NORMALISERS OF MAXIMAL TORI AND
A CONJECTURE OF VDOVIN

TIMOTHY C. BURNESS AND ADAM R. THOMAS

ABSTRACT. Let $G = O^{p'}(\bar{G}^F)$ be a finite simple group of Lie type defined over a field of characteristic p, where F is a Steinberg endomorphism of the ambient simple algebraic group $\bar{G}$. Let $\bar{T}$ be an F-stable maximal torus of $\bar{G}$ and set $N = N_G(\bar{T})$. A conjecture due to Vdovin asserts that if $G \not\cong L_3(2)$ then $N \cap N^x$ is a p-group for some $x \in G$. In this paper, we use a combination of probabilistic and computational methods to calculate the base size for the natural action of G on G/N, which allows us to prove a stronger, and suitably modified, version of Vdovin's conjecture.

1. INTRODUCTION

Let G be a finite simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. Write $G = O^{p'}(\bar{G}^F)$, where $\bar{G}$ is a simple algebraic group of adjoint type over the algebraic closure k of $\mathbb{F}_p$ and F is an appropriate Steinberg endomorphism of $\bar{G}$ with fixed point subgroup $\bar{G}^F$. Let $\bar{T}$ be an F-stable maximal torus of $\bar{G}$ and set $N = N_G(\bar{T})$. The following conjecture of Evgeny Vdovin is presented as Problem 17.42 in the Kourovka Notebook [30] (it first appeared in the 17th edition, which was published in 2010).

Conjecture. *Let $G = O^{p'}(\bar{G}^F)$ be a finite simple group of Lie type and define $N = N_G(\bar{T})$ as above. If $G \not\cong L_3(2)$ then $N \cap N^x$ is a p-group for some $x \in G$.*

The special case $G \cong L_3(2)$ is a genuine exception. Indeed, if $N = 7{:}3$ is the normaliser of a Singer cycle, then $|N \cap N^x| = 3$ for all $x \in G \setminus N$.

In this paper, we will prove a suitably modified version of Vdovin's conjecture (it turns out that there are two additional exceptions, so an adjustment is necessary). In order to state our main result (see Theorem 1 below), we need some additional terminology. Let G and N be as above and view G as a transitive permutation group on the set $\Omega = G/N$ of cosets of N. Then the *base size* of G, denoted $b(G, N)$, is the minimal size of a subset of Ω with trivial pointwise stabiliser in G. Equivalently, $b(G, N)$ is the smallest number of conjugates of N so that the intersection of these subgroups is trivial. In particular, $b(G, N) = 2$ if and only if $N \cap N^x = 1$ for some $x \in G$. As a consequence, let us observe that if p does not divide the order of the Weyl group $N_{\bar{G}}(\bar{T})/\bar{T}$ of $\bar{G}$, then $N \cap N^x$ is a p-group for some $x \in G$ if and only if $b(G, N) = 2$.

Determining the base size of a finite permutation group is both a classical and fundamental problem in permutation group theory (we refer the reader to the survey articles [2, 28] and [6, Section 5] for more background on bases and their diverse applications in group theory and related areas). In particular, there has been a great deal of recent interest in studying base sizes for almost simple primitive permutation groups, partly motivated by a circle of highly influential conjectures of Babai, Cameron, Kantor and Pyber from the 1990s, which have all been resolved in recent years. In this context, our main result can be viewed as a contribution to research in this direction. It also constitutes further progress towards a classification of the finite primitive groups with a base of size 2, which is an active and ambitious project initiated by Saxl in the 1990s.

$b(G,N)$	G	N	
3	$L_2(q)$	$D_{2(q+1)}$	$q \geqslant 4$ even
	$L_3(2)$	$7{:}3$	
	$U_3(3)$	$4^2{:}S_3$	
	$U_5(2)$	$3^4{:}S_5$	
	$U_6(2)$	$3^4{:}S_6$	
	$Sp_6(2)$	$3^3{:}(S_2 \wr S_3)$	
	$\Omega_8^+(2)$	$3^4{:}(2^3{:}S_4)$	
4	$U_4(2)$	$3^3{:}S_4$	

TABLE 1. The groups in Theorem 1 with $b(G,N) \geqslant 3$

Theorem 1. Let $G = O^{p'}(\bar{G}^F)$ be a finite simple group of Lie type and set $N = N_G(\bar{T})$ as above. Then either

  (i) $b(G,N) = 2$; or

  (ii) G, N and $b(G,N)$ are recorded in Table 1 (up to isomorphism).

By inspecting the cases appearing in Table 1, we obtain the following corollary, which establishes a modified form of Vdovin's conjecture.

Corollary 2. There exists an element $x \in G$ such that $N \cap N^x$ is a p-group if and only if (G, N) is not one of the following (up to isomorphism):

$$(L_3(2), 7{:}3), \ (U_4(2), 3^3{:}S_4), \ (U_5(2), 3^4{:}S_5). \tag{1}$$

Remark 1. Let us comment on the three special cases recorded in (1).
  (a) First assume $G = L_3(2)$. Here $\bar{G} = \mathrm{PSL}_3(k)$ and we recall that there is a bijection between the set of G-classes of F-stable maximal tori of $\bar{G}$ and the set of conjugacy classes of the Weyl group S_3 (see Section 2.2 for more details). One of these G-classes corresponds to the split maximal tori in G, which are trivial since $q = 2$, so in this case we observe that $N = N_G(\bar{T}) = S_3$ is the subgroup of monomial matrices in G and it is easy to check that $b(G,N) = 2$. The other two G-classes yield subgroups of the form $N_G(T)$ with T a cyclic maximal torus of G. If $|T| = 3$ then $N = D_6$ and $b(G,N) = 2$. On the other hand, if $|T| = 7$ then T is a Singer cycle, $N = 7{:}3$ and we find that $|N \cap N^x| = 3$ for all $x \in G \setminus N$ (in addition, it is easy to identify elements $x, y \in G$ such that $N \cap N^x \cap N^y = 1$, so $b(G,N) = 3$).
  (b) Next suppose $G = U_4(2)$ and $N = 3^3{:}S_4$ is the normaliser of a split maximal torus. This case is also an exception to the main assertion in Vdovin's conjecture since $|N \cap N^x| \in \{24, 54\}$ for all $x \in G \setminus N$. In fact, $b(G,N) = 4$ and it is worth noting that there exist $x, y \in G$ such that $N \cap N^x \cap N^y$ has order 2.
  (c) Similarly, if $G = U_5(2)$ and $N = 3^4{:}S_5$ then we find that $b(G,N) = 3$ and $|N \cap N^x|$ is divisible by 12 for all $x \in G \setminus N$.

Some special cases of Theorem 1 have been studied in earlier work. For example, [13, Proposition 4.2(i)] states that if G is an almost simple exceptional group of Lie type and $N = N_G(\bar{T})$ is a maximal subgroup, then $b(G,N) = 2$. Similarly, if G is an almost simple classical group and $N = N_G(\bar{T})$ is maximal, then $b(G,N) \leqslant 4$ by the main theorem of [5] (in addition, the exact base size is computed in [7] if N is soluble and maximal, which includes the cases studied here with $G = L_2(q)$ and $q \geqslant 13$).

Bases for the action of the ambient algebraic group $\bar{G}$ on the coset variety $\bar{\Omega} = \bar{G}/\bar{N}$ have also been investigated, where $\bar{N} = N_{\bar{G}}(\bar{T})$. Here the main result is [9, Theorem 9], which states that $b(\bar{G}, \bar{N}) = 2$ unless $\bar{G}$ is isomorphic to $\mathrm{PSL}_2(k)$. (More precisely, if $\bar{G} \neq \mathrm{PSL}_2(k)$ then the *generic* base size is 2, which means that the 2-point stabiliser $\bar{G}_{\alpha,\beta}$ is trivial for all (α, β) in a non-empty open subset of $\bar{\Omega} \times \bar{\Omega}$.) As a consequence, if $G \neq L_2(q)$ is a finite

simple group of Lie type over $\mathbb{F}_q$ then [9, Proposition 2.7] implies that $b(G, N) = 2$ for all sufficiently large q (moreover, the probability $\mathcal{P}(G, N, 2)$ that a random pair of points in $\Omega = G/N$ forms a base for G tends to 1 as q tends to infinity). This result for algebraic groups is reflected in Theorem 1, where we see that Table 1 contains an infinite family of exceptions with $G = \mathrm{L}_2(q)$. In addition, let us observe that if $G = \mathrm{L}_2(q)$ then

$$\mathcal{P}(G, N, 2) \to \begin{cases} 1/2 & \text{if } q \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

as q tends to infinity (see the proof of [7, Lemmas 4.7, 4.8]).

Remark 2. Our main theorem has already found an application in [11], which we briefly describe. Let G be a finite insoluble group with souble radical $R(G)$ and consider the graph $\Gamma_{\mathcal{S}}(G)$ with vertices $G \setminus R(G)$, where distinct vertices x and y are adjacent if the subgroup $\langle x, y \rangle$ is soluble. This is called the *soluble graph* of G and the main theorem of [11] states that $\Gamma_{\mathcal{S}}(G)$ is connected and its diameter, denoted $\delta_{\mathcal{S}}(G)$, is at most 5. By a celebrated theorem of Thompson, a finite group is soluble if and only if every 2-generated subgroup is soluble. This implies that $\delta_{\mathcal{S}}(G) \geqslant 2$ and it remains an open problem to determine all the simple groups with $\delta_{\mathcal{S}}(G) = 2$; the only known examples are as follows (up to isomorphism):

$$\mathrm{L}_2(q) \ (q \geqslant 4 \text{ even}), \ \mathrm{L}_3(2), \ \mathrm{U}_4(2).$$

In [11], Theorem 1 is used to reduce this problem to unitary, symplectic and orthogonal groups (see [11, Propositions 6.9, 6.15]). For groups of Lie type, the connection is as follows. Suppose there exists a semisimple element $g \in G$ such that $\langle g \rangle$ is a maximal torus and $N = N_G(\langle g \rangle)$ is the unique maximal soluble subgroup of G containing g (for example, if $n \geqslant 3$ then this property holds if $G = \mathrm{L}_n(q)$ and $g \in G$ is a Singer element of order $(q^n - 1)/d(q - 1)$ with $d = (n, q - 1)$). Excluding the special cases in Table 1, it follows that $N \cap N^x = 1$ for some $x \in G$. Since the neighbours of g and g^x in $\Gamma_{\mathcal{S}}(G)$ coincide with the nontrivial elements in N and N^x, respectively, we conclude that the distance between g and g^x is at least 3 and thus $\delta_{\mathcal{S}}(G) \geqslant 3$.

We will apply a combination of probabilistic and computational methods in the proof of Theorem 1, handling the classical and exceptional groups separately. Our main approach involves the application of fixed point ratio estimates in order to derive an upper bound on $\mathcal{Q}(G, N, 2)$, which is the probability that a random pair of points in G/N do not form a base for G. Clearly, if $\mathcal{Q}(G, N, 2) < 1$ then $b(G, N) = 2$. This powerful method for studying base sizes was originally introduced by Liebeck and Shalev [27] in their proof of a conjecture of Cameron and Kantor on bases for almost simple primitive groups. For appropriate low rank groups defined over small fields, we will also use a range of computational methods to calculate $b(G, N)$, working with MAGMA [3]. We refer the reader to Section 2.3 for further details on some of these computations.

The classical groups require a detailed analysis and a key tool is the following zeta-type function

$$\eta_G(t) = \sum_{i=1}^{m} |x_i^G|^{-t}$$

where $t \in \mathbb{R}$ and $x_1, \ldots, x_m$ is a complete set of representatives of the conjugacy classes in G of elements of prime order. In order to explain the relevance of this function, let

$$\mathrm{fpr}(x, G/N) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap N|}{|x^G|}$$

be the fixed point ratio of $x \in G$, where $C_\Omega(x)$ is the set of fixed points of x on $\Omega = G/N$. As explained in Section 2.1, if we can establish the existence of a constant $c > 0$ such that

$\mathrm{fpr}(x_i, G/N) \leqslant |x_i^G|^{-c}$ for all i, then

$$\mathcal{Q}(G, N, 2) \leqslant \sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i, G/N)^2 \leqslant \eta_G(2c - 1)$$

and thus $b(G, N) = 2$ if $\eta_G(2c - 1) < 1$. With this observation in hand, a key result is [5, Proposition 2.2], which states that $\eta_G(1/3) < 1$ if $n \geqslant 6$, where n is the dimension of the natural module for G. For $n \geqslant 6$, we are therefore interested in establishing an upper bound of the form

$$\mathrm{fpr}(x, G/N) < |x^G|^{-\frac{2}{3}}$$

for each $x \in G$ of prime order, which in turn requires a careful analysis of $|x^G \cap N|$ and $|x^G|$. There is an extensive literature on the conjugacy classes of prime order elements in G and the main challenge here is to derive an effective upper bound on $|x^G \cap N|$. The low rank classical groups with $n < 6$ will require special attention and they are handled separately.

Notation. Let G be a finite group and let n be a positive integer. We will write C_n, or just n, for a cyclic group of order n and G^n will denote the direct product of n copies of G. If X is a subset of G, then $i_n(X)$ is the number of elements in X of order n. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits then we may write $G{:}H$. We adopt the standard notation for simple groups of Lie type from [22] and all logarithms in this paper are in base 2.

Acknowledgements. Burness thanks the Department of Mathematics at the University of Padua for their generous hospitality during a research visit in autumn 2021. Thomas is supported by EPSRC grant EP/W000466/1.

2. PRELIMINARIES

In this section we present some preliminary results which will be needed in the proof of Theorem 1.

2.1. **Probabilistic methods.** Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group of degree d with point stabiliser N and base size $b(G, N)$. Since the elements of G are uniquely determined by their action on a base, it follows that $|G| \leqslant d^{b(G,N)}$ and we obtain the lower bound $b(G, N) \geqslant \log_d |G|$.

Let c be a positive integer and let $\mathcal{Q}(G, N, c)$ be the probability that a random c-tuple of elements in Ω do not form a base for G. Although it is difficult to compute $\mathcal{Q}(G, N, c)$ precisely, a powerful approach for determining an effective upper bound was introduced by Liebeck and Shalev in [27]. Indeed, it is straightforward to show that

$$\mathcal{Q}(G, N, c) \leqslant \sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i, G/N)^c =: \widehat{\mathcal{Q}}(G, N, c),$$

where $x_1, \ldots, x_m$ form a complete set of representatives of the conjugacy classes in G of elements of prime order and

$$\mathrm{fpr}(x_i, G/N) = \frac{|C_\Omega(x_i)|}{|\Omega|} = \frac{|x_i^G \cap N|}{|x_i^G|}$$

is the fixed point ratio of x_i on $\Omega = G/N$ with $C_\Omega(x_i) = \{\alpha \in \Omega : \alpha^{x_i} = \alpha\}$. The following is an immediate consequence.

Proposition 2.1. *If $N \neq 1$ and $\widehat{\mathcal{Q}}(G, N, 2) < 1$ then $b(G, N) = 2$.*

The following result (see [5, Lemma 2.1]) is a useful tool for estimating $\widehat{\mathcal{Q}}(G, N, 2)$.

Lemma 2.2. *Suppose $x_1, \ldots, x_s$ represent distinct G-classes such that $\sum_i |x_i^G \cap N| \leqslant A$ and $|x_i^G| \geqslant B$ for all i. Then*

$$\sum_{i=1}^{s} |x_i^G| \cdot \mathrm{fpr}(x_i, G/N)^2 \leqslant A^2/B.$$

In our analysis of classical groups, we will work with the zeta-type function

$$\eta_G(t) = \sum_{i=1}^{m} |x_i^G|^{-t} \tag{2}$$

where $t \in \mathbb{R}$. The next result (see [5, Proposition 2.2]) will be an essential ingredient.

Proposition 2.3. *Let G be an almost simple classical group with natural module of dimension $n \geqslant 6$. Then $\eta_G(1/3) < 1$.*

Corollary 2.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple transitive group with nontrivial point stabiliser N and socle G_0. Assume G_0 is a classical group with natural module of dimension $n \geqslant 6$. Then $b(G, N) = 2$ if*

$$\mathrm{fpr}(x, G/N) \leqslant |x^G|^{-\frac{2}{3}} \tag{3}$$

for all $x \in G$ of prime order.

Proof. We have

$$\widehat{\mathcal{Q}}(G, N, 2) \leqslant \sum_{i=1}^{m} |x_i^G|^{-\frac{1}{3}} = \eta_G(1/3) < 1$$

by Proposition 2.3 and thus $b(G, N) = 2$ by Proposition 2.1. $\qquad\square$

For $x \in G$, it will be convenient to set

$$\alpha(x) = \frac{\log |x^G \cap N|}{\log |x^G|}, \tag{4}$$

noting that the bound in (3) holds if and only if $\alpha(x) \leqslant 1/3$.

Remark 2.5. For some low dimensional classical groups over small fields, it is often possible to establish a stronger form of Proposition 2.3 with $\eta_G(t) < 1$ for some explicit constant $t < 1/3$ (see Lemmas 3.4, 4.2, 5.1 and 6.2). In this situation, it then suffices to show that $\alpha(x) \leqslant (1 - t)/2$ for all $x \in G$ of prime order.

2.2. **Maximal tori.** There is a well developed theory of maximal tori in finite groups of Lie type and here we briefly recall some of the key features and results, following [15, Section 3.3] and [31, (2.1)–(2.4)].

As in the introduction, let $\bar{G}$ be a simple algebraic group of adjoint type over the algebraic closure k of $\mathbb{F}_p$ and let F be a Steinberg endomorphism of $\bar{G}$ so that $O^{p'}(\bar{G}^F)$ is a simple group of Lie type over $\mathbb{F}_q$. Let $\bar{T}$ be an F-stable maximal torus of $\bar{G}$ and observe that there is a natural action of F on the Weyl group $W = N_{\bar{G}}(\bar{T})/\bar{T}$. We say $w_1, w_2 \in W$ are F-*conjugate* if there exists $x \in W$ such that $w_2 = x^F w_1 x^{-1}$. This defines an equivalence relation on W and the equivalence classes are called F-*classes*. The F-*centraliser* of $w \in W$ is the subgroup

$$C_{W,F}(w) = \{x \in W \ : \ x^F w x^{-1} = w\} \tag{5}$$

of W.

