Forum of Mathematics, Sigma (2022), **Vol. 10**:e83 1–30
doi:10.1017/fms.2022.69

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Products of derangements in simple permutation groups

Michael Larsen[1], Aner Shalev[2] and Pham Huu Tiep[3]

[1]Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A; E-mail: mjlarsen@indiana.edu.
[2]Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel; E-mail: aner.shalev@mail.huji.ac.il.
[3]Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA; E-mail: tiep@math.rutgers.edu.

Received: 30 May 2022; **Revised:** 10 July 2022; **Accepted:** 29 July 2022

2020 Mathematics subject classification: *Primary* – 20D06; *Secondary* – 20F69, 20G40, 20P05, 20B15, 20C33

Abstract
We prove that any element in a sufficiently large transitive finite simple permutation group is a product of two derangements.

Dedicated to Bob Guralnick on the occasion of his seventieth birthday

Contents

1. Introduction

The study of *derangements* – that is, fixed-point-free permutations – goes back three centuries to 1708, when Montmort observed that the proportion $\delta(\mathsf{S}_n)$ of derangements in the symmetric group S_n (in its natural action on n symbols) satisfies $\delta(\mathsf{S}_n) \to 1/e$ as $n \to \infty$. In the 1870s, Jordan proved that every finite transitive permutation group of degree $n > 1$ contains a derangement (this result is an immediate consequence of the orbit counting lemma). Since then, derangements have been studied extensively and have proved useful in various areas of mathematics, including group theory, graph theory, probability, number theory and topology. See the book [BG] for background and new results.

The classification of finite simple groups has revolutionised the study of derangements, and various powerful results have been obtained. These include the well-known result of Fein, Kantor and Schacher [FKS], strengthening Jordan's theorem, that every finite transitive permutation group of degree $n > 1$ has a derangement of prime power order. Note, however, that there are finite transitive groups with no derangements of prime order. The question of the existence of derangements of prime order is discussed extensively in [BG].

In recent years, there has been considerable interest in invariable generation of groups, which has sparked renewed interest in derangements. Recall that a group G (finite or infinite) is said to be invariably generated by a subset $S \subseteq G$ if, whenever we replace each $s \in S$ by any conjugate s^g of s (where $g \in G$ depends on s), we obtain a generating set for G. It is easy to see that G is invariably generated by G if and only if whenever G acts transitively on some set X with $|X| > 1$, the set $\mathcal{D}(G, X)$ of elements of G that act as derangements on X is nonempty. This in turn is equivalent to $\cup_{g\in G} H^g \subsetneq G$ for every proper subgroup $H < G$. Thus finite groups are invariably generated by themselves, but some infinite groups – for instance, any infinite group with exactly two conjugacy classes – are not.

For a finite group G and a positive integer k, let $P_I(G, k)$ denote the probability that k randomly chosen elements of G invariably generate G. For a subgroup H of G, let $\delta(G, H)$ denote the proportion of elements of G that act as derangements in the transitive action of G on H-cosets. The study of these probabilities is motivated by computational Galois theory; see, for example, [D], [LP], [KLSh], [Mc], [PPR], and [EFG]. The latter two papers show that $P_I(\mathsf{S}_n, 4)$ is bounded away from zero, while $P_I(\mathsf{S}_n, 3)$ is not.

It is easy to see (see for instance [KLSh, 2.3]) that

$$1 - P_I(G, k) \leq \sum_H (1 - \delta(G, H))^k,$$

where H ranges over a set of representatives of the conjugacy classes of the maximal subgroups of G. Thus the study of derangements and their proportions has applications to invariable generation and related topics.

A lower bound of the form $1/n$ on the proportion $\delta(G)$ of derangements in arbitrary transitive permutation groups G of degree n was provided in [CC]. This bound is sharp. It is attained if and only if G is a Frobenius group of degree $n(n-1)$. If $n \geq 7$ and G is not a Frobenius group of size $n(n-1)$ or $n(n-1)/2$, then a better lower bound of the form $\delta(G) > 2/n$ was subsequently provided in [GW], with a number-theoretic application. In contrast to the proof of the bound $1/n$ in [CC], the proof of the $2/n$ bound in [GW] already uses the Classification of Finite Simple Groups.

The case where the transitive permutation group G is simple has been studied thoroughly in the past two decades by Fulman and Guralnick [FG1, FG2, FG3], proving a conjecture of Boston and Shalev that $\delta(G) \geq \epsilon$ for some fixed $\epsilon > 0$. Thus the set of derangements in such a group is a large normal subset.

Our main result is the following.

Theorem A. *Let G be a finite simple transitive permutation group of sufficiently large order. Then every element of G is a product of two derangements.*

Our computations have not revealed any counterexample to the conclusion of Theorem A among simple groups of small order, which seems to suggest it should hold for arbitrary finite simple groups. To prove this for simple groups of Lie type, however, seems to be a daunting task. The character-theoretic approach that we are exploiting would require substantial improvements on results of Sections 2–5 (below), which at the moment we know only for groups of large enough rank, after which it would still leave a large number of possible exceptions, to be excluded by *ad hoc* arguments far beyond the current reach of computational group theory. For alternating groups, we are able to prove that the conclusion of Theorem A holds universally:

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

Theorem B. *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite transitive permutation group. Suppose that $G \cong \mathsf{A}_n$ for some $n \geq 5$. Then every element in G is a product of two derangements.*

A key input for this paper is Theorem 6.2, proved in the companion paper [LST2], which asserts that given r and $\epsilon > 0$, for every normal subset S of a sufficiently large finite simple group G of Lie type and rank r, $|S| > \epsilon|G|$ implies $S^2 \supseteq G \setminus \{e\}$. The same is true if G is an alternating group of sufficiently large degree instead of a group of bounded rank. It is not true, however, for finite simple groups in general. We use the Frobenius formula for the number of solutions $x_1x_2 = x_3$, where x_i belongs to a fixed conjugacy class C_i, $i = 1, 2, 3$, to prove that certain products of two conjugacy classes cover all nontrivial elements of G. To do this in the cases of interest, we need detailed information about the characters of classical groups of unbounded rank to complete the proof of Theorem A in the most difficult case: when G is a classical group of high rank over a small finite field with a subspace action. This in turn necessitates proving various results on products of conjugacy classes in finite classical groups, which extend and refine previous results obtained in [MSW], [LST1], [GM2], [GT3], [GLBST] and which will be useful in other applications as well.

Our paper is organised as follows. In Section 2, we prove several results concerning character values and products of conjugacy classes for $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$. In Section 3, we review Lusztig's theory of symbols, which we use in Sections 4 and 5 to prove results like those of Section 2 in the case of orthogonal groups. Theorem A is then proved in Section 6. Finally, in Section 7, we prove Theorem B.

