stable.

At this point we divide the discussion between exceptional and classical groups.
Table 2. $A_b = \{x_1, x_2\}$ in Theorem 1.5 for exceptional groups $G \neq F_4(2^n)$.

| $G$                   | $|x_1|$ | $|x_2|$ |
|-----------------------|--------|--------|
| $^2B_2(q^2)$          | $\Phi'_8$ | $\Phi'_8(-q)$ |
| $^2G_2(q^2)$          | $\Phi'_{12}$ | $\Phi'_{12}(-q)$ |
| $G_2(q), 3 \nmid q$   | $\Phi_3$ | $\Phi_3(-q)$ |
| $^3D_4(q)$            | $\Phi_{12}$ | $(q^3 + 1)(q - 1)/(2, q - 1)$ |
| $^2F_4(q^2)$          | $\Phi'_{24}$ | $\Phi'_{24}(-q)$ |
| $F_4(q), q$ odd       | $\Phi_{12}$ | $\Phi_8$ |
| $E_6(q)$              | $\Phi_9 \Phi_{12}/(3, q - 1)$ | $\Phi_9 \Phi_8/\delta$ |
| $^2E_6(q)$            | $\Phi_9 \Phi_{12}/(3, q + 1)$ | $\Phi_9 \Phi_8/\delta'$ |
| $E_7(q)$              | $\Phi_2 \Phi_{18}/(2, q - 1)$ | $\Phi_9/(2, q - 1)$ |
| $E_8(q)$              | $\Phi_{30}$ | $\Phi_{30}(-q)$ |

4. Exceptional groups

In this section we will prove Theorem 1.5 for simple exceptional groups, which implies Theorem 1.5(1) for these groups, and we will prove Theorem 1.5(3) for $G_2(3^n)$.

We choose $X$ of adjoint type. The maximal subgroups of $X_\sigma$ of maximal rank have been classified by Liebeck–Saxl–Seitz [LSS92].

We can assume that $q$ is sufficiently large in the proof. This implies that every maximal torus $S_\sigma$ of $X_q$ contains regular semisimple elements. (In fact, more is true. By Theorem 3.5, almost all elements of $X_q$ are regular semisimple. By Theorem 3.8, the proportion of elements of $X_q$ lying in $\tilde{S}_\sigma$ is bounded away from zero; therefore, almost all elements of $\tilde{S}_\sigma$ are regular semisimple.) In particular, it follows that whenever $S_\sigma \leq M^n_2$, with $M^n_2 \in \mathcal{M}_c$, then $S \leq M^n$. We define $A_b$ as the set of elements of $(X_q)^\sigma$ appearing in Table 2. We assume that $X_q \neq G_2(2), G_2(3), F_4(2)$. In the table, the case $F_4(q)$ with $q$ even is missing. In this case the set $A_b$ has size 6, hence for aesthetic reasons we have not included it. We will treat this case in detail in Subsection 4.6.

Each element in Table 2 is regular semisimple. The existence of these elements follows from the general theory of the structure of maximal tori, cf. [MT11, Section 25]. For the element $x_2$ in case $G = E_6(q)$, $\delta = (3, q - 1)(4, q - 1)$. For the element $x_2$ in case $G = \mathbb{F}_q(q)$, $\delta' = (3, q + 1)(4, q + 1)$.

We write $\Phi_n = \Phi_n(q)$ for the $n$-th cyclotomic polynomial evaluated at $q$. Moreover $\Phi'_8 = \Phi'_8(q) = q^2 + \sqrt{2}q + 1$, $\Phi'_{12} = \Phi'_{12}(q) = q^2 + \sqrt{3}q + 1$, $\Phi'_{24} = \Phi'_{24}(q) = q^4 + \sqrt{2}q^3 + q^2 + \sqrt{2}q + 1$ (this notation is taken from [GM12a]). We will refer to [GM12a, Table 6] and [GM12b, Table 1] for the overgroups of many elements in Table 2. We remark that the aforementioned tables from [GM12a] and [GM12b] rely mostly on [We92].

4.1. Some twisted groups, and $E_8(q)$. In many cases we can exploit a very convenient situation. Indeed, consider the groups $^2B_2(q^2), ^2G_2(q^2), ^3D_4(q), ^2F_4(q^2)$ and $E_8(q)$. Then by [GM12a, Table 6] we see that the element $x_1$ lies only in one maximal subgroup of $X_q$, namely $N_{X_q}(S_\sigma)$, where $S_\sigma$ is the unique maximal torus of $X_q$ containing $x_1$. Since $q$ is large, $S_\sigma$ contains regular semisimple elements, and in particular $N_{X_q}(S_\sigma) = N_{X_q}(S)$. (We note that, in fact, $N_{X_q}(S_\sigma) = N_{X_q}(S)$ holds
under the weaker probability that \( S_\sigma \) is nondegenerate; see [Car93, Section 3.6] for this notion.) The connected component of \( N_X(S) \) is \( S \), since \( S \) has finite index in its normalizer. By definition, we deduce that \( T(x) \) contains only the conjugates of \( S_\sigma \).

Then, in order to prove Theorem 3.13 in these cases, we just need to show that the element \( x_2 \) does not belong to any conjugate of \( N_X(S_\sigma) \). This is easily done by order considerations.

4.2. \( E_6(q) \) and \( ^2E_6(q) \). We write \( E_6(q) = + \) \( E_6(q) \) and \( ^2E_6(q) = -E_6(q) \). Consider \( ^2E_6(q) \) with \( \varepsilon \in \{+,-\} \). By [GM12] Table 1, \( x_1 \) is contained only in \(( ^2D_4(q) \times (q^2 + \varepsilon q + 1)) / \delta_\varepsilon \) (among the maximal subgroups of \( X_\sigma \)). The order of \( x_2 \) is \( (q^4 + 1)(q^2 - 1)/\delta_\varepsilon \), where \( \delta_\varepsilon = (3, q - \varepsilon 1)h_\varepsilon \) and \( h_\varepsilon = (4, q - \varepsilon 1) \). For \( \varepsilon = -1 \), \( x_2 \) is contained in a maximal subgroup \( M = h_\varepsilon.(PQ_{10}(q) \times (q - \varepsilon)/h_\varepsilon).h_\varepsilon \); and for \( \varepsilon = + \), \( x_2 \) is contained in a parabolic subgroup with Levi complement of type \( D_5 \) (cf. [LSS92 Table 5.1]). By order considerations we see that if \( \varepsilon = + \) then \( \mathcal{M}(x_2) \) contains only parabolics of type \( D_5 \), while if \( \varepsilon = - \) then \( \mathcal{M}(x_2) \) contains the conjugates of \( M \), and parabolics with Levi complement of type \( ^2D_4 \). Using the knowledge of maximal tori of \( ^2E_6(q) \) (see [DF91]), we deduce by order considerations that \( T(x_1) \cap T(x_2) = \emptyset \), which proves Theorem 3.13 in these cases.

In Subsections 4.3, 4.4 we employ the notation of Subsection 4.1.

4.3. \( G_2(q) \) with \( 3 \nmid q \). Let \( G = G_2(q) \) with \( q \geq 3 \). We immediately recall some facts regarding maximal tori of \( G_2(q) \) that we will use also in Subsection 4.3. We have \( W = W(G_2) \cong D_{12} \), hence by the general theory (see [MT11 Section 25]) there are six \( G_2(q) \)-classes of maximal tori, with representatives \( T_1, \ldots, T_6 \), and with orders \( q^2 - 1, q^2 - 1, (q - 1)^2, (q + 1)^2, q^2 + q + 1, q^2 - q + 1 \), respectively. We assume \( T_i = (T_{w_i})_x \), where \( w_1 \) is a reflection in a short root, \( w_2 \) is a reflection in a long root, \( w_3 = 1, w_4 = -1, |w_3| = 3, |w_4| = 6 \). For \( i = 1, \ldots, 6 \), we will write \( \Delta_i \) instead of \( \Delta_{T_i} \).

By Theorem 3.8 the proportion of elements lying in \( \bar{T}_1 \cup \bar{T}_2 \) is equal to \( O(1/q) \) plus the proportion of noncentral involutions of \( D_{12} \), which is \( 1/2 \). Consequently, the proportion of elements lying in \( \cup_{i=3}^6 \bar{T}_i \) is \( 1/2 + O(1/q) \). By Theorem 3.6, the same estimates hold if we replace each \( \bar{T}_i \) by \( \Delta_i \).

Assume now \( 3 \nmid q \). By [LSS92 Table 5.1] and by order considerations, \( \mathcal{M}(x_1) \) contains only the conjugates of \( SL_3(q), 2 \), and \( \mathcal{M}(x_2) \) contains only the conjugates of \( SU_3(q) \). In order to prove Theorem 3.13 in this case, we need to show that these two subgroups do not contain a common maximal torus (up to conjugacy). By order considerations, if there exists a common torus of \( SL_3(q).2 \) and \( SU_3(q).2 \), then it must be \( T_1 = (T_{w_1})_x \) or \( T_2 = (T_{w_2})_x \). For \( i = 1, 2 \), fix \( g_i \in X = G_2 \) such that \( T_{w_i} = T^{g_i} \) (and \( g_i^{-1} \) maps to \( w_i \) in \( W \)). By Lemma 3.15 the closed connected subgroups of \( G_2 \) containing \( T_{w_i} \) are precisely the subgroups \( K(\Psi)^{g_i} \), where \( K(\Psi) = (T, U_\alpha, \alpha \in \Psi) \) and \( \Psi \) is \( p \)-closed and \( \Psi \)-stable. Since \( 3 \nmid q \), by [MT11 Theorem 13.14] we deduce that every \( p \)-closed subset of \( \Phi \) is closed; in particular there is only one \( p \)-closed subset \( \Psi \) of type \( A_2 \): the set of all long roots. Note that \( W_\Psi = N_W(\Psi) / W(\Psi) \cong C_2 \), hence by Lemma 3.14 there are two corresponding \( G_2(q) \)-classes. Now \( w_2 \in W(\Psi) \), while \( w_1 \notin W(\Psi) \); then by Lemma 3.14 \( K(\Psi)^{g_2} \) is \( G_2(q)-\)conjugate to \( K(\Psi) \), and \( K(\Psi)_x \cong SL_3(q) \), while \( K(\Psi)^{g_1} \cong SU_3(q) \). This implies that \( SL_3(q).2 \) and \( SU_3(q).2 \) do not contain a common maximal torus (up to conjugacy), and Theorem 3.13 follows in this case.
4.4. $G_2(q)$ with $3 \mid q$. We keep the notation from the beginning of Subsection 4.3. Let $G = G_2(q)$. We want to prove $P_{\text{inv}}(G, G) = 1/2 + O(1/q)$, namely, Theorem 4.5(3) in this case. We will prove the following more precise statement, which we will use in Section 6. We note that $x \in G$ contributes to $P_{\text{inv}}(G, G)$ if and only if $P_{\text{inv}}(G, x) > 0$.

**Theorem 4.1.** Let $G = G_2(q)$ with $3 \mid q$.

(i) $P_{\text{inv}}(G, x) \geq 1/6 + O(1/q)$ for a proportion of elements $x \in G$ of the form $1/2 + O(1/q)$.

(ii) $P_{\text{inv}}(G, x) = 0$ for a proportion of elements $x \in G$ of the form $1/2 + O(1/q)$.

**Proof.** There is an automorphism $\gamma$ of $G_2(q)$ which induces a graph automorphism of order two on the Dynkin diagram, exchanging long and short roots. The set $\Psi'$ of short roots is 3-closed (cf. [MTT1 Proposition 13.15]). There are two conjugacy classes of subgroups $\text{SL}_3(q).2$, with representatives $H_1$ and $H_2$, and two conjugacy classes of subgroups $\text{SU}_3(q).2$, with representatives $K_1$ and $K_2$. We have $H_1^\gamma = H_2$ and $K_1^\gamma = K_2$. Moreover $\gamma$ exchanges the classes of $T_1$ and $T_2$. Up to changing indices, $T_1$ is contained in a conjugate of $H_1$ and $K_1$. What is more, the only overgroups of $T_5$ (resp. $T_6$) are conjugates of $H_1$ and $H_2$ (resp. conjugates of $K_1$ and $K_2$).

Therefore, by definition of $\Delta$, every element of $\Delta_3$ (resp. $\Delta_4$, resp. $\Delta_5$) invariably generates with every element of $\Delta_6$ (resp. $\Delta_5$, resp. $\Delta_6$). We observed that the proportion of elements belonging to $\cup_{j=3}^5 \Delta_j$ is $1/2 + O(1/q)$. Moreover, for $j \in \{5,6\}$, we have $|\Delta_j / \Gamma| = 1/6 + O(1/q)$. Therefore item (i) is proved.

We move to (ii). We want to show that

\[(\star)\] for every $x \in G$, $x$ belongs to a maximal subgroup containing a conjugate of $T_1$, and to a maximal subgroup containing a conjugate of $T_2$.

This implies that all elements $y$ lying in $\tilde{T}_1 \cup \tilde{T}_2$ are such that $P_{\text{inv}}(G, y) = 0$. We observed that these elements have proportion $1/2 + O(1/q)$, hence in order to prove (ii) we only need to prove (\star).

It is sufficient to focus on $i = 1$, since the two tori are exchanged by an automorphism of $G$. Representatives of the conjugacy classes of maximal subgroups containing $T_1$ are the following:

$$\{P, H_1, K_1, C\}.$$ 

Here $P$ is a parabolic subgroup with respect to the short root of a base, and $C \cong (\text{SL}_2(q) \circ \text{SL}_2(q)).2$ is the centralizer of an involution in $G_2(q)$ (cf. [Kle88 Theorem A]; recall that $G$ contains a unique conjugacy class of involutions).

Let $x \in G$. If $x$ is unipotent, then $x$ is contained in both conjugacy classes of maximal parabolic subgroups. Assume then $x = su$, with $1 \neq s$ semisimple, $u$ unipotent, and $[s, u] = 1$. Then $x \in C_G(s) < G$. If $C_G(s)$ is a maximal torus of even order, it is contained in a conjugate of $C$. The remaining classes of maximal tori have representatives $T_5$ (contained in $H_1$) and $T_6$ (contained in $K_1$). Examining [Kle88 Table II, p. 41], we see that all other possibilities for $C_G(s)$ contain a central involution, hence are contained in a conjugate of $C$. Then (\star) is proved and we are done. \qed
4.5. $E_7(q)$. By [GM12a Table 6] and [GM12b Table 1] we see that $x_1$ is contained only in a maximal subgroup $^2E_6(q)_{sc} \cdot D_{q+1}$ of $X_\sigma$, and $x_2$ is contained in two (conjugate) parabolics $P$ and $P'$ of type $E_6$, and in the normalizer of a common Levi complement $L$. Our aim is to show that $T(x_1) \cap T(x_2) = \emptyset$.

**Claim 4.2.** Assume $g \in X = E_7$ and assume $g^w g^{-1} \in N_X(T)$ maps to $w \in W$. Assume $\Psi$ and $\Psi'$ are two $p$-closed subsets of $\Phi$ of type $E_6$. If $w \in N_W(W(\Psi)) \cap N_W(W(\Psi'))$, then either $w \in W(\Psi) \cap W(\Psi')$ or $w \notin W(\Psi) \cup W(\Psi')$.