Remark 2.6. We refer the reader to [29, Section 22.1] for more information on the action of F on W and the character group of $\bar{T}$. For our purposes, let us note that the action of F on W is determined by the corresponding automorphism ρ induced by F on the Coxeter diagram of $\bar{G}$ (the non-oriented Dynkin diagram). If ρ is trivial (in which case $\bar{G}^F$ is an untwisted group), then the F-classes of W are just the usual conjugacy classes of W and we see that $C_{W,F}(w) = C_W(w)$ is the centraliser of w. Similarly, if ρ corresponds to an

involutory graph automorphism of the Coxeter diagram and $\bar{G}$ is not of type D_r with $r \geqslant 4$ even, then there is a bijection from the F-classes of W to the usual conjugacy classes, and we note that $C_{W,F}(w)$ is isomorphic to $C_W(w)$. In the remaining cases, there is a distinction to be made between the F-classes of W and the usual conjugacy classes of W, and we refer the reader to [19, Sections 6.5 and 7] for more details. Further comments on the case where $G = \mathrm{P\Omega}_{2r}^-(q)$ and $r \geqslant 4$ is even are presented in Remark 6.1.

A fundamental result (see [15, Proposition 3.3.3], for example) states that there is a bijection from the set of F-classes of W to the set of $\bar{G}^F$-classes of F-stable maximal tori in $\bar{G}$. Fix an F-stable maximal torus $\bar{T}_w$ in the $\bar{G}^F$-class corresponding to the F-class of w. Since any two maximal tori in $\bar{G}$ are conjugate, it follows that $\bar{T}_w = \bar{T}^g$ for some $g \in \bar{G}$ and the F-stability of $\bar{T}_w$ implies that $g^F g^{-1} \in N_{\bar{G}}(\bar{T})$ (indeed, up to F-conjugacy we may assume w is the image of $g^F g^{-1}$ in W). By [15, Proposition 3.3.6] we have

$$N_{\bar{G}^F}(\bar{T}_w)/\bar{T}_w^F \cong C_{W,F}(w).$$

The order of $\bar{T}_w^F$ can be computed using [15, Proposition 3.3.5] and the following useful upper bound is proved in [31, (2.4)].

Lemma 2.7. *Let $\bar{S}$ be an F-stable ℓ-dimensional torus in $\bar{G}$. Then*

$$|\bar{S}^F| \leqslant (q^a + 1)^\ell,$$

where $a = 1/2$ if $\bar{G}^F = {}^2B_2(q)$, ${}^2G_2(q)$ or ${}^2F_4(q)$, otherwise $a = 1$.

Set $G = O^{p'}(\bar{G}^F)$. Then each $\bar{G}^F$-class of F-stable maximal tori in $\bar{G}$ intersects G in a single G-class and we set $T = G \cap \bar{T}_w^F$. If we now define $d = |\bar{G}^F : G|$, which is the order of the centre of the simply connected version of $\bar{G}$, then $|\bar{T}_w^F : T| = d$ and it follows that

$$N = N_G(\bar{T}_w) = T.R,$$

where $R = C_{W,F}(w)$ as above. Here it is important to note that N may be a proper subgroup of $N_G(\bar{T}_w^F)$. For example, if $G = \mathrm{L}_n(2)$ and $w = 1$, then $\bar{T}_w^F$ is trivial and $N \cong S_n$ is the subgroup of monomial matrices in G.

We close with the following result, which will be useful in our proof of Theorem 1 for exceptional groups of Lie type. In the statement, ρ_R denotes the number of reflections in R.

Lemma 2.8. *Let $N = T.R$ as above. If $x \in N$ is a root element in G, then $p = 2$ and*

$$|x^G \cap N| \leqslant \rho_R |T|.$$

Proof. By [24, Proposition 1.13], if $y \in N_{\bar{G}}(\bar{T})$ is a root element, then $p = 2$ and y centralises a subtorus in $\bar{T}$ of codimension 1. In particular, each root element in N corresponds to a reflection in $R = N_{\bar{G}^F}(\bar{T}_w)/\bar{T}_w^F$, so N contains at most $\rho_R |T|$ root elements and the result follows. $\qquad\square$

2.3. **Computational methods.** In this final preliminary section, we briefly discuss some of the main computational methods we use in the proof of Theorem 1. In order to perform these computations, we use MAGMA [3], version V2.26-12.

There are essentially two different ways in which we apply computational methods. Firstly, if G is a low rank simple group of Lie type defined over a small field, then it may be possible to verify Theorem 1 directly, typically by constructing G and N as permutation groups and using random search to find an element $x \in G$ such that $N \cap N^x = 1$. These are the sort of computations we focus on here, with Lemmas 2.9 and 2.10 as our main results. Note that we do not need to construct N explicitly in all cases; indeed, to conclude that $b(G, N) = 2$, it suffices to show that there exists an overgroup L of N with $L \cap L^x = 1$ for some $x \in G$.

For other groups where this direct approach is not feasible, we may still be able to use MAGMA to obtain useful information about G and N, which can then be combined with the probabilistic techniques described in Section 2.1. For example, see Lemmas 3.4, 4.2, 5.1 and 6.2, where we use MAGMA to show that $\eta_G(t) < 1$ for various classical groups G and explicit

constants $t < 1/3$, which allows us to work with slightly weaker fixed point ratio estimates in order to establish the bound $\widehat{\mathcal{Q}}(G, N, 2) < 1$. Similarly, for certain exceptional groups we will use MAGMA to help us estimate $\widehat{\mathcal{Q}}(G, N, 2)$. For instance, see the proof of Proposition 7.5, where the groups $G = E_6^\varepsilon(2)$ require special attention.

The following lemma establishes Theorem 1 for some specific low dimensional classical groups defined over small fields.

Lemma 2.9. *The conclusion to Theorem 1 holds if G is one of the following groups:*

$$\mathrm{L}_6^\varepsilon(2), \mathrm{L}_6^\varepsilon(3), \mathrm{L}_7^\varepsilon(2), \mathrm{L}_8^\varepsilon(2)$$
$$\mathrm{Sp}_6(2), \mathrm{PSp}_6(3), \mathrm{Sp}_6(4), \mathrm{PSp}_6(5), \mathrm{Sp}_8(2), \mathrm{PSp}_8(3)$$
$$\Omega_7(3), \Omega_8^\varepsilon(2), \mathrm{P}\Omega_8^\varepsilon(3), \Omega_9(3), \Omega_{10}^\varepsilon(2)$$

Proof. As noted above, we will use MAGMA [3] to verify the result, working with a standard permutation representation of G of degree $n \leqslant 22204$ (with equality if $G = \mathrm{U}_6(3)$). Write $N = T.R$ as above and recall from Section 2.2 that we can describe the possibilities for N in terms of the Weyl group of G (for example, see the opening paragraphs in Sections 3–6 below). Also note that the precise cyclic structure of T is given in [14].

We start by handling the following possibilities for (G, N):

$$(\mathrm{U}_6(2), 3^4{:}S_6), (\mathrm{Sp}_6(2), 3^3{:}(S_2 \wr S_3)), (\Omega_8^+(2), 3^4{:}(2^3{:}S_4)). \tag{6}$$

Note that each of these cases appears in Table 1 and we need to prove that $b(G, N) = 3$. First we construct N by observing that $N = N_G(K)$, where K is an elementary abelian normal subgroup of a Sylow 3-subgroup of G of order 3^4, 3^3 and 3^4, respectively. In each case, we can find elements $x, y \in G$ by random search such that $N \cap N^x \cap N^y = 1$, which implies that $b(G, N) \leqslant 3$ (in the same way, we can identify an element $x \in G$ such that $|N \cap N^x| = 2, 4, 4$ in the respective cases, so these cases still satisfy the main statement in Vdovin's conjecture). For $G = \mathrm{Sp}_6(2)$ and $\Omega_8^+(2)$ we have $\log_d |G| > 2$, where $d = |G : N|$, whence $b(G, N) = 3$ as claimed. For $G = \mathrm{U}_6(2)$, we can use MAGMA to find a complete set S of (N, N) double coset representatives in G and we then check that $|NxN| < |N|^2$ for all $x \in S$. This implies that $N \cap N^x \neq 1$ for all $x \in G$, so $b(G, N) \geqslant 3$ and the result follows.

Now let us turn to the remaining cases, where we need to show that $b(G, N) = 2$. First consider the special case $T = 1$, which only arises when $R = W$ and G is one of the following:

$$\mathrm{L}_6(2), \mathrm{L}_7(2), \mathrm{L}_8(2), \mathrm{Sp}_6(2), \mathrm{Sp}_8(2), \Omega_8^+(2), \Omega_{10}^+(2).$$

In each of these cases, it is straightforward to construct $N = W$ as a subgroup of G by applying some of the in-built functions in MAGMA for handling groups of Lie type. It is then a routine exercise to check that there exists an element $x \in G$ with $N \cap N^x = 1$ and thus $b(G, N) = 2$.

Finally, let us assume $T \neq 1$, excluding the cases in (6) handled above. Here we adopt the following uniform approach, which is straightforward to implement in MAGMA. As above, we work with a standard permutation representation of G and we write $|T|_p = p^a$, where p is defined to be the largest prime divisor of $|T|$. We start by constructing a set of representatives of the conjugacy classes of abelian subgroups of $N_G(P)$ of order p^a, where P is a Sylow p-subgroup of G. For each representative K, we construct $L = N_G(K)$ and we discard K if $|L|$ is not divisible by $|N|$. We now have a collection of subgroups of the form $N_G(K)$, at least one of which contains a conjugate of N (this is because N normalises $O_p(T)$, which is an abelian subgroup of order p^a). Fix a subgroup $L = N_G(K)$ whose order is divisible by $|N|$. We then use random search to see if there exists an element $x \in G$ with $L \cap L^x = 1$. If we find such an element, then we move to the next compatible subgroup of the form $N_G(K)$ and repeat. On the other hand, if the random search is inconclusive, then we construct a set of representatives of the L-classes of subgroups J of L of order $|N|$ and we use random search once again to show that $b(G, J) = 2$. In this way, one can check that $b(G, N) = 2$ in every case. $\square$

For the exceptional groups of Lie type, we present the following result.

Lemma 2.10. *Let G be one of the following groups*

$$G_2(3), \ G_2(4), \ G_2(5), \ {}^3D_4(2), \ {}^3D_4(4), \ {}^2F_4(2)'$$

and let $N = N_G(\bar{T})$ as above. Then $b(G, N) = 2$.

Proof. Once again we use MAGMA [3]. Let $\mathcal{A}$ be the set of orders of the subgroups N we need to consider. For instance, if $G = G_2(q)$, then $W = D_{12}$ has 6 conjugacy classes (which coincide with the F-classes of W; see Remark 2.6) and we see that N is one of the following

$$(C_{q\pm1})^2.D_{12}, \ C_{q^2\pm q+1}.6, \ C_{q^2-1}.2^2,$$

noting that G has two conjugacy classes of maximal tori of the form C_{q^2-1}. So for example, if $q = 5$ then $\mathcal{A} = \{96, 126, 186, 192, 432\}$. The corresponding information for the relevant twisted groups can be found in [17, Table 1.1] for ${}^3D_4(q)$ and [32] for ${}^2F_4(2)$.

Suppose $G \neq {}^3D_4(4), {}^2F_4(2)'$ and $|N| = n \in \mathcal{A}$. First we construct G as a permutation group via the function `AutomorphismGroupOfSimpleGroup` and we then identify a set of representatives of the conjugacy classes of order n subgroups of G. It is then straightforward to find a random element $x \in G$ such that $H \cap H^x = 1$ for each representative H and we conclude that $b(G, N) = 2$.

A very similar argument applies when $G = {}^2F_4(2)'$. Here it is convenient to work in $L = {}^2F_4(2) = G.2$, noting that the possibilities for $|N_L(\bar{T})|$ can be read off from [32, Table III] (also see [19, Table 7.3]). As before, we construct a set of representatives of the L-classes of subgroups H of order $|N_L(\bar{T})|$ and we then use random search to find an element $x \in G$ with $H \cap H^x = 1$. Once again, this allows us to deduce that $b(G, N) = 2$ in all cases.

Finally, let us assume $G = {}^3D_4(4)$. As above, we can construct G as a permutation group of degree 328965, but the `Subgroups` function is ineffective and so a slightly different approach is needed. Let T be a maximal torus of G. If $T = (C_{21})^2$, $(C_{13})^2$ or C_{241} then N is a maximal subgroup of G and thus $b(G, N) = 2$ by [13, Proposition 4.2]. So to complete the proof, we may assume $T = C_{65} \times C_5$, $C_{63} \times C_3$, C_{315} or C_{195}. To handle these cases, we first construct a Sylow 3-subgroup H and a Sylow 5-subgroup K of G, working with the given permutation representation of G. Now H has an element x of order 3 such that $C_G(x) = L_2(64) \times C_3$ contains the maximal tori $C_{63} \times C_3$ and C_{195}. Similarly, we find an element $y \in K$ of order 5 such that $C_G(y) = L_2(64) \times C_5$ contains $C_{65} \times C_5$ and C_{315}. We can now construct N by taking the normalisers of these tori and it is easy to check that $b(G, N) = 2$ by random search. $\qquad\square$

3. LINEAR AND UNITARY GROUPS

In this section, we prove Theorem 1 for the classical groups with socle $L_n^\varepsilon(q)$. The low dimensional groups with $n < 6$ require special attention and they will be treated separately at the end of the section. We begin by recording some preliminary observations.

Write $G = O^{p'}(\bar{G}^F)$, where $\bar{G} = \mathrm{PSL}_n(k)$ is the ambient simple algebraic group defined over the algebraic closure k of $\mathbb{F}_p$ and F is a suitable Steinberg endomorphism of $\bar{G}$. Fix an F-stable maximal torus $\bar{T}$ of $\bar{G}$ and set $\bar{N} = N_{\bar{G}}(\bar{T}) = \bar{T}.W$, where $W = S_n$ is the Weyl group of $\bar{G}$. We may assume $\bar{T}$ is the image (modulo scalars) of the group of diagonal matrices in $\mathrm{SL}_n(k)$ with respect to a standard basis $\{e_1, \ldots, e_n\}$ of the natural module $\bar{V}$ for $\mathrm{SL}_n(k)$. If we set $\bar{V}_i = \langle e_i \rangle$, then $\bar{N}$ is the stabiliser in $\bar{G}$ of the direct sum decomposition $\bar{V} = \bar{V}_1 \oplus \cdots \oplus \bar{V}_n$ and we will abuse notation by writing $(\lambda_1, \ldots, \lambda_n)\sigma$ for a typical element of $\bar{N}$, where $\lambda_i \in k^\times$ and $\sigma \in S_n$.

Recall from Section 2.2 that there is a bijection from the set of $\bar{G}^F$-classes of F-stable maximal tori in $\bar{G}$ to the set of F-classes in W. As recorded in Remark 2.6, the F-classes in W are in bijection with the usual conjugacy classes in this case, which are in turn parameterised by the set of partitions of n. Let $w \in W$ be a permutation with cycle-shape $\mu = (n^{a_n}, \ldots, 1^{a_1})$, where $a_\ell \geqslant 0$ is the multiplicity of ℓ as a part of μ. Then in the notation

of Section 2.2, the W-class of w corresponds to an F-stable maximal torus $\bar{T}_w$ of $\bar{G}$ and we set $N = N_G(\bar{T}_w) = T.R$. Here T is the image in G of the intersection $\widehat{T} \cap \mathrm{SL}_n^{\varepsilon}(q)$, where

$$\widehat{T} = (C_{q^n - \varepsilon^n})^{a_n} \times \cdots \times (C_{q - \varepsilon})^{a_1}$$

is a maximal torus of $\mathrm{GL}_n^{\varepsilon}(q)$ (the precise cyclic structure of T is given in [14, Section 2]). In addition,

$$R = C_{W,F}(w) \cong C_W(w) = (C_n \wr S_{a_n}) \times \cdots \times (C_1 \wr S_{a_1}).$$

We refer the reader to [8, Chapter 3] for detailed information on prime order elements and their conjugacy classes in the finite classical groups. We will also work with the following parameter, noting that bounds on $|x^G|$ in terms of $\nu(x)$ are presented in [4, Section 3].

Definition 3.1. Let G be a finite simple classical group over $\mathbb{F}_q$ with natural module V and set $\bar{V} = V \otimes k$, where k is the algebraic closure of $\mathbb{F}_q$. Given $x \in G$, let $\hat{x} \in \mathrm{GL}(V)$ be a pre-image of x and set

$$\nu(x) = \min \left\{ \dim [\bar{V}, \lambda \hat{x}] \; : \; \lambda \in k^{\times} \right\},$$

where $[\bar{V}, y] = \langle v - vy \; : \; v \in \bar{V} \rangle$. Note that $\nu(x)$ is equal to the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$.

Remark 3.2. Let $G = \mathrm{L}_n^{\varepsilon}(q) = L/Z$, where $L = \mathrm{SL}_n^{\varepsilon}(q)$ and $Z = Z(L)$. Let $x \in G$ be an element of prime order r. By [4, Lemma 3.11], if r is odd then either

(a) $x = Z\hat{x}$, where $\hat{x} \in L$ has order r; or

(b) r divides $(n, q - \varepsilon)$, $C_{\bar{G}}(x)$ is disconnected and

$$|x^G| > \frac{1}{2r} \left(\frac{q}{q+1} \right)^{r-1} q^{n^2 \left(1 - \frac{1}{r} \right)}. \tag{7}$$

It is straightforward to see that the same conclusion also holds when $r = 2$. In particular, if $r \neq p$ and $C_{\bar{G}}(x)$ is connected, then x lifts to an element of order r in L.

Recall that if X is a subset of G and r is a positive integer, then $i_r(X)$ denotes the number of elements of order r in X. The following upper bound will be useful.

Lemma 3.3. *Let $G = \mathrm{L}_n^{\varepsilon}(q)$ and define $N = T.R$ as above. Then*

$$i_r(N) \leqslant \sum_{j=0}^{\lfloor n/r \rfloor} \frac{n!}{j!(n-jr)!r^j}(q+1)^{n-1-j}$$

for every prime divisor r of $|N|$.