2. Character estimates in groups of type A_n and ${}^2A_n$

Proposition 2.1. *For all integers L, there exists a constant $A = A(L) > 0$ such that for all integers $n > L$ and all prime powers q, the degree of the unipotent character of $\mathrm{GL}_n(q)$ associated to a partition whose largest piece is $n - L$ is at least $q^{\frac{n^2-n}{2}-A}$.*

Proof. Choosing A large enough, without loss of generality, we may assume $n > 2L$. The partition $\lambda = \lambda_1 \geq \lambda_2 \geq \cdots$ of n associated to the character has $\lambda_1 = n - L$. It is well known (see, for instance, [Ol, (21)] or [Ma1]) that this character has degree

$$\chi_\lambda(1) = q^{\sum_i \binom{\lambda_i}{2}} \frac{\prod_{j=1}^n (q^j - 1)}{\prod_{k=1}^n (q^{h_k} - 1)},$$

where h_k denotes the length of the hook of the k^{th} box in the Ferrers diagram of λ. Now, the last $n - 2L$ boxes in the first row of the Ferrers diagram belong to one-box columns. Therefore, their hooks have lengths $n - 2L, \ldots, 3, 2, 1$. All hooks of boxes not in the first row have lengths $\leq L$, and the hooks of the first L boxes in the first row have length $\leq n$. We conclude that

$$\frac{\prod_{j=1}^n (q^j - 1)}{\prod_{k=1}^n (q^{h_k} - 1)} \geq \frac{\prod_{j=n-2L+1}^n (q^j - 1)}{q^{L^2+Ln}}.$$

As

$$\prod_{i=1}^{\infty} (1 - q^{-i}) > 1/4 \geq q^{-2},$$

we have

$$\dim \chi_\lambda(1) > q^{\binom{\lambda_1}{2}} q^{-2+L(n+(n-2L+1))-L^2-Ln} = q^{\frac{n^2-n-5L^2+3L-4}{2}}. \qquad \square$$

Up to conjugacy, $\mathbb{F}_q$-rational maximal tori in the algebraic groups SL_n and SU_n over a finite field $\mathbb{F}_q$ are both indexed by partitions of n. We do not distinguish between the maximal torus as an algebraic group and the finite subgroup of G obtained by taking $\mathbb{F}_q$-points. If G is either $\mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$ and $a_1,\dots,a_k$ are positive integers summing to n (not necessarily arranged in order), then we denote by $T_{a_1,\dots,a_k} < G$ a maximal torus in the class belonging to the partition with parts $a_1,\dots,a_k$.

Theorem 2.2. *Let $a \geq 3$ be a fixed positive integer. Then there exists an integer $N = N(a) \geq 2a^2+6$ such that the following statements hold whenever $n > N$, q any prime power and $G = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$:*

(i) *If t_1 and t_1' are regular semisimple elements of G belonging to tori T and T' of type T_n and $T_{1,a,n-a-1}$, respectively, then $t_1^G \cdot (t_1')^G \supseteq G \setminus \mathbf{Z}(G)$.*

(ii) *If t_2 and t_2' are regular semisimple elements of G belonging to tori T and T' of type $T_{1,n-1}$ and $T_{a,n-a}$, respectively, then $t_2^G \cdot (t_2')^G \supseteq G \setminus \mathbf{Z}(G)$.*

Proof. (i) Consider any $g \in G \setminus \mathbf{Z}(G)$ and any $\chi \in \mathrm{Irr}(G)$ such that $\chi(t_1)\chi(t_1') \neq 0$. By [LST1, Proposition 3.1.5] and its proof, then χ must be a unipotent character of the form $\chi^{(n-k,1^k)}$. Moreover, either $k = 0$ (in which case χ is the principal character 1_G), $k = a$, $k = n-a-1$ or $k = n-1$ (in which case χ is the Steinberg character St); moreover, $|\chi(t_1)\chi(t_1')| = 1$, and the last two characters both have degree $\geq C|G|/q^n$ for a universal constant $C > 0$. In the terminology of [GLT, p. 3], the character $\chi_2 := \chi^{(n-a,1^a)}$ has level

$$a \leq \min\{\sqrt{n-3/4} - 1/2, \sqrt{(8n-17)/12} - 1/2\}$$

by [GLT, Theorem 3.9], so $\chi_2(1) > q^{a(n-a)-3}$ by [GLT, Theorem 1.3] and

$$|\chi_2(g)| \leq (2.43)\chi_2(1)^{1-1/n}$$

by [GLT, Theorem 1.6]. In particular,

$$|\chi_2(g)|/\chi_2(1) \leq 2.43/\chi_2(1)^{1/n} \leq 2.43/q^{a-1/2} \leq 2.43/2^{2.5} < 0.43.$$

On the other hand, for the latter two (large degree) characters, by [LST1, Proposition 6.2.1], we have $|\chi(g)|/\chi(1) < 0.25$ if we take $N(a)$ large enough. It follows that

$$\left|\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t_1)\chi(t_1')\overline{\chi(g)}}{\chi(1)}\right| \geq 1 - 0.43 - 2(0.25) = 0.07 > 0,$$

so $g \in t_1^G \cdot (t'1)^G$.

(ii) Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi(t_2)\chi(t_2') \neq 0$. By [LST1, Proposition 3.1.5] and its proof, we have

$$\chi \in \{1_G, \chi_2 := \chi^{(n-a,2,1^{a-2})}, \chi^{(a,2,1^{n-a-2})}, \mathsf{St}\};$$

moreover, $|\chi(t_2)\chi(t_2')| = 1$, and the last two characters both have degree $\geq C|G|/q^n$ for a universal constant $C > 0$. Now we can repeat the arguments in (i) verbatim. □

We will need a similar result, using [GLBST, Proposition 8.4] and its notation. But first we prove an auxiliary lemma.