We first observe that Claim 4.2 implies $T(x_1) \cap T(x_2) = \emptyset$. Consider a maximal torus $S$ of $X_\sigma$; assume $S = (T_w)_\sigma$, where $T_w = T^g$ and $g^w g^{-1}$ maps to $w \in W$. By Lemma 3.15 the closed connected reductive subgroups of $E_7$ containing $T_w$ are precisely the subgroups $K(\Psi)^\sigma$, where $K(\Psi) = (T, U_\alpha, \alpha \in \Psi)$ and $\Psi$ is $p$-closed and $w$-stable (i.e., $w \in N_W(W(\Psi))$). Then Claim 4.2 together with Lemma 3.14 implies that $S = (T_w)_\sigma$ cannot be contained in both a maximal subgroup of type $^2E_6(q)_{sc} \cdot D_{q+1}$ and a Levi complement of type $E_6$, so that $S \notin T(x_1) \cap T(x_2)$ and (since $S$ was arbitrary) $T(x_1) \cap T(x_2) = \emptyset$.

In order to prove Claim 4.2 we recall that $W = \langle x \rangle \times W^+$, where $|x| = 2$ and $W^+ \cong Sp_6(2)$ is the “reflection subgroup”, consisting of the elements of $W$ with determinant 1 in the action on $R^7$. We will view the elements of $W$ as pairs, according to this decomposition. If $\Psi$ is a subset of type $E_6$, then $W(\Psi) \cong SO_6^\perp(2)$. Clearly we cannot have $W(\Psi) \subseteq W^+$, since $W(\Psi)$ contains reflections. Let $K$ be the unique subgroup of $W(\Psi)$ of index 2, isomorphic to $\Omega_6^\perp(2)$. Then $K \subseteq W^+$. Let $H \cong SO_6^\perp(2)$ be the normalizer of $K$ in $W^+$; we have $H = K \times \langle r \rangle$, where $r$ is a reflection in a non-singular vector (for the orthogonal geometry on $F_2^7$). We have $W(\Psi) = \langle (x, r), K \rangle$ and $N_W(W(\Psi)) = \langle x \rangle \times H$. Now if $\Psi'$ is another subset of type $E_6$, we have $\Psi' = \Psi^g$ with $g \in W^+$, and consequently $W(\Psi') = \langle (x, r^g), K^g \rangle$ and $N_W(W(\Psi')) = \langle x \rangle \times H^g$. We see that Claim 4.2 is equivalent to the following condition:

$$(\ast)$$ Fix $\Psi$ as above. Then, for every $g \in W^+$, $W(\Psi) \cap N_W(W(\Psi^g)) \subseteq W(\Psi^g)$.

It is easy to see that $(\ast)$ is equivalent to

$$(\ast\ast)$$ Fix $K \subseteq W^+$ and $H \subseteq W^+$ as above. Then, for every $g \in W^+$, $K \cap H^g \subseteq K^g$.

Here the condition in $(\ast\ast)$ holds in general, in the following sense. Assume $q$ is even, and recall that $Sp_{2m}(q) \cong SO_{2m+1}(q)$ (see Remark 5.4 for further details concerning this isomorphism). Denote by $V$ the $(2m + 1)$-dimensional orthogonal module. Then $(\ast\ast)$ is a particular case of the following lemma.

**Lemma 4.3.** Assume $W$ and $W'$ are nondegenerate hyperplanes of $V$ (not necessarily of the same sign). Then $\Omega(W) \cap SO(W') \subseteq \Omega(W')$.

**Proof.** Recall that $\Omega(W)$ can be characterized as the subset of $SO(W)$ consisting of the elements $g$ such that $\dim C_W(g)$ is even (cf. [W109 p. 77]). We have $V = W \perp V^\perp$, and $g$ acts trivially on $V^\perp$, therefore $\dim C_W(g) = \dim C_V(g) - 1$, which is independent of $W$. This proves the lemma.

Claim 4.2 is proved and Theorem 3.13 follows in this case.

4.6. $F_4(q)$. For exceptional groups, we proved Theorem 3.13 in all cases except for $F_4(q)$, which is handled in this subsection.
We first fix some notation taken from [Law99]. Let $\mathbb{R}^4$ be equipped with the usual orthonormal basis $e_1, \ldots, e_4$. We may take $\Phi \subseteq \mathbb{R}^4$ with set of positive roots

$$\Phi^+ = \{e_i \pm e_j, 1 \leq i < j \leq 4\} \cup \{e_i, 1 \leq i \leq 4\} \cup \{(e_1 \pm e_2 \pm e_3 \pm e_4)/2\}$$

and base

$$\Sigma = \{e_2 - e_3, e_3 - e_4, e_4, (e_1 - e_2 - e_3 - e_4)/2\}.$$

As in [Law99], we will write 1 in place of $e_1$, 1 − 2 in place of $e_1 - e_2$, + − −− in place of $(e_1 - e_2 - e_3 - e_4)/2$, etc. The corresponding reflections in the Weyl group will be denoted by $w_1, w_{1-2}, w_{4-}, \ldots,$ etc. In [Law99] the complete list of maximal tori of $F_4(q)$ is given. In particular, for each $(\delta, \delta') \in \{+, -\}^2$, there are two conjugacy classes of maximal tori of order $(q^3 + 1)(q + 1)(q + 1)^2$; we let $T_{\delta, \delta'}^1, i = 1, 2$, be representatives for the two classes (so for instance $T_{1, -}^1$ is a representative of a class of tori of order $(q^3 + 1)(q - 1)$). Assume $T_{\delta, \delta'}^1 = (\mathcal{F}_w)_{\sigma}$ with $w = w_{\delta, \delta'}^i$. With notation as in [Law99] pp. 94–96, we may choose

$$w_{1,+}^1 = w^{(13)} = w_3 w_{2-3} w_{1-2} w_4 \quad w_{2,+}^1 = w^{(20)} = w_1 w_2 w_4 w_{++-}$$
$$w_{1,-}^1 = w^{(15)} = w_4 w_{3-4} w_{2-3} \quad w_{2,-}^1 = w^{(13)} = w_4 w_{3-4} w_{++-}$$
$$w_{1,+}^1 = w^{(14)} = w_1 w_3 w_{4-3} w_{2-3} \quad w_{2,+}^1 = w^{(15)} = w_{1-2} w_4 w_{++-}$$
$$w_{1,-}^1 = w^{(12)} = w_3 w_{4-3} w_{2-3} \quad w_{2,-}^1 = w^{(7)} = w_4 w_{+-}$$

Here composition is right-to-left; this however makes no difference, because in a Weyl group every element is conjugate to its inverse, cf. [Car93, Corollary p. 45].

We are now ready to begin the proof of Theorem 3.13 in this case. We divide the cases $q$ even and $q$ odd.

(a) Assume $q$ is odd. By [GM12a, Table 6] we have that $x_1$ is contained only in a subgroup $^3D_4(q)$, and by [GM12b, Table 1] $x_2$ is contained only in a subgroup $2\Omega_3(q)$. We need to show that $T(x_1) \cap T(x_2) = \emptyset$. By order inspection, the only possibilities for $T(x_1) \cap T(x_2)$ are the eight tori $T_{\delta, \delta'}^1$. By our choice (see [Law99] pp. 94–95) the maximal tori of type 1 (i.e., the tori $T_{\delta, \delta'}^1$) are contained in $2\Omega_3(q)$. This subgroup is obtained as the fixed points of a connected reductive subgroup of $F_4$ of type $B_4$. In order to conclude the proof, we need to show that none of the tori $T_{\delta, \delta'}^1$ belongs to a conjugate of $^3D_4(q)$.3. Fix $(\delta, \delta')$, and fix $g \in X$ such that $T_{w, \delta'}^1 = T^g$. There is a unique $p$-closed subset $\Psi$ of $\Phi$ of type $D_4$, namely the set of all long roots (the set of all short roots is only 2-closed). Of course $\Psi$ is fixed by every element of $W$. Correspondingly, by Lemma 3.15, $T_{w, \delta'}^1$ has a unique connected reductive overgroup of type $D_4$, namely $\langle T, U_\alpha, \alpha \in \Psi \rangle^g$. The fixed points of such a subgroup is of type $D_4(q)$ or $^2D_4(q)$. Indeed, this is true for every maximal torus of $B_4$. It follows that $T_{\delta, \delta'}^3$ is contained in $D_4(q)$ or $^2D_4(q)$, but not in $^3D_4(q)$. This concludes the proof in case $q$ is odd.

(b) Assume $q$ is even. There is an automorphism $\gamma$ of $F_4(q)$ which induces a graph automorphism of order two on the Dynkin diagram, sending 2 − 3 to + − −− and 3 − 4 to 4. In this case, there are two conjugacy classes of maximal subgroups isomorphic to $\Omega_9(q)$: we pick representatives $B_4^1$ and $B_4^2$ for them. Similarly, there are two conjugacy classes of maximal subgroups isomorphic to $^3D_4(q)$, $^3D_4(q)S_4$, $P^1, Q^i$; we pick representatives $^3D_4^1, D_4^1, P^i, Q^i$, $i = 1, 2$, in the respective cases. Here $P^1$ (resp. $P^2$) denotes a parabolic subgroup of type $B_3$ (resp. $C_3$); $Q^1$ (resp. $Q^2$) denotes a parabolic subgroup of type $A_2 \times A_1$ (resp. $A_2 \times A_1$), where $A_i$
denotes a subset consisting of short roots. (The reason why there are two classes of reductive subgroups as above is that there are subsets of $\Phi$ of type $C_4$ and $D_4$ which are 2-closed; see [MT11 Proposition 3.15].) We see that all the pairs of classes above are fused by $\gamma$, i.e., $(B_2^1)\gamma = B_2^1$ and similarly for the others. There are also maximal subgroups $e.(\text{PSL}_3^2(q) \times \text{PSL}_3^2(q)).e.2$, with $e \in \{+, -\}$ (one class for each sign; here $\text{PSL}_3^2(q)$, $\text{PSL}_3^2(q) = \text{PSU}_3(q)$ and $e = (3, q - e1)$). We let $R_\varepsilon$ be representatives of these classes.

We observe that for every $(\delta, \delta') \in \{+, -\}^2$, $\gamma$ exchanges the classes of $T_{\delta, \delta'}^1$ and $T_{\delta, \delta'}^2$. This can be seen as follows. In [Gut72 Table 1], the action of $\gamma$ on $\Phi$ is computed (see also (2.15) of the same paper). In particular we have

\[
\begin{align*}
(w_{1,+})^\gamma &= w_{3+4} w_{-} - - w_{2} w_{-4} \\
(w_{1,-})^\gamma &= w_{3-4} w_{+} - - \\
(w_{1,+})^\gamma &= w_{1+2} w_{4} w_{+} - - \\
(w_{1,-})^\gamma &= w_{3} w_{+} - - \\
\end{align*}
\]

At this point one computes that in each case $(w_{1,\pm})^\gamma$ is $W$-conjugate to $w_{2,\pm}$. This is immediate if $(\delta, \delta') = (-, -)$. In general, it is sufficient to prove that $(w_{1,\pm})^\gamma$ is not conjugate to $w_{1,\pm}$. This can be done for instance by showing that $(w_{1,\pm})^\gamma$ and $w_{1,\pm}$ have different root lengths inside the $(-\delta')$-eigenspace relative to the action on $\mathbb{R}^4$. It follows that $(T_{\delta, \delta'}^1)^\gamma$ is $F_4(q)$-conjugate to $T_{\delta, \delta'}^2$.

Now note that for every $(\delta, \delta')$, each subgroup $B_4^1, 3D_4^1, D_4^1, P^1$ and $Q^1$ contains members of at most one class of tori of type $T_{\delta, \delta'}$. By the same argument as in item (a), we may choose notation such that for every $(\delta, \delta')$, $T_{\delta, \delta'}^1$ belongs to a conjugate of $B_4^1, 3D_4^1$ and, possibly, $D_4^1$ (but not $D_2^1$). We now want to show that the maximal tori $T_{\delta, \delta'}^1$ can possibly belong only to conjugates of $P^1$ and $Q^1$, but not to conjugates of $P^2$ and $Q^2$. If we prove this, it will automatically follow that the tori $T_{\delta, \delta'}^2$ can belong only to type 2 subgroups. Note that by the previous considerations, if $T_{\delta, \delta'}^1$ belongs to a conjugate of $P^1$ (resp. $Q^1$), then it does not belong to a conjugate of $P^2$ (resp. $Q^2$).

By order considerations, $P^1$ and $P^2$ can contain the tori $T_{i,-}^i$ and $T_{i,+}^i$ for $i = 1, 2$. Moreover $Q^1$ and $Q^2$ can contain the tori $T_{i,-}^i$ and $T_{i,+}^i$ for $i = 1, 2$. No other embedding of the tori $T_{\delta, \delta'}^1$ in parabolic subgroups occurs. We see that $w_{1,-}^\gamma = w_{1,-}^{(12)}$ and $w_{1,+}^\gamma = w_{1,+}^{(15)}$ belong to the Weyl subgroup of type $B_3$ corresponding to removing $+- -$ from the base $\Sigma$. Therefore we deduce that $T_{i,-}^i$ and $T_{i,+}^i$ belong to $\text{Levi}$ complements of $F_4(q)$-conjugates of $P^1$. Therefore the case $P$ is done. We move to case $Q$, which is similar. We have $w_{1,-}^\gamma = w_{1,+}^{(14)}$. We see that both $w_{1,-}^{(12)}$ and $w_{1,+}^{(14)}$ belong to Weyl subgroups corresponding to a subset of type $A_2 \times A_1$. Indeed $w_{1,-}^{(12)}$ lies in the natural one corresponding to removing 4 from the base $\Sigma$; and $w_{1,+}^{(14)}$ lies in the subset in which a base of $A_2$ is $\{2 - 3, 3 - 4\}$ and a base of $A_1$ is $\{1\}$. Therefore, we obtain that $T_{i,-}^i$ and $T_{i,+}^i$ belong to $\text{Levi}$ complements of $F_4(q)$-conjugates of $Q^1$.

With all the information we have gathered, it is not difficult to complete the proof of Theorem 3.13 in this case. With this aim, we choose a generator $x_{i,-}^i$ of the cyclic torus $T_{i,-}^i$, $i = 1, 2$, and a generator $x_{i,+}^i$ of the cyclic torus $T_{i,+}^i$, $i = 1, 2$. Moreover we choose elements $x_1$ and $x_2$ as in item (a); in particular
$x_1$ belongs only to $3D_4^1$ and $3D_2^2$, and $x_2$ belongs only to $B_4^1$ and $B_4^2$. Our set of elements is therefore

$$A_b = \{x_1, x_2, x_{1,-}, x_{2,-}, x_{1,+}, x_{2,+}\}.$$ 

We now want to show that there is not a maximal torus of $F_4(q)$ belonging to an overgroup of all these elements. By order considerations, if a torus belongs to $T(x_1)$ and $T(x_2)$, then it must be one of the eight tori $T^{i, \delta}_q$. Assume $i = 1$: the argument is entirely symmetric and the case $i = 2$ is handled in the same way. By our choice of notation, $x_{1,-}$ and $x_{2,+}$ belong to type 2 subgroups. However $T^{1, \delta}_q$ does not belong to any of these. The only other overgroups of maximal rank of $(x_{1,-})$ and $(x_{2,+})$ are, respectively, $R_-$ and $R_+$. However, our torus $T^{1, \delta}_q$ belongs to exactly one of these (depending on the value of $\delta$). Therefore we have shown that the overgroups of our six elements cannot contain a common maximal torus, and the proof of Theorem 3.13 (and therefore Theorem 1.5(1)) for exceptional groups is concluded.