Proof. Recall that $N = T.R$, where $T = G \cap \bar{T}_w^F$, $R = C_{W,F}(w) \cong C_W(w)$ and $\bar{T}_w = \bar{T}^g$ for some $g \in \bar{G}$. Set $\Lambda = \{\sigma \in R \; : \; \sigma^r = 1\}$ and observe that

$$i_r(N) \leqslant \sum_{\sigma \in \Lambda} i_r(T\sigma).$$

Fix $\sigma \in \Lambda$ with cycle-shape $(r^j, 1^{n-jr})$ as an element of $W = S_n$. We claim that

$$i_r(T\sigma) \leqslant (q+1)^{n-1-j}.$$

To see this, first observe that $i_r(T\sigma) = |A|$, where $A = \{s \in gTg^{-1} \; : \; |s\sigma'| = r\}$ and $\sigma' = g\sigma g^{-1}$. Now A is contained in $\{s \in \bar{T} \; : \; |s\sigma'| = r\}$ and by considering the action of σ' on $\bar{T}$ we deduce that A is contained in an F-stable subtorus $\bar{S}$ of $\bar{T}$ with $\dim \bar{S} = n - 1 - j$. For example, if

$$\sigma' = (1, \ldots, r)(r+1, \ldots, 2r) \ldots ((j-1)r + 1, \ldots, jr)$$

as an element of S_n, then we may identify $\bar{S}$ with the image of the standard maximal torus of $\mathrm{SL}_r(k)^j \times \mathrm{SL}_{n-jr}(k) < \mathrm{SL}_n(k)$, which has dimension $j(r-1) + (n-jr-1) = n-1-j$.

Therefore, $|A| \leqslant (q+1)^{n-1-j}$ by Lemma 2.7 and this justifies the claim. The result now follows since there are at most

$$\frac{n!}{j!(n-jr)!r^j}$$

elements in R with cycle-shape $(r^j, 1^{n-jr})$.   □

Recall that if $n \geqslant 6$ then Proposition 2.3 states that $\eta_G(1/3) < 1$, where $\eta_G(t)$ is the function defined in (2). For certain low dimensional groups over small fields we can use a computational approach to show that $\eta_G(t) < 1$ for some smaller constant $t < 1/3$.

Lemma 3.4. *Let $G = \mathrm{L}_n^\varepsilon(q)$, where $n \geqslant 6$.*

(i) *If (n, q) is one of the following, then $\eta_G(t) < 1$ where t is defined as in the table:*

	$n = 7$	8	9	10	11	12	13	14
$q = 2$	21/100	9/50	3/25	7/50	3/25	2/25	1/10	9/100
3	7/50	11/100						

(ii) *If $n = 6$ and $q \leqslant 7$, then $\eta_G(t) < 1$ where t is defined as follows:*

q	2	3	4	5	7
t	1/5	4/25	17/100	13/100	3/25

Proof. We use MAGMA [3]. Set $d = (n, q - \varepsilon)$ and let r be a prime divisor of $|G|$.

First assume $(d, r) = 1$. We take the standard matrix representation of $L = \mathrm{SL}_n^\varepsilon(q)$ and we use the functions `Classes` ($\varepsilon = +$) and `ClassicalClasses` ($\varepsilon = -$) to determine the list of conjugacy class sizes of elements of order r in L, noting that this coincides precisely with the corresponding list of class sizes in G.

Now suppose r divides d and set $Z = Z(L)$, so $G = L/Z$. As above, we first determine the sizes of the L-classes of the form x^L, where $x \in L \setminus Z$ and $x^r \in Z$. Fix a class x^L and let s be the multiplicity of $|x^L|$ in this list of class sizes. If s is divisible by r, then G has exactly s/r classes of elements of order r with size $|x^L|$, otherwise G has s such classes of size $|x^L|/r$ (see [8, Propositions 3.2.2, 3.3.3], for example).

In this way, we obtain the complete list $a_1, \ldots, a_m$ of conjugacy class sizes of elements of prime order in G, and it is now a routine exercise to verify the bound $\sum_i a_i^{-t} < 1$ for the given value of t.   □

Theorem 3.5. *Suppose $G = \mathrm{L}_n^\varepsilon(q)$ and $n \geqslant 6$. Then $b(G, N) \leqslant 3$, with equality if and only if $G = \mathrm{U}_6(2)$ and $N = 3^4{:}S_6$, in which case $|N \cap N^x| = 2$ for some $x \in G$.*

Proof. In view of Lemma 2.9, we may assume

$$(n, q) \notin \{(6, 2), (6, 3), (7, 2), (8, 2)\}. \tag{8}$$

For the remaining groups, we set $t = 1/3$, with the exception of the specific low dimensional groups over small fields appearing in Lemma 3.4, where we define $t < 1/3$ as in the lemma. As explained in Section 2.1, if

$$\alpha(x) \leqslant \frac{1}{2}(1 - t) \tag{9}$$

for all $x \in N$ of prime order, where $\alpha(x)$ is defined as in (4), then

$$\mathcal{Q}(G, N, 2) \leqslant \eta_G(t) < 1$$

and thus $b(G, N) = 2$. Therefore, our goal is to verify the bound in (9).

Fix an element $x \in N$ of prime order r and let $\omega \in k$ be a primitive r-th root of unity. We now divide the argument into several cases and we freely adopt the notation introduced at the start of Section 3.

Case 1. $r = p$.

First assume $r = p$, so x is unipotent and $p \leqslant n$ (since p must divide $|W| = n!$). Here x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(1, \ldots, 1)\sigma$, where $\sigma \in S_n$ has cycle-shape $(p^h, 1^{n-hp})$ for some positive integer h. Then x has Jordan form (J_p^h, J_1^{n-hp}) on V and thus

$$|x^G| = \frac{|\mathrm{GL}_n^\varepsilon(q)|}{q^{h(2n-hp-h)}|\mathrm{GL}_h^\varepsilon(q)||\mathrm{GL}_{n-hp}^\varepsilon(q)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{h(p-1)(2n-hp)}.$$

By arguing as in the proof of Lemma 3.3 we deduce that

$$|x^G \cap N| \leqslant \frac{n!}{h!(n-hp)!p^h}(q+1)^{h(p-1)} \tag{10}$$

and by combining this with the lower bound on $|x^G|$ we get $\alpha(x) \leqslant \beta(x)$, where $\beta(x)$ is a function of n, h, p and f, where $q = p^f$. So in order to establish the bound in (9), it suffices to show that $\beta(x) \leqslant (1-t)/2$. Now if we fix h, p and f, then $\beta(x)$ is a decreasing function of n. Therefore, we may assume $n = hp$. Then the corresponding expression for $\beta(x)$ is decreasing in both f and h, so we may additionally assume that $f = h = 1$ and thus $n = p$. Now $\beta(x)$ is a decreasing function of p and one checks that $\beta(x) \leqslant 1/3$ for $p = 5$. So for the remainder, we may assume $p \in \{2, 3\}$.

Suppose $p = 3$. If $h \geqslant 3$ then $\beta(x)$ is maximal when $(n, h, f) = (9, 3, 1)$ and it is easy to check that $\beta(x) \leqslant 1/3$. Similarly, if $h \in \{1, 2\}$ then we reduce to the case $f = 1$. Here $n \geqslant 7$ (see (8)) and once again it is straightforward to verify the bound $\beta(x) \leqslant (1-t)/2$ (note that $\beta(x)$ is maximal when $n = 7$).

Finally, suppose $p = 2$. If $f \geqslant 2$ then one can check that $\beta(x) \leqslant (1-t)/2$, so we may assume $f = 1$ and $n \geqslant 9$ (see (8)). Working with $\beta(x)$, and recalling that t is defined in Lemma 3.4 for $n \leqslant 14$, we may assume $(n, h) = (9, 1)$, $(9, 2)$ or $(10, 1)$. In each of these cases, we can establish the desired bound by working with a precise expression for $|x^G|$. For example, if $(n, h) = (9, 2)$ then $t = 3/25$ and

$$|x^G \cap N| \leqslant \frac{9!}{2!5!2^2}3^2 = 3402, \quad |x^G| = \frac{|\mathrm{GL}_9^\varepsilon(2)|}{2^{24}|\mathrm{GL}_2^\varepsilon(2)||\mathrm{GL}_5^\varepsilon(2)|} \geqslant 236251890,$$

which implies that $\alpha(x) \leqslant (1-t)/2$.

Case 2. $r \neq p$, $C_{\bar{G}}(x)$ disconnected.

Here r divides n, (7) holds and one can check that the trivial bound

$$|x^G \cap N| \leqslant i_r(N) \leqslant |N| \leqslant (q+1)^{n-1}n!$$

is sufficient if $n \geqslant 22$. For $n \leqslant 21$ we can evaluate the upper bound on $i_r(N)$ in Lemma 3.3 and this yields $\alpha(x) \leqslant (1-t)/2$ as required.

Case 3. $r \neq p$, $C_{\bar{G}}(x)$ connected, $(r, |T|) = 1$.

This is very similar to Case 1, noting that the connectedness of $C_{\bar{G}}(x)$ implies that x lifts to an element of order r in $\mathrm{SL}_n^\varepsilon(q)$ (see Remark 3.2). Here $r \leqslant n$ and x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(1, \ldots, 1)\sigma$, where $\sigma \in S_n$ has cycle-shape $(r^h, 1^{n-hr})$ for some $1 \leqslant h < n/r$ (note that $h \neq n/r$ since we are assuming $C_{\bar{G}}(x)$ is connected). Therefore, x is $\bar{G}$-conjugate to $(I_{n-h(r-1)}, \omega I_h, \ldots, \omega^{r-1} I_h)$, modulo scalars, so

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{r-1}q^{h(r-1)(2n-hr)} \tag{11}$$

and by arguing as in Case 1 we see that

$$|x^G \cap N| \leqslant \frac{n!}{h!(n-hr)!r^h}(q+1)^{h(r-1)}.$$

One can now check that these bounds yield $\alpha(x) \leqslant (1-t)/2$.

Case 4. $r \neq p$, $C_{\bar{G}}(x)$ connected, r divides $|T|$.

To complete the proof, we may assume $r \neq p$ and r divides $|T|$. Let $0 \leqslant h < n/r$ be maximal such that x is $\bar{G}$-conjugate to an element in a coset $\bar{T}\sigma$, where $\sigma \in S_n$ has cycle-shape $(r^h, 1^{n-hr})$.

First assume $h = 0$, in which case $x^G \cap N \subseteq T$ and thus $|x^G \cap N| \leqslant (q+1)^{n-1}$. Set $s = \nu(x)$ (see Definition 3.1). If $s \geqslant 3$ then [4, Corollary 3.38] gives

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{6n-18}$$

and we deduce that $\alpha(x) \leqslant (1-t)/2$ as required. Similarly, if $s \in \{1, 2\}$ then the bounds

$$|x^G \cap N| \leqslant s\binom{n}{s}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{2s(n-s)}$$

are sufficient.

For the remainder, let us assume $h \geqslant 1$. Then $r \leqslant n$ and each r-th root of unity has multiplicity at least h as an eigenvalue of x on $\bar{V}$ (and by the maximality of h, the multiplicity of at least one eigenvalue is exactly h). One can check that $|x^G|$ is minimal when x is $\bar{G}$-conjugate to $(I_{n-h(r-1)}, \omega I_h, \ldots, \omega^{r-1}I_h)$ and thus (11) holds. Next observe that there exists an integer j in the range $0 \leqslant j \leqslant h$ such that x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(z_1, \ldots, z_n)\sigma$, where

$$\sigma = (1, \ldots, r)(r+1, \ldots, 2r)\cdots((j-1)r+1, \ldots, jr) \in S_n$$

has cycle-shape $(r^j, 1^{n-jr})$ and z_i is nontrivial (of order r) only if $i > jr$. Since there are at most r possibilities for each z_i with $i > jr$, it follows that

$$|x^G \cap N| \leqslant \sum_{j=0}^{h} \frac{n!}{j!(n-jr)!r^j}(q+1)^{j(r-1)}r^{n-jr}, \tag{12}$$

which in turn implies that

$$|x^G \cap N| \leqslant (q+1)^{h(r-1)}r^n \sum_{j=0}^{h}\left(\frac{n^r}{r}\right)^j \leqslant 2\left(\frac{n^r}{r}\right)^h (q+1)^{h(r-1)}r^n. \tag{13}$$

For now, let us assume $r \geqslant 3$ and $q \geqslant 3$. By combining the lower bound on $|x^G|$ in (11) with the upper bound on $|x^G \cap N|$ in (13), we deduce that $\alpha(x) \leqslant 1/3$ if $n \geqslant 22$ or $q \geqslant 31$, which means that we may assume $n \leqslant 21$ and $q \leqslant 29$. Then by evaluating the upper bound in (12), we may further assume that $n \leqslant 12$ and $q \leqslant 5$, with $r \in \{3, 5\}$ and $h = 1$.

Suppose $(r, h) = (3, 1)$. If x is $\bar{G}$-conjugate to $(I_{n-2}, \omega, \omega^2)$ then the bounds

$$|x^G \cap N| \leqslant 2\binom{n}{2} + \frac{n!}{(n-3)!3}(q+1)^2, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^2 q^{4n-6}$$

are sufficient. Otherwise,

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^2 q^{6n-14}$$

(minimal if x is of the form $(I_{n-3}, \omega I_2, \omega^2)$) and one can check that the upper bound on $|x^G \cap N|$ in (12) gives $\alpha(x) \leqslant (1-t)/2$. A very similar argument applies if $(r, h) = (5, 1)$. Indeed, if x is conjugate to $(I_{n-4}, \omega, \omega^2, \omega^3, \omega^4)$ then the bounds

$$|x^G \cap N| \leqslant 4!\binom{n}{4} + \frac{n!}{(n-5)!5}(q+1)^4, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^4 q^{8n-20}$$

are good enough. And if x is not of this form, then

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^4 q^{10n-32}$$

and we obtain $\alpha(x) \leqslant (1-t)/2$ via the upper bound on $|x^G \cap N|$ in (12).

To complete the proof, we may assume $r = 2$ or $q = 2$. We will first deal with the case $r = 2$, so $q \geqslant 3$ is odd and $x = (-I_h, I_{n-h})$ (modulo scalars) with $\nu(x) = h < n/2$ (recall that we are assuming $C_{\bar{G}}(x)$ is connected). Here

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{2h(n-h)}$$

and by arguing as in the proof of Lemma 3.3 we see that

$$|x^G \cap N| \leqslant \sum_{j=0}^{h} \frac{n!}{j!(n-2j)!2^j}(q+1)^j \binom{n-2j}{h-j}. \tag{14}$$

In particular, if $h = 1$ then

$$|x^G \cap N| \leqslant n + \frac{n!}{(n-2)!2}(q+1), \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{2n-2}$$

and we deduce that $\alpha(x) \leqslant (1-t)/2$. Now assume $h \geqslant 2$. If $n = 6$ then $h = 2$ and the above bounds are sufficient. For $n \geqslant 7$, one can check that the upper bound on $|x^G \cap N|$ given in (13) yields $\alpha(x) \leqslant 1/3$ if $n \geqslant 24$ or $q \geqslant 23$, so we may assume $n \leqslant 23$ and $q \leqslant 19$. At this point, we can now switch to the upper bound on $|x^G \cap N|$ in (14) and we obtain the desired bound $\alpha(x) \leqslant (1-t)/2$.

Finally, let us assume $q = 2$, so $r \geqslant 3$ and $n \geqslant 9$. There are several cases that require special attention.

First assume $(r, h) = (3, 1)$ and set $s = \nu(x)$. Since $h = 1$, it follows that either ω or ω^2 has multiplicity 1 as an eigenvalue of x on $\bar{V}$ and therefore

$$|x^G \cap N| \leqslant n \cdot 2^{n-1} + \frac{n!}{(n-3)!3}3^2 \cdot 2^{n-3}.$$

If $s \geqslant 4$ then $|x^G| > \frac{2}{9}2^{8n-26}$ and we deduce that $\alpha(x) \leqslant (1-t)/2$. Similarly, if $s = 3$ then we may assume $x = (I_{n-3}, \omega I_2, \omega^2)$, so $|x^G| > \frac{2}{9}2^{6n-14}$ and the bound

$$|x^G \cap N| \leqslant n\binom{n-1}{2} + \frac{n!}{(n-3)!3}3^2(n-3)$$

is sufficient. Finally, if $s = 2$ then $x = (I_{n-2}, \omega, \omega^2)$, $|x^G| > \frac{2}{9}2^{4n-6}$ and the result follows since

$$|x^G \cap N| \leqslant 2\binom{n}{2} + \frac{n!}{(n-3)!3}3^2.$$

Next suppose $(r, h) = (5, 1)$. Here we observe that r is a primitive prime divisor of $q^4 - 1$, so the condition $h = 1$ implies that x is of the form $(I_{n-4}, \omega, \omega^2, \omega^3, \omega^4)$. Therefore,

$$|x^G \cap N| \leqslant 4!\binom{n}{4} + \frac{n!}{(n-5)!5}3^4, \quad |x^G| > \frac{1}{3}2^{8n-20}$$

and we deduce that $\alpha(x) \leqslant (1-t)/2$.

For the remainder, we may assume $(r, h) \neq (3, 1), (5, 1)$. Now

$$|x^G| > \frac{1}{2}\left(\frac{2}{3}\right)^{r-1}2^{h(r-1)(2n-hr)} \tag{15}$$

and one can check that the upper bound in (13) gives $\alpha(x) \leqslant 1/3$ if $n \geqslant 54$. Similarly, if $n \leqslant 53$ then the bound in (12) is sufficient if $n \geqslant 31$. Therefore, to complete the proof we may assume $n \leqslant 30$.

Suppose $(r, h) = (7, 1)$ and note that r is a primitive prime divisor of $q^3 - 1$. If x is of the form $(I_{n-6}, \omega, \ldots, \omega^6)$ then the bounds

$$|x^G \cap N| \leqslant 6!\binom{n}{6} + \frac{n!}{(n-7)!7}3^6, \quad |x^G| > \frac{1}{3}2^{12n-42}$$

are sufficient. On the other hand, if x is not of this form, then $n \geqslant 10$, $|x^G| > \frac{1}{3}2^{18n-96}$ and the bound in (12) yields $\alpha(x) \leqslant (1-t)/2$. The case $(r, h) = (11, 1)$ is handled in an entirely similar fashion.