Lemma 2.3. *Let $k, n \in \mathbb{Z}_{\geq 1}$ with $n \geq \max(5, 2k)$, and let q be any prime power. Let*

$$N := \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q-1)(q^2-1)\dots(q^k-1)},$$

and let G be a primitive subgroup of S_N with a unique minimal normal subgroup $S \cong \mathrm{PSL}_n(q)$, which acts on $\{1,2,\dots,N\}$ via the action of $\mathrm{SL}_n(q)$ on the set of k-dimensional subspaces of the natural module $\mathbb{F}_q^n$. Then the following statements hold for any nontrivial element $g \in G$:

(i) *g has at most αN fixed points on $\{1,2,\ldots,N\}$, where*

$$\alpha := q^{-k} + 9q^{-(n-1)/2}.$$

(ii) *The permutation character ρ associated to the action of G on $\{1,2,\ldots,N\}$ has a unique irreducible constituent χ that extends the unipotent character $\chi^{(n-k,k)}$ of $\mathrm{PSL}_n(q)$. Furthermore,*

$$\frac{|\chi(g)|}{\chi(1)} \le \alpha + (\alpha+1)\frac{q^k-1}{q^{n-k+1}-q^k}.$$

Proof. (i) is a consequence of [FM, Theorem 1] (note that $9q^{-(n-1)/2} > 11q^{-n/2}$). For (ii), recall that the restriction of ρ to S is $\sum_{i=0}^{k}\chi^{(n-i,i)}$, where we view the unipotent character $\chi^{(n-i,i)}$ as an S-character. The character $\chi^{(n-k,k)}$ has degree

$$\frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-q^k)}{(q-1)(q^2-1)\ldots(q^k-1)},$$

which is larger than $N/2$. Since $S \lhd G$, this implies that there is a unique irreducible constituent χ of ρ that extends $\chi^{(n-k,k)}$. Now, $\rho-\chi$ is a character of G of degree $N-\chi(1)$, so

$$|\rho(g)-\chi(g)| \le N-\chi(1) = \beta\chi(1),$$

where $\beta := (q^k-1)/(q^{n-k+1}-q^k)$. Together with (i), this implies that

$$\frac{|\chi(g)|}{\chi(1)} \le \frac{|\rho(g)|+|\rho(g)-\chi(g)|}{\chi(1)} \le \frac{\alpha N}{\chi(1)} + \beta = \alpha + (\alpha+1)\beta,$$

as stated. □

Recall the notion of *weakly orthogonal pairs* of maximal tori in connected reductive groups, introduced in [LST1, Definition 2.2.1].

Theorem 2.4. *If t and t' are regular semisimple elements of G belonging to tori T and T' of type $T_{n-2,2}$ and $T_{n-3,3}$, respectively, then $t^G \cdot (t')^G \supseteq G \setminus \mathbf{Z}(G)$ in each of the following cases:*

(i) $G = \mathrm{SL}_n(q)$, $n \ge 33$,
(ii) $G = \mathrm{SL}_n(q)$, $n \ge 7$, $q > 7^{481}$,
(iii) $G = \mathrm{SU}_n(q)$, $n \ge 33$, $q \ge 3$,
(iv) $G = \mathrm{SU}_n(q)$, $n \ge 7$, $q > 7^{481}$.

Proof. Suppose $\chi \in \mathrm{Irr}(G)$ is such that

$$\chi(t)\chi(t') \ne 0. \tag{2.1}$$

By [GLBST, Proposition 8.4], the two tori are weakly orthogonal, and hence $\chi = \chi^\lambda$ is a unipotent character labelled by a partition $\lambda \vdash n$. Now, as in the proof of [LST1, Proposition 3.1.5], the condition in equation (2.1) implies that the irreducible character ψ^λ of S_n labelled by λ takes nonzero values at permutations $\sigma_1 = (1,2)(3,4,\ldots,n)$ and $\sigma_2 = (1,2,3)(4,5,\ldots,n)$. By the Murnaghan-Nakayama rule [LST1, Proposition 3.1.1] and by [LST1, Corollary 3.1.2], it follows that we can remove a rim $(n-2)$-hook from the Young diagram $Y(\lambda)$ of λ, and likewise we can remove a rim $(n-3)$-hook from $Y(\lambda)$ (so that the remainder is a proper diagram). The list of λ that a rim $(n-2)$-hook can be removed from $Y(\lambda)$ is given in [LST1, Corollary 3.1.4]. Checking through them for a removal of a rim $(n-3)$-hook, we see that λ is one of the following 8 partitions:

$$(n),\ (1^n),\ \lambda_2 := (n-1,1),\ (2,1^{n-2}),$$
$$\lambda_3 := (n-3,3),\ (2^3,1^{n-6}),\ \lambda_4 := (n-4,2^2),\ (3^2,1^{n-6}).$$

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

Moreover, [LST1, Proposition 3.1.1] implies that

$$\chi^{\lambda}(t)\chi^{\lambda}(t') = \pm 1 \tag{2.2}$$

in all these cases. Let $\epsilon = 1$ if $G = \mathrm{SL}_n(q)$ and $\epsilon = -1$ if $G = \mathrm{SU}_n(q)$. Using [Ca, §13.8], we can write down the degrees of these 8 characters:

$$\begin{aligned}
\chi^{(n)}(1) &= 1,\\
\chi^{(1^n)}(1) &= q^{n(n-1)/2},\\
\chi^{(n-1,1)}(1) &= q\tfrac{q^{n-1}+\epsilon^n}{q-\epsilon},\\
\chi^{(2,1^{n-2})}(1) &= q^{n(n-1)/2-(n-1)}\tfrac{q^{n-1}+\epsilon^n}{q-\epsilon},\\
\chi^{(n-3,3)}(1) &= q^3\tfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-5}-\epsilon^{n-5})}{(q^3-\epsilon^3)(q^2-\epsilon^2)(q-\epsilon)},\\
\chi^{(2^3,1^{n-6})}(1) &= q^{n(n-1)/2-(3n-9)}\tfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-5}-\epsilon^{n-5})}{(q^3-\epsilon^3)(q^2-\epsilon^2)(q-\epsilon)},\\
\chi^{(n-4,2^2)}(1) &= q^6\tfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-4}-\epsilon^{n-4})(q^{n-5}-\epsilon^{n-5})}{(q^3-\epsilon^3)(q^2-\epsilon^2)^2(q-\epsilon)},\\
\chi^{(3^2,1^{n-6})}(1) &= q^{n(n-1)/2-(4n-12)}\tfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-4}-\epsilon^{n-4})(q^{n-5}-\epsilon^{n-5})}{(q^3-\epsilon^3)(q^2-\epsilon^2)^2(q-\epsilon)}.
\end{aligned} \tag{2.3}$$

The first two characters in this list are the principal character 1_G and the Steinberg character St of G.

Next, consider any $g \in G \setminus \mathbf{Z}(G)$. If $n \geq 7$ and $q > 7^{481}$, then using equation (2.2) and [LST1, Theorem 1.2.1], we get

$$\left|\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(t)\chi(t')\overline{\chi(g)}}{\chi(1)}\right| \geq 1 - \frac{7}{q^{1/481}} > 0,$$

so $g \in t^G \cdot (t')^G$.