5. Classical groups of bounded rank

As promised at the beginning of Section 3, we immediately deal with $G \cong \text{PSL}_2(q)$.

Proof of Theorem 3.1. Let $G = \text{PSL}_2(q)$. The subgroup structure of $G$ is well known, cf. [Suz82, Chapter 3.6]. Let $d = (2, q - 1)$. Let $S_\pm$ be the set of elements of $G$ with order strictly larger than 5 and dividing $(q \pm 1)/d$, and let $S = S_+ \cup S_-$. We have $|S_\pm|/|G| = 1/2 + \Omega(1/q)$. Let $F$ be the set of elements of $G$ lying in subfield subgroups; we have $|F|/|G| = O(1/q^{1/2})$ (we observed this in Remark 1.2).

Let $A_b = \{x_1, x_2\}$, where $x_1$ has order $(q - 1)/d$ and $x_2$ has order $(q + 1)/d$. Every element of $S_+ \ (\text{resp. } S_-)$ invariably generates with $x_1 \ (\text{resp. } x_2)$. This proves Theorem 1.5. Every element of $S_+ \setminus F \ (\text{resp. } S_- \setminus F)$ invariably generates with every element of $S_- \ (\text{resp. } S_+)$. This proves Theorem 1.2. Now consider $B = (S_+ \times S_-) \cup (S_- \times S_+) \subseteq G^2$; we have $|B|/|G|^2 = 1/2 + \Omega(1/q)$. Moreover $B \setminus F^2$ consists of invariable generating pairs, which proves Theorem 1.4.

Remark 5.1. If $q$ is a square, every semisimple element of $\text{PGL}_2(q^{1/2})$ of order strictly larger than 5 belongs to $S_-$. Hence, by Theorem 3.10 almost all elements of $\text{PGL}_2(q^{1/2})$ are contained in $S_-$. Therefore, in the above proof we only need to consider elements belonging to $\text{PSL}_2(q^{1/2})$ with $r$ odd, and in Theorem 1.2 we could get an error term of type $O(1/q^{3/2})$; but we do not insist on this.

In the remainder of this section, we will prove Theorem 3.13 for classical groups. Together with Section 4, this will conclude the proof of Theorem 3.13 (which in turn implies Theorem 1.5(1)).

We first make our choice for the type of $X$. Let $k$ be an algebraic closure of a finite field of characteristic $p$ and let $X$ be one of the simple algebraic groups $\text{SL}_n(k)$ where $n \geq 2$, $\text{Sp}_n(k)$ where $n \geq 4$, or $\text{SO}_n(k)$ where $n \geq 7$. We require that if $X = \text{SO}_n(k)$ and $p = 2$ then $n$ is even.

Denote by $V = k^n$ the natural module of $X$. Here $\text{Sp}_n(k)$ is the group of isometries of a nondegenerate bilinear alternating form on $V$ (a square), while $\text{SO}_n(k)$ is the connected component of the isometry group $\text{O}_n(k)$ of a quadratic form on $V$, with associated nondegenerate bilinear form. We have $|\text{O}_n(k) : \text{SO}_n(k)| = 2.$
These groups are well defined up to conjugation in $GL_n(k)$ since all such forms are equivalent (for all this, see for instance [MT11 Section 1.2 and Definition 1.15]).

Let $\sigma : X \to X$ be a Steinberg morphism, as in [LS98] p. 434, such that $X_{\sigma}$ is one of the following finite groups:

$$X_{\sigma} = SL_n(q), SU_n(q), Sp_n(q) \ (n \text{ even}), SO_n^+(q) \ (q \text{ odd}), \Omega_n^\pm(q) \ (q, n \text{ even})$$

where $\varepsilon = \pm$ for $n$ even and $\varepsilon = \circ$ for $n$ odd, where by convention $SO_n^+(q) = SO_n(q)$.

Specifically, $\sigma = \sigma^\tau$, where $\sigma$ is a Frobenius morphism corresponding to the field automorphism $\alpha \mapsto \alpha^q$ of $k$ (for $q$ a power of $p$), and $\tau = 1$, or $X = SO_n(k)$ and $\tau$ is conjugation by a reflection in a nonsingular vector, or $X = SL_n(k)$ and $\tau$ is the inverse-transpose map (all this with respect to certain fixed bases).

Except for $SO_n^+(q)$, which has a derived subgroup $\Omega_n^+(q)$ of index 2, and except for finitely many other cases, the group $X_{\sigma}$ is perfect. See [KL90] Chapter 2) for the definition of $\Omega_n^+(q)$.

5.1. **Subgroups of maximal rank in classical groups.** We need to understand the subgroups of maximal rank in $X_{\sigma}$. The proof of the following theorem is largely taken from [LS98], with additional claims from [MT11 Section 13]. We prefer to give a proof, since we have not found it in the literature.

**Theorem 5.2.** Let $X$ and $\sigma$ be as above. Let $M$ be a $\sigma$-stable closed subgroup of $X$ of maximal rank. Then, $M$ is contained in a $\sigma$-stable subgroup of the following types.

(i) Stabilizer in $X$ of a nonzero proper subspace of $V$. If $X = Sp_n(k)$ or $SO_n(k)$, the space is totally singular or nondegenerate. If it is nondegenerate, it can be chosen of even dimension.

(ii) In case $X = SL_n(k)$, stabilizer in $X$ of a pair of proper subspaces $U$ and $W$ such that $\dim U + \dim W = \dim V$, $\dim U \neq \dim W$ and either $U \leq W$ or $U \cap W = 0$.

(iii) Stabilizer in $X$ of a decomposition $V = V_1 \oplus \cdots \oplus V_t$ with $t \geq 2$. If $X = Sp_n(k)$ or $SO_n(k)$, the spaces $V_i$ are isometric, and either pairwise orthogonal and nondegenerate of even dimension, or $t = 2$ and the spaces are totally singular.

(iv) $p = 2$, $X = Sp_n(k)$ and $M \leq N_X(SO_n(k)) = O_n(k)$.

**Proof.** We assume for the first part of the proof that we are not in case $X = SL_n(k)$ with $\sigma$ involving the inverse-transpose map. In particular $\sigma$ can be regarded as a semilinear map of $V$.

Assume first $M$ fixes a proper nonzero $\sigma$-stable subspace $W$, and choose it to be of minimal dimension. If there is a form, then $M$ fixes also $W^\perp$, which is $\sigma$-stable (cf. [LS98 Proposition 2.5]). Then $M$ fixes $W \cap W^\perp$, which is $\sigma$-stable, hence by minimality $W$ is either nondegenerate or totally isotropic. If the space is nondegenerate of odd dimension $\ell$, the only possibility is $X = SO_\ell(k)$ and $M^\circ \leq SO_\ell(k) \times SO_{n-\ell}(k)$. If $n$ is odd, then $M$ stabilizes also a nondegenerate space of even dimension $n - \ell$. If $n$ is even, instead, the stabilizer of $W$ has rank $n/2 - 1$, hence it is not of maximal rank. Assume now $W$ is totally isotropic. Then $M$ fixes also the set of singular vectors of $W$, which is $\sigma$-stable, hence by minimality either $W$ is totally singular, or $X = SO_n(k)$, $p = 2$, $n$ is even and $W$ is a nonsingular 1-space. In the latter case, however, the stabilizer is isomorphic to
Sp_{n-2}(k), which is not of maximal rank. In particular, if $M$ fixes a proper nonzero $\sigma$-stable subspace, we are in case (i) of the statement.

Then we assume that $M$ does not fix any proper nonzero $\sigma$-stable subspace of $V$. Let $H := M^\circ$ be the connected component of $M$. The proof of \cite{LS98} Lemma 3.2 shows that either both $M$ and $H$ act homogeneously, or we are in case (iii) of the statement. The parity requirement in (iii) comes from the following reason: if $X = SO_n(k)$ and the decomposition $V = V_1 \perp \cdots \perp V_t$ is isometric, then the connected component of the stabilizer of the decomposition is $SO(V_1) \times \cdots \times SO(V_t)$, which has maximal rank only if $V_i$ has even dimension.

Therefore assume $M$ and $H$ act homogeneously. By assumption $M$, hence $H$, contains a maximal torus $S$. Using the explicit description of maximal tori in classical groups, we note that as a $kS$-module $V$ is the sum of 1-dimensional pairwise nonisomorphic modules. In particular, it follows that both $M$ and $H$ act irreducibly.

Since $H$ is connected and it acts faithfully and irreducibly on $V$, it follows that $H$ is reductive (cf. \cite{MT11} Proposition 15.1)). Then $M = [H, H/Z(H)^\circ]$. It follows by Schur’s lemma that $Z(H) \subseteq Z(X)$, which is a finite group, hence $Z(H)^\circ \subseteq Z(X)^\circ = 1$. In particular, $H = [H, H]$ is semisimple. In \cite{MT11} Chapter 13, $H$ is called a subsystem subgroup of $X$. One checks easily that the examples in \cite{MT11} Theorem 13.12 give (well recognizable) reducible subgroups. In \cite{MT11} Proposition 13.15, item (1) corresponds to item (iv) in this theorem, and item (2) does not arise by assumption (if $X = SO_n(k)$ and $p = 2$ then $n$ is even). By \cite{MT11} Theorem 13.14], there are no other possibilities for $H$. This concludes the proof, except when $X = SL_n(k)$ and $\sigma$ involves the inverse-transpose map (the previous proof works also if $\sigma$ is not the identity).

Let us consider the remaining case. As in the proof of \cite{LS98} Lemma 3.7, we view $SL_n(k)$ as a subgroup of $SO_{2n}(k)$: we may decompose the orthogonal module as $E \oplus F$, in such a way that the embedding of $SL_n(k)$ is given by $g \mapsto \text{diag}(g, g^{-T})$. It follows from the proof of \cite{LS98} Lemma 3.7 that either we are in cases (i), (ii) or (iii) of the statement, or $M$ and $M^\circ$ act homogeneously on $E$. Then we may proceed exactly as in the first part of the proof (once $M^\circ$ was shown to be homogeneous, the morphism $\sigma$ was not used anymore).

\[\Box\]

5.2. Descending to finite groups. Aschbacher \cite{Asc84} described the core-free maximal subgroups of the finite almost simple classical groups, dividing them into nine classes, denoted by $C_1, \ldots, C_9, S$. We refer the reader to \cite{KL90} for a detailed description of the first eight classes. (Although in the present paper this does not make any difference, we remark that classes in \cite{Asc84} and classes in \cite{KL90} differ slightly; we take \cite{KL90} as a reference, modulo the change explained in Convention 5.3 below.)

Consider the following groups:

$$GL_n(q), GU_n(q), Sp_n(q) \ (n \text{ even}), SO_n^\pm(q) \ (q \text{ odd}), \Omega_n^\pm(q) \ (q, n \text{ even}) \quad (6)$$

with $\varepsilon \in \{+, -, \circ\}$. Let $H$ be a group as in (6). We will refer to a group $G$ with $H' \leq G \leq H$ as a finite classical group.

Let $G$ be a finite classical group with $G'$ quasisimple. Note that if $M$ is a maximal subgroup of $G$ not containing $G'$, then $Z(G) \leq M$, and in particular $M$ corresponds to a core-free maximal subgroup of the almost simple group $G/Z(G)$, so Aschbacher’s description applies to $M$. 

For a finite classical group $G$ with $G'$ quasisimple, set $u = 2$ if $G' = \text{SU}_n(q)$ and $u = 1$ otherwise. We give here a rough description of the maximal subgroups of $G$ of classes $C_1, C_2, C_3$. Maximal subgroups from class $C_1$ are subspace stabilizers; maximal subgroups from class $C_2$ stabilize suitable direct sum decompositions of the natural module, so they are subgroups of $\text{GL}_n(q^\ell) \wr S_n/\ell < \text{GL}_n(q^u)$ for some $\ell < n$; and maximal subgroups from class $C_3$ preserve an extension field structure on the natural module, so they are subgroups of $\text{GL}_{n/b}(q^{ub}) \rtimes \text{Gal}(F_{q^{ub}}/F_{q^u}) < \text{GL}_n(q^u)$ for some prime $b$.

It is convenient for us to adopt the following convention throughout.

**Convention 5.3.** When $q$ and $n$ are even, we consider the maximal subgroups $\text{SO}_n^+(q) < \text{Sp}_n(q)$ as members of Aschbacher’s class $C_1$.

**Remark 5.4.** Convention 5.3 is justified by the following discussion. When $q$ is even, $\text{Sp}_{2m}(q) \cong \text{SO}_{2m+1}(q) = O_{2m+1}(q)$, the group of isometries of a nonsingular quadratic form $Q$ on a $(2m + 1)$-dimensional space $V$. (Here, by nonsingular we mean that there are no nonzero vectors $v$ of $V^\perp$ such that $Q(v) = 0$.) Under these assumptions, it turns out that $V^\perp$ is a 1-dimensional subspace of $V$. Since $q$ is even and $Q$ does not vanish on $V^\perp$, it follows that $\text{SO}_{2m+1}(q)$ centralizes $V^\perp$. Through this identification, the subgroups $\text{SO}_{2m}^+(q)$ correspond to stabilizers of nondegenerate hyperplanes of $V$ (i.e., complements of $V^\perp$) of plus or minus type.

In the following statement, $\text{Cl}_n(q)$ denotes a group as in (8) (this is unusual notation; however it will not be used elsewhere and it should not cause any confusion). When we write in brackets “class $C_i$”, we mean that the subgroup $M_\sigma$ under consideration is contained in a maximal subgroup of $X_\sigma$ of class $C_i$.

**Theorem 5.5.** Let $X$, $\sigma$ and $M$ be as in Theorem 5.2. Then, $M_\sigma$ is contained in a maximal subgroup of $X_\sigma$ from classes $C_1$, $C_2$ or $C_3$.

Now assume that $M$ is contained in the stabilizer of a decomposition $V = V_1 \oplus \cdots \oplus V_t$ as in Theorem 5.2(iii).

1. If $X_\sigma = \text{SL}_n(q)$ or the decomposition is nondegenerate, then either $M_\sigma^o \leq \text{Cl}_n(q)^{t} \cap X_\sigma$ (class $C_2$), or $M_\sigma^o \leq \text{Cl}_n/\ell(q^\ell)^{t} \cap X_\sigma$ (class $C_3$), or $X_\sigma = \text{SU}_n(q)$ with $n$ even and $M_\sigma^o \leq \text{GL}_{n/b}(q^\ell)^{t} \cap X_\sigma$ (class $C_2$). In case $X_\sigma$ is orthogonal, $\ell$ and $n/b$ must be even.

2. If the decomposition is totally singular, then $X = \text{Sp}_n(k)$ or $\text{SO}_n(k)$, $n$ is even, and either $M_\sigma^o \leq \text{GL}_{n/2}(q)$ (class $C_2$), or $M_\sigma^o \leq \text{GU}_{n/2}(q)$ (class $C_3$).