Next assume $r = 3$ and $h \in \{2, 3\}$, in which case there are two possibilities for x (up to scalars). If $x = (I_{n-2h}, \omega I_h, \omega^2 I_h)$ then

$$|x^G \cap N| \leqslant \sum_{j=0}^{h} \frac{n!}{j!(n-3j)!3^j} \frac{(n-3j)!}{(n-2h-j)!(h-j)!^2} 3^{2j}$$

and we deduce that $\alpha(x) \leqslant (1-t)/2$ since $|x^G| > \frac{2}{9}2^{2h(2n-3h)}$. Otherwise, x is of the form $(I_{n-2h-1}, \omega I_{h+1}, \omega^2 I_h)$ and the bounds

$$|x^G \cap N| \leqslant \sum_{j=0}^{h} \frac{n!}{j!(n-3j)!3^j} \frac{(n-3j)!}{(n-2h-j-1)!(h+1-j)!(h-j)!} 3^{2j}$$

and

$$|x^G| > \frac{2}{9}2^{4nh+2n-6h^2-6h-2}$$

are sufficient.

Finally, suppose $q = 2$, $n \leqslant 30$ and $hr \notin \{3, 5, 6, 7, 9, 11\}$. In these cases one can check that the bounds in (12) and (15) are good enough. $\qquad\square$

To complete the proof of Theorem 1 for linear and unitary groups, it remains to consider the following low-dimensional groups

$$\mathrm{L}_2(q), \ \mathrm{L}_3^\varepsilon(q), \ \mathrm{L}_4^\varepsilon(q), \ \mathrm{L}_5^\varepsilon(q).$$

Proposition 3.6. *If $G = \mathrm{L}_2(q)$ then $b(G, N) \leqslant 3$, with equality if and only if $q \geqslant 4$ is even and $N = D_{2(q+1)}$, in which case $|N \cap N^x| = 2$ for all $x \in G \setminus N$.*

Proof. Set $d = (2, q-1)$ and note that $N = D_{2(q-\varepsilon)/d}$ with $\varepsilon = \pm 1$. The groups with $q < 13$ can be checked directly using Magma [3] and so we may assume $q \geqslant 13$. Here N is a soluble maximal subgroup of G and [7, Lemmas 4.7, 4.8] imply that $b(G, N) \leqslant 3$, with equality if and only if q is even and $N = D_{2(q+1)}$. In the latter case, every nontrivial subdegree for the action of G on G/N is $q+1$ (see [18, Table 2], for example), so $|N \cap N^x| = 2$ for all $x \in G \setminus N$ and the result follows. $\qquad\square$

Proposition 3.7. *If $G = \mathrm{L}_3^\varepsilon(q)$ then $b(G, N) \leqslant 3$, with equality if and only if one of the following holds:*

(i) $(G, N) = (\mathrm{L}_3(2), 7{:}3)$, *in which case $|N \cap N^x| = 3$ for all $x \in G \setminus N$.*

(ii) $(G, N) = (\mathrm{U}_3(3), 4^2{:}S_3)$, *in which case $|N \cap N^x| = 3$ for some $x \in G$.*

Proof. Here $W = S_3$ has 3 conjugacy classes and we observe that the maximal tori in $\mathrm{SL}_3^\varepsilon(q)$ are as follows, up to conjugacy:

$$C_{q^2+\varepsilon q+1}, \ C_{q^2-1}, \ (C_{q-\varepsilon})^2 \tag{16}$$

and the corresponding possibilities for $N = T.R$ are $C_{q^2+\varepsilon q+1}{:}3$, $C_{q^2-1}{:}2$ and $(C_{q-\varepsilon})^2{:}S_3$, respectively (modulo scalars). The groups with $q \leqslant 5$ can be handled using Magma (see the proof of Lemma 2.9, for example), so we will assume $q \geqslant 7$.

In the first and third cases in (16) we observe that N is a soluble maximal subgroup of G and thus $b(G, N) = 2$ by [7, Lemmas 6.4, 6.5]. For the remainder we may assume that $N = \widehat{N}/Z$, where $\widehat{N} = C_{q^2-1}{:}2$ and $Z = Z(\mathrm{SL}_3^\varepsilon(q))$. We may identify $\widehat{N}$ with the normaliser in $\mathrm{GL}_2^\varepsilon(q)$ of an element of order $q^2 - 1$. Set $d = |Z| = (3, q-\varepsilon)$. By Proposition 2.1, it suffices to show that $\widehat{\mathcal{Q}}(G, N, 2) < 1$.

Let $x \in N$ be an element of prime order r. First assume $r = 2$ and note that G has a unique conjugacy class of involutions, so $|x^G \cap N| = i_2(\widehat{N})$. Write $\mathbb{F}_{q^2}^\times = \langle \lambda \rangle$ and identify

$\widehat{N}$ with $\langle\lambda\rangle{:}\langle\phi\rangle$, where $\phi : \lambda \mapsto \lambda^{\varepsilon q}$. It is straightforward to show that the coset $\langle\lambda\rangle\phi$ contains precisely $q + \varepsilon$ involutions, whence $|x^G \cap N| \leqslant q + 2 = a_1$ and we note that $|x^G| \geqslant (q^3 + 1)(q - 1) = b_1$ (minimal if $p = 2$ and $\varepsilon = -$).

Now assume r is odd, so r divides $q^2 - 1$. If x is regular (that is, if $C_{\bar{G}}(x)^0$ is a maximal torus), then

$$|x^G| \geqslant \frac{|\mathrm{GU}_3(q)|}{3|\mathrm{GU}_1(q)|^3} = \frac{1}{3}q^3(q - 1)(q^2 - q + 1) = b_2$$

and we note that $|N| \leqslant 2(q^2 - 1) = a_2$. On the other hand, if x is non-regular then r divides $q - \varepsilon$, $|x^G \cap N| = 1$ and

$$|x^G| = \frac{|\mathrm{GL}_3^\varepsilon(q)|}{|\mathrm{GL}_2^\varepsilon(q)||\mathrm{GL}_1^\varepsilon(q)|} \geqslant q^2(q^2 - q + 1) = b_3.$$

In view of Lemma 2.2, it follows that the combined contribution to $\widehat{\mathcal{Q}}(G, N, 2)$ from non-regular semisimple elements of odd order is at most

$$\sum_{r\in\pi}(r - 1)/b_3 < q\log(q + 1)/b_3 = c,$$

where π is the set of odd prime divisors of $q - \varepsilon$ (here we are using the fact that $r \leqslant q + 1$ and $|\pi| \leqslant \log(q + 1)$).

By bringing together the above estimates, using Lemma 2.2 once again, we obtain

$$\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1 + a_2^2/b_2 + c < 1$$

for all $q \geqslant 7$, so $b(G, N) = 2$ and the result follows. $\qquad\square$

Proposition 3.8. *If* $G = \mathrm{L}_4^\varepsilon(q)$ *then either* $b(G, N) = 2$, *or* $G = \mathrm{U}_4(2)$ *and* $N = 3^3{:}S_4$, *with* $b(G, N) = 4$ *and* $|N \cap N^x| \in \{24, 54\}$ *for all* $x \in G \setminus N$.

Proof. There are 5 conjugacy classes in the Weyl group $W = S_4$ and so there are 5 classes of maximal tori in $\mathrm{SL}_4^\varepsilon(q)$. The groups with $q \leqslant 5$ can be handled using MAGMA, so we will assume $q \geqslant 7$.

If T is the image of the split torus $(C_{q-\varepsilon})^3$, then N is a soluble maximal subgroup of G and thus [7, Lemma 6.6] gives $b(G, N) = 2$. For the remainder, we may assume $|N| \leqslant 8(q+1)^3/d$, where $d = (4, q - \varepsilon)$. As in the proof of the previous proposition, our aim is to verify the bound $\widehat{\mathcal{Q}}(G, N, 2) < 1$. Let $x \in N$ be an element of prime order r.

First assume $r \geqslant 5$ and observe that x is semisimple and $x^G \cap N \subseteq T$. If $\nu(x) \geqslant 2$ then

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{|\mathrm{GU}_2(q)|^2} = q^4(q^2 - q + 1)(q^2 + 1) = b_1$$

and we note that there are at most $a_1 = (q + 1)^3$ such elements in N (since $|T| \leqslant (q + 1)^3$). On the other hand, if $\nu(x) = 1$ then r must divide $q - \varepsilon$ and we observe that $|x^G \cap N| \leqslant 4$ and

$$|x^G| = \frac{|\mathrm{GL}_4^\varepsilon(q)|}{|\mathrm{GL}_3^\varepsilon(q)||\mathrm{GL}_1^\varepsilon(q)|} \geqslant q^3(q^2 + 1)(q - 1) = b.$$

Therefore, the total contribution to $\widehat{\mathcal{Q}}(G, N, 2)$ from these elements is at most

$$\sum_{r\in\pi} 4^2(r - 1)/b < 16q\log(q + 1)/b = c,$$

where π is the set of odd prime divisors $r \geqslant 5$ of $q - \varepsilon$.

Next assume $r = 3$. If $x^G \cap N \not\subseteq T$ then x is of the form (I_2, ω, ω^2) if $p \neq 3$ and (J_3, J_1) if $p = 3$, so

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{|\mathrm{GU}_2(q)||\mathrm{GU}_1(q)|^2} = q^5(q^2 - q + 1)(q^2 + 1)(q - 1) = b_2$$

and we have the trivial bound $|x^G \cap N| \leqslant |N| \leqslant 8(q+1)^3/d = a_2$. On the other hand, if $x^G \cap N \subseteq T$ then $|x^G| \geqslant q^3(q^2+1)(q-1) = b_3$ and we note that $i_3(T) \leqslant 3^3 - 1 = a_3$ since T is the direct product of at most three cyclic groups.

Finally, let us assume $r = 2$. If $\nu(x) = 1$ then $|x^G| \geqslant q^3(q^2+1)(q-1) = b_4$ and we calculate that N contains at most $(2^3 - 1) + 2\binom{4}{2}(q+1) = 12q + 19 = a_4$ involutions of this form. Similarly, if $\nu(x) = 2$ then $|x^G| \geqslant \frac{1}{2}q^4(q-1)(q^3-1) = b_5$ and by evaluating the upper bound in Lemma 3.3 we obtain $|x^G \cap N| \leqslant (q+1)(q^2+8q+10) = a_5$.

In conclusion, we have

$$\widehat{\mathcal{Q}}(G,N,2) < \sum_{i=1}^{5} a_i^2/b_i + c < 1$$

for all $q \geqslant 7$ and the result follows.   □

Proposition 3.9. *If $G = \mathrm{L}_5^\varepsilon(q)$ then $b(G,N) \leqslant 3$, with equality if and only if $G = \mathrm{U}_5(2)$ and $N = 3^4{:}S_5$, in which case $|N \cap N^x| \in \{12, 36, 72, 120, 324\}$ for all $x \in G \setminus N$.*

Proof. Here $W = S_5$ and so there are 7 conjugacy classes of maximal tori to consider. The groups with $q \leqslant 5$ can be handled using MAGMA, so we will assume $q \geqslant 7$. As before, our aim is to verify the bound $\widehat{\mathcal{Q}}(G,N,2) < 1$. Let $x \in N$ be an element of prime order r.

First observe that the contribution to $\widehat{\mathcal{Q}}(G,N,2)$ from the elements $x \in G$ with $|x^G| > \frac{1}{2}q^{14} = b_1$ is less than a_1^2/b_1, where $a_1 = 120(q+1)^4$ is an upper bound on the order of N. For the remainder, we may assume $|x^G| \leqslant \frac{1}{2}q^{14}$. If $r = p$ then r must divide $|W|$, so $r \in \{2,3,5\}$, and by considering the given condition on $|x^G|$ we deduce that $r = 2$ and x has Jordan form (J_2^j, J_1^{5-2j}) on the natural module, where $j = 1$ or 2. If $j = 1$ then $|x^G| > \frac{1}{2}q^8 = b_2$ and (10) gives $|x^G \cap N| \leqslant 10(q+1) = a_2$. Similarly, if $j = 2$ then $|x^G| > \frac{1}{2}q^{12} = b_3$ and $|x^G \cap N| \leqslant 15(q+1)^2 = a_3$.

Now assume $r \neq p$ (we continue to assume that $|x^G| \leqslant \frac{1}{2}q^{14}$). Suppose $x^G \cap N \subseteq T$. If $\nu(x) \geqslant 2$ then $|x^G| > \frac{1}{2}q^{12} = b_4$ and we note that $|T| \leqslant (q+1)^4 = a_4$. On the other hand, if $\nu(x) = 1$ then r must divide $q - \varepsilon$ and we have $|x^G \cap N| \leqslant 5$ and $|x^G| > \frac{1}{2}q^8 = b$. Therefore, the combined contribution from semisimple elements x with $x^G \cap N \subseteq T$ and $\nu(x) = 1$ is less than

$$\sum_{r \in \pi}(r-1) \cdot 5^2/b < 25q \log(q+1)/b = c,$$

where π is the set of prime divisors of $q-\varepsilon$. Finally, let us assume $x^G \cap N \nsubseteq T$, so $r \in \{2,3,5\}$. In fact, the assumption $|x^G| \leqslant \frac{1}{2}q^{14}$ implies that $r = 2$ and $x = (-I_h, I_{5-h})$ with $h \in \{1,2\}$. If $h = 1$ then $|x^G| > \frac{1}{2}q^8 = b_5$ and we compute $|x^G \cap N| \leqslant 5 + \binom{5}{2}(q+1) = 10q + 15 = a_5$. And if $h = 2$ we get $|x^G| > \frac{1}{2}q^{12} = b_6$ and (14) yields

$$|x^G \cap N| \leqslant \binom{5}{2} + 3\binom{5}{2}(q+1) + \frac{5!}{2!1!2^2}(q+1)^2 = 15q^2 + 60q + 55 = a_6.$$

Putting these estimates together, we deduce that

$$\widehat{\mathcal{Q}}(G,N,2) < \sum_{i=1}^{6} a_i^2/b_i + c < 1$$

for $q \geqslant 7$ and the result follows.   □

4. SYMPLECTIC GROUPS

In this section we prove Theorem 1 for symplectic groups. Let $G = O^{p'}(\bar{G}^F) = \mathrm{PSp}_n(q)'$, where $n = 2m \geqslant 4$ and $q = p^f$ for some prime p. Let W be the Weyl group of $\bar{G}$ and note that $W = S_2 \wr S_m < S_n$ is the hyperoctahedral group. Fix an F-stable maximal torus $\bar{T}$ of $\bar{G}$ and set $\bar{N} = \bar{T}.W$. We may assume $\bar{T}$ is the group of diagonal matrices in $\bar{G} = \mathrm{PSp}_n(k)$ (modulo scalars) with respect to a standard symplectic basis $\{e_1, f_1, \ldots, e_m, f_m\}$ of the natural module

$\bar{V}$. Set $\bar{V}_i = \langle e_i, f_i \rangle$ and observe that $\bar{N}$ is contained in the stabiliser of the orthogonal decomposition $\bar{V} = \bar{V}_1 \perp \cdots \perp \bar{V}_m$. More precisely, $\bar{N}$ is the image (modulo scalars) of $\bar{L} \wr S_m$, where

$$\bar{L} = \langle \operatorname{diag}(\lambda, \lambda^{-1}), z \ : \ \lambda \in k^{\times} \rangle < \operatorname{Sp}_2(k) \tag{17}$$

and $z = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right)$.

Next recall that the conjugacy classes in W (and hence the F-classes as well; see Remark 2.6) are parameterised by pairs of partitions (λ, μ) with $|\lambda| + |\mu| = m$ (here $|\lambda| \geqslant 0$ denotes the sum of the parts comprising λ, and similarly for $|\mu|$). Fix an element $w \in W$ corresponding to the pair (λ, μ), where $\lambda = (m^{a_m}, \ldots, 1^{a_1})$ and $\mu = (m^{b_m}, \ldots, 1^{b_1})$. Then in the notation of Section 2.2, the W-class of w corresponds to an F-stable maximal torus $\bar{T}_w$ of $\bar{G}$ and we set $N = N_G(\bar{T}_w) = T.R$. Here $R \cong C_W(w)$ and T is the image (modulo scalars) of a maximal torus

$$\widehat{T} = (C_{q^m-1})^{a_m} \times \cdots \times (C_{q-1})^{a_1} \times (C_{q^m+1})^{b_m} \times \cdots \times (C_{q+1})^{b_1}$$

of $\operatorname{Sp}_n(q)$. See [14, Theorem 3] for the precise cyclic structure of T.

Lemma 4.1. *Let $G = \operatorname{PSp}_n(q)$, where $n = 2m$ and $N = T.R$ is defined as above. Then*

$$i_r(N) \leqslant \sum_{j=0}^{\lfloor m/r \rfloor} 2^{j(r-1)} \frac{m!}{j!(m - jr)!r^j} (q+1)^{m-j}$$

for every odd prime divisor r of $|N|$.