Now we will assume $n \geq 33$. Then $\chi_i := \chi^{\lambda_i}$ with $i = 3, 4$ has level

$$i \leq \min\{\sqrt{n-3/4} - 1/2, \sqrt{(8n-17)/12} - 1/2\}$$

by [GLT, Theorem 3.9], so

$$\frac{|\chi_i(g)|}{\chi_i(1)} \leq \frac{2.43}{\chi_i(1)^{1/n}} \tag{2.4}$$

by [GLT, Theorem 1.6]; furthermore,

$$\chi_3(1) > q^{3n-12}, \ \ \chi_4(1) > q^{4n-15}. \tag{2.5}$$

On the other hand, $\chi_2 := \chi^{\lambda_2}$ is a unipotent Weil character, and using the character formula [TZ1, Lemma 4.1], one can show that

$$\frac{|\chi_2(g)|}{\chi_2(1)} \leq \frac{q^{n-1}+q^2}{q^n-q}. \tag{2.6}$$

Now, if $q \geq 3$, then equations 2.4–2.6 imply

$$\sum_{i=2}^{4} \frac{|\chi_i(g)|}{\chi_i(1)} \leq \frac{q^{n-1}+q^2}{q^n-q} + \frac{2.43}{q^{(3n-12)/n}} + \frac{2.43}{q^{(4n-15)/n}} < 0.9324. \tag{2.7}$$

If $q = 2$, then $|\chi_2(g)|/\chi(1) < 0.1252$ by Lemma 2.3 applied to $(k, q) = (3, 2)$, whence

$$\sum_{i=2}^{4} \frac{|\chi_i(g)|}{\chi_i(1)} \leq \frac{q^{n-1} + q^2}{q^n - q} + 0.1252 + \frac{2.43}{q^{(4n-15)/n}} < 0.8334.$$

Thus equation (2.7) holds for $q = 2$ as well.

Note that the second, fourth, sixth and eighth characters in equation (2.3) have degree $> q^{n(n-1)/2-9}$. Applying [LST1, Proposition 6.2.1] as in the proof of Theorem 2.2, we obtain that

$$|\chi(g)| \leq |\mathbf{C}_G(g)|^{1/2} < q^{(n^2-2n+3)/2},$$

and so

$$\frac{|\chi(g)|}{\chi(1)} < q^{(21-n)/2} < 0.0157 \tag{2.8}$$

for all four of them. Using equations (2.7) and (2.8), we now see that

$$\sum_{i=2}^{8} \frac{|\chi_i(g)|}{\chi_i(1)} < 0.9324 + 4 \cdot 0.0157 = 0.9952.$$

It now follows from equation (2.2) that

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)\chi(t')\overline{\chi(g)}}{\chi(1)} \right| \geq 1 - 0.9952 = 0.0048,$$

so $g \in t^G \cdot (t')^G$. □

In fact, for $\mathrm{SU}_n(2)$, we will need an analogue of Theorem 2.4 for tori of types $T_{3,n-3}$ and $T_{4,n-4}$. We begin by classifying characters of S_n, which vanish on neither of the corresponding permutations.

Proposition 2.5. *Let $n \geq 10$, and let*

$$\sigma_1 = (1, 2, 3)(4, \ldots, n),\ \sigma_2 = (1, 2, 3, 4)(5, \ldots, n) \in \mathsf{S}_n.$$

There are exactly 12 characters $\psi = \psi^\lambda$ of S_n such that $\psi(\sigma_1)\psi(\sigma_2) \neq 0$. For each of these characters, the product is ± 1, and for each such λ, either λ or its transpose belongs to the following set:

$$\{(n), (n-1, 1), (n-2, 1^2), (n-4, 4), (n-5, 3, 2), (n-6, 2^3)\}.$$

Proof. As $\lambda \vdash n \geq 10$, transposing if necessary, we may assume $\lambda_1 \geq 4$. As $\psi(\sigma_1) \neq 0$, by the Murnaghan-Nakayama rule, removal of a rim $n-3$-hook leaves a Young diagram μ with 3 boxes, and it follows that this rim hook must include the last box in the first row (which implies, in particular, that there is no other rim $n-3$-hook, so the character value at σ_1 is ± 1). There are three cases to consider:

(i) $\mu = (3)$. In this case, λ must be (n) or $(n-k-4, 4, 1^k)$ for $0 \leq k \leq n-8$.
(ii) $\mu = (2, 1)$. In this case, λ must be either $(n-1, 1)$, or $(n-3, 3)$ or $(n-k-5, 3, 2, 1^k)$ for $0 \leq k \leq n-8$.
(iii) $\mu = (1^3)$. In this case, λ must be $(n-2, 1^2)$, $(n-3, 2, 1)$, $(n-4, 2^2)$ or $(n-6-k, 2^3, 1^k)$, where $0 \leq k \leq n-8$.

As $\psi(\sigma_2) \neq 0$, λ must have a rim $n-4$-hook whose removal leaves a Young diagram, which is a 4-hook. In case (i), this is possible for (n) and possible for $(n-k-4, 4, 1^k)$ if and only if $k = 0$. In case (ii), this is possible for $(n-1, 1)$, impossible for $(n-3, 3)$ and possible for $(n-5-k, 3, 2, 1^k)$ if and only if $k = 0$. In case (iii), this is possible only for $(n-2, 1^2)$ and $(n-6, 2^3)$. In every case where it is possible, the rim hook contains the last box in the first row and is therefore unique, implying that $\psi(\sigma_2)$ is ± 1. □

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

Recall [LST1, Definition 4.1.1], which states that the *support* $\mathsf{supp}(g)$ of an element g in a finite classical group $\mathrm{Cl}(V)$ is the codimension of the largest eigenspace of g on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$.

Theorem 2.6. *The following statement holds for $G = \mathrm{SU}_n(2)$ with $n \geq 43$. If t and t' are regular semisimple elements of G belonging to tori T and T' of type $T_{n-3,3}$ and $T_{n-4,4}$, respectively, and $g \in G$ has $\mathsf{supp}(g) \geq 2$, then $g \in t^G \cdot (t')^G$.*