**Proof.** Note that if $M$ stabilizes $V = V_1 \oplus \cdots \oplus V_t$ as in Theorem 5.2(iii), then $M^o$ fixes each $V_i$ (indeed the subgroup stabilizing each $V_i$ is a closed subgroup of finite index of $M$, hence contains the connected component). What is more, if $X = \text{SO}_n(k)$ and the $V_i$ are nondegenerate then $M^o \leq \text{SO}(V_1) \times \cdots \times \text{SO}(V_t)$. Keeping in mind this observation, the proof of the theorem follows from the arguments in LS98 Section 4, together with Theorem 5.2.

Before we define the set $A_k$ from Theorem 5.13 for the reader’s convenience we recall some facts about maximal tori in classical groups. We begin with some observations regarding conjugacy classes in wreath products, which we will use also later in the paper (see Remark 6.2).

**Remark 5.6.** Let $H$ be a finite group and let $G = H \wr S_m$, where $(x_1, \ldots, x_m)^\tau = (x_{1\tau^{-1}}, \ldots, x_{m\tau^{-1}})$ for $(x_1, \ldots, x_m) \in H^m$ and $\tau \in S_m$. It is well known and easily
seen that conjugacy classes in $G$ are in bijection with partitions of $m$, where each part is labelled by a conjugacy class of $H$ (see, for example, [?, Section 4.2]).

Moreover, it follows from a straightforward calculation that, given an element $x = (x_1, \ldots, x_m) \in H \wr S_m$, with $(x_1, \ldots, x_m) \in H$ and $\tau \in S_m$, one can identify its class as follows. Let $c_1, \ldots, c_t$ be the cycles of $\tau$; assume that $c_i = (i_1, \ldots, i_{\ell_i})$, so in particular $m = \sum_{i=1}^{t} \ell_i$. Then, the class of $x$ corresponds to the labelled partition of $m$ with parts $p_1, \ldots, p_t$, of length $\ell_1, \ldots, \ell_t$ respectively, where the part $p_i$ is labelled by the $H$-class containing the $H$-class splitting into two

Consider now the special case $H = C_2$, so $G = C_2 \wr S_m \cong W(B_m)$. In particular, conjugacy classes of $G$ are in bijection with partitions of $m$, where each part is equipped with a sign $\pm$ (we will refer to these as signed partitions).

Let $K$ be the subgroup of $G$ consisting of the elements $(x_1, \ldots, x_m) \tau$ with $x_i = \pm$ and $\prod_{i=1}^{m} x_i = \pm$; in particular, $|G : K| = 2$ and $K \cong W(D_m)$. The $W(B_m)$-classes of elements of $K$ are in bijection with signed partitions of $m$ where the product of the signs is $\pm$. Moreover, for $x \in K$, it follows from an easy computation that $x^K \neq x^G$ if and only if $x^G$ corresponds to a signed partition in which all parts have even length and have plus sign.

5.3. Maximal tori in classical groups. The conjugacy classes of maximal tori in finite classical groups have an interpretation in terms of (signed) partitions. We quickly recall some facts. For more details, see for instance [FG17, Section 5]. In each of the cases below, $\sigma$ denotes the defining Steinberg endomorphism.

(i) Let $G = SL_n(q)$. We have $W(A_{n-1}) \cong S_n$, so conjugacy classes of maximal tori in $G$ are in bijection with partitions of $n$. The torus $(T_w)_\sigma$ corresponding to a partition $w = (a_1, \ldots, a_t)$ of $n$ fixes a decomposition $V = V_1 \oplus \cdots \oplus V_i$, acting irreducibly on the $a_i$-th dimensional space $V_i$ for every $i$.

(ii) Let $G = SU_n(q)$. As in (i), conjugacy classes of maximal tori in $G$ are in bijection with partitions of $n$. The torus $(T_w)_\sigma$ corresponding to a partition $w = (a_1, \ldots, a_t)$ of $n$ fixes a decomposition $V = V_1 \oplus \cdots \oplus V_i$, where $V_i$ is nondegenerate and of dimension $a_i$. If $a_i$ is odd then $(T_w)_\sigma$ acts irreducibly on $V_i$; if $a_i$ is even then $(T_w)_\sigma$ fixes $V_i = A_i \oplus B_i$, where $A_i$ and $B_i$ are totally singular (of dimension $a_i/2$), and $(T_w)_\sigma$ acts irreducibly on both.

(iii) Let $G = Sp_{2m}(q)$. Since $W(C_m) \cong C_2 \wr S_m$, by Remark 5.3, conjugacy classes of maximal tori in $G$ are in bijection with signed partitions of $m$. The torus $(T_w)_\sigma$ corresponding to a signed partition $w = (a_1^{\varepsilon_1}, \ldots, a_t^{\varepsilon_t})$ of $m$, with $\varepsilon_i \in \{+, -\}$, fixes a decomposition $V = V_1 \perp \cdots \perp V_i$, where $V_i$ is nondegenerate and of dimension $2a_i$. If $\varepsilon_i = -$ then $(T_w)_\sigma$ acts irreducibly on $V_i$, while if $\varepsilon_i = +$ it acts irreducibly on two complementary totally singular subspaces.

(iv) Let $G = SO_{2m+1}(q)$. Since $W(B_m) \cong W(C_m)$, the conjugacy classes of maximal tori of $G$ are in bijection with signed partitions of $m$. The torus $(T_w)_\sigma$ corresponding to a signed partition $w = (a_1^{\varepsilon_1}, \ldots, a_t^{\varepsilon_t})$ of $m$, with $\varepsilon_i \in \{+, -\}$, fixes the decomposition $V = V_1 \perp V_2$, where $\dim(V_1) = 1$, $(T_w)_\sigma$ centralizes $V_1$, and acts on $V_2$ as explained for symplectic groups in (iii). (We note that this discussion holds also for $q$ even, recalling Remark 5.4.)

(v) Let $G = SO_{2m}^+(q)$ (for odd $q$) or $G = SO_{2m}^-(q)$ (for even $q$). Then the conjugacy classes of maximal tori in $G$ are in bijection with the conjugacy classes of $W(D_m)$.

Recall from Remark 5.0 that a $W(B_m)$-class splits into two $W(D_m)$-classes if and only if it corresponds to a signed partition where all parts have even length and plus sign. Let $n_1$ be such a signed partition, and let $T_1$ and $T_2$ be corresponding
non-conjugate maximal tori of $G$. Consider an embedding $G \leq \text{SO}_{2m+1}(q) = S$, where $F_{2m+1} = V = V_1 \perp V_2$, $\dim(V_1) = 1$, and $G \leq \text{O}(V_2) \cong \text{O}^+_m(q)$, centralizing $V_1$ (see Remark 5.4 for the case $q$ even, where we have $V_1 = V$). Then, $T_1$ and $T_2$ are maximal tori of $S$, corresponding to the same signed partition $w$, hence they are conjugate in $S$. More precisely, it is easy to see that they must be conjugate by an element $(-1, g)$, where $g \in \text{O}(V_2) \cong \text{O}^+_m(q)$ (and $-1 = 1$ if $q$ is even). In particular, despite being non-conjugate in $G$, $T_1$ and $T_2$ are conjugate in $\text{O}^+_m(q)$, and therefore act on the orthogonal module in the same way. Therefore, for many purposes it is sufficient to look at the underlying signed partition of a maximal torus of $G$.

Accordingly, we will write $(T_w)_\sigma$ to denote any representative of a conjugacy class of maximal tori in $G$ corresponding to a $W(D_m)$-class whose underlying signed partition is $w$. With this convention, the torus $(T_w)_\sigma$ acts as explained in (iii). (Recall by Remark 5.4 that $w = (a_1^{\epsilon_1}, \ldots, a_t^{\epsilon_t})$ with $\prod_{i=1}^t \epsilon_i = +$.)

(vi) Let $G = \text{SO}_{2m}(q)$ ($q$ odd) or $G = \Omega_{2m}(q)$ ($q$ even). It turns out that the conjugacy classes of maximal tori of $G$ are in bijection with the $W(D_m)$-classes in the nontrivial coset of $W(D_m)$ in $W(B_m)$. These are clearly $W(B_m)$-classes; in particular, the conjugacy classes of maximal tori in $G$ are in bijection with signed partitions $w = (a_1^{\epsilon_1}, \ldots, a_t^{\epsilon_t})$ with $\prod_{i=1}^t \epsilon_i = -$, and $(T_w)_\sigma$ acts as explained in (iii).

5.4. Definition of the set $A_k$. Assume our finite classical group has natural module $V$ of dimension $n \geq 2$, defined over the field with $q^u$ elements, with $u = 2$ in case of unitary groups, and $u = 1$ otherwise. In view of Theorem 3.1 we can also assume $n \geq 3$ (although this will not be relevant for the argument). In light of various isomorphisms between groups of small rank (see, for example, [KL90, Proposition 2.9.1]), we assume $n \geq 3$ for unitary groups, $n \geq 4$ for symplectic groups and $n \geq 7$ for orthogonal groups. Recall also that, for orthogonal groups, if $n$ is odd we have $q$ odd.

We define $A_k$ as the set of elements appearing in Table 3. More precisely, each element $x \in A_k$ is semisimple, and the corresponding entry in the table denotes the conjugacy class of a maximal torus containing $x$. (For the element $x_1$ in $\Omega^+_m(q)$ with $m \geq 4$ even, see the convention in (v) of Subsection 5.3.)

Of course, the torus alone does not determine uniquely the element (not even its order).

We require that the element $x$ has the following order on each irreducible fixed space. For convenience we will identify the spaces with the corresponding parts of the partition, as explained above.

We deal separately with linear and unitary groups, as we need to take care of the determinant. In $\text{SL}_n(q)$, $x_1$ has order $(q^n - 1)/(q - 1)$, and $x_2$ has order $q^n - 1$. In $\text{SU}_n(q)$, $x_1$ has order $(q^n + 1)/(q + 1)$ for $n$ odd, and order $(q^n - 1)/(q + 1)$ for $n$ even; while $x_2$ has order $q^n - 1$ for $n$ odd, and order $q^n - 1 + 1$ for $n$ even.

If $x \in \text{Sp}_{2m}(q)$, then $x$ has order $q^n + 1$ on each $(a^+)$, and order $q^n - 1$ on each $(a^-)$. If $x \in \Omega^+_m(q)$, then $x$ has order $(q^n + 1)/(2, q - 1)$ on each $(a^+)$, and order $(q^n - 1)/(2, q - 1)$ on each $(a^-)$. If $x \in \Omega_{2m+1}(q)$ the same holds; recall that $x$ also centralizes a 1-space.

We impose two further conditions. The element $x_3$ in $\text{Sp}_4(q)$ with $q$ even acts as $(-1, -1)$. Accordingly, we require $x_3 = (g, g^2)$ with $g$ of order $q + 1$. Similarly, the element $x_3$ in $\Omega^+_8(q)$ acts as $(2, 2)$, and we have $x_3 = (g, g^2)$ with $g$ of order $(q^2 + 1)/(2, q - 1)$. 
Table 3. \( A_b = \{x_1, x_2, x_3, x_4\} \) in Theorem 1.3 for classical groups.

| \( G \)                  | \( x_1 \) | \( x_2 \) | \( x_3 \) | \( x_4 \) |
|-------------------------|---------|---------|---------|---------|
| \( \text{SL}_n(q), n \geq 2 \) | \( n \)  | \( n-1,1 \) |         |         |
| \( \text{SU}_n(q), n \geq 3 \) | \( n \)  | \( n-1,1 \) |         |         |
| \( \Omega_{2m+1}(q), m \geq 3, q \text{ odd} \) | \( m^- \) | \( m^+ \) |         |         |
| \( \Omega_{2m}^-(q), m \geq 4 \) | \( (m-1)^-,1^+ \) |         |         |         |
| \( \text{Sp}_{2m}(q), m \geq 2 \text{ even}, q \text{ odd} \) | \( (m-1)^-,1^+ \) |         |         |         |
| \( \text{Sp}_{2m}(q), m \geq 3 \text{ odd}, q \text{ odd} \) | \( (m-1)^-,1^- \) | \( m^+ \) |         |         |
| \( \Omega_{2m}^+(q), m \geq 2 \text{ even} \) | \( (m-1)^-,1^+ \) | \( (m-1)^-,1^- \) | \( m^+ \) |         |
| \( \Omega_{2m}^+(q), m \geq 5 \text{ odd} \) | \( (m-1)^-,1^- \) |         |         |         |
| \( \Omega_{2m}^-(q), m \geq 4 \text{ even} \) | \( (m-1)^-,1^- \) | \( (m-2)^-,2^- \) | \( (m-2)^-,1^- \) | \( 1^+ \) |

With these choices, it is not difficult to check that, if \( q \) is sufficiently large (\( q \geq 11 \)), then every \( x \in A_b \) is separable, i.e., it has distinct eigenvalues on the natural module of the ambient algebraic group \( X \). In Lemma 5.7 below we will prove a little more.

5.5. **Focusing on \( C_1 \) and \( C_3 \).** By Theorem 5.5 \( \mathcal{M} \) consists of members from Aschbacher’s classes \( C_1, C_2, C_3 \) (recall Convention 5.3). We will show that, in fact, we can focus on overgroups of \( x \in A_b \) from classes \( C_1 \) and \( C_3 \) (see Lemma 5.8 and the comments following it), which is a quite useful fact.

**Lemma 5.7.** Let \( f \) be a positive integer. If \( q \geq 11f \) and \( x \in A_b \), then \( x^f \) is separable.

**Proof.** Let \( x \in A_b \). As observed at the end of Subsection 5.4 since \( q \geq 11 \) we have that \( x \) is separable, hence contained in a unique maximal torus, which we denote by \( T \). We need to prove two things:

(i) if \( W \leq V \) is irreducible for \( T \), then \( W \) is irreducible for \( x^f \), and

(ii) if \( W_1 \) and \( W_2 \) are distinct irreducible modules for \( T \), then \( x^f \) has distinct eigenvalues on \( W_1 \) and \( W_2 \).

(Note that, since \( x \in T \) is separable, any two distinct irreducible \( T \)-modules \( W_1 \) and \( W_2 \) are not isomorphic.) Items (i) and (ii) imply that \( x^f \) has the same fixed spaces as the torus \( T \), and therefore \( x^f \) is separable. The argument is essentially the same in all cases.

For item (i), we show that if \( q \geq 11f \) then the order of \( x^f \) is large enough to imply that \( x^f \) acts irreducibly on \( W \). For instance, assume the torus \( T \) acts irreducibly on a nondegenerate module \( W \) of dimension 2a (and assume we are not in the unitary case). Then by our choices the order of \( x \) on \( W \) is larger than \((q^a+1)/2\). Then the order of \( x^f \) is larger than \((q^a+1)/2f\), which is strictly larger than \( q^{a-1}+1 \); in particular \( x \) does not fix any proper nondegenerate submodule of \( W \). What is more, if \( x^f \) fixes a proper totally singular submodule \( U \), then this has dimension \( \ell \leq a \). If \( \ell < a \), the same argument as above gives a contradiction, and if \( \ell = a \), then the order of \( x^f \) would divide both \( q^a-1 \) and \( q^a+1 \), hence it would divide 2, which is false. In unitary groups, the argument is the same; and in case \( W \) is totally singular, the argument is similar (we note also that the dimension of any \( \langle x^f \rangle \)-submodule of \( W \) divides the dimension of \( W \)).