Proof. Suppose $\sigma \in R$ has order r. Then σ is W-conjugate to $(1, \ldots, 1)\rho$, where $\rho \in S_m$ has cycle-shape $(r^j, 1^{m-jr})$ for some $j \geqslant 1$, and we note that

$$|\sigma^W| = 2^{j(r-1)} \frac{m!}{j!(m - jr)!r^j}.$$

We can now proceed as in the proof of Lemma 3.3 and we omit the details. □

Lemma 4.2. *Let $G = \operatorname{PSp}_n(q)$, where $n \geqslant 6$.*

(i) *If $n \leqslant 12$ and $q \leqslant 7$ then $\eta_G(t) < 1$, where t is defined as follows:*

	$q = 2$	3	4	5	7
$n = 6$	31/100	6/25	19/100	9/50	3/20
8	23/100	9/50	7/50	7/50	3/25
10	9/50	7/50	11/100	11/100	9/100
12	7/50	11/100	9/100	9/100	7/100

(ii) *If $n = 6$ and $8 \leqslant q \leqslant 32$ then $\eta_G(t) < 1$ for $t = 7/50$.*

(iii) *If $n \in \{8, 10\}$ and $8 \leqslant q \leqslant 16$ then $\eta_G(t) < 1$ for $t = 3/25$.*

(iv) *If $14 \leqslant n \leqslant 24$ and $q = 2$ then $\eta_G(t) < 1$ for $t = 3/25$.*

Proof. This is very similar to the proof of Lemma 3.4, using MAGMA and the function `ClassicalClasses` to compute the size of every conjugacy class in the matrix group $L = \operatorname{Sp}_n(q)$ comprising elements of prime order. Note that if q is odd, then to obtain the sizes of the involution classes in G we first compute the sizes of the L-classes of the form x^L, where $x \in L \setminus Z$ and $x^2 \in Z$ for $Z = Z(L)$. Fix a class x^L and let s be the multiplicity of $|x^L|$ in this list of class sizes. If s is even, then G has $s/2$ classes of involutions with size $|x^L|$, otherwise G has s classes of size $|x^L|/2$ (see [8, Table B.5], for example). □

Theorem 4.3. *Suppose $G = \operatorname{PSp}_n(q)$ and $n \geqslant 6$. Then $b(G, N) \leqslant 3$, with equality if and only if $G = \operatorname{Sp}_6(2)$ and $N = 3^3{:}(S_2 \wr S_3)$, in which case $|N \cap N^x| = 4$ for some $x \in G$.*

Proof. By considering Lemma 2.9, we may assume

$$(n, q) \notin \{(6, 2), (6, 3), (6, 4), (6, 5), (8, 2), (8, 3)\} \tag{18}$$

and so we will exclude these cases for the remainder of the proof. Set $t = 1/3$, with the exception of the groups in Lemma 4.2, where we define t as in the lemma. As in the proof of Theorem 3.5, it suffices to show that $\alpha(x) \leqslant (1 - t)/2$ for all $x \in N$ of prime order and we partition the proof into several cases. Let $\omega \in k$ be a primitive r-th root of unity and let us adopt the notation introduced at the beginning of Section 4.

Case 1. $r = p = 2$.

Here x is a unipotent involution and we adopt the standard notation from [1]. In particular, if x has Jordan form (J_2^h, J_1^{n-2h}) on V, then either h is odd and x is of type b_h, or h is even and x is of type a_h or c_h. Recall that $z = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) \in \bar{L}$ (see (17)).

We begin by describing the involutions in the algebraic group $\bar{N} = N_{\bar{G}}(\bar{T}) = \bar{L} \wr S_m$. Clearly, there are no involutions in $\bar{T}$, while every involution in $\bar{L}$ is conjugate to z, which is of type b_1 as an element of $\mathrm{Sp}_2(k)$. Therefore, if $x = (z_1, \ldots, z_m) \in \bar{L}^m$ is an involution with ℓ nontrivial components, then x is of type b_ℓ if ℓ is odd, otherwise x is of type c_ℓ (see [8, Lemma 3.4.14]). If $x \in \bar{N} \setminus \bar{L}^m$ is an involution, then there exists $1 \leqslant j \leqslant m/2$ such that x is conjugate to an element of the form $(1, \ldots, 1, z_{2j+1}, \ldots, z_m)\sigma$, where $\sigma = (1, 2) \cdots (2j - 1, 2j) \in S_m$ and $z_i^2 = 1$ for all i. If $\ell \geqslant 0$ denotes the number of nontrivial z_i, then x is of type a_{2j} if $\ell = 0$, type $b_{2j+\ell}$ if ℓ is odd and type $c_{2j+\ell}$ if $\ell \geqslant 2$ is even.

First assume $x \in G$ is an involution of type a_h, so h is even and $|x^G| > \frac{1}{2}q^{h(n-h)}$ (see [4, Proposition 3.22]). From the above description of the involutions in $\bar{N}$ we deduce that x is $\bar{G}$-conjugate to $(1, \ldots, 1)\sigma \in \bar{N}$, where $\sigma = (1, 2) \cdots (h - 1, h) \in S_m$. Now

$$|\sigma^W| = 2^{h/2} \frac{m!}{(h/2)!(m - h)!2^{h/2}} = \frac{m!}{(h/2)!(m - h)!}$$

and by arguing as in the proof of Lemma 4.1 we deduce that

$$|x^G \cap N| \leqslant \frac{m!}{(h/2)!(m - h)!}(q + 1)^{h/2}$$

(this is equality if $T = (C_{q+1})^m$). It is straightforward to verify the bound $\alpha(x) \leqslant (1 - t)/2$.

Now assume x is of type b_h or c_h, according to the parity of h. The case $h = 1$ requires special attention. Here $|x^G| = q^n - 1$ and x is $\bar{G}$-conjugate to $(z, 1, \ldots, 1) \in \bar{L}^m$, which implies that $|x^G \cap N| \leqslant m(q + 1)$ and we deduce that $\alpha(x) \leqslant (1 - t)/2$. Now assume $h \geqslant 2$, so $|x^G| > \frac{1}{2}q^{h(n-h+1)}$. Here there exists an integer j in the range $0 \leqslant j < h/2$ such that x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(z_1, \ldots, z_m)\sigma$, where $\sigma = (1, 2) \cdots (2j - 1, 2j) \in S_m$ and z_i is nontrivial (and equal to z) if and only if $2j + 1 \leqslant i \leqslant h$. As a consequence, we deduce that

$$|x^G \cap N| \leqslant \sum_{j=0}^{\lceil h/2 \rceil - 1} \frac{m!}{j!(m - 2j)!2^j}2^j(q + 1)^j \binom{m - 2j}{h - 2j}(q + 1)^{h-2j} \tag{19}$$

(once again, this is equality if $T = (C_{q+1})^m$) and thus

$$|x^G \cap N| \leqslant \frac{m!}{(m - h)!}(q + 1)^h f(h),$$

where

$$f(h) = \sum_{j=0}^{\lceil h/2 \rceil - 1} \frac{1}{j!(h - 2j)!3^j}.$$

One can check that $f(h)$ is a decreasing function, so $f(h) \leqslant f(2) = 1/2$ and we deduce that

$$|x^G \cap N| \leqslant \frac{m!}{(m - h)!2}(q + 1)^h. \tag{20}$$

By considering the bound in (20), we may assume $n \leqslant 20$ and $q = 2$. In each of these cases, one can check that the upper bound in (19) is sufficient unless $(n, q) = (10, 2)$ and $x = b_3$.

In the latter case, the more accurate bounds $|x^G| > 2^{24}$ and

$$|x^G \cap N| \leqslant \binom{5}{3} 3^3 + 2 \cdot \frac{5!}{3!2} 3^3 = 810$$

are sufficient.

Case 2. $r \neq p$, $r = 2$.

Now suppose x is a semisimple involution, so q is odd. First assume x lifts to an element of order 4 in $\mathrm{Sp}_n(q)$, in which case

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{2|\mathrm{GL}_m^\varepsilon(q)|} > \frac{1}{4} \left(\frac{q}{q+1} \right) q^{m(m+1)},$$

where $q \equiv \varepsilon \pmod 4$. Here the trivial bound

$$|x^G \cap N| \leqslant |N| \leqslant (q+1)^m |W|$$

is sufficient if $n \geqslant 18$ or $q \geqslant 81$, so we may assume $n \leqslant 16$ and $q \leqslant 79$. To handle these cases, we can work with the more accurate bound

$$|x^G \cap N| \leqslant i_2(N) \leqslant (q+1)^m (1 + i_2(W)),$$

where

$$1 + i_2(W) = \sum_{j=0}^{\lfloor m/2 \rfloor} \frac{m!}{j!(m-2j)!} 2^{m-2j}.$$

One can check that the given bounds on $|x^G \cap N|$ and $|x^G|$ are sufficient.

For the remainder, let us assume x lifts to an involution in $\mathrm{Sp}_n(q)$ of the form $(-I_{2\ell}, I_{n-2\ell})$ for some $1 \leqslant \ell \leqslant \lfloor m/2 \rfloor$. Then for some integer $0 \leqslant j \leqslant \ell$, x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(z_1, \ldots, z_m)\sigma$, where $\sigma = (1,2) \cdots (2j-1, 2j) \in S_m$ and z_i is nontrivial (and equal to $-I_2$) if and only if $2j+1 \leqslant i \leqslant \ell + j$. This implies that

$$|x^G \cap N| \leqslant \sum_{j=0}^{\ell} \frac{m!}{j!(m-2j)!2^j} 2^j (q+1)^j \binom{m-2j}{\ell-j},$$

which in turn yields

$$|x^G \cap N| \leqslant \frac{m!}{(m-2\ell)!} (q+1)^\ell \left(\sum_{j=0}^{\ell} \frac{1}{j!(\ell-j)!} \right) \leqslant \frac{m!}{(m-2\ell)!} 2(q+1)^\ell. \tag{21}$$

Now $|x^G| > \frac{1}{2a} q^{2\ell(n-2\ell)}$, where $a = 2$ if $\ell = m/2$, otherwise $a = 1$, and one can check that this bound with (21) is always sufficient.

Case 3. $r > 2$, $(r, |T|) = 1$.

Here x is $\bar{G}$-conjugate to an element of the form $(1, \ldots, 1)\sigma \in \bar{N}$, where $\sigma \in S_m$ has cycle-shape $(r^j, 1^{m-jr})$ for some integer j in the range $1 \leqslant j \leqslant \lfloor m/r \rfloor$. If $r = p$ then x has Jordan form (J_r^{2j}, J_1^{n-2jr}) on V, so

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{q^{j(2n-2j-2jr)}|\mathrm{Sp}_{2j}(q)||\mathrm{Sp}_{n-2jr}(q)|} > \frac{1}{2} q^{j(r-1)(2n-2jr+1)}$$

and by arguing as in the proof of Lemma 4.1 we deduce that

$$|x^G \cap N| \leqslant 2^{j(r-1)} \frac{m!}{j!(m-jr)!r^j} (q+1)^{j(r-1)}. \tag{22}$$

Similarly, if $r \neq p$ then x has Jordan form $(I_{n-2j(r-1)}, \omega I_{2j}, \ldots, \omega^{r-1} I_{2j})$ on the natural module for $\bar{G}$, so

$$|x^G| > \frac{1}{2} \left(\frac{q}{q+1} \right)^{(r-1)/2} q^{j(r-1)(2n-2jr+1)}$$

and (22) holds. In all cases, one can check that these bounds are sufficient.

Case 4. $r > 2$, r *divides* $|T|$.

To complete the proof, we may assume x is semisimple and r is an odd prime divisor of $|T|$. Let $0 \leqslant \ell \leqslant \lfloor m/r \rfloor$ be maximal such that x is $\bar{G}$-conjugate to an element in a coset $\bar{T}\pi$, where $\pi \in W$ is of the form $(1,\ldots,1)\sigma$ and $\sigma \in S_m$ has cycle-shape $(r^\ell, 1^{m-r\ell})$.

First assume $\ell = 0$, so $x^G \cap N \subseteq T$. Set $s = \nu(x)$ (see Definition 3.1). If $s = 2$ then x is $\bar{G}$-conjugate to an element of the form $(I_{n-2}, \omega, \omega^{-1})$, so $|x^G \cap N| \leqslant 2m$ and the bound $|x^G| > \frac{1}{2}(q+1)^{-1}q^{2n-1}$ is sufficient. Next assume $n = 6$ and $s \geqslant 3$. Here $|x^G| > \frac{1}{2}(q+1)^{-1}q^{13}$ and one can check that the bound $|x^G \cap N| \leqslant (q+1)^3$ is good enough (recall that we may assume $q \geqslant 7$; see (18)). Finally, if $n \geqslant 8$ and $s \geqslant 4$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{4n-15}$ and the trivial bound $|x^G \cap N| \leqslant (q+1)^m$ is sufficient.

Now suppose $\ell \geqslant 1$, so $r \leqslant m$ and each r-th root of unity has multiplicity at least 2ℓ as an eigenvalue of x on $\bar{V}$. Now $|x^G|$ is minimal when x is $\bar{G}$-conjugate to an element of the form $(I_{n-2\ell(r-1)}, \omega I_{2\ell}, \ldots, \omega^{r-1} I_{2\ell})$, which implies that

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{(r-1)/2} q^{\ell(r-1)(2n-2\ell r+1)}.$$

Next observe that there exists an integer j in the range $0 \leqslant j \leqslant \ell$ such that x is $\bar{G}$-conjugate to an element of the form $(z_1, \ldots, z_m)\rho \in \bar{N}$, where

$$\rho = (1, \ldots, r)(r+1, \ldots, 2r) \cdots ((j-1)r+1, \ldots, jr) \in S_m$$

has cycle-shape $(r^j, 1^{m-rj})$ and $z_i = \mathrm{diag}(\lambda_i, \lambda_i^{-1})$ is nontrivial (of order r) only if $i > jr$. Since there are at most r possibilities for each z_i with $i > jr$, we deduce that

$$|x^G \cap N| \leqslant \sum_{j=0}^{\ell} 2^{j(r-1)} \frac{m!}{j!(m-jr)!r^j}(q+1)^{j(r-1)}r^{m-jr}, \qquad (23)$$

which in turn implies that

$$|x^G \cap N| \leqslant (2(q+1))^{\ell(r-1)}r^m \sum_{j=0}^{\ell}\left(\frac{m^r}{r}\right)^j \leqslant 2\left(\frac{m^r}{r}\right)^{\ell}(2(q+1))^{\ell(r-1)}r^m. \qquad (24)$$

Suppose $q \geqslant 3$. Here one checks that the upper bound on $|x^G \cap N|$ in (24) is sufficient if $n \geqslant 18$ or $q \geqslant 23$, so we may assume $n \leqslant 16$ and $q \leqslant 19$. In the remaining cases, we find that the more accurate upper bound in (23) is sufficient. Similarly, if $q = 2$ then the bound in (24) is good enough for $n \geqslant 40$ and we see that (23) is sufficient if $12 \leqslant n \leqslant 38$. Finally, suppose $(n, q) = (10, 2)$. Here (24) is sufficient unless $(r, \ell) = (3, 1)$, which means that x is of the form $(I_6, \omega I_2, \omega^2 I_2)$ or $(I_4, \omega I_3, \omega^2 I_3)$. In the latter case, $|x^G| > 2^{35}$ and the bound in (24) is good enough. On the other hand, if $x = (I_6, \omega I_2, \omega^2 I_2)$ then $|x^G| > 2^{29}$ and the result follows since

$$|x^G \cap N| \leqslant \binom{5}{2}2^2 + 2^2 \cdot \frac{5!}{2!3}3^2 = 760.$$

$\square$

The following result completes the proof of Theorem 1 for symplectic groups.

Proposition 4.4. *The conclusion to Theorem 1 holds if* $G = \mathrm{PSp}_4(q)'$.

Proof. Set $\widehat{G} = \mathrm{Sp}_4(q)$ and $Z = Z(\widehat{G})$, so we may write $G = \widehat{G}/Z$, $T = \widehat{T}/Z$ and $N = \widehat{N}/Z$, where $\widehat{N} = N_{\widehat{G}}(\bar{T})$. The Weyl group $W = S_2 \wr S_2 = D_8$ has 5 conjugacy classes and up to conjugacy we see that $\widehat{T}$ is one of the following:

$$(C_{q-\varepsilon})^2, \ C_{q+1} \times C_{q-1}, \ C_{q^2-\varepsilon}$$

with $\varepsilon = \pm$ and thus $N = [(q-\varepsilon)^2/d].D_8$, $[(q^2-1)/d].2^2$ or $[(q^2+1)/d].4$, where $d = (2, q-1)$. The groups with $q \leqslant 8$ can be handled using MAGMA, so we will assume $q \geqslant 9$.

We claim that $\widehat{\mathcal{Q}}(G, N, 2) < 1$ and thus $b(G, N) = 2$. Let $x \in N$ be an element of prime order r. If $\dim x^{\bar{G}} \geqslant 6$ then we have the trivial bound $|x^G \cap N| \leqslant |N| \leqslant 8(q+1)^2/d = a_1$ and $|x^G| \geqslant b_1$, where

$$b_1 = \begin{cases} \frac{1}{2}q(q-1)(q^4-1) & q \text{ odd} \\ q^3(q-1)(q^2+1) & q \text{ even.} \end{cases}$$

Therefore, the contribution to $\widehat{\mathcal{Q}}(G, N, 2)$ from these elements is less than $a_1^2/b_1 < 2/3$. For the remainder, we may assume $\dim x^{\bar{G}} = 4$, so x is an involution and either q is odd and $x = (-I_2, I_2)$, or q is even and x is a long or short root element.

First assume q is odd, so

$$|x^G| = \frac{|\mathrm{Sp}_4(q)|}{2|\mathrm{Sp}_2(q)|^2} = \frac{1}{2}q^2(q^2+1) = b_2$$

and $|x^G \cap N| = (i_2(\widehat{N}) - 1)/2$. We claim that $i_2(\widehat{N}) \leqslant 2q+5$ and thus $|x^G \cap N| \leqslant q+2 = a_2$. To see this, first assume $\widehat{T} = (C_{q-\varepsilon})^2$ and note that $\widehat{N} = Q_{2(q-\varepsilon)} \wr S_2 < \mathrm{Sp}_2(q) \wr S_2$, where $Q_{2(q-\varepsilon)}$ is the generalised quaternion group of order $2(q-\varepsilon)$. Here $i_2(\widehat{N}) = 3 + 2(q-\varepsilon) \leqslant 2q+5$ as required. Similarly, if $\widehat{T} = C_{q+1} \times C_{q-1}$ then $\widehat{N} = Q_{2(q+1)} \times Q_{2(q-1)}$ and $i_2(\widehat{N}) = 3$.