Proof. Suppose $\chi \in \mathrm{Irr}(G)$ is such that

$$\chi(t)\chi(t') \neq 0. \tag{2.9}$$

By [GLBST, Proposition 8.4], the two tori are weakly orthogonal, and hence $\chi = \chi^\lambda$ is a unipotent character labelled by a partition $\lambda \vdash n$. Then by Proposition 2.5, λ is one of the following 6 partitions:

$$(n),\ \lambda_1 := (n-1,1),\ \lambda_2 := (n-2,1^2),$$
$$\lambda_4 := (n-4,4),\ \lambda_5 := (n-5,3,2),\ \lambda_6 := (n-6,2^3)$$

or their dual partitions λ_i, $7 \leq i \leq 12$; moreover,

$$\chi^\lambda(t)\chi^\lambda(t') = \pm 1 \tag{2.10}$$

in all these cases. Let $\chi_i := \chi^{\lambda_i}$ for $i \geq 2$. Since $n \geq 43$, χ_i with $i = 4,5,6$ has level $i \leq \sqrt{n-3/4} - 1/2$ by [GLT, Theorem 3.9], so

$$\frac{|\chi_i(g)|}{\chi_i(1)} \leq \frac{2.43}{\chi_i(1)^{1/n}} \tag{2.11}$$

by [GLT, Theorem 1.6]; furthermore, with $q := 2$, we have

$$\chi_i(1) > q^{in-i^2-3} \tag{2.12}$$

by [GLT, Theorem 1.2]. On the other hand, χ_1 is a unipotent Weil character, and using the character formula [TZ1, Lemma 4.1] and the assumption $\mathsf{supp}(g) \geq 2$, one can show that

$$|\chi_1(g)| \leq \frac{q^{n-2}+q^2}{q+1} < q^{n-3},\ \frac{|\chi_1(g)|}{\chi_1(1)} \leq \frac{q^{n-2}+q^3}{q^n-q}. \tag{2.13}$$

Next, as shown in [Ma2, Table 7.1], $\chi_2 = \chi_1\overline{\chi}_1 - 1_G$ with $\chi_2(1) > q^{2n-4}$. Together with equation (2.13), this implies that

$$\frac{|\chi_2(g)|}{\chi_2(1)} < \frac{q^{2n-6}}{q^{2n-4}} = \frac{1}{q^2}. \tag{2.14}$$

Since $n \geq 43$, it now follows from equations 2.11–2.14 that

$$\sum_{i=1,2,4,5,6} \frac{|\chi_i(g)|}{\chi_i(1)} < \frac{q^{n-2}+q^3}{q^n-q} + \frac{1}{q^2} + \sum_{i=4,5,6} \frac{2.43}{q^{(in-i^2-3)/n}} < 0.899. \tag{2.15}$$

Consider any j with $7 \leq j \leq 12$. Then χ_j extends to the unipotent characters ψ_j of $\mathrm{GU}_n(q)$ labelled by the same partition λ_j, which is dual to (n) or one of the partitions λ_i with $i \in \{1,2,4,5,6\}$. By [GLT, Proposition 4.3], ψ_j is the Alvis-Curtis dual of the unipotent character of $\mathrm{GU}_n(q)$ labelled by the latter partition. By explicitly writing down the degrees of χ_j with $7 \leq j \leq 12$ using [Ca, §13.8], or by applying [Al, Corollary (3.6)], we can check that $\chi_j(1) = \psi_j(1) > q^{n(n-1)/2-14}$. Using [LST1, Proposition 6.2.1] as in the proof of equation (2.8), we have

$$|\chi(g)|/\chi(1) < q^{-(n-31)/2} < 0.016$$

for all χ_j with $7 \le j \le 12$. It now follows from equations (2.10) and (2.15) that

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(t)\chi(t')\overline{\chi(g)}}{\chi(1)} \right| \ge 1 - 0.899 - 6 \cdot 0.016 = 0.005,$$

so $g \in t^G \cdot (t')^G$. □

3. Other classical types: symbols, hooks and cohooks

To treat the unipotent characters of finite simple groups of orthogonal and symplectic types, we use Lusztig's theory of symbols [Lu2]. For a subset $X \subseteq \mathbb{Z}_{\ge 0}$, we define the shift $\mathcal{S}(X) = \{0\} \cup \{x+1 \mid x \in X\}$. If X is finite, we define the *inefficiency* of X to be the nonnegative integer

$$i(X) = -\binom{|X|}{2} + \sum_{x \in X} x. \tag{3.1}$$

Thus, $i(\mathcal{S}(X)) = i(X)$. Every finite X is uniquely of the form $\mathcal{S}^m(X_0)$ for some X_0 (possibly empty) that does not contain 0. For such an X_0, we have $i(X_0) \ge |X_0|$ by equation (3.1). Hence, subject to $i(X) \le j$ for any fixed j, we have $\sum_{x \in X_0} x \le \binom{j+1}{2}$ again by equation (3.1), so there are only finitely many, indeed at most $2^{j(j+1)/2}$, possibilities for X_0. More generally, for any given j, k, the number of X with $i(X) \le j$ and $|X| \le k$ is at most

$$2^{j+k(k-1)/2} \tag{3.2}$$

(since $\sum_{x \in X} x \le j + k(k-1)/2$ by equation (3.1)).

A *d-hook* in X is an element $x \in X$ such that $x - d \in \mathbb{Z}_{\ge 0} \setminus X$; in what follows, we also label this hook by $(x - d, x)$. If x is a d-hook of X, then *removing the d-hook* x means replacing x by $x - d$ in X. The resulting set X' satisfies $i(X') = i(X) - d$. In particular, if X contains a d-hook, then $i(X) \ge d$. If $x - d \in X$ and $x \notin X$, then *adding the d-hook* x to X means replacing $x - d$ with x.

We recall that a *symbol* is an ordered pair (X, Y) of finite subsets of $\mathbb{Z}_{\ge 0}$. We define an equivalence relation of symbols by imposing the relations $(X, Y) \sim (Y, X)$ and $(X, Y) \sim (\mathcal{S}(X), \mathcal{S}(Y))$ and taking transitive closure. If $X = Y$, the symbol is *degenerate*. We will say a symbol is *minimal* if $0 \notin X \cap Y$; in particular, every symbol is equivalent to at least one minimal symbol. The *rank* of a symbol is given by

$$r = -\left\lfloor \frac{(|X| + |Y| - 1)^2}{4} \right\rfloor + \sum_{x \in X} x + \sum_{y \in Y} y = i(X) + i(Y) + \left\lfloor \frac{(|X| - |Y|)^2}{4} \right\rfloor, \tag{3.3}$$

so equivalent symbols have the same rank.