For item (ii), we first observe that if \( W_1 \) and \( W_2 \) have different dimensions, the claim is obvious. There are cases that can be checked separately, namely \( x_2 \) in
SL_2(q), x_2 in SU_3(q), x_3 in Sp_4(q) with q even, and x_3 in Omega^+_4(q). In all other cases, if W_1 and W_2 have equal dimension, say a, then they are totally singular and T acts irreducibly on both, with W_1 \oplus W_2 nondegenerate. Let us assume we are not in the unitary case. If x has eigenvalues \{\lambda, \lambda^q, \ldots, \lambda^{q^{a-1}}\} on W_1, then it has eigenvalues \{\lambda^{-1}, \lambda^{-q}, \ldots, \lambda^{-(q^{a-1})}\} on W_2. By our choices, |\lambda| \geq (q^{a-1})/2. Since, by (i), x^f acts irreducibly on both W_1 and W_2, the eigenvalues of x^f on W_1 and W_2 either coincide (as sets) or are disjoint. Assume for a contradiction that they coincide. In particular, \lambda^f = \lambda^{-f}q^i for some 0 \leq i \leq a - 1. Then |\lambda| divides f(q^i + 1) \leq f(q^{a-1} + 1), which contradicts q \geq 11f. The unitary case is similar (in this case the eigenvalues of x on W_2 are the q-th powers of the inverses of the eigenvalues on W_1).

Lemma 5.8. Assume \(q \geq 11n^4\), take \(x \in A_b\) and let \(T\) be the corresponding maximal torus in \(X_\sigma\). Then for \(M_\sigma \in M(x)\) we have \(x \in T \leq M_\sigma^2\). In particular, \(T(x)\) consists of the maximal tori contained in some overgroup of \(x\) belonging to \(M_{con}\).

Proof. By Theorems 5.2 and 5.5 and by the fact that \(x\) is separable, we see that the result is easily established unless \(M_\sigma\) preserves a direct sum decomposition or is an extension field subgroup.

Note that \(x\) fixes at most four irreducible spaces on the natural module. In particular, if \(x \in M_\sigma \leq \text{GL}_{n/2}(q^{a}) \wr S_t\), then \(x\) induces a permutation in \(S_t\) having at most four cycles, and therefore having order at most \(n^4\). It follows that \(x^f \in M_{\sigma}^2\) for some \(f \leq n^4\). If \(x \in M_{\sigma}\) and \(M_{\sigma}\) is an extension field subgroup, then the index of \(M_{\sigma}^2\) in \(M_{\sigma}\) is at most \(n\). In particular, \(x^f \in M_{\sigma}^2\) for some \(f \leq n\).

Since \(q \geq 11n^4 \geq 11f\), by Lemma 5.7, \(x^f\) is separable, and in particular regular semisimple. Therefore, the maximal torus corresponding to \(x^f\), which is \(T\), is contained in \(M_{\sigma}^2\).

The conclusion to Lemmas 5.7 and 5.8 hold under slightly weaker conditions on \(q\), but this is not required for the proof of Theorem 5.12 where we assume \(q \geq C r^r\).

A very useful consequence of Lemma 5.8 is that, for each element of \(A_b\), we just need to determine the overgroups of its maximal torus contained in the Aschbacher’s classes \(C_1\) and \(C_3\); in class \(C_3\) we only have to consider the linear subgroup \(GL_{n/2}(q^{a}) \wr S_t\) \(< \text{GL}_{n}(q^{a})\). We will now determine such overgroups.

5.6. Overgroups of the elements of \(A_b\). The overgroups from class \(C_1\) (except for \(\text{SO}_{2m}^+(q) < \text{Sp}_{2m}(q)\)) are easily determined by looking at Table 8 since the elements are separable. We now deal with the remaining case. We have \(M_{\sigma} = \text{SO}_{2m}^+(q) < \text{Sp}_{2m}(q) \cong \text{SO}_{2m+1}(q)\) with \(q\) even, and we have \(M_{\sigma}^2 = \Omega_{2m}^+(q)\).

Lemma 5.9. Let \(q\) be even, let \(\sigma\) be the defining Steinberg endomorphism of \(G = \text{SO}_{2m+1}(q)\), and let \(w\) be a signed partition of \(m\) in which the product of the signs is \(\varepsilon\), with \(\varepsilon \in \{+, -\}\). Then, the associated maximal torus \((T_w)_\sigma\) of \(G\) is contained in a subgroup \(\text{SO}_{2m}(q)\). If moreover \((T_w)_\sigma\) contains regular semisimple elements, then \((T_w)_\sigma\) is not contained in any subgroup \(\text{SO}_{2m}^{-\varepsilon}(q)\).

Proof. Observe that \((T_w)_\sigma\) stabilizes a non-degenerate hyperplane \(W\) of \(\varepsilon\) sign (see [KL90 Proposition 2.5.11]), so it is contained in a subgroup \(\text{SO}(W) \cong \text{SO}_{2m}(q)\). Moreover, if \((T_w)_\sigma\) contains regular semisimple elements, then \((T_w)_\sigma\) fixes only one nondegenerate hyperplane, and the last part of the statement follows. \(\Box\)
In the last part of the statement of Lemma 5.9 it is necessary to assume that \((T_w)_\sigma\) contains regular semisimple elements. For instance, for \(q = 2\) the torus corresponding to \(w = (1^+, \ldots, 1^+)\) is trivial – hence contained in every subgroup of \(G\).

We now prove two lemmas concerning extension field subgroups.

**Lemma 5.10.** Assume \(x \in \text{GL}_{n/b}(q^b) < \text{GL}_n(q)\) for some prime \(b\) dividing \(n\). Assume \(x\) is separable over \(F_q\). Then \(b\) divides the dimension of each irreducible constituent of the natural \(F_q[x]\)-module.

**Proof.** Assume \(U\) is an irreducible space for \(x\) over \(F_q^\times\) of dimension \(a\). Then \(U\) has dimension \(ab\) over \(F_q\). Moreover, \(x\) acts homogeneously on \(U\) over \(F_q\). Since \(x\) is separable, it follows that \(x\) acts reducibly on \(U\) over \(F_q\). The lemma follows. \(\square\)

Now we aim to describe the maximal tori contained in extension field subgroups of maximal rank. In the case of unitary groups, recall that the subgroups of type \(\text{GU}_{n/b}(q^b) < \text{GU}_n(q)\) only arise when \(b\) is odd (cf. [KL90] Section 4.3), and that for \(m\) odd \(\text{GU}_m(q)\) embeds in \(\text{SO}_{2m}(q)\), while for \(m\) even it embeds in \(\text{SO}_{2m}^+(q)\). Also note that, as observed in Theorem 5.5 the extension field subgroups of type \(\text{GU}_{n/b}(q^b) < \text{GU}_n(q)\) with \(n/b\) odd and \(\varepsilon \in \{+, -, 0\}\) are not of maximal rank, so we will not consider them.

As in (v) of Subsection 5.5 for \(G = \text{SO}_{2m}^+(q)\) or \(\Omega_{2m}^+(q)\) we denote by \((T_w)_\sigma\) any representative of a conjugacy class of maximal tori corresponding to a \(W(D_m)\)-class whose underlying signed partition is \(w\).

**Lemma 5.11.** Let \(b\) be prime, and in each of the cases below, denote by \(\sigma\) the defining Steinberg endomorphism.

1. The subgroup \(\text{GL}_{n/b}(q^b) \cap \text{SL}_n(q) < \text{SL}_n(q)\) or \(\text{GU}_{n/b}(q^b) \cap \text{SU}_n(q) < \text{SU}_n(q)\) contains a conjugate of \((T_w)_\sigma\), for every partition \(w\) of \(n\) in which each part has length divisible by \(b\).

2. Assume that \(2m/b\) is even. The subgroup \(\text{Sp}_{2m/b}(q^b) < \text{Sp}_{2m}(q)\) or \(\text{SO}_{2m/b}^\pm(q^b) < \text{SO}_{2m}^\pm(q)\) (\(q\) odd) or \(\Omega_{2m/b}(q^b) < \Omega_{2m}^\pm(q)\) (\(q\) even) contains a conjugate of \((T_w)_\sigma\), for every signed partition \(w\) of \(m\) in which all parts have length divisible by \(b\).

3. The subgroup \(\text{GU}_m(q) < \text{Sp}_{2m}(q)\) or \(\text{GU}_m(q) < \text{SO}_{2m}^+(q)\) (\(q\) odd) or \(\text{GU}_m(q) < \Omega_{2m}^\pm(q)\) (\(q\) even) contains a conjugate of \((T_w)_\sigma\), for every signed partition \(w\) of \(m\) in which odd parts have minus sign and even parts have plus sign.

If moreover \((T_w)_\sigma\) contains separable elements, then each embedding of \((T_w)_\sigma\) in extension field subgroups of maximal rank has been listed in (1), (2), (3).

**Proof.** Let \(H\) be an extension field subgroup as in the statement. Each maximal torus of the ambient group contained in \(H\) is a maximal torus of \(H\), hence it admits a description in terms of its Weyl group. It is then easy to establish the lemma with the help of Lemma 5.10 (see [KL90] Section 4.3] for a detailed description of the various embeddings).

Let us give the details of (1) for \(\text{SL}_n(q)\). Let \(H = \text{GL}_{n/b}(q^b) \cap \text{SL}_n(q) < \text{SL}_n(q)\), let \(w\) be a partition of \(n\) and let \((T_w)_\sigma\) be the corresponding maximal torus of \(\text{SL}_n(q)\). If all parts of \(w\) have length divisible by \(b\), then it is easy to see that \((T_w)_\sigma\) is contained in a subgroup conjugate to \(H\).
Assume, on the other hand, that \((T_w)_\sigma\) is contained in a subgroup conjugate to \(H\), and assume that \((T_w)_\sigma\) contains a separable element \(g\); we want to show that all parts of \(w\) have length divisible by \(b\). Since \(g \in H\), we see by Lemma 5.10 that \(b\) divides the dimension of each irreducible \(F_q[[x]]\)-submodule of \(F_q^n\). In particular, \(g\) is contained in a torus \((T_w)_\sigma\) of \(\text{SL}_n(q)\), where all parts of \(w'\) have length divisible by \(b\). Since \(g\) is separable and belongs to both \((T_w)_\sigma\) and \((T_w)_\sigma\), we deduce that \(w = w'\), as required.

5.7. **Proof of Theorem 1.5** We are now ready to prove Theorem 3.13 (hence Theorem 1.5) for classical groups of bounded rank.

Let us prove the statement for unitary groups, for symplectic groups, and for \(\Omega_{2m}(q)\) with \(m\) even. The other cases are dealt with similarly. (In fact, we are omitting the proof of the easiest cases.)

Since \(q \geq C r^r\) for some large constant \(C\), it is easy to see that each maximal torus of \(X_q\) contains separable elements, so Lemmas 5.9 and 5.11 apply.

For \(x \in X_\sigma\), we denote by \(\mathcal{M}_{\text{con}}(x)\) the members of \(\mathcal{M}_{\text{con}}\) containing \(x\) (this notation is used only here). Moreover, referring to the defining Steinberg endomorphism, we denote by \(N_{\ell}^\pm\) the fixed points of the connected component of the stabilizer of a nondegenerate subspace of sign \(\pm\) and of dimension \(\ell\), and by \(P_{\ell}\) the stabilizer of a totally singular \(\ell\)-space. Finally, in the following discussion we identify each torus with the corresponding (signed) partition; hence a partition can be contained in a subgroup.

(i) \(\text{SU}_n(q)\). If \(n\) is odd, \(\mathcal{M}_{\text{con}}(x_1)\) consists only of (unitary) extension field subgroups of type \(\text{GU}_{n/b}(q^b)\) (\(b\) odd). On the other hand \(\mathcal{M}_{\text{con}}(x_2)\) consists of \(P_{(n-1)/2}\) and \(N_1\). Therefore \(\mathcal{T}(x_2)\) contains only the partitions with a 1-cycle. By Lemma 5.11, none of these belongs to \(\mathcal{T}(x_1)\), hence \(\mathcal{T}(x_1) \cap \mathcal{T}(x_2) = \emptyset\). Assume now \(n\) is even. Again \(\mathcal{T}(x_2)\) contains the partitions with a 1-cycle. Moreover \(\mathcal{M}_{\text{con}}(x_1)\) consists of unitary extension field subgroups, and \(P_{n/2}\). Then \(\mathcal{T}(x_1) \cap \mathcal{T}(x_2) = \emptyset\) (note that \(P_{n/2}\) contains the partitions with all even parts).

(ii) \(\text{Sp}_{2m}(q)\). If \(m\) is even and \(q\) is odd, then \(\mathcal{M}_{\text{con}}(x_1)\) contains every \(\text{Sp}_{2m/b}(q^b)\), but not \(\text{GU}_m(q)\) (by Lemma 5.11). On the other hand \(\mathcal{M}_{\text{con}}(x_2)\) consists only of \(P_1\) and \(N_2\). Hence \(\mathcal{T}(x_2)\) contains the signed partitions with a 1-cycle. By Lemma 5.11 none of these partitions belongs to \(\mathcal{T}(x_1)\), hence \(\mathcal{T}(x_1) \cap \mathcal{T}(x_2) = \emptyset\).

If \(m\) is odd and \(q\) is odd, the difference is that \(\mathcal{M}_{\text{con}}(x_1)\) contains \(\text{GU}_m(q)\), and as before every \(\text{Sp}_{2m/b}(q^b)\) (here \(b\) is odd). On the other hand \(\mathcal{M}_{\text{con}}(x_3)\) contains \(P_m\), every \(\text{Sp}_{2m/b}(q^b)\), and does not contain \(\text{GU}_m(q)\). Moreover \(\mathcal{M}_{\text{con}}(x_2)\) contains only \(N_2\). Then \(\mathcal{T}(x_2)\) contains signed partition with a 1-cycle. But \((1^-, \ldots)\) is not contained in \(\mathcal{T}(x_3)\), and \((1^+, \ldots)\) is not contained in \(\mathcal{T}(x_1)\) (note that a partition contained in \(P_m\) has all positive cycles). Hence \(\mathcal{T}(x_1) \cap \mathcal{T}(x_2) \cap \mathcal{T}(x_3) = \emptyset\).

Assume now \(q\) is even. Note that \(\text{GU}_m(q)\) is contained in \(\Omega_{2m}^+(q)\) or in \(\Omega_{2m}^-(q)\) according to whether \(m\) is even or odd (cf. [1992, Section 4.3]). Moreover, by Lemma 5.9 we deduce that a partition contained in \(P_m\) is contained in \(\Omega_{2m}^+(q)\). As a consequence we can ignore \(\text{GU}_m(q)\) and \(P_m\). The result follows with arguments as above. Indeed, \(\mathcal{T}(x_2) \cap \mathcal{T}(x_3)\) consists of the signed partitions \(w\) with a 1-cycle. If the product of the signs of \(w\) is 1 (resp. \(-1\)), then \(w\) does not belong to \(\mathcal{T}(x_1)\) (resp. \(\mathcal{T}(x_4)\)). Therefore \(\mathcal{T}(x_1) \cap \mathcal{T}(x_2) \cap \mathcal{T}(x_3) \cap \mathcal{T}(x_4) = \emptyset\).