Finally, suppose $\widehat{T} = C_{q^2-\varepsilon}$, so $\widehat{T} < \mathrm{Sp}_2(q^2)$ and $\widehat{N} = N_{\mathrm{Sp}_2(q^2)}(\widehat{T}).\langle\phi\rangle = Q_{2(q^2-\varepsilon)}.\langle\phi\rangle$, where ϕ is an involutory field automorphism of $\mathrm{Sp}_2(q^2)$. Since $Q_{2(q^2-\varepsilon)}$ has a unique involution, it remains to show that there are at most $2q+4$ involutions in the coset $Q_{2(q^2-\varepsilon)}\phi$. First assume $\varepsilon = +$ and write $\mathbb{F}_{q^2}^\times = \langle\lambda\rangle$. Then by taking $\widehat{T}$ to be the diagonal matrices in $\mathrm{Sp}_2(q^2)$ we get

$$\widehat{N} = \left\langle \mathrm{diag}(\lambda, \lambda^{-1}), \tau, \phi \right\rangle, \ \text{with } \tau = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{Sp}_2(q^2)$$

and it is straightforward to show that $i_2(\widehat{N}) = 2q+1$. On the other hand, if $\varepsilon = -$ then $\widehat{N} = C_{q^2+1}.4$ and every involution in $\widehat{N}$ is contained in $C_{q^2+1}.2 = Q_{2(q^2+1)}$. Therefore $i_2(\widehat{N}) = 1$ and thus $|x^G \cap N| = 0$.

This justifies the claim and we conclude that

$$\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1 + a_2^2/b_2 < 1$$

if $q \geqslant 9$ is odd.

Finally, let us assume $q \geqslant 16$ is even and x is a long or short root element, so $|x^G| = q^4 - 1 = b_3$. We claim that $|x^G \cap N| \leqslant 2q+2 = a_3$. In order to establish the claim, let us first assume $T = (C_{q-\varepsilon})^2$, so $N = D_{2(q-\varepsilon)} \wr S_2$. The long root elements in N correspond to the involutions in each $D_{2(q-\varepsilon)}$ factor, so $|x^G \cap N| = 2(q - \varepsilon)$. Similarly, the short root elements in N are the involutions outside $(D_{2(q-\varepsilon)})^2$, so once again $|x^G \cap N| = 2(q - \varepsilon)$. Next suppose $T = C_{q+1} \times C_{q-1}$. Here $N = D_{2(q+1)} \times D_{2(q-1)}$ and the long root elements correspond to the involutions in each factor, so $|x^G \cap N| = 2q$, and we note that N does contain any short root elements. Finally, suppose $T = C_{q^2-\varepsilon}$, in which case $N = D_{2(q^2-\varepsilon)}.2$ with $D_{2(q^2-\varepsilon)} < \mathrm{Sp}_2(q^2)$ and we note that N does not contain any long root elements. If $\varepsilon = -$ then $N = C_{q^2+1}.4$ and every involution in N is contained in $D_{2(q^2+1)}$, so N does not contain any root elements at all in this case. On the other hand, if $\varepsilon = +$ then

$$N = \left\langle \mathrm{diag}(\lambda, \lambda^{-1}), \tau, \phi \right\rangle, \ \text{with } \tau = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{Sp}_2(q^2),$$

where ϕ is an involutory field automorphism of $\mathrm{Sp}_2(q^2)$. It is straightforward to check that the coset $D_{2(q^2-1)}\phi$ contains $q + 1$ involutions.

For $q \geqslant 16$ even, we conclude that

$$\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1 + 2a_3^2/b_3 < 1$$

and this completes the proof of the proposition. $\qquad\square$

5. Odd dimensional orthogonal groups

In order to complete the proof of Theorem 1 for classical groups, we may assume G is an orthogonal group. In this section we assume $G = \Omega_n(q)$, where $n \geqslant 7$ is odd; the even dimensional orthogonal groups will be handled in Section 6.

Write $n = 2m + 1$ and note that q is odd. Fix an F-stable maximal torus $\bar{T}$ of $\bar{G}$ and set $\bar{N} = N_{\bar{G}}(\bar{T}) = \bar{T}.W$, where $W = S_2 \wr S_m$ is the hyperoctahedral group. We may assume $\bar{T}$ is the group of diagonal matrices in $\bar{G} = \mathrm{SO}_n(k)$ of the form

$$\mathrm{diag}(\lambda_1, \lambda_1^{-1}, \ldots, \lambda_m, \lambda_m^{-1}, 1)$$

with respect to a standard orthogonal basis $\{e_1, f_1, \ldots, e_m, f_m, v\}$ of the natural module $\bar{V}$. Note that $\bar{N}$ stabilises the orthogonal decomposition $\bar{V} = \bar{V}_1 \perp \cdots \perp \bar{V}_m \perp \langle v \rangle$, where $\bar{V}_i = \langle e_i, f_i \rangle$. More precisely, if we set

$$\bar{L} = \left\langle \mathrm{diag}(\lambda, \lambda^{-1}), z \, : \, \lambda \in k^\times \right\rangle = \mathrm{O}_2(k),$$

where $z = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$, then

$$\bar{N} = \left\{ \mathrm{diag}(A, 1), \mathrm{diag}(B, -1) \, : \, A, B \in \bar{L} \wr S_m, \det(A) = 1, \det(B) = -1 \right\}.$$

We will use the notation $(z_1, \ldots, z_m, y)\sigma$ to denote a general element of $\bar{N}$, where $z_i \in \bar{L}$, $y = \prod_i \det(z_i) \in \{-1, 1\}$ and $\sigma \in S_m$.

Recall from Section 2.2 that there is a bijection from the set of conjugacy classes in W to the set of $\bar{G}^F$-classes of F-stable maximal tori in $\bar{G}$. As recorded in the previous section, the conjugacy classes in W are parameterised by pairs of partitions (λ, μ) with $|\lambda| + |\mu| = m$. Fix an element $w \in W$ corresponding to the pair (λ, μ), where $\lambda = (m^{a_m}, \ldots, 1^{a_1})$ and $\mu = (m^{b_m}, \ldots, 1^{b_1})$. Then the W-class of w corresponds to an F-stable maximal torus $\bar{T}_w$ of $\bar{G}$ and we set $N = N_G(\bar{T}_w) = T.R$, where $R \cong C_W(w)$ and $T = \hat{T} \cap G$ with

$$\hat{T} = (C_{q^m-1})^{a_m} \times \cdots \times (C_{q-1})^{a_1} \times (C_{q^m+1})^{b_m} \times \cdots \times (C_{q+1})^{b_1} < \mathrm{SO}_n(q).$$

We refer the reader to [14, Theorem 4] for the cyclic structure of T.

Lemma 5.1. Let $G = \Omega_n(q)$, where $n \geqslant 7$ is odd.

(i) If $n \leqslant 11$ and $q \leqslant 13$ then $\eta_G(t) < 1$, where t is defined as follows:

	$q = 3$	5	7	9	11	13
$n = 7$	23/100	17/100	7/50	7/50	13/100	13/100
9	17/100	13/100	11/100	1/10	11/100	11/100
11	13/100	1/10	9/100	2/25	2/25	2/25

(ii) If $13 \leqslant n \leqslant 21$ and $q = 3$ then $\eta_G(t) < 1$ for $t = 11/100$.

Proof. This is an entirely straightforward MAGMA calculation, working with the standard matrix representation of G over $\mathbb{F}_q$ and the function `ClassicalClasses` to compute the relevant conjugacy class sizes. $\qquad\square$

Theorem 5.2. If $G = \Omega_n(q)$ with $n \geqslant 7$, then $b(G, N) = 2$.

Proof. The cases $(n, q) \in \{(7, 3), (9, 3)\}$ can be handled using MAGMA (see Lemma 2.9), so we may (and will) assume $(n, q) \neq (7, 3), (9, 3)$ for the remainder. Set $t = 1/3$, with the exception of the cases in Lemma 5.1, where we define t as in the lemma. Let $x \in N$ be an element of prime order r. As before, our aim is to show that $\alpha(x) \leqslant (1 - t)/2$. We will adopt the notation introduced at the start of Section 5.

Case 1. $r = 2$.

Here x is of the form $(-I_{2\ell}, I_{n-2\ell})$ with $1 \leqslant \ell \leqslant m$, whence

$$|x^G| > \frac{1}{4} q^{2\ell(n-2\ell)}. \tag{25}$$

The cases $\ell \in \{1, m - 1, m\}$ require special attention. Set $z = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) \in \mathrm{O}_2(k)$.

First assume $\ell = m$. Here x is $\bar{G}$-conjugate to elements in $\bar{N}$ of the form $(-I_2, \ldots, -I_2, 1)$ and $(z, -I_2, \ldots, -I_2, -1)$, which implies that $|x^G \cap N| \leqslant m(q+1) + 1$. One can now check that the bound on $|x^G|$ in (25) is sufficient.

Next assume $\ell = 1$. In this case, x is $\bar{G}$-conjugate to the following elements in $\bar{N}$:

$$(-I_2, I_2, \ldots, I_2, 1), \; (z, I_2, \ldots, I_2, -1), \; (z, z, I_2, \ldots, I_2, 1), \; (I_2, \ldots, I_2, 1)\sigma,$$

where $\sigma = (1, 2) \in S_m$. This implies that

$$|x^G \cap N| \leqslant m + m(q+1) + \binom{m}{2}(q+1)^2 + 2\binom{m}{2}(q+1)$$

and once again the bound in (25) is good enough. Similarly, if $\ell = m-1$ then x is $\bar{G}$-conjugate to the following:

$$(I_2, -I_2, \ldots, -I_2, 1), \; (z, I_2, -I_2, \ldots, -I_2, -1), \; (z, z, -I_2, \ldots, -I_2, 1),$$

$$(z, z, z, -I_2, \ldots, -I_2, -1), \; (I_2, I_2, -I_2, \ldots, -I_2, 1)\sigma, \; (I_2, I_2, z, -I_2, \ldots, -I_2, -1)\sigma$$

where $\sigma = (1, 2) \in S_m$. Therefore,

$$|x^G \cap N| \leqslant m + 2\binom{m}{2}(q+1) + \binom{m}{2}(q+1)^2 + \binom{m}{3}(q+1)^3$$
$$+ 2\binom{m}{2}(q+1) + 2\binom{m}{2}(m-2)(q+1)^2$$

and it is routine to check that (25) is sufficient.

To complete the analysis of involutions, we may assume $n \geqslant 9$ and $2 \leqslant \ell \leqslant m - 2$. First observe that the combined contribution to $|x^G \cap N|$ from elements in cosets of the form Ty with $y \in (S_2)^m < W$ is at most $(2(q+1))^m$. Similarly, the contribution from elements in cosets Ty such that $y \in (S_2)^m\sigma$ and $\sigma \in S_m$ has cycle-shape $(2^j, 1^{m-2j})$ with $1 \leqslant j \leqslant \min\{\ell, (n - 2\ell - 1)/2\}$ is at most

$$\frac{m!}{j!(m-2j)!2^j}(2(q+1))^j \cdot (2(q+1))^{m-2j}.$$

Therefore, if we set $a = \min\{\ell, (n - 2\ell - 1)/2\}$, then

$$|x^G \cap N| \leqslant 2^m(q+1)^m \sum_{j=0}^{a} \frac{m!}{j!(m-2j)!2^j}. \tag{26}$$

Now

$$\sum_{j=0}^{a} \frac{m!}{j!(m-2j)!2^j} \leqslant \sum_{j=0}^{a} \left(\frac{m^2}{2}\right)^j < 2\left(\frac{m^2}{2}\right)^a$$

and this implies that

$$|x^G \cap N| \leqslant 2^{m+1}(q+1)^m \left(\frac{m^2}{2}\right)^a. \tag{27}$$

One can now check that the bounds in (27) and (25) are sufficient if $n \geqslant 39$ or $q \geqslant 23$. And if $n \leqslant 37$ and $q \leqslant 19$, then the bounds in (26) and (25) are good enough.

Case 2. $r > 2$, $(r, |T|) = 1$.

First assume $r = p$. Here x is $\bar{G}$-conjugate to an element of the form $(1, \ldots, 1)\sigma \in \bar{N}$, where $\sigma = (1, \ldots, 1)\rho \in W$ and $\rho \in S_m$ has cycle-shape $(r^j, 1^{m-jr})$ for some $1 \leqslant j \leqslant \lfloor m/r \rfloor$. Then x has Jordan form (J_r^{2j}, J_1^{n-2jr}) on V and we deduce that

$$|x^G \cap N| \leqslant \frac{m!}{j!(m-jr)!r^j}(2(q+1))^{j(r-1)}. \tag{28}$$

In addition, we have

$$|x^G| > \frac{1}{8}q^{j(r-1)(2n-2jr-1)}$$

and one can check that these bounds yield $\alpha(x) \leqslant (1 - t)/2$.

Similarly, if $r \neq p$ then x is $\bar{G}$-conjugate to $(I_{n-2j(r-1)}, \omega I_{2j}, \ldots, \omega^{r-1} I_{2j})$ for some integer j in the range $1 \leqslant j \leqslant \lfloor m/r \rfloor$, so

$$|x^G| > \frac{1}{2} \left(\frac{q}{q+1} \right)^{(r-1)/2} q^{j(r-1)(2n-2jr-1)}$$

and the upper bound on $|x^G \cap N|$ in (28) is satisfied. Once again, it is straightforward to show that these bounds are sufficient.

Case 3. $r > 2$, r divides $|T|$.

Here we proceed as in Case 4 in the proof of Theorem 4.3. Let $0 \leqslant \ell \leqslant \lfloor m/r \rfloor$ be maximal such that x is $\bar{G}$-conjugate to an element in a coset $\bar{T}\pi$, where $\pi = (1, \ldots, 1)\sigma \in W$ and $\sigma \in S_m$ has cycle-shape $(r^\ell, 1^{m-r\ell})$. Set $s = \nu(x)$.

Suppose $\ell = 0$, so $x^G \cap N \subseteq T$. If $s = 2$ then $x = (I_{n-2}, \omega, \omega^{-1})$ up to $\bar{G}$-conjugacy and one can check that the bounds $|x^G \cap N| \leqslant 2m$ and $|x^G| > \frac{1}{2}(q+1)^{-1} q^{2n-3}$ are sufficient. Now assume $s \geqslant 4$. If $n = 7$ then $|x^G| > \frac{1}{2}(q+1)^{-1} q^{13}$ (minimal if $x = (I_1, \omega I_3, \omega^{-1} I_3)$) and the trivial bound $|x^G \cap N| \leqslant (q+1)^3$ yields $\alpha(x) \leqslant 1/3$. For $n \geqslant 9$ we have $|x^G| > \frac{1}{2}(q+1)^{-1} q^{4n-13}$ and once again the bound $|x^G \cap N| \leqslant (q+1)^m$ is good enough.

Finally, suppose $\ell \geqslant 1$. Here $r \leqslant m$ and each r-th root of unity has multiplicity at least 2ℓ as an eigenvalue of x on $\bar{V}$ (in particular, the 1-eigenspace of x is at least 3-dimensional). Since $|x^G|$ is minimal when $x = (I_{n-2\ell(r-1)}, \omega I_{2\ell}, \ldots, \omega^{r-1} I_{2\ell})$, it follows that

$$|x^G| > \frac{1}{2} \left(\frac{q}{q+1} \right)^{(r-1)/2} q^{\ell(r-1)(2n-2\ell r-1)}$$

and the upper bounds on $|x^G \cap N|$ in (23) and (24) are satisfied. One can check that the bound in (24) is sufficient if $n \geqslant 13$ or $q \geqslant 23$; in each of the remaining cases, we can evaluate the bound in (23) and the result follows. $\square$

6. EVEN DIMENSIONAL ORTHOGONAL GROUPS

Here we complete the proof of Theorem 1 for classical groups by handling the even dimensional orthogonal groups $G = \mathrm{P\Omega}_n^\varepsilon(q)$, where $n = 2m \geqslant 8$ and $\varepsilon = \pm$.

Write $\bar{N} = \bar{T}.W$, where $\bar{T}$ is the image (modulo scalars) of the diagonal matrices in $\mathrm{SO}_n(k)$ of the form $\mathrm{diag}(\lambda_1, \lambda_1^{-1}, \ldots, \lambda_m, \lambda_m^{-1})$ with respect to a standard basis $\{e_1, f_1, \ldots, e_m, f_m\}$ for the natural module $\bar{V}$. Set

$$\bar{L} = \langle \mathrm{diag}(\lambda, \lambda^{-1}), z \, : \, \lambda \in k^\times \rangle = \mathrm{O}_2(k),$$

where $z = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$. Then $\bar{N}$ is the image in $\bar{G}$ of the subgroup

$$\langle \bar{T}, (z, z, 1, \ldots, 1), S_m \rangle < \bar{L} \wr S_m$$

and thus $W = 2^{m-1}{:}S_m$ is an index-two subgroup of $S_2 \wr S_m$. We will use the notation $(z_1, \ldots, z_m)\sigma$ to denote a general element of $\bar{N}$, where $z_i \in \bar{L}$ and $\sigma \in S_m$. Without loss of generality, we may assume $\bar{T}$ is F-stable.

Recall that there is a bijection from the set of F-classes in W to the set of $\bar{G}^F$-classes of F-stable maximal tori in $\bar{G}$. First assume $\varepsilon = +$. Here the F-classes in W coincide with the usual conjugacy classes in W, which can be parameterised by pairs of partitions (λ, μ), where $|\lambda| + |\mu| = m$ and the number of parts in μ is even, with the additional condition that if every part of λ is even and μ is the empty partition, then there are two W-classes corresponding to (λ, μ). Similarly, if $\varepsilon = -$ and $m \geqslant 5$ is odd, then the F-classes in W are in bijection with the usual classes and they have essentially the same parameterisation, the only difference being that each partition μ in the pair (λ, μ) should have an odd number of parts (in particular, μ is non-empty). On the other hand, if $\varepsilon = -$ and $m \geqslant 4$ is even, then there is a distinction to be made between the F-classes in W and the usual conjugacy classes

λ	μ	T	$C_{W_0}(w)$	$|R|$	$|N|$
(3)	(1)	C_{21}	$C_6 \times C_2$	6	126
$(2,1)$	(1)	$(C_3)^2$	$(C_2)^4$	8	72
(1^3)	(1)	C_3	$(C_2 \wr S_3) \times C_2$	48	144
(2)	(2)	C_{15}	$C_4 \times (C_2)^2$	8	120
(1^2)	(2)	C_5	$D_8 \times C_4$	16	80
(1)	(3)	C_9	$C_6 \times C_2$	6	54
(1)	(1^3)	$(C_3)^3$	$(C_2 \wr S_3) \times C_2$	48	1296
$\emptyset$	(4)	C_{17}	C_8	4	68
$\emptyset$	$(2,1^2)$	$C_{15} \times C_3$	$D_8 \times C_4$	16	720

TABLE 2. The case $G = \Omega_8^-(2)$

(see Remark 6.1 for more details). But in any case, the F-classes are still parameterised by pairs of partitions (λ, μ) as above, where μ has an odd number of parts (for example, if $m = 4$ then W has 13 conjugacy classes, but we find that there are only 9 distinct F-classes when $\varepsilon = -$).