For any q, the unipotent representations of orthogonal and symplectic groups of Lie type of rank r for specified q are given by equivalence classes of symbols of rank r; classes of symbols with $|X| - |Y|$ odd correspond to representations of groups of type B_r and C_r, and those with $|X| - |Y|$ divisible by 2 but not 4, correspond to representations of groups of type ${}^2D_r$. Those with $|X| - |Y|$ divisible by 4 correspond to representations of type D_r, with the additional proviso that each *degenerate* symbol class – that is, where $X = Y$ – corresponds to a pair of unipotent representations for groups of type D_r. We note that the total number of minimal symbols (X, Y) of rank $\le s$ (regardless of congruences modulo 4 of the *defect* $||X| - |Y||$) is at most

$$A(s) := 2^{5s(s+1)/2+1}. \tag{3.4}$$

Indeed, since the symbol is minimal, we have that either $0 \notin X$ or $0 \notin Y$. Suppose for instance that $0 \notin X$. Then $|X| \le i(X) \le s$, and there are at most $2^{s(s+1)/2}$ possibilities for X by equation (3.2). Next,

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

equation (3.3) shows that $i(Y) \le s$ and $s \ge \lfloor (|X| - |Y|)^2/4 \rfloor \ge (|Y| - |X|)^2/4 - 1/4$, so

$$|Y| \le |X| + \lfloor \sqrt{4s+1} \rfloor \le 2s + 1.$$

Hence the number of possibilities for Y is at most $2^{s+s(2s+1)}$ by equation (3.2).

By a d-hook of a symbol (X, Y), we mean either a d-hook of X or a d-hook of Y. By a *d-cohook* of (X, Y), we mean either an element $x \in X$ such that $x - d \in \mathbb{Z}_{\ge 0} \setminus Y$ or $y \in Y$ such that $y - d \in \mathbb{Z}_{\ge 0} \setminus X$; again, we will sometimes label this cohook by $(x - d, x)$. *Removing a d-cohook $x \in X$ from the symbol* (X, Y) means removing x from X and adding $x - d$ to Y and likewise for removing a d-cohook $y \in Y$; from the middle term of equation (3.3), it is clear that either way, the effect is to reduce the rank of the symbol by d. Likewise, if $x - d \in Y$ and $x \notin X$ (respectively, $y - d \in X$ and $y \notin Y$), we can reverse this operation and *add the cohook x* (respectively, y) to the symbol (X, Y).

We also note that, for a fixed $k \in \mathbb{Z}_{\ge 1}$ and a fixed minimal symbol $\Lambda = (X, Y)$ of rank $r \ge k$, both the number of $(r-k)$-hooks in Λ and the number of $(r-k)$-cohooks in Λ are at most

$$A'(k) := (4k+2)A(k) + 2. \tag{3.5}$$

Indeed, let's consider the case of hooks, the other case being essentially the same. It suffices to show that the number of $(r-k)$-hook (x, y) with $y = x + (r-k) \in X$ is at most $(2k+1)A(k) + 1$. Indeed, if $x > 0$, then removing the hook yields a new symbol $\Lambda' = (X', Y)$ of rank k, which is also minimal. Now Λ is obtained from Λ' by adding the hook (x, y) in X', and, given Λ', there are at most $|X'| \le (2k+1)$ possibilities for x; thus the total number of such possibilities is $\le (2k+1)A(k)$ by equation (3.4). Now we add 1 to the bound to account for the possible $(r-k)$-hook $(0, r-k)$ in X.

Next we recall that for G, an orthogonal or symplectic group (of simply connected type) defined over $\mathbb{F}_q$, the degree of the unipotent representation of G labelled by the symbol $S = (X, Y)$ is given by

$$q^{a(S)} \frac{|G|_{q'}}{2^{b(S)} \prod_{(b,c) \text{ hook}} (q^{c-b} - 1) \prod_{(b,c) \text{ cohook}} (q^{c-b} + 1)} \tag{3.6}$$

for some integers $a(S), b(S) \ge 0$ (see [Ma1, Remarks 3.12 and 6.8]).

Proposition 3.1. *For $k, k' \in \mathbb{Z}_{\ge 1}$, let*

$$B(k, k') := A(k + k') + (4k + 2k' + 3)A(k) + (4k' + 2k + 3)A(k'),$$

with $A(k)$ as defined in equation (3.4). Then the following statements hold:

(i) *If $k \ne k'$ are fixed, there exists a bound $B_1 \le B(k, k')$ such that for each r, there are at most B_1 minimal symbols of rank r that contain both an $(r-k)$-hook and an $(r-k')$-hook.*
(ii) *If $k \ne k'$ are fixed, there exists a bound $B_2 \le B(k, k')$ such that for each r, there are at most B_2 minimal symbols of rank r that contain both an $(r-k)$-cohook and an $(r-k')$-cohook.*
(iii) *If k, k' are fixed (and possibly equal), there exists a bound $B_3 \le B(k, k')$ such that for each r, there are at most B_3 minimal symbols of rank r that contain both an $(r-k)$-hook and an $(r-k')$-cohook.*

Proof. We treat only the case of two hooks, the other two cases being essentially the same.

If at least one of the hooks is of the form (x_1, x_2), where $x_1 > 0$, then removing that hook from (X, Y) leaves a minimal symbol (X', Y') of rank k' or k, of which there are at most $A(k')$, respectively $A(k)$, possibilities. In the first case, the proof of equation (3.4) shows that $|X'| + |Y'| \le 3k' + 1$; moreover, (X, Y) is obtained from (X', Y') by adding an $(r-k)$-hook, the number of which is at most $|X'| + |Y'|$. Hence the number of (X, Y) arising this way is at most $(3k'+1)A(k') + (3k+1)A(k)$. We may therefore assume without loss of generality that the two hooks are $(0, r-k)$ and $(0, r-k')$.

By equation (3.4), there are at most $A(k+k')$ minimal symbols of rank $\le k + k'$. We may now assume that $r > k + k'$, so it is impossible to remove both an $(r-k)$-hook and an $(r-k')$-hook (removing these two hooks would yield a symbol of rank $r - (r-k) - (r-k') = k + k' - r < 0$, which is absurd).

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

This means the two hooks $(0, r-k)$ and $(0, r-k')$ must be both in X or both in Y. Without loss of generality, we may assume both hooks are in X. Now, all integers in $[1, r-k-k'-1]$ must belong to X since it is impossible to remove the two hooks $(0, r-k')$ and $(i, r-k)$ from the rank r symbol (X, Y) for $1 \le i < r-k-k'$ (removing these two hooks would yield a symbol of rank $k+k'-r+i < 0$). Likewise, $[0, r-k-k'-1] \subseteq Y$ since it is impossible to remove both the hook $(0, r-k')$ and the cohook $(i, r-k)$ from (X, Y).