(iii) \(\Omega_{2m}^+(q)\) with \(m\) even. As in (v) of Subsection 5.3, we only look at the underlying signed partition of a \(W(D_m)\)-class (although, in fact, all the \(W(D_m)\)-classes
that will be mentioned are \( W(B_m) \)-classes. We see that \( T(x_4) \) contains \((1^+, \ldots), (1^-, \ldots), (2^-, \ldots) \). Now \( \mathcal{M}_{\text{con}}(x_3) \) consists of \( N^- \) and subgroups of type \( \Omega^+_m(q^2) \).

Of the three subpartitions listed above, only \((2^-, \ldots)\) can belong to \( \Omega^+_m(q^2) \). Therefore, \( T(x_3) \cap T(x_4) \) contains \((1^+, 1^-, \ldots)\) and \((2^-, \ldots)\). At this point we note that \( \mathcal{M}_{\text{con}}(x_1) \) contains \( P_m, \text{GU}_m(q) \) and every \( \Omega^+_{2m/b}(q^2) \). Then \( T(x_1) \cap T(x_3) \cap T(x_4) \) consists of the partitions contained in \( \Omega^+_m(q^2) \) and of type \((2^-, \ldots)\).

We observe that none of these belongs to \( T(x_2) \), and the proof is concluded.

We summarize the fact that the proof of Theorem 1.5(1) is complete.

**Theorem 5.12.** The conclusion to Theorem 1.5(1) holds.

**Proof.** For \( G \cong \text{PSL}_2(q) \), see Theorem 3.1. In the other cases, the statement follows from Theorem 5.13, which was proved in Section 4 for exceptional groups, and in this section for classical groups.

We note that, by the same proof, with more care one can improve the value of \( b \). We will say that \( (4^+, \ldots) \) is regular semisimple: let \( g \) be its maximal torus in \( T \). Then \( |T| \) contains \((1^+, \ldots)\) if for every \( g_1, \ldots, g_t \in T \), every maximal overgroup of \( \langle x_1^{g_1}, \ldots, x_t^{g_t} \rangle \) in \( T \) contains \((1^+, \ldots)\). Moreover, set

\[
\alpha = \alpha(X) = \begin{cases} 
1/|W(E_8)| & \text{if } X \text{ is exceptional} \\
1/(4r) & \text{if } X \text{ is classical}.
\end{cases}
\]

**Theorem 6.1.** Assume \( r \geq 2 \) and \( q \geq Cr^r \) for some large constant \( C \). Assume \( X_q \not\cong G_2(q) \) when \( 3 \mid q \). Then \( \mathbf{P}^{\text{inv}}_{\text{en}}(X_q, x) \geq \alpha + O(r^r/q) \) for a proportion of elements \( x \in X_q \) of the form \( 1 \mapsto O(r^r/q) \).

**Proof.** Let \( A_b \) be the set of elements of \((X_q)^*\) listed in Tables 2 and 3. Let \( x \in \Delta \), recalling the definition of \( \Delta \) in Notation 3.4(8). By Remark 3.11 and Theorem 3.13, we deduce that \( x \) invariably generates at least \((X_q)^*\) with some \( y \in A_b \). By our choice of the set \( A_b \) in the various cases, \( y \) is regular semisimple: let \( S = (T_w)_{\sigma} \), with \( w \in W \), be its maximal torus in \( X_q \).

By the choice of \( y \), and by the definition of \( \Delta_S \), we see that \( \{x, z\} \) invariably generates at least \((X_q)^*\) for every \( z \in \Delta_S \).

In order to conclude the proof, we only need to establish an appropriate lower bound on the proportions \( |\Delta|/|X_q| \) and \( |\Delta_S|/|X_q| \). We know that \( |\Delta|/|X_q| = 1 - O(r^r/q) \) by Theorem 3.6. Moreover \( |\Delta_S|/|X_q| = \mathbf{P}(W, \sigma, w) + O(r^r/q) \) by Theorems 3.6 and 3.8. Clearly \( \mathbf{P}(W, \sigma, w) \geq 1/|W| \), which is at least \( 1/|W(E_8)| \) for exceptional groups. For classical groups, one can check that \( \mathbf{P}(W, \sigma, w) \geq 1/(4r) \), which is attained for \((2^-, 2^-)\) in \( W(D_4) \) and for \((1^-, 1^-)\) in \( W(C_2) \) (see Remark 6.2 below). The proof is concluded.

We note that, by the same proof, with more care one can improve the value of \( \alpha \) in case \( X \) is exceptional.
Remark 6.2. We make some observations regarding the conjugacy class of a random element in wreath products which, in particular, readily imply the bound $\mathbf{P}(W, \sigma, w) \geq 1/(4r)$ stated in the last paragraph of the proof of Theorem 6.1.

Let $H$ be a finite group and let $G = H \wr S_m$. Recall by Remark 5.6 that conjugacy classes in $G$ are in bijection with partitions of $m$ where each part is labelled by a conjugacy class of $H$. Now, a random element of $H \wr S_m$ is clearly given by a random permutation $\tau \in S_m$ and a random element $(x_1, \ldots, x_m) \in H^m$. It follows immediately from the first paragraph of Remark 5.6 that the conjugacy class of a random element of $H \wr S_m$ can be computed in two steps: first draw a random permutation $\tau$ of $S_m$, and then label each cycle of $\tau$ by a conjugacy class $C$ of $H$ with probability $|C|/|H|$ (this gives naturally a labelled partition, just by viewing cycles as parts).

In particular, in the case $H = C_2$, so $G = C_2 \wr S_m \cong W(B_m)$, the conjugacy class of a random element of $G$ can be computed by drawing a random permutation $\tau$ of $S_m$, and equipping each cycle of $\tau$ with a sign $\pm$ with equal probability. For example, if $C$ is the class corresponding to $(m^+)$, then $|C|/|G| = 1/(2m)$.

Consider now the subgroup $K \cong W(D_m)$ of $G \cong W(B_m)$ consisting of the elements $(x_1, \ldots, x_m)\tau$ with $x_i = \pm$ and $\prod_{i=1}^m x_i = \pm$. Then, the $G$-classes of elements of $K$ are in bijection with signed partitions of $m$ where the product of the signs is $\pm$. For a $K$-class $D$ whose $G$-class is $C$, we clearly have $|D|/|K| = |\delta|C|/|G|$ if $D = C$ and $\delta = 1$ otherwise. For example, if $m$ is even and if $D$ is a $K$-class whose $G$-class $C$ corresponds to $(m^+)$, then $|D|/|K| = 1/(2m)$.

Finally, the $K$-classes of elements in $G \setminus K$ are $G$-stable, and are in bijection with signed partitions of $m$ where the product of the signs is $\pm$.

From this discussion, we can easily deduce the bound $\mathbf{P}(W, \sigma, w) \geq 1/(4r)$, stated in the last paragraph of the proof of Theorem 6.1, which is attained for $(2^-, 2^-)$ in $W(D_4)$ and for $(1^-, 1^-)$ in $W(C_2)$. Note that there are other cases close to this bound; for instance, $((m - 1)^\pm, 1^\pm)$ in $W(C_m)$ for $m \geq 3$ gives probability $1/(4(m-1)) = 1/(4(r-1))$.

We now deduce Theorem 1.2 from Theorem 6.1.

Proof of Theorem 7.2. By Theorem 3.1, we may assume $r \geq 2$. With notation as in the proof of Theorem 6.1, we have that for every $x \in \Delta' := \Delta \cap (X_q)'$, $x$ invariably generates $(X_q)'$ with every element of $\Delta'_S := \Delta_S \cap (X_q)'$. Therefore we only need to establish an appropriate lower bound on $|\Delta'|/(X_q)'$ and $|\Delta'_S|/(X_q)'$. By our choice of the type of $X$, the index of $(X_q)'$ in $X_q$ is bounded (it is at most 3), hence $|\Delta'|/(X_q)' = 1 - O(r^*/q)$. Moreover, with reasoning similar to that in Lemma 3.12 and using Theorem 3.8, we see that

$$|\cup_{g \in X_q} (S \cap (X_q)'^g)|/(X_q)' \geq \mathbf{P}(W, \sigma, w) + O(1/q),$$

whence

$$|\Delta'_S|/(X_q)' \geq \alpha + O(r^*/q).$$

This concludes the proof. \hfill \Box

Proof of Theorem 1.4. For the group $G = G_2(3^n)$, Theorem 1.4 follows from Theorem 6.1(i). The remaining cases follow from Theorem 1.2. \hfill \Box
6.1. An elaboration on Theorem 1.4. We obtain here an asymptotic for the probability in Theorem 1.4. For simplicity, we take $X$ of simply connected type (so $X_r = X_q$ is quasisimple). Let $\{T_1, \ldots, T_\ell\}$ be a set of representatives for the $X_\ell$-conjugacy classes of maximal tori of $X_q$. Write $T_i = (T_{w_i})_r$ with $w_i \in W$, as we did in Subsection 5.2. Define a relation $\sim$ on $\{1, \ldots, \ell\}$ as follows. If $1 \leq i, j \leq \ell$, then $i \sim j$ if there are no conjugates of $T_i$ and $T_j$ with a common overgroup in $\mathcal{M}_{\text{con}}$.

**Theorem 6.3.** Assume $r \geq 2$. Let $x_1, x_2 \in X_q$ be chosen uniformly at random. Then,

$$P(\langle x_1, x_2 \rangle_I = X_q) = \sum_{i \neq j} P(W, \sigma, w_i)P(W, \sigma, w_j) + \frac{d(r)}{q}$$

for some function $d(r)$.

**Proof.** Note that $\Delta = \bigcup_{i=1}^\ell \Delta_{T_i}$, a disjoint union. By the definition of $\Delta$ and by Lemma 5.3 whenever $i \sim j$ every element of $\Delta_{T_i}$ invariably generates $X_q$ with every element of $\Delta_{T_j}$. Clearly this is not true if $i \not\sim j$. By Theorems 3.6 and 3.8 we have $|\Delta_{T_i}|/|X_q| = P(W, \sigma, w_i) + O(r^*/q)$. The statement follows. \hfill $\square$

**Remark 6.4.** We have a nice and rather explicit expression for the main term of $P(\langle x_1, x_2 \rangle_I = X_q)$, which one should be able to estimate with accuracy (for all exceptional groups it should be possible to compute the exact value). For instance, with notation as in Subsections 4.3 and 4.4, in case $G = G_2(3^a)$ we have $3 \sim 5$ and $5 \sim 6$. One deduces easily that $P(\langle x_1, x_2 \rangle_I = G) = 1/9 + O(1/q)$. A very easy case is $\text{SL}_2(q)$, where the probability is $1/2 + O(1/q)$ (for the error term, see the proof of Theorem 3.1 at the beginning of Section 5).

Note, also, that this is quite an unusual way to address a problem of random generation. Indeed, in these problems one usually proves that there is a small chance to be trapped in a maximal subgroup – and, as a consequence, there is a large probability to generate. Here, on the other hand, we are directly exhibiting many pairs of elements which (invariably) generate, which is a sort of opposite approach. In the language of Subsection 1.2, we are exhibiting large complete bipartite subgraphs of the graph $\Lambda_c(X_q)$.

7. A lower bound on $|A_b|$ We show that there are cases in which we need $|A_b| \geq 4$ in Theorem 1.5 (note that we used a set of size at least 5 only in the case $G = F_4(2^a)$).

**Lemma 7.1.** Assume $q$ is even and $m \geq 2$. Let $G = \text{PSp}_{2m}(q) = \text{Sp}_{2m}(q)$, and let $Y$ be a subset of $G$ of size 3. Then, $P_{\text{inv}}(G, Y) \leq 1 - 1/2^{m^2} + O(1/q)$.

**Proof.** Note that $2^{m^2} = |W(C_m)|$. Let $y_1, y_2, y_3$ be elements of $G$; we claim that $\Omega := \cap T(y_i) \neq \emptyset$. Assume we prove the claim, and assume $S \in \Omega$. Then, the elements lying in $\tilde{S}$ contribute to $1 - P_{\text{inv}}(G, Y)$. By Theorem 5.8 the proportion of elements lying in $\tilde{S}$ is at least $1/|W(C_m)| + O(1/q)$. Therefore it is sufficient to prove the claim.

Note that the maximal torus corresponding to $w = (1^+, \ldots, 1^+)$ is contained in every maximal subgroup from class $C_1$. Therefore, if the $y_i$ all act reducibly then this torus belongs to $\Omega$. 

Now note that the torus corresponding to $w = (1^+, \ldots, 1^+, 1^-)$ is contained in $SO_{2m}(q)$, and in every subspace stabilizer except for the stabilizer of a totally singular $m$-space. Therefore, if none of the $y_i$ acts as $(m^+)$ (i.e., irreducibly on two complementary totally singular subspaces), then this torus belongs to $\Omega$.

By the previous two paragraphs, we may assume that $y_1$ acts irreducibly and that $y_2$ acts as $(m^+)$. Note that both $y_1$ and $y_2$ belong to $Sp_{2m/2}(q^k)$ for every prime divisor $b$ of $m$. Assume now $y_3$ lies in $SO_{2m}(q)$, with $\varepsilon \in \{+, -\}$ (it is well known that every element belongs to such a subgroup; cf. [Dye79]). Now observe that $Sp_{2m/2}(q^k)$ and $SO_{2m}(q)$ contain a common maximal torus: the maximal torus corresponding to $w = (m^\varepsilon)$, for instance. This concludes the proof. \hfill \square

Next, we show that for groups of bounded rank we cannot have $|A_b| = 1$ in Theorem 1.5.

**Lemma 7.2.** Let $X$ be a simple linear algebraic group, $\sigma$ a Steinberg morphism, and $x \in X_\sigma$. Then, $x$ is contained in a subgroup of $X_\sigma = X_q$ of maximal rank. In particular, $\mathbf{P}^*_{\text{inv}}(X_q, x) \leq 1 - 1/|W| + O(1/q)$.

**Proof.** Write $x = us$ for the Jordan decomposition into the unipotent part $u$ and the semisimple part $s$. Every parabolic subgroup of $X_\sigma$ contains a Sylow $p$-subgroup of $X_\sigma$; hence $u$ belongs to a conjugate of every parabolic subgroup. Moreover $Z(X_\sigma)$ is contained in every parabolic of $X_\sigma$. Therefore if $s \in Z(X_\sigma)$ we have that $x$ is contained in a parabolic of $X_\sigma$. Assume then $s \notin Z(X_\sigma)$. Then $x \in C_X(s) < X$, which is $\sigma$-stable. By Lemma 6.3, $s$ is contained in a $\sigma$-stable maximal torus $T$ of $X$, hence $T \leq C_X(s)$ and $C_X(s)$ is of maximal rank. The first part of the statement is proved. The last part follows from Theorem 6.8 and the fact that, if $S \in T(x)$, then the elements of $S$ contribute to $1 - \mathbf{P}^*_{\text{inv}}(X_q, x)$. \hfill \square

8. Groups of Lie type of large rank

In this final section we prove Theorem 1.1 and Theorem 1.5 for groups of Lie type of large rank. We work with quasisimple groups $G$ rather than the simple quotients $G/Z(G)$ (this makes no difference, since $Z(G)$ is contained in every maximal subgroup of $G$). Specifically, consider the following groups:

$$G = \text{SL}_n(q), \text{SU}_n(q), \text{Sp}_n(q), \Omega^\varepsilon_n(q)$$

with $\varepsilon \in \{+, -, \circ\}$. We will denote by $V$ the natural $n$-dimensional module for $G$. We may assume that $n$ is large.