So in all cases we may associate the F-class of $w \in W$ with a pair of partitions (λ, μ) as described above, according to the type of F. Write

$$\lambda = (m^{a_m}, \ldots, 1^{a_1}), \, \mu = (m^{b_m}, \ldots, 1^{b_1}) \tag{29}$$

and let $\bar{T}_w$ be the corresponding F-stable maximal torus of $\bar{G}$. We can then define $N = N_G(\bar{T}_w) = T.R$, where $R = C_{W,F}(w)$ (see (5)) and T is the image (modulo scalars) of $\widehat{T} \cap \Omega_n^\varepsilon(q)$, where

$$\widehat{T} = (C_{q^m-1})^{a_m} \times \cdots \times (C_{q-1})^{a_1} \times (C_{q^m+1})^{b_m} \times \cdots \times (C_{q+1})^{b_1}$$

is a maximal torus of $\mathrm{SO}_n^\varepsilon(q)$. Note that $C_{W,F}(w) \cong C_W(w)$ if $\varepsilon = +$, or if $\varepsilon = -$ and $m \geqslant 5$ is odd. See [14, Theorems 5-7] for the precise cyclic structure of T.

Remark 6.1. Suppose $G = \mathrm{P}\Omega_{2m}^-(q)$ with $m \geqslant 4$ even and set $N = T.R$ as above with respect to the pair of partitions (λ, μ) in (29). Let $w \in W$ be a representative of the corresponding F-class in W. We can identify the F-centraliser $R = C_{W,F}(w)$ with an index-two subgroup of $C_{W_0}(w)$, where we view W as an index-two subgroup of the Weyl group $W_0 = S_2 \wr S_m$ of $\mathrm{SO}_{2m+1}(k)$. Now $C_{W_0}(w) = A \times B$, where

$$A = ((C_2 \times C_m) \wr S_{a_m}) \times ((C_2 \times C_{m-1}) \wr S_{a_{m-1}}) \times \cdots \times (C_2 \wr S_{a_1})$$
$$B = (C_{2m} \wr S_{b_m}) \times (C_{2(m-1)} \wr S_{b_{m-1}}) \times \cdots \times (C_2 \wr S_{b_1})$$

and so it is straightforward to compute $|R|$. For example, if $G = \Omega_8^-(2)$ then each F-class in W corresponds to one of the pairs (λ, μ) in Table 2. In the table, we also describe the structure of T (see [14, Theorem 7]) and $C_{W_0}(w)$, and we compute $|N|$.

Lemma 6.2. Let $G = \mathrm{P}\Omega_n^\varepsilon(q)$, where $n \geqslant 8$ is even.

(i) If $n = 8$ and $q \leqslant 16$ then $\eta_G(t) < 1$, where t is defined as follows:

q	2	3	4	5	7	8	9	11	13	16
t	7/25	11/50	9/50	4/25	7/50	13/100	13/100	7/50	7/50	3/20

(ii) *If (n, q) is one of the following, then $\eta_G(t) < 1$ where t is defined as in the table:*

	$n = 10$	12	14	16	18	20
$q = 2$	9/50	7/50	11/100	1/10	2/25	7/100
3	13/100	11/100	9/100	2/25	7/100	3/50
4	3/25	9/100				
5	11/100	9/100				
7	1/10	7/100				

Proof. This is very similar to the proof of Lemma 4.2. With the aid of MAGMA, we work with the standard matrix representation of $L = \Omega_n^\varepsilon(q)$ and we use the function `ClassicalClasses` to compute the relevant class lengths in L. In this way, with an appropriate adjustment for involutions when q is odd and $Z(L)$ is nontrivial, we obtain the list of class sizes of elements of prime order in G. Note that the sizes of the classes of involutions in G can be read off from [8, Tables B.10, B.11] when q is odd. $\square$

Theorem 6.3. *Suppose $G = \mathrm{P}\Omega_n^\varepsilon(q)$ and $n \geqslant 8$ is even. Then $b(G, N) \leqslant 3$, with equality if and only if $G = \Omega_8^+(2)$ and $N = 3^4{:}(2^3{:}S_4)$, in which case $|N \cap N^x| = 4$ for some $x \in G$.*

Proof. In view of Lemma 2.9 we may assume $(n, q) \notin \{(8, 2), (8, 3), (10, 2)\}$. Let $x \in N$ be an element of prime order r. As before, we seek to establish the bound $\alpha(x) \leqslant (1 - t)/2$, where either $t = 1/3$, or G is one of the groups in Lemma 6.2 and we define t as in the lemma. There are several cases to consider.

Case 1. $r = p = 2$.

Here x has Jordan form (J_2^h, J_1^{n-2h}) on V for some even integer $h = 2\ell \geqslant 2$, whence x is of type a_h or c_h with respect to the notation in [1]. Note that every involution in $\bar{L}^m \cap \bar{G}$ is of type c.

If $x = a_h$ then x is $\bar{G}$-conjugate to $(1, \ldots, 1)\sigma \in \bar{N}$ with $\sigma = (1, 2) \cdots (h - 1, h) \in S_m$, so

$$|x^G \cap N| \leqslant 2^\ell \frac{m!}{\ell!(m - 2\ell)!2^\ell}(q + 1)^\ell$$

and it is straightforward to check that the bound $|x^G| > \frac{1}{2}q^{h(n-h-1)}$ is sufficient.

Now suppose $x = c_h$. If $h = 2$ then $|x^G| > \frac{1}{2}q^{2(n-2)}$ and we observe that x is $\bar{G}$-conjugate to $(z, z, 1, \ldots, 1) \in \bar{N}$, which implies that $|x^G \cap N| \leqslant \binom{m}{2}(q + 1)^2$. These bounds are sufficient. Now assume $h \geqslant 4$. Here there exists an integer j in the range $0 \leqslant j < h/2$ such that x is $\bar{G}$-conjugate to an element in $\bar{N}$ of the form $(z_1, \ldots, z_m)\sigma$, where $\sigma = (1, 2) \cdots (2j - 1, 2j) \in S_m$ and z_i is nontrivial (and equal to z) if and only if $2j + 1 \leqslant i \leqslant h$. Therefore,

$$|x^G \cap N| \leqslant \sum_{j=0}^{h/2-1} 2^j \frac{m!}{j!(m - 2j)!2^j}(q + 1)^j \binom{m - 2j}{h - 2j}(q + 1)^{h-2j} \tag{30}$$

and we deduce that

$$|x^G \cap N| \leqslant \frac{m!}{(m - h)!}(q + 1)^h \sum_{j=0}^{h/2-1} \frac{1}{j!(h - 2j)!3^j} \leqslant \frac{m!}{(m - h)!4}(q + 1)^h. \tag{31}$$

Since $|x^G| > \frac{1}{2}q^{h(n-h)}$, one can check that the bound in (31) is sufficient unless $(n, q) = (12, 2)$. In this case, we can evaluate the bound in (30) and the result follows.

Case 2. $r = 2$, $p \neq 2$.

Now assume $x \in N$ is a semisimple involution. We begin by considering the special case where x lifts to an element of order 4 in $\Omega_n^\varepsilon(q)$ (that is, $x = Z\hat{x}$ where $Z = Z(\Omega_n^\varepsilon(q))$, $\hat{x} \in \Omega_n^\varepsilon(q)$ and $\hat{x}^2 = -I_n$). Here

$$|x^G| > \frac{1}{4}\left(\frac{q}{q + 1}\right)q^{n(n-2)/4}$$

and one can check that the trivial bound $|x^G \cap N| \leqslant |N| \leqslant (q+1)^m |W|$ is sufficient unless $n \in \{8, 10\}$, or $n \in \{12, 14, 16\}$ and $q \leqslant 13$. To handle the remaining cases, we can work with the more accurate estimate

$$|x^G \cap N| \leqslant \sum_{j=0}^{\lfloor m/2 \rfloor} 2^j (q+1)^j \cdot 2^{m-2j} \frac{m!}{j!(m-2j)!2^j},$$

which is obtained by carefully considering the relevant elements of order 4 in the normaliser of a maximal torus of $\mathrm{SO}_n(k)$. Indeed, working modulo scalars, we observe that x is $\bar{G}$-conjugate to an element of the form $(z_1, \ldots, z_m)\pi \in \bar{N}$, where $\pi = (y_1, \ldots, y_m)\sigma \in W$, $\sigma = (1, 2) \cdots (2j-1, 2j) \in S_m$ for some $0 \leqslant j \leqslant \lfloor m/2 \rfloor$, $z_i = \mathrm{diag}(\lambda_i, \lambda_i^{-1})$ has order 4 for all i, $y_i = 1$ if $i > 2j$ and $y_{2\ell-1} = y_{2\ell} \in \{1, z\}$ if $1 \leqslant \ell \leqslant j$. By combining this with the above lower bound on $|x^G|$, we deduce that $\alpha(x) \leqslant (1-t)/2$ as required.

To complete the analysis of involutions, we may assume x is $\bar{G}$-conjugate to an element of the form $(-I_{2\ell}, I_{n-2\ell})$, where $1 \leqslant \ell \leqslant \lfloor m/2 \rfloor$. First observe that

$$|x^G| > \frac{1}{4d} \left(\frac{q}{q+1} \right) q^{2\ell(n-2\ell)}, \tag{32}$$

where $d = 2$ if $\ell = m/2$, otherwise $d = 1$. The cases with $\ell \in \{1, 2\}$ require special attention.

Suppose $\ell = 1$. Then x is $\bar{G}$-conjugate to the following elements in $\bar{N}$:

$$(-I_2, I_2, \ldots, I_2), \ (z, z, I_2, \ldots, I_2), \ (I_2, \ldots, I_2)\sigma,$$

where $\sigma = (1, 2) \in S_m$. This implies that

$$|x^G \cap N| \leqslant m + \binom{m}{2}(q+1)^2 + \binom{m}{2}2(q+1)$$

and one can check that the bound in (32) is sufficient.

Now assume $\ell = 2$. Here x is $\bar{G}$-conjugate to the following elements in $\bar{N}$:

$$(-I_2, -I_2, I_2, \ldots, I_2), \ (-I_2, z, z, I_2, \ldots, I_2), \ (z, z, z, z, I_2, \ldots, I_2),$$

$$(I_2, I_2, -I_2, I_2, \ldots, I_2)\sigma, \ (I_2, I_2, z, z, I_2, \ldots, I_2)\sigma, \ (I_2, \ldots, I_2)\rho,$$

where $\sigma = (1, 2) \in S_m$ and $\rho = (1, 2)(3, 4) \in S_m$. As a consequence, we deduce that

$$|x^G \cap N| \leqslant \binom{m}{2} + m\binom{m-1}{2}(q+1)^2 + \binom{m}{4}(q+1)^4 + \binom{m}{2}2(q+1)(m-2)$$

$$+ \binom{m}{2}2(q+1)\binom{m-2}{2}(q+1)^2 + \frac{m!}{2!(m-4)!2^2}(2(q+1))^2$$

and once again the result follows via the bound in (32).

Finally, let us assume $3 \leqslant \ell \leqslant \lfloor m/2 \rfloor$ and note that $m \geqslant 6$. Here we can repeat the argument in the final paragraph of Case 1 in the proof of Theorem 5.2 to show that (26) and (27) hold (with $a = \ell$). It is straightforward to check that (27) is sufficient if $n \geqslant 24$ or $q \geqslant 13$, so we may assume $12 \leqslant n \leqslant 22$ and $q \leqslant 11$. In these cases, we can evaluate the upper bound on $|x^G \cap N|$ in (26), which is sufficient unless $(n, q) = (12, 3)$. In the latter case, one can check that the trivial upper bound $|x^G \cap N| \leqslant (q+1)^m(1 + i_2(W))$ is good enough.

Case 3. $r > 2$.

If r does not divide $|T|$ then we can proceed as in Case 2 in the proof of Theorem 5.2; the argument goes through essentially unchanged and we omit the details.

Finally, let us assume r is an odd prime divisor of $|T|$. Here the analysis is similar to Case 3 in the proof of Theorem 5.2, but one or two cases require special attention and so we give the details.

Let $0 \leqslant \ell \leqslant \lfloor m/r \rfloor$ be maximal such that x is $\bar{G}$-conjugate to an element in a coset $\bar{T}\pi$, where $\pi = (1, \ldots, 1)\sigma \in W$ and $\sigma \in S_m$ has cycle-shape $(r^\ell, 1^{m-r\ell})$. Write $s = \nu(x)$.

First assume $\ell = 0$, so $x^G \cap N \subseteq T$. If $s = 2$ then x is $\bar{G}$-conjugate to $(I_{n-2}, \omega, \omega^{-1})$ and the bounds $|x^G \cap N| \leqslant 2m$ and $|x^G| > \frac{1}{2}(q+1)^{-1}q^{2n-3}$ are sufficient. Now assume $s \geqslant 4$. If $n \geqslant 10$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{4n-15}$ and the trivial bound $|x^G \cap N| \leqslant (q+1)^m$ is good enough. If $n = 8$ and x is not of the form $(\omega I_4, \omega^{-1}I_4)$, then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{19}$ and the result follows since $|x^G \cap N| \leqslant (q+1)^4$. On other hand, if $n = 8$ and x is conjugate to $(\omega I_4, \omega^{-1}I_4)$, then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{13}$ and we note that $|x^G \cap N| \leqslant 2^4$, which yields $\alpha(x) \leqslant (1-t)/2$ as required.

For the remainder, let us assume $\ell \geqslant 1$, so $r \leqslant m$ and each r-th root of unity has multiplicity at least 2ℓ as an eigenvalue of x on $\bar{V}$. The upper bounds on $|x^G \cap N|$ in (23) and (24) are satisfied and we note that $|x^G|$ is minimal when $x = (I_{n-2\ell(r-1)}, \omega I_{2\ell}, \ldots, \omega^{r-1}I_{2\ell})$, which implies that

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{(r+1)/2} q^{\ell(r-1)(2n-2\ell r-1)}.$$

For $q \geqslant 3$, one can check that the bound in (24) is sufficient if $n \geqslant 18$ or $q \geqslant 13$, while (23) is effective in each of the remaining cases. Similarly, if $q = 2$ then the same bounds are sufficient unless $n \leqslant 28$, $r = 3$ and $\ell = 1$. So to complete the proof, we may assume the latter conditions are satisfied, in which case x is of the form $(I_{n-4}, \omega I_2, \omega^{-1}I_2)$ or $(I_{n-6}, \omega I_3, \omega^{-1}I_3)$. In the latter case, $|x^G| > \frac{1}{2}(q+1)^{-1}q^{6n-29}$ and the upper bound on $|x^G \cap N|$ in (23) is sufficient. Finally, if $x = (I_{n-4}, \omega I_2, \omega^{-1}I_2)$ then

$$|x^G \cap N| \leqslant 2^2\binom{m}{2} + \frac{m!}{(m-3)!3}(2(q+1))^2, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-14}$$

and the result follows. $\square$

This completes the proof of Theorem 1 for classical groups.

7. EXCEPTIONAL GROUPS

In this final section we complete the proof of Theorem 1 by handling the exceptional groups. Let $G = O^{p'}(\bar{G}^F)$ be a simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. Note that $G_2(2)' \cong U_3(3)$ and ${}^2G_2(3)' \cong L_2(8)$, so we may assume $q \geqslant 3, 27$ if $G = G_2(q), {}^2G_2(q)$, respectively. We adopt the notation from Section 2.2. In particular we have $N = N_G(\bar{T}_w) = T.R$, where $T = G \cap \bar{T}_w^F$ and $R = C_{W,F}(w)$ for some element w in the Weyl group $W = N_{\bar{G}}(\bar{T})/\bar{T}$, where $\bar{T}$ is an F-stable maximal torus of $\bar{G}$. Our aim is to show that $b(G, N) = 2$ in every case.

We begin by recalling the following result, which handles the special cases where N is a maximal subgroup of G. Note that these cases are recorded in [25, Table 5.2].

Proposition 7.1. *If N is a maximal subgroup of G, then $b(G, N) = 2$.*

Proof. This is [13, Proposition 4.2]. $\square$

Corollary 7.2. *If $G = {}^2B_2(q)$, then $b(G, N) = 2$.*

Proof. By [33], N is a maximal subgroup of G and so we may apply Proposition 7.1 (the original reference is [10, Lemma 4.39]). $\square$

Proposition 7.3. *If $G = E_8(q)$, then $b(G, N) = 2$.*

Proof. This is a straightforward application of Proposition 2.1. Let $x \in G$ be an element of prime order. If x is a long root element, then $|x^G| > q^{58} = b_1$ and Lemma 2.8 implies that there are at most $a_1 = 120(q+1)^8$ such elements in N since the Weyl group $W = 2.O_8^+(2)$ contains 120 reflections. In all other cases, we have $|x^G| > q^{92} = b_2$ (see [13, Proposition 2.11]) and we note that $|N| \leqslant (q+1)^8|W| = a_2$. Therefore, by applying Lemma 2.2, we deduce that

$$\hat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1 + a_2^2/b_2 < 1 \tag{33}$$

and the result follows. $\square$

Proposition 7.4. *If $G = E_7(q)$, then $b(G, N) = 2$.*

Proof. For $q \geqslant 3$ we can repeat the argument in the proof of the previous proposition and we deduce that (33) holds on substituting $a_1 = 63(q+1)^7$, $b_1 = q^{34}$, $b_2 = q^{52}$ and $a_2 = (q+1)^7|W|$, where $W = 2 \times \mathrm{Sp}_6(2)$ is the Weyl group of G.