Removing $(0, r-k)$ from (X, Y) leads to a symbol (X_1, Y_1) of rank k, where both X_1 and Y_1 contain $[0, r-k-k'-1]$ but $r-k \notin X_1$. It must therefore be of the form $(\mathcal{S}^j(X_2), \mathcal{S}^j(Y_2))$ for some integer j in the interval $[r-k-k'-1, r-k-1]$ and some minimal symbol (X_2, Y_2) of rank k. Equivalently, (X, Y) is obtained from (X_2, Y_2) by shifting by j and then adding the $(r-k)$-hook $(0, r-k)$. The number of possibilities for (X_2, Y_2) is at most $A(k)$, and the number of possibilities for j is at most $k'+1$. Counting the symmetry of X and Y and using $k < k'$, we see that the total number of possibilities for (X, Y) is at most $B(k, k')$. (Note that in the case of (iii), we have 4 possible locations, in X or in Y, for the hook and the cohook, and this leads to an increase in $B(k, k')$ to account for this.) □

Every conjugacy class of maximal tori of a group of type B_r, C_r, D_r or ${}^2D_r$ can be identified with a conjugacy class in $W_r = C_2 \wr \mathsf{S}_r$. Any $\alpha \in W_r$ is determined up to conjugacy by the cycle lengths of its image in S_r and the sign ± 1 attached to each cycle. Therefore, up to conjugacy, such a maximal torus is determined by a partition of r and a sign for each part.

Proposition 3.2. *Let k and k' be fixed integers. Let*

$$T = T^{\epsilon_1, \dots, \epsilon_p}_{d_1, \dots, d_p}, \quad T' = T^{\epsilon'_1, \dots, \epsilon'_{p'}}_{d'_1, \dots, d'_{p'}},$$

with $\epsilon_i, \epsilon'_i = \pm 1$, be a pair of weakly orthogonal maximal tori of an orthogonal or symplectic group G of rank r defined over $\mathbb{F}_q$, and let $t, t' \in G$ denote regular elements of T, T', respectively. Suppose that

$$r - d_1 = k, \quad r - d'_1 = k', \quad (\epsilon_1, k) \neq (\epsilon'_1, k').$$

Then the following statements hold:

(i) *The number of irreducible characters χ of G for which $\chi(t)\chi(t') \neq 0$ is bounded by $2B(k, k')$, with $B(k, k')$ as defined in Proposition 3.1.*

(ii) *Assume in addition that*
   (a) *either at least one of $\{\epsilon_1, \dots, \epsilon_p\}$ is -1 or at least one of $\{d_1, \dots, d_p\}$ is odd, and*
   (b) *either at least one of $\{\epsilon'_1, \dots, \epsilon'_{p'}\}$ is -1 or at least one of $\{d'_1, \dots, d'_{p'}\}$ is odd,*
   if G is of type D_r. Then the values $|\chi(t)\chi(t')|$ are also bounded effectively and independently of anything but k and k'; see equation (3.7).

Proof. As T and T' are weakly orthogonal, by [LST1, Proposition 2.2.2], we need only consider unipotent characters χ. Any such character is associated with an equivalence class of symbols of rank r. Let (X, Y) represent such a class. By [LM, Theorem 3.3], the values $\chi(t)$ and $\chi(t')$ are independent of the choices of t and t'; moreover $\chi(t) = 0$ unless (X, Y) has a d_1-hook assuming $\epsilon_1 = 1$, respectively a d_1-cohook assuming $\epsilon_1 = -1$. Similarly, $\chi(t') = 0$ unless (X, Y) has a d'_1-hook assuming $\epsilon'_1 = 1$, respectively a d'_1-cohook assuming $\epsilon'_1 = -1$. By Proposition 3.1, the number of possibilities for (X, Y) is bounded by $B(k, k')$; in particular, the number of possibilities for χ is bounded by $2B(k, k')$. By equation (3.5), (X, Y) has at most $A'(k)$ d_1-hooks and at most $A'(k')$ d'_1-cohooks. Removal of such a hook or cohook leads to a unipotent (or sum of two unipotent characters in the degenerate case) character of a Levi subgroup of G of semisimple rank k or k', evaluated at the same regular elements t and t', and these values can be bounded purely in terms of k and k', say by $2W(k)$, respectively $2W(k')$, for the largest order $W(k)$ and $W(k')$ of Weyl groups of such ranks; see [GM1, Theorem 5.4] and [LTT, Proposition 5.2]. Note that the factor 2 is added to account for the degenerate symbols obtained after

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

a removal. Hence, [LM, Theorem 3.3] implies that the character values $\chi(t)$ and $\chi(t')$ also belong to finite sets independent of r, and

$$|\chi(t)\chi(t')| \leq 4W(k)W(k')A'(k)A'(k') \tag{3.7}$$

if none of (X, Y) is degenerate. In the case some (X, Y) is degenerate, which can happen only when G is of type D_r, then our extra assumption ensures that both t and t' are nondegenerate. As mentioned in [LM, §3.4], the two unipotent characters corresponding to a degenerate symbol take the same values at nondegenerate regular semisimple elements, and their sum is still governed by [LM, Theorem 3.3], whence our statement follows in this case as well. □

4. Character estimates in groups of type D_n and ${}^2D_n$

Lemma 4.1. *Let q be an odd prime power, and let $G = \Omega^{\epsilon}_{2n}(q)$ with $n \geq 4$ and $\epsilon = \pm$. Let*

$$T < \mathrm{SO}^{\alpha}_{2a}(q) \times \mathrm{SO}^{\beta}_{2b}(q)$$

be a maximal torus of type $T^{\alpha,\beta}_{a,b}$ in G with $1 \leq a < b$ and $n = a + b$. Then we can find a regular semisimple element $g = \mathrm{diag}(u, v) \in T$ with $u \in \mathrm{SO}^{\alpha}_{2a}(q)$ having order $q^a - \alpha$ and $v \in \mathrm{SO}^{\beta}_{2b}(q)$ having order $q^b - \beta$.

Proof. First we consider the maximal torus $T^{\alpha}_a = \langle x\rangle \cong C_{q^a-\alpha}$ in $\mathrm{SO}^{\alpha}_{2a}(q)$. If $\alpha = +$ or if $\alpha = -$ but $2 \nmid a$, then, as shown in [TZ2, Lemma 8.14], $T^{\alpha}_a \cap \Omega^{\alpha}_{2a}(q) = \langle x^2\rangle$. On the other hand, if $\alpha = -$ and $2|a$, then as $1 = (-1)^{a(q-1)/2}$, by [KL, Proposition 2.5.13], we have $\mathrm{SO}^{\alpha}_{2a}(q) = \langle z\rangle \times \Omega^{\alpha}_{2a}(q)$ for a central involution z, which is contained in T^{α}_a. Since $C_{q^a-\alpha} \cong C_{(q^a-\alpha)/2} \times C_2$ with $2 \nmid (q^a - \alpha)/2$, we again see that $T^{\alpha}_a \cap \Omega^{\alpha}_{2a}(q) = \langle x^2\rangle$.