Recall that, in the bounded rank case, for classical groups we could focus on Aschbacher’s classes $C_1, C_2, C_3$ (Theorem 5.3). In the large rank case, the same happens. If $G$ is a finite quasisimple classical group, denote by $M' = M'(G)$ the set of all maximal subgroups of $G$ contained in one of the classes $C_1, C_2$ or $C_3$ (recall Convention 5.3).

**Theorem 8.1.** [FG12, Theorem 7.7] Let $G$ be a finite quasisimple classical group of untwisted Lie rank $r$ defined over $\mathbf{F}_q$. For $r$ sufficiently large, the proportion of elements of $G$ which lie in subgroups not belonging to $M'$ is $O(q^{-r/3})$.

8.1. General case. In large rank, if $G$ is not symplectic in even characteristic and not orthogonal in odd dimension, we can easily deduce Theorems 1.1 and 1.5(2) from known results.
Theorem 8.2. The conclusions to Theorems 1.1 and 1.5(2) hold for the groups $\text{PSL}_n(q)$, $\text{PSU}_n(q)$, $\text{PSp}_{2m}(q)$ with $q$ odd, and $\text{PO}_{2m}^+(q)$.

Proof. In view of Theorem 1.2 we may assume that $n$ and $m$ are large. We will prove Theorem 1.5(2) (in these cases) with $|A_\ell| = 1$, which, for $n$ or $m$ large, clearly implies Theorem 1.1.

We work with the corresponding groups $G$ as in (7). Let $x \in G$ be the element defined in [GK00, Table II], and set $A_\ell = \{x\}$. By the proof of [GK00, Proposition 4.1] it follows that $x$ is contained in no irreducible maximal subgroup of $G$. Next, let $\Omega$ be the set of integers which occur as the dimension of a proper non zero subspace of $V$ fixed by $x$. By [GK00, Table II], we see that $\Omega$ has very small size (bounded absolutely from above), and $\Omega$ contains only integers $\ell$ such that both $\ell$ and $n - \ell$ are comparable to $n$ (up to constants). By [FG18, Theorems 2.2, 2.3, 2.4, 2.5],

$$|M(x)| \leq O(n^{-0.005}).$$

We deduce by Lemma 1.9 that $P_{\text{inv}}(G, x) = 1 - O(n^{-0.005})$, which concludes the proof. □

Now we need to deal with the remaining cases. We devote one subsection to each. The difference, in these cases, is that every element belongs to maximal subgroups whose union of conjugates is large.

8.2. Orthogonal groups in odd dimension. Here we assume $G = \Omega_{2m+1}(q)$ with $q$ odd. Let $R^+$ and $R^-$ denote the union of the stabilizers of hyperplanes of plus and minus sign, respectively, and let $P_1$ denote the union of the stabilizers of singular 1-spaces. It is well known and easy that every element of $G$ has eigenvalue 1 on the natural module; in particular, $G = R^+ \cup R^- \cup P_1$. We can now establish Theorem 1.2 in this special case.

Theorem 8.3. The conclusion to Theorem 1.1 holds in the case $G = \Omega_{2m+1}(q)$ with $q$ odd.

Proof. In view of Theorem 1.2 we may assume that $m$ is large. Let $x \in G = \Omega_{2m+1}(q)$ be as in [GK00, Table II]. By the proof of [GK00, Proposition 4.1] it follows that the only maximal overgroup of $x$ is the stabilizer of a nondegenerate hyperplane of minus type. It follows from [FG17, Theorem 9.26] that the proportion of elements of $G$ lying in $R^-$ is bounded away from 1 absolutely (it is at most 0.93 for $n$ sufficiently large). We conclude by Lemma 1.9. □

We will see in Lemma 8.10 that $P_{\text{inv}}(G, x)$ remains bounded away from 1 for every $x \in G$. Next we want to prove Theorem 1.5 in this case. We have a strong dichotomy between the cases $q$ fixed and $q \to \infty$.

Recall that, in orthogonal groups, regular semisimple elements might have eigenvalues of multiplicity greater than 1 (i.e., they need not be separable). We recall a lemma which specifies how this can happen, whose proof is straightforward and left to the reader.

Lemma 8.4. Assume $g \in G$ is regular semisimple. Then $g$ centralizes a nondegenerate 1-space, and $\dim C_V(g) = 1$. Moreover, either $g$ fixes no other nondegenerate 1-space, or it acts as $-1$ on a nondegenerate 2-space, and fixes no other nondegenerate 1-space.
We next prove that, if \( q \) is large, with high probability an element is separable.

**Theorem 8.5.** Assume \( m \geq 3 \). The proportion of elements of \( G = \Omega_{2m+1}(q) \) which are separable is larger than \( 1 - 6/q \). These elements fix only one nondegenerate hyperplane.

**Proof.** By Lemma 8.3, a separable element fixes only one nondegenerate 1-space, hence only one nondegenerate hyperplane. Therefore we only need to prove the first part of the statement.

By [GL01] Theorem 2.3, the proportion of regular semisimple elements in \( G \) is at least \( 1 - 2/(q-1) - 2/(q-1)^2 \). Since \( 2/(q-1) + 2/(q-1)^2 + 1/(q-1) \leq 6/q \), by Lemma 8.4 we just need to prove that the proportion of elements which act as \(-1\) on a nondegenerate 2-space \( W \) is at most \( 1/(q-1) \) (note that a regular semisimple element cannot have equivalent modules of dimension at least 2). Let \( E \) be the set of such elements.

For fixed \( W \), there are at most \( |\Omega_{2m-1}(q)| \) choices for the element; indeed, for fixed \( W \), it is determined whether the restriction of the element to \( W^\perp \) belongs to \( \Omega(W^\perp) \) or to \( SO(W^\perp) \setminus \Omega(W^\perp) \). Now we have to sum over all possible \( W \)’s. Since \( 2(q-1) = |O_2^+(q)| < |O_2(q)| = 2(q+1) \), there are at most \( 2|O_{2m+1}(q)|/|O_2^+(q)||O_{2m-1}(q)| \) choices. In particular, we deduce that

\[
|E| \leq 2|O_{2m-1}(q)|/|O_2^+(q)||O_{2m-1}(q)| \leq \frac{2|O_{2m-1}(q)|}{|O_2(q)|} = \frac{|\Omega_{2m+1}(q)|}{q-1}.
\]

The proof is finished. \( \Box \)

**Theorem 8.6.** The conclusion to Theorem 1.5(2) holds for the case \( G = \Pi \Omega_{2m+1}(q) \) with \( q \) odd.

**Proof.** Let \( x = x_1 \) be as in [GK08] Table II, and let \( x_2 \) act on the space as \((m \oplus m) \perp 1\) and having order \((q^m-1)/2\). Set \( A_\ell = \{x_1, x_2\} \).

We claim that \( x_2 \) does not lie in maximal subgroups from classes \( C_2 \) and \( C_3 \). If this is true, then by Theorem 8.1 and [FG18] Theorem 2.5, the proportion of elements of \( G \) lying in conjugates of overgroups of both \( x_1 \) and \( x_2 \) is \( |R^+ \cap R^-|/|G| + O(n^{-0.005}) \).

By Theorem 8.6 \( |R^+ \cap R^-|/|G| \leq 6/q \), therefore \( P_{\text{inv}}(G, A_\ell) \geq 1 - 6/q + O(n^{-0.005}) \) by Lemma 1.9.

Therefore it suffices to prove the claim. Assume first \( x_2 \in \text{GL}_{n/b}(q^b) \times C_b \) for some prime \( b \) dividing \( n \). If \( m \) is large then \((q^m-1)/2b > q^{m/2} - 1\). In particular, \( x_2 \in \text{GL}_{n/b}(q^b) \) fixes only \( m \)-spaces, and only one 1-space, which is impossible.

Assume now \( x_2 \in \text{GL}_k(q) \) \( \not\in S_\ell \) with \( n = kt \) and \( t > 1 \). The element \( x_2 \) induces a permutation \( \pi \) of \( S_\ell \) having at most 3 cycles; hence the order of \( \pi \), say \( \ell \), is at most \( n^3 \). Then \( x_2^\ell \in \text{GL}_k(q)^\ell \). Again, for \( m \) large \( x_2^\ell \) fixes \( m \)-spaces and a 1-space. Provided \( n > 3 \), this is impossible for an element of \( \text{GL}_k(q)^\ell \), and the proof is finished. \( \Box \)

Next we want to prove Theorem 1.5(3) in this case. The key fact is that, for \( q \) fixed, the proportion of regular semisimple elements acting as \(-1\) on a nondegenerate 2-space is bounded away from zero. We recall an important result.

**Theorem 8.7.** In the limit as \( m \to \infty \), the proportion of elements of \( \Omega_{2m+1}(q) \) which are separable is equal to the proportion of elements of \( SO_{2m+1}(q) \setminus \Omega_{2m+1}(q) \) which are separable. This proportion is at least 0.348 for \( m \) sufficiently large.
Proof. See [FG17] Theorems 7.19 and 7.24.

Theorem 8.8. If \( m \) is sufficiently large, the proportion of elements of \( G \) which are regular semisimple, and which act as \(-1\) on a nondegenerate 2-space of plus type, is at least \( 1/6q \). These elements fix hyperplanes of both signs, and fix a singular 1-space.

Proof. The last statement is clear, since a 2-space of plus type contains a singular 1-space, and contains nondegenerate 1-spaces of square and non-square discriminant. Therefore we only need to prove the first part of the statement. The proof is similar (although opposite in spirit) to Theorem 8.5. Let \( E \) be the set of regular semisimple elements which act as \(-1\) on a nondegenerate 2-space of plus type \( W \). For fixed \( W \), by Theorem 8.7 there are exactly \( |\Omega_{2m-1}(q)|/3 \) choices for the element on \( W^\perp \). Then we have to sum through all \( W \)'s. We have

\[
|E| \geq \frac{|\Omega_{2m-1}(q)|}{3} \frac{|\Omega_{2m+1}(q)|}{|O_2^+(q)| - |\Omega_{2m-1}(q)|} = \frac{|\Omega_{2m+1}(q)|}{3|O_2^+(q)|} \geq \frac{|\Omega_{2m+1}(q)|}{6q},
\]

which concludes the proof. (Conceptually, there is nothing special here in considering a 2-space: the same argument applies to elements acting as \(-1\) on a space of bounded dimension.)

Theorem 8.9. The conclusion to Theorem 1.5(3) holds for the case \( G = P\Omega_{2m+1}(q) \) with \( q \) odd.

Proof. We already observed that \( G = R^+ \cup R^- \cup P_1 \). By Theorem 8.8 we have \( |R^+ \cap R^- \cap P_1|/|G| \geq 1/6q \) for sufficiently large \( m \), hence \( P_{\text{inv}}(G, G) \leq 1 - 1/6q \) by Lemma 1.9 which concludes the proof.

We finally observe that we cannot have \( |A_\ell| = 1 \) in Theorem 1.5(2) (not even for \( q \to \infty \)).

Lemma 8.10. Let \( \varepsilon \in \{+,-\} \). Then, the proportions \( |R^\varepsilon|/|G| \) and \( |P_1|/|G| \) are at least \( \delta_1 \) for some absolute constant \( \delta_1 > 0 \). In particular, for every \( x \in G \), \( P_{\text{inv}}(G, x) \leq 1 - \delta_1 \).

Proof. If we prove the first part of the statement, the last part will follow from Lemma 1.9 and the fact that \( G = R^+ \cup R^- \cup P_1 \). Therefore we only need to prove the first part. For \( q \) fixed, we proved a stronger statement in Theorem 8.8.

Next we deal with large \( q \). By Theorem 8.5 the proportion of separable elements in \( G \) is \( 1 - O(1/q) \). If a separable element \( g \) fixes a nondegenerate hyperplane \( W \), then the maximal torus of \( g \) is contained in the stabilizer of \( W \) (indeed in a subgroup \( S\perp(W) \) of the stabilizer). The same is certainly true for the stabilizer of a singular 1-space, since this is obtained as the fixed points of a connected subgroup of the algebraic group. Therefore, using Theorem 8.8 we see that the proportion of elements belonging to \( R^\varepsilon \) (resp. \( P_1 \)) is equal to \( O(1/q) \) plus the proportion of elements of the Weyl group \( W(B_m) \cong C_2 S_m \) corresponding to maximal tori fixing a nondegenerate hyperplane of \( \varepsilon \) sign (resp. a singular 1-space). For a nondegenerate hyperplane of \( \varepsilon \) sign, these are the elements \((x_1, \ldots, x_m)\tau \) with \( \tau \in S_m \), \( x_i = \pm 1 \) and \( \prod x_i = \varepsilon \) (see Remark 8.4 which explains how to identify the class of an element), so their proportion is exactly \( 1/2 \). For a singular 1-space, these are the elements \((x_1, \ldots, x_m)\tau \) with \( j\tau = j \) and \( x_j = + \) for some \( j \), and their proportion is at least \((1 - 1/e)/2 \) for sufficiently large \( m \); this follows from the fact that, for random
Assume moreover $x \mod 4$, it acts as $\left(\begin{array}{c} m \\ 1 \end{array}\right)$ stabilizers of subspaces, the only maximal overgroup of $x$ large. (Subgroups of class $C_1$ can easily prove that $q_4$ we choose irreducible modules whose dimensions differ by 2; recall Lemma 5.11.) In this way, our element $m$ on the symplectic module as $\left(\begin{array}{c} 1 \\ 1 \end{array}\right)$ odd, for convenience we modify $x$.

**Proof.** Let $q$ with $q_2$, with $q_1$ even. With $q_1$ even.

**Theorem 8.11.** The conclusion to Theorem 1.1 holds in the case $G = \text{PSp}_{2m}(q)$ with $q$ even.

**Proof.** In view of Theorem 1.2, we may assume that $m$ is large. Let $x \in G = \text{Sp}_{2m}(q)$ be as in [GK00, Table II]. The same argument given for the other classical groups in Subsection 8.3 applies, except that $x$ stabilizes a unique nondegenerate hyperplane of plus or minus type. Therefore

$$\frac{|\mathcal{A}(x)|}{|G|} = \frac{|R^\pm|}{|G|} + O(n^{-0.005}).$$

Since $|R^\pm|/|G|$ is bounded away from 1 by [FG17, Theorem 9.15] (it is at most 0.86 for $n$ sufficiently large), the statement follows from Lemma 1.9.

We have now completed the proof of Theorem 1.1 and we summarize this fact here.

**Proof of Theorem 1.1.** For $G = A_n$, see Theorem 2.1. For $G = G_2(3^n)$, see Theorem 4.1(i). For the remaining groups of Lie type of bounded rank, we proved the stronger Theorem 1.2 in Section 8. For groups of Lie type of large rank, see Theorems 5.2, 5.3 and 5.11.