Now assume $q = 2$ and write $N = T.R$ as before, with $R \cong C_W(w)$ for some $w \in W$ (see Section 2.2). First note that if $N = 3^7.W$ then N is maximal and we can apply Proposition 7.1. In each of the remaining cases, we claim that $|N| \leqslant 729 \times 46080 = a_2$, noting that this bound clearly holds if $N = W$. For $N \neq W$, we see that $|T| \leqslant 729$ by inspecting [16, Tables II, III] and a routine calculation with centralisers in W yields $|R| \leqslant 46080$, which justifies the claim. Similarly, we calculate that $\rho_R \leqslant 31$ if $w \neq 1$ and $\rho_R = 63$ if $w = 1$, where we recall that ρ_R is the number of reflections in R. Then by applying Lemma 2.8, recalling that we may assume $N = W$ if $w = 1$, we see that N contains at most $a_1 = 31.3^7$ long root elements. So if we define b_1 and b_2 as above, we deduce that (33) holds and the result follows. $\square$

Next we turn to the groups $G = E_6^\epsilon(q)$. For $\varepsilon = +$, the possibilities for $N = T.R$ can be read off from [20, Table 1]. Now assume $\varepsilon = -$. Here we recall that there is a bijection from the set of F-classes in W to the set of usual conjugacy classes of W, and similarly the F-centraliser $R = C_{W,F}(w)$ is isomorphic to $C_{W,F'}(w) \cong C_W(w)$, where F' is the standard Steinberg endomorphism of $\bar{G}$ with fixed point group $E_6(q)$. This allows us to determine the structure of $\bar{T}_w^F$ from the cyclic structure of $\bar{T}_w^{F'}$ given in [20, Table 1] by simply substituting $-q$ for q in the order of each cyclic factor, adjusting the sign appropriately. For example, the first three rows in the table correspond to the following possibilities for $N_{\bar{G}^F}(\bar{T}_w)$:

$$(C_{q+1})^6{:}W, \ ((C_{q+1})^4 \times C_{q^2-1}){:}(S_2 \times S_6), \ ((C_{q+1})^2 \times (C_{q^2-1})^2){:}(D_8 \times S_4).$$

Proposition 7.5. *If $G = E_6^\epsilon(q)$, then $b(G, N) = 2$.*

Proof. Let $x \in G$ be an element of prime order and note that $|x^G| > (q-1)q^{21} = b_1$ if x is a long root element, otherwise $|x^G| > (q-1)q^{31} = b_2$ (see [13, Proposition 2.11]). Now $|N| \leqslant (q+1)^6|W| = a_2$, where $W = \mathrm{PGSp}_4(3)$ is the Weyl group of G, and we note that N contains at most $a_1 = 36(q+1)^6$ long root elements by Lemma 2.8. Putting these estimates together, we deduce that (33) holds for $q \geqslant 4$.

Next assume $q = 3$. If $G = {}^2E_6(3)$ and $N = 4^6.W$ then N is maximal and we may apply Proposition 7.1. In each of the remaining cases one can check that $|N| \leqslant 2^6|W| = a_2$ (for example, this follows by inspecting [20, Table 1]) and we deduce that (33) holds, where a_1, b_1 and b_2 are defined as before.

For the remainder of the proof, we may assume $q = 2$ and $N = T.R$. By inspecting [25, Table 5.2] we first observe that N is maximal when $(\varepsilon, N) = (+, 7^3{:}3^{1+2}.\mathrm{SL}_2(3))$ in which case the result follows from Proposition 7.1. In considering the remaining cases, let us assume for now that (ε, N) is not one of the following:

$$(+, W), \ (+, 3^4.\mathrm{O}_4^+(3)), \ (-, 3^5.W), \ (-, 3^4.(2 \times \mathrm{Sp}_4(2))), \ (-, (3^2 \times 9).(3 \times (S_3 \wr S_2))). \quad (34)$$

If we exclude these cases, then one can check that $\rho_R|T| \leqslant 810 = a_1$, with equality if $\epsilon = +$ and $N = (3^2 \times 15).(4 \times S_4)$, where ρ_R is the number of reflections in R. In addition, by inspecting [20, Table 1] we find that $|N| \leqslant 12960 = a_2$. Therefore, Lemma 2.8 implies that the contribution to $\widehat{\mathcal{Q}}(G, N, 2)$ from long root elements is at most a_1^2/b_1 and one can check that (33) holds, where b_1 and b_2 are defined as above.

Finally, we handle the cases listed in (34). In order to determine an upper bound on $\widehat{\mathcal{Q}}(G, N, 2)$, it will be convenient to work in $\tilde{N} = N.(2 - \epsilon) = N_{\bar{G}^F}(\bar{T}_w)$. First let a_1 be the number of long root elements in $\tilde{N}$ and let a_2 be the number of involutions in $\tilde{N}$ that are contained in the G-class labelled A_1^2 in [26, Table 22.2.3]. Similarly, let a_3 be the number of elements $x \in \tilde{N}$ of order 3 with $C_{\bar{G}}(x)^0 = D_5T_1$ and let a_4 be the number of remaining

ε	N	a_1	a_2	a_3	a_4
$+$	W	36	270	0	6539
$+$	$3^4.\mathrm{O}_4^+(3)$	36	198	0	4481
$-$	$3^5.W$	108	2430	54	672083
$-$	$3^4.(2 \times \mathrm{Sp}_4(2))$	46	450	30	19571
$-$	$(3^2 \times 9).(3 \times (S_3 \wr S_2))$	18	81	18	4262

TABLE 3.

prime order elements in $\tilde{N}$. Then

$$\widehat{\mathcal{Q}}(G, N, 2) < \sum_{i=1}^{4} a_i^2 / b_i, \tag{35}$$

where b_1 and $b_2 = b_3$ are defined as above and we set $b_4 = 2^{41}$, noting that $|x^G| > b_4$ for all $x \in G$ of prime order other than long root elements, involutions in the A_1^2 class and order 3 elements with a centraliser of type D_5T_1.

To complete the argument, we need to compute a_1, a_2, a_3 and a_4. To do this, we proceed as in the proof of [12, Proposition 2.2], first working with MAGMA to construct $\tilde{N}$ as a subgroup of $\bar{G}^{F^\ell} = \mathrm{Inndiag}(E_6(2^\ell))$ for $\ell = 1, 2, 2, 4, 6$, respectively (referring to the five cases in (34)). In terms of this embedding, we then construct a set of representatives of the conjugacy classes of elements in $\tilde{N}$ of prime order and we compute the Jordan form of each representative on the adjoint module V for $\bar{G}$. If $x \in \tilde{N}$ is an involution, we can then determine the G-class of x by inspecting [23, Table 6]. Similarly, if x has order 3 then we read off $\dim C_V(x) = \dim C_{\bar{G}}(x)$, which allows us to identify the structure of $C_{\bar{G}}(x)^0$. In this way, we deduce that a_i takes the values recorded in Table 3 and it is straightforward to check that the upper bound in (35) yields $\widehat{\mathcal{Q}}(G, N, 2) < 1$. $\qquad\square$

Proposition 7.6. *If $G = F_4(q)$, then $b(G, N) = 2$.*

Proof. Let $W = \mathrm{O}_4^+(3)$ be the Weyl group of G and note that $|N| \leqslant |W|(q+1)^4 = a_1$ and [13, Proposition 2.11] gives $|x^G| > q^{16} = b_1$ for all $x \in G$ of prime order. By Lemma 2.2, this implies that $\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1$, which is less than 1 for $q \geqslant 7$.

For the remainder of the proof we may assume $q \leqslant 5$. We will postpone the analysis of the cases $N = (q+1)^4.W$ with $q \in \{2, 3\}$ to the end of the proof. Let $x \in N$ be an element of prime order r.

Suppose q is odd. If $r = 2$ then $|x^G| > q^{16} = b_1$, whereas $|x^G| > \frac{1}{2}(q-1)q^{21} = b_2$ if r is odd (note that there are no root elements in N by Lemma 2.8). We claim that $i_2(N) \leqslant a_1$ and $|N| \leqslant a_2$, where a_1 and a_2 are defined as in Table 4. Here the upper bound on $|N|$ can be read off from [19, Table 5.2]. To obtain the upper bound on $i_2(N)$, we use MAGMA to construct each possibility for N as a subgroup of $F_4(q^\ell)$ for some suitable ℓ, which allows us to compute $i_2(N)$ precisely in each case. It is now straightforward to check that (33) holds.

Now assume q is even. If $r = 2$ then $|x^G| > q^{16} = b_1$ and we have $|x^G| > q^{28} = b_2$ if r is odd, or if $r = 2$ and x is in the class labelled $A_1\tilde{A}_1$. As above, we note that $|N| \leqslant a_2$, where a_2 is defined in Table 4. With the aid of MAGMA, we also calculate that there are at most a_1 involutions in N that are not in the class labelled $A_1\tilde{A}_1$, where a_1 is also given in Table 4 (here we can proceed as in the final part of the proof of Proposition 7.5 in order to determine the G-class of each N-class of involutions). Once again, one can check that (33) holds and the result follows.

It remains to deal with the two excluded cases. First assume $q = 3$ and $N = 4^4.W$, in which case we use MAGMA to construct N as a subgroup of $F_4(9)$. Let $x \in N$ be an element of prime order r. If $r = 3$ then $|x^G| > 3^{21} = b_3$ since N contains no root elements and we calculate that $i_3(N) = 5120 = a_3$. Similarly, if $r = 2$ and $C_{\bar{G}}(x) = B_4$, then $|x^G| > 3^{16} = b_1$

q	a_1	a_2	b_1	b_2
5	16000	$6^4.|W|$	5^{16}	2.5^{21}
4	6000	$5^4.|W|$	4^{16}	3^{28}
3	847	12288	3^{16}	3^{21}
2	234	3528	2^{16}	2^{28}

TABLE 4.

and there are $a_1 = 51$ such elements in N. And if $r = 2$ and $C_{\bar{G}}(x) \neq B_4$, or if $r \geqslant 5$, then $|x^G| > 3^{28} = b_2$ and we set $a_2 = |N|$. Therefore, we conclude that

$$\widehat{\mathcal{Q}}(G, N, 2) < \sum_{i=1}^{3} a_i^2/b_i < 1$$

and the result follows.

Finally suppose $q = 2$ and $N = 3^4.W$. Here we use MAGMA to construct G as a permutation group of degree 139776 and we find a Sylow 3-subgroup H of G. Now H has a unique abelian subgroup of order 3^4, which we may assume is the relevant maximal torus T. We can now construct $N = N_G(T)$ and then find a random element $x \in G$ with $N \cap N^x = 1$. $\square$

Proposition 7.7. *If* $G = G_2(q)'$, *then* $b(G, N) = 2$.

Proof. Here $|N| \leqslant 12(q+1)^2 = a_1$ and we may assume $q \geqslant 7$ by Lemma 2.10. Let $\mathcal{A}$ be the set of elements $x \in G$ that are either long root elements, or short root elements if $p = 3$, or semisimple elements of order 3 with $C_{\bar{G}}(x) = A_2$. Then if $x \in G$ has prime order, [13, Proposition 2.11] implies that $|x^G| > (q-1)q^5 = b_2$ if $x \in \mathcal{A}$, otherwise $|x^G| > (q-1)q^7 = b_1$. Set $a_2 = |N \cap \mathcal{A}|$.

If $q \geqslant 16$ then $\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_2 < 1$ and so we may assume $7 \leqslant q \leqslant 13$. If q is odd then with the aid of MAGMA we compute $a_2 \leqslant 2$ (note that N does not contain any long root elements by Lemma 2.8) and one checks that (33) holds. Similarly, if $q = 8$ then $a_2 \leqslant 29$ and (33) holds once again. $\square$

Proposition 7.8. *If* $G = {}^3D_4(q)$, *then* $b(G, N) = 2$.

Proof. The possibilities for T and N are recorded in [17, Table 1.1]. Note that if $x \in G$ has prime order, then either $|x^G| > q^{16} = b_1$, or x is a long root element and $|x^G| > q^{10} = b_2$ (see [13, Proposition 2.11]).

First observe that if $T = C_{q^2 \pm q+1} \times C_{q^2 \pm q+1}$ or $C_{q^4-q^2+1}$ then N is a maximal subgroup of G and thus $b(G, N) = 2$ by Proposition 7.1. For the remainder, we may assume N is not one of these possibilities, in which case $|N| \leqslant 12(q^3+1)(q+1) = a_1$.

If q is odd then N does not contain long root elements by Lemma 2.8 and thus $\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_1 < 1$. Now assume q is even. By Lemma 2.10, we may assume $q \geqslant 8$. Here $\widehat{\mathcal{Q}}(G, N, 2) < a_1^2/b_2$, which is less than 1 if $q \geqslant 16$. Finally, suppose $q = 8$ and write $N = T.R$. Here we check that $i_2(R) \leqslant 7$, so N contains at most $7|T| \leqslant 7(q^3+1)(q+1) = a_2$ long root elements by Lemma 2.8. It is now routine to check that (33) holds, with a_1, b_1 and b_2 defined as above. $\square$

Proposition 7.9. *If* $G = {}^2F_4(q)'$, *then* $b(G, N) = 2$.

Proof. By Lemma 2.10 we may assume $q \geqslant 8$. As explained in [19, Section 7.4], there are 11 possibilities for $N = T.R$, up to conjugacy, and the structure in each case is recorded in [19, Table 7.3]. Let $x \in G$ be an element of prime order. If x is a long root element, then $|x^G| > (q-1)q^{10} = b_1$, otherwise $|x^G| > (q-1)q^{13} = b_2$ (see [13, Proposition 2.11]). Now $|T| \leqslant (\sqrt{q}+1)^4$ (see Lemma 2.7), $|R| \leqslant 96$ and by applying Lemma 2.8 we see that N contains at most $a_1 = 24(\sqrt{q}+1)^4$ long root elements since the Weyl group of type F_4 contains 24 reflections. One can now check that (33) holds, with $a_2 = 96(\sqrt{q}+1)^4$. $\square$

Proposition 7.10. *If $G = {}^2G_2(q)'$, then $b(G, N) = 2$.*

Proof. Recall that we may assume $q \geqslant 27$. The four possibilities for $N = T.R$ (up to conjugacy) are given in [19, Proposition 7.4]. By [21, Theorem C], either N is maximal and hence $b(G, N) = 2$ by Proposition 7.1, or $N = C_{q-1}.2$. To handle the latter case, set $a = |N|$ and note that $|x^G| > (q-1)q^3 = b$ for any prime order element $x \in N$ by [13, Proposition 2.11]. By Lemma 2.2, this implies that $\widehat{\mathcal{Q}}(G, N, 2) < a^2/b$, which is less than 1 for $q \geqslant 27$. $\qquad\square$

This completes the proof of Theorem 1 when G is a simple exceptional group of Lie type. By combining this with the main results on classical groups in Sections 3-6, we conclude that the proof of Theorem 1 is complete. Finally, we establish Corollary 2.

Proof of Corollary 2. Let $G = O^{p'}(\bar{G}^F)$ be a finite simple group of Lie type over a field of characteristic p and let $N = N_G(\bar{T})$, where $\bar{T}$ is an F-stable maximal torus of $\bar{G}$. If $b(G, N) = 2$ then $N \cap N^x = 1$ for some $x \in G$, so by Theorem 1 we may assume (G, N) is one of the cases listed in Table 1. The result now follows by combining the statements of Theorems 3.5, 4.3 and 6.3 with Propositions 3.6–3.9. $\qquad\square$

References

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

[2] R.F. Bailey and P.J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc. **43** (2011), 209–242.

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

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

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

[6] T.C. Burness, *Simple groups, fixed point ratios and applications*, in Local representation theory and simple groups, 267–322, EMS Ser. Lect. Math., Eur. Math. Soc., Zürich, 2018.

[7] T.C. Burness, *Base sizes for primitive groups with soluble stabilisers*, Algebra Number Theory **15** (2021), 1755–1807.

[8] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series, vol. 25, Cambridge University Press, Cambridge, 2016.

[9] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for algebraic groups*, J. Eur. Math. Soc. (JEMS) **19** (2017), 2269–2341.

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

[11] T.C. Burness, A. Lucchini and D. Nemmi, *On the soluble graph of a finite group*, J. Combin. Theory Ser. A **194** (2023), 105708, 39pp.

[12] T.C. Burness and A.R. Thomas, *Computations concerning the classification of almost simple extremely primitive groups*, available at `http://seis.bristol.ac.uk/~tb13602/epcomp.pdf`.

[13] T.C. Burness and A.R. Thomas, *The classification of extremely primitive groups*, Int. Math. Res. Not. IMRN (2022), no.13, 10148–10248.

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

[15] R.W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters*, John Wiley and Sons, New York, 1985.

[16] 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** (1991), 889–903.

[17] D.I. Deriziotis and G.O. Michler, *Character table and blocks of finite simple triality groups ${}^3D_4(q)$*, Trans. Amer. Math. Soc. **303** (1987), 39–70.

[18] I.A. Faradžev and A.A. Ivanov, *Distance-transitive representations of groups G with $PSL_2(q) \trianglelefteq G \leqslant P\Gamma L_2(q)$*, Europ. J. Combinatorics **11** (1990), 347–356.

[19] P.C. Gager, *Maximal tori in finite groups of Lie type*, PhD thesis, University of Warwick, 1973.

[20] A. Galt and A. Staroletov, *On splitting of the normalizer of a maximal torus in $E_6(q)$*, Algebra Colloq **26** (2019), 329–350.

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

[22] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[23] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, Comm. Algebra **23** (1995), 4125–4156.

[24] R. Lawther, M.W. Liebeck and G.M. Seitz, *Fixed point spaces in actions of exceptional algebraic groups*, Pacific J. Math. **205** (2002), 339–391.

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

[26] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, vol. 180, Amer. Math. Soc., 2012.

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

[28] M.W. Liebeck and A. Shalev, *Bases of primitive permutation groups*, in Groups, combinatorics & geometry (Durham, 2001), 147–154, World Sci. Publ., River Edge, NJ, 2003.

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

[30] V.D. Mazurov and E.I. Khukhro, *Unsolved problems in group theory: The Kourovka notebook, no. 20* (arXiv:1401.0300), 2022.

[31] G.M. Seitz, *The root subgroups for maximal tori in finite groups of Lie type*, Pacific J. Math. **106** (1983), 153–244.

[32] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), J. Fac. Sci. Univ. Tokyo **22** (1975), 1–15.

[33] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: t.burness@bristol.ac.uk

A.R. Thomas, Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK
Email address: adam.r.thomas@warwick.ac.uk