**Theorem 8.12.** The conclusion to Theorem 1.5(2) holds in the case $G = \text{PSp}_{2m}(q)$ with $q$ even.

**Proof.** Let $x = x_1 \in G = \text{Sp}_{2m}(q)$ be as in Table [GK00, Table II]. In case $m$ is odd, for convenience we modify $x_1$ as follows. If $m \equiv 1 \mod 4$, we choose $x_1$ acting on the symplectic module as $(m - 1)/2 \perp (m + 3)/2 \perp (m - 1)$; and if $m \equiv 3 \mod 4$ we choose $x_1$ acting as $(m + 1)/2 \perp (m - 3)/2 \perp (m + 1)$. We let $x_1$ have order $q^b + 1$ on each block of dimension $2b$. Similarly to the proof of Theorem 8.6 we can easily prove that $x_1$ does not belong to subgroups of classes $C_2$ and $C_3$ if $m$ is large. (Subgroups of class $C_3$ are ruled out since the element has nondegenerate irreducible modules whose dimensions differ by 2; recall Lemma 5.11.) In this way, our element $x_1$ belongs to $\text{SO}_{2m}(q)$ in all cases, both for $m$ even and $m$ odd.

Next, define $x_2 \in G$ as follows: if $m$ is odd, it acts as $(m - 1) \perp (m + 1)$; if $m \equiv 0 \mod 4$, it acts as $(m - 2) \perp (m + 2)$; if $m \equiv 2 \mod 4$, it acts as $(m - 4) \perp (m + 4)$. Assume moreover $x_2$ has order $q^b + 1$ on each block of dimension $2b$. Except for stabilizers of subspaces, the only maximal overgroup of $x_2$ is a conjugate of $\text{SO}_{2m}(q)$.
(see [BH19] Lemma 6.2]; in fact, a simpler argument applies since we only need to consider classes $C_2$ and $C_3$).

Set now $A_t = \{x_1, x_2\}$. By Theorem [SX] and [FG18] Theorem 2.4, the proportion of elements lying in conjugates of overgroups of both $x_1$ and $x_2$ is $|R^+ \cap R^-|/|G| + O(n^{-0.005})$.

By [GL01] Theorem 2.3, the proportion of regular semisimple elements in $G$ is at least $1 - 6/q$. A regular semisimple element does not have eigenvalue $1$ on the symplectic module (or, in other words, centralizes only $V^\perp$ on the orthogonal module $V$). It follows that a regular semisimple element $g$ fixes only one nondegenerate hyperplane, namely $[g, V]$. Then $|R^+ \cap R^-|/|G| \leq 6/q$, which shows that $P_{\text{inv}}(G, A_t) \geq 1 - 6/q + O(n^{-0.005})$. □

Next we prove Theorem [L3] in this case, which is the final remaining step in the proof of all the main results.

Let $G = \text{Sp}_{2m}(q)$ with $m \geq 2$ and $q$ even. We first observe that, if $g \in G$ is semisimple and centralizes a 2-space, then $g$ fixes hyperplanes of both signs. In the case $q$ odd, we could exploit the discriminant to see this; here we use a different argument.

**Lemma 8.13.** Assume $g \in G$ is semisimple and dim $C_V(g) \geq 2$ on the orthogonal module. Then $g$ fixes nondegenerate hyperplanes of both signs.

**Proof.** Assume $V^\perp = \langle v \rangle$. Since every element of $F_q$ is a square, by rescaling we may assume $Q(v) = 1$. Assume now $g$ is semisimple and fixes a nondegenerate hyperplane $W$; we want to show that $g$ fixes also a hyperplane of opposite sign.

Since $V = W \perp V^\perp$, by assumption there exists $0 \neq e \in W$ such that $eg = e$. Write $W = \langle e \rangle \oplus T$, with $T$ fixed by $g$. Assume first $Q(e) \neq 0$. Consider $e' := Q(e)^{-1/2}e + v$. Clearly $e'g = e'$ and $Q(e') = 0$. Moreover, $g$ fixes $W' := \langle e' \rangle \oplus T$, which is a complement of $V^\perp$, i.e., a nondegenerate hyperplane. If $W'$ has opposite sign with respect to $W$, the proof is finished. Hence, replacing $W$ by $W'$ and $e$ by $e'$, we may assume from the beginning that $Q(e) = 0$.

Since $g$ is semisimple, $g$ centralizes a nondegenerate 2-subspace $\langle e, f \rangle$ of $W$, where $Q(f) = 0$ and $\langle e, f \rangle = 1$. Write now $W = \langle e, f \rangle \perp U$, with $U$ fixed by $g$. Pick $\xi \in F_q$ such that the polynomial $X^2 + X + \xi^2$ is irreducible over $F_q$. Then set $e' := e + v, f' := f + \xi v$ and $W' := \langle e', f' \rangle \perp U$. A straightforward computation shows that $\langle e', f' \rangle$ is a nondegenerate anisotropic space, i.e., $Q(x) \neq 0$ for every $0 \neq x \in \langle e', f' \rangle$ (cf. [KL90] p. 26). It follows now from [KL90] Propositions 2.5.3 and 2.5.11] that $W'$ has opposite sign with respect to $W$. This concludes the proof. □

**Theorem 8.14.** [FGT17] Theorem 7.11] The proportion of elements in $\text{Sp}_{2m}(q)$ which are regular semisimple is at least $0.283$ for $m$ sufficiently large.

**Theorem 8.15.** If $m$ is sufficiently large, the proportion of elements of $G$ which act (on the symplectic module) as the identity on a nondegenerate 2-space, and which are regular semisimple on the orthogonal complement, is at least $1/4q^3$. These elements fix nondegenerate hyperplanes of both signs.

**Proof.** The last part of the statement follows from Lemma 8.13. The first part is exactly the same as in Theorem [SX] (one essentially replaces $\Omega$ by $\text{Sp}$ throughout, and we use $|\text{Sp}_2(q)| \leq q^3$). □
Theorem 8.16. The conclusion to Theorem 1.5(3) holds in the case $G = \text{PSp}_{2m}(q)$ with $q$ even.

Proof. We already recalled that $G = R^+ \cup R^-$, and by Theorem 8.15 we have that $|R^+ \cap R^-|/|G| \geq 1/4q^3$ for sufficiently large $m$. Therefore $P_{\text{inv}}(G, G) \leq 1 - 1/4q^3$ by Lemma 1.9.

The proof of Theorem 1.5 is now complete, and we summarize it here.

Proof of Theorem 1.5. For part (1), see Theorem 5.12. For part (2), the case of alternating groups is completed in Theorem 2.1, and for groups of Lie type see Theorems 8.2, 8.6 and 8.12. For part (3), the case $G = G_2(3^a)$ follows from Theorem 4.1(ii). When $G = \text{PO}_{2m+1}(q)$ with $q$ odd and $m$ large, see Theorem 8.9. Finally, when $G = \text{PSp}_{2m}(q)$ with $q$ even and $m$ large, see Theorem 8.16.

Thus the proof of all the main results of the paper is complete. We conclude by showing that we cannot have $|A_{\ell}| = 1$ in Theorem 1.5 for $G = \text{PSp}_{2m}(q)$ with $q$ even.

Lemma 8.17. Let $\varepsilon \in \{+,-\}$. Then, $|R^\varepsilon|/|G| \geq \delta_2$ for an absolute constant $\delta_2 > 0$. In particular, for every $x \in G$, $P_{\text{inv}}(G, x) \leq 1 - \delta_2$.

Proof. The last part follows from the first, Lemma 1.9 and $G = R^+ \cup R^-$. We now prove the first statement. For $q$ fixed, we proved a stronger statement in Theorem 8.15. Next we deal with large $q$. By Theorem 8.9 the proportion of regular semisimple elements in $G$ is $1 - O(1/q)$. If a regular semisimple element $g$ fixes a nondegenerate hyperplane $W$, then the maximal torus of $g$ is contained in the stabilizer of $W$. As in the proof of Lemma 8.10 we deduce that the proportion of elements belonging to $R^\varepsilon$ is equal to $O(1/q)$ plus the proportion of elements of $W(B_m)$ with product of sign $\varepsilon$, which is $1/2$. \hfill $\square$

References

[Asc84] M. Aschbacher. On the maximal subgroups of the finite classical groups. Invent. Math., 76(3):469–514, 1984.
[BH19] T. C. Burness and S. Harper. On the uniform domination number of a finite simple group. Trans. Amer. Math. Soc., 372(1):545–583, 2019.
[BT71] A. Borel and J. Tits. Éléments unipotents et sous-groupes paraboliques de groupes réductifs. I. Invent. Math., 12:95–104, 1971.
[Car78] R. W. Carter. Centralizers of semisimple elements in finite groups of Lie type. Proc. London Math. Soc. (3), 37(3):491–507, 1978.
[Car93] R. W. Carter. Finite groups of Lie type. Wiley Classics Library, John Wiley & Sons, Ltd., Chichester, 1993. Conjugacy classes and complex characters.
[DF91] D. I. Deriziotis and A. P. Fakiolas. The maximal tori in the finite Chevalley groups of type $E_6$, $E_7$ and $E_8$. Comm. Algebra, 19(3):889–903, 1991.
[Dix92] J. D. Dixon. Random sets which invariably generate the symmetric group. Discrete Math., 105(1-3):25–39, 1992.
[Dye79] R. H. Dye. Interrelations of symplectic and orthogonal groups in characteristic two. Journal of Algebra, 59(1):202–221, 1979.
[EFG16] S. Eberhard, K. Ford, and B. Green. Permutations fixing a $k$-set. Int. Math. Res. Not. IMRN, (21):6713–6731, 2016.
[EFG17] S. Eberhard, K. Ford, and B. Green. Invariable generation of the symmetric group. Duke Math. J., 166(8):1573–1590, 2017.
[EFK16] S. Eberhard, K. Ford, and D. Koukoulopoulos. Permutations contained in transitive subgroups. Discrete Anal., 12:1–34, 2016.
[FG03] J. Fulman and R. M. Guralnick. Derangements in simple and primitive groups. In Groups, combinatorics & geometry (Durham, 2001), pages 99–121. World Sci. Publ., River Edge, NJ, 2003.

[FG12] J. Fulman and R. M. Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. Trans. Amer. Math. Soc., 364(6):3023–3070, 2012.

[FG17] J. Fulman and R. M. Guralnick. Derangements in subspace actions of finite classical groups. Trans. Amer. Math. Soc., 369(4):2521–2572, 2017.

[FG18] J. Fulman and R. M. Guralnick. Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture. Trans. Amer. Math. Soc., 370(7):4601–4622, 2018.

[FNP05] J. Fulman, P. M. Neumann, and C. E. Praeger. A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Amer. Math. Soc., 176(830):vi+90, 2005.

[Gar20] D. Garzoni. The invariably generating graph of the alternating and symmetric groups. Journal of Group Theory, 23(6):1081–1102, 2020.

[GK00] R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups. J. Algebra, 234(2):743–792, 2000. Special issue in honor of Helmut Wielandt.

[GKS94] R. M. Guralnick, W. M. Kantor, and J. Saxl. The probability of generating a classical group. Comm. Algebra, 22(4):1395–1402, 1994.

[GL01] R. M. Guralnick and F. Lübeck. On $p$-singular elements in Chevalley groups in characteristic $p$. In Groups and computation, III (Columbus, OH, 1999), volume 8 of Ohio State Univ. Math. Res. Inst. Publ., pages 169–182. de Gruyter, Berlin, 2001.

[GLSS99] R. M. Guralnick, M. W. Liebeck, J. Saxl, and A. Shalev. Random generation of finite simple groups. J. Algebra, 219(1):345–355, 1999.

[GLT12] R. M. Guralnick, M. Larsen, and P. H. Tiep. Representation growth in positive characteristic and conjugacy classes of maximal subgroups. Duke Math. J., 161(1):107–137, 2012.

[GM12a] R. M. Guralnick and G. Malle. Products of conjugacy classes and fixed point spaces. J. Amer. Math. Soc., 25(1):77–121, 2012.

[GM12b] R. M. Guralnick and G. Malle. Simple groups admit Beauville structures. J. Lond. Math. Soc. (2), 85(3):694–721, 2012.

[Gut72] M. M. Guterman. A characterization of the groups $F_4(2^n)$. J. Algebra, 20:1–23, 1972.

[KL90] P. Kleidman and M. W. Liebeck. The subgroup structure of the finite classical groups, volume 129 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1990.

[Kle88] P. B. Kleidman. The maximal subgroups of the Chevalley groups $G_2(q)$ with $q$ odd, the Ree groups $^2G_2(q)$, and their automorphism groups. J. Algebra, 117(1):30–71, 1988.

[KLS11] W. M. Kantor, A. Lubotzky, and A. Shalev. Invariable generation and the Chebotarev invariant of a finite group. J. Algebra, 348:302–314, 2011.

[KZ12] E. Kowalski and D. Zywina. The Chebotarev invariant of a finite group. Exp. Math., 21(1):38–56, 2012.

[Law99] R. Lawther. The action of $F_4(q)$ on cosets of $B_4(q)$. J. Algebra, 212(1):79–118, 1999.

[LMS05] M. W. Liebeck, B. M. S. Martin, and A. Shalev. On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function. Duke Math. J., 128(3):541–557, 2005.

[LP93] T. Łuczak and L. Pyber. On random generation of the symmetric group. Combin. Probab. Comput., 2(4):505–512, 1993.

[LS98] M. W. Liebeck and G. M. Seitz. On the subgroup structure of classical groups. Invent. Math., 134(2):427–453, 1998.

[LS99] M. W. Liebeck and A. Shalev. Simple groups, permutation groups, and probability. J. Amer. Math. Soc., 12(2):497–520, 1999.

[LSS92] M. W. Liebeck, J. Saxl, and G. M. Seitz. Subgroups of maximal rank in finite exceptional groups of Lie type. Proc. London Math. Soc. (3), 65(2):297–325, 1992.

[LT17] A. Lucchini and G. Tracey. An upper bound on the Chebotarev invariant of a finite group. Israel J. Math., 219(1):449–467, 2017.

[Luc18] A. Lucchini. The Chebotarev invariant of a finite group: a conjecture of Kowalski and Zywina. Proc. Amer. Math. Soc., 146(11):4549–4562, 2018.
[McK21] E. McKemmie. Invariable generation of finite classical groups. *J. Algebra*, 585:592–615, 2021.

[MT11] G. Malle and D. Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011.

[PPR16] R. Pemantle, Y. Peres, and I. Rivin. Four random permutations conjugated by an adversary generate $S_n$ with high probability. *Random Structures Algorithms*, 49(3):409–428, 2016.

[Sha98] A. Shalev. A theorem on random matrices and some applications. *J. Algebra*, 199(1):124–141, 1998.

[Suz82] M. Suzuki. *Group theory*, volume 247. Springer, 1982.

[Wei92] T. S. Weigel. Generation of exceptional groups of Lie-type. *Geom. Dedicata*, 41(1):63–87, 1992.

[Wil09] R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
Email address: danieleg@mail.tau.ac.il

Department of Mathematics, Rutgers University, Piscataway, NJ, 08854, USA
Email address: emck@rutgers.edu