Let $T^{\beta}_b = \langle y\rangle \cong C_{q^b-\beta}$. By the above, $x^2, y^2 \in G$, but $x \in \mathrm{SO}^{\alpha}_{2a}(q) \setminus \Omega^{\alpha}_{2a}(q)$ and $y \in \mathrm{SO}^{\beta}_{2b}(q) \setminus \Omega^{\beta}_{2b}(q)$. We can now choose $g = xy$. As $q \geq 3$ and $a < b$, g has a simple spectrum acting on the natural module $V = \mathbb{F}^{2n}_q$ of G and so is regular unless $(q, \alpha, a) = (3, +, 1)$. But even in this exceptional case, $\mathbf{C}_{\mathrm{SO}(V\otimes\overline{\mathbb{F}}_q)}(g)^{\circ}$ is still a torus of type $T_{1,n-1}$, so g is again regular. □

Proposition 4.2. *Let $G = \mathrm{Spin}^{\epsilon}_{2n}(q)$ with $n \geq 4$ and $\epsilon = \pm$. Then the following statements hold:*

(i) *If $2|n$ and $\epsilon = -$, then the pair of maximal tori T^-_n and $T^{+,-}_{n-1,1}$ is weakly orthogonal.*
(ii) *If $a \in \mathbb{N}$ and $n \geq 2a + 2$, then the pair of maximal tori $T^{-,-\epsilon}_{n-a,a}$ and $T^{-,-\epsilon}_{n-a-1,a+1}$ is weakly orthogonal.*

Proof. We follow the proof of [LST1, Proposition 2.6.1]. In this case, the dual group G^* is the adjoint group $\mathrm{PCO}(V)^{\circ}$, where $V = \mathbb{F}^{2n}_q$ is endowed with a quadratic form Q of type ϵ, $G^* = H/\mathbf{Z}(H)$, and $H = \mathrm{CO}(V)^{\circ} := \mathrm{CO}_{2n}(q)^{\circ}$ (as defined on [Ca, pp. 39, 40]). Consider the complete inverse images in H of the tori dual to the given two tori, and assume g is an element belonging to both of them. We need to show that $g \in \mathbf{Z}(H)$. We will consider the spectrum S of the semisimple element g on V as a multiset. Let $\gamma \in \mathbb{F}^{\times}_q$ be the *conformal coefficient* of g – that is, $Q(g(v)) = \gamma Q(v)$ for all $v \in V$.

In the case of (i), S can be represented as the multiset X but also as the join of multisets $Z \sqcup T$, where

$$X := \{x, x^q, \ldots, x^{q^{n-1}}, \gamma x^{-1}, \gamma x^{-q}, \ldots, \gamma x^{-q^{n-1}}\},$$
$$Z := \{z, z^q, \ldots, z^{q^{n-2}}, \gamma z^{-1}, \gamma z^{-q}, \ldots, \gamma z^{-q^{n-2}}\},\quad T := \{t, \gamma t^{-1}\}$$

for some $x, z, t \in \overline{\mathbb{F}}^{\times}_q$ with $x^{q^n+1} = \gamma = t^{q+1}$ and $z^{q^{n-1}-1} = 1$. Since $|X| = 2n > |Z|$, we may assume that $x \in X \cap T$, whence $x^{q^n+1} = x^{q+1} = \gamma$. As $2|n$, it follows that

$$x^{q^n-1} = (\gamma^{q-1})^{(q^n-1)/(q^2-1)} = 1,$$

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

whence $\gamma = x^2$. In turn, this implies that $x^{q+1} = x^2$ – that is, $x \in \mathbb{F}_q^\times$. Since we now have $S = X = \{\underbrace{x, x, \ldots, x}_{2n}\}$, $g \in \mathbf{Z}(H)$.

In the case of (ii), S can be represented as the joins $X \sqcup Y$ and $Z \sqcup T$, where

$$\begin{aligned}
X &:= \{x, x^q, \ldots, x^{q^{n-a-1}}, \gamma x^{-1}, \gamma x^{-q}, \ldots, \gamma x^{-q^{n-a-1}}\},\\
Y &:= \{y, y^q, \ldots, y^{q^{a-1}}, \gamma y^{-1}, \gamma y^{-q}, \ldots, \gamma y^{-q^{a-1}}\},\\
Z &:= \{z, z^q, \ldots, z^{q^{n-a-2}}, \gamma z^{-1}, \gamma z^{-q}, \ldots, \gamma z^{-q^{n-a-2}}\},\\
T &:= \{t, t^q, \ldots, t^{q^a}, \gamma t^{-1}, \gamma t^{-q}, \ldots, \gamma t^{-q^a}\}
\end{aligned}$$

for some $x, y, z, t \in \bar{\mathbb{F}}_q^\times$ with $x^{q^{n-a}+1} = \gamma = z^{q^{n-a-1}+1}$, and $y^{q^a+\epsilon} = \gamma = t^{q^{a+1}+\epsilon}$ if $\epsilon = +$ and $y^{q^a+\epsilon} = 1 = t^{q^{a+1}+\epsilon}$ if $\epsilon = -$. Since $|X| = 2(n-a) > |T| = 2(a+1)$, we may assume that $x \in X \cap Z$, whence $x^{q^{n-a}+1} = x^{q^{n-a-1}+1} = \gamma$. It follows that

$$x^{q^{n-a-1}(q-1)} = 1,$$

whence $x \in \mathbb{F}_q^\times$, $\gamma = x^2$, and $X = \{\underbrace{x, x, \ldots, x}_{2(n-a)}\}$, $Z = \{\underbrace{x, x, \ldots, x}_{2(n-a-1)}\}$. This also implies that $x \in T$, whence $T = \{\underbrace{x, x, \ldots, x}_{2a+2}\}$ and $g \in \mathbf{Z}(H)$. □

Proposition 4.3. *Let $G = \mathrm{Spin}_{2n}^\epsilon(q)$ with $n \geq 4$ and $\epsilon = \pm$. Then the following statements hold:*

(i) *Suppose $2|n$ and $\epsilon = -$. Then there exist regular semisimple elements $x \in T_n^-$ and $y \in T_{n-1,1}^{+,-}$ such that $x^G \cdot y^G \supseteq G \setminus \mathbf{Z}(G)$.*

(ii) *Suppose $a \in \mathbb{N}$, $a \geq 3$ and $n \geq 2a+2$. Then there exist regular semisimple elements $x \in T_{n-a,a}^{-,-\epsilon}$, $y \in T_{n-a-1,a+1}^{-,-\epsilon}$ and an explicit constant $C = C(a)$ such that if $g \in G$ has $\mathsf{supp}(g) \geq C$, then $g \in x^G \cdot y^G$.*

Proof. (i) As $2|n \geq 4$, by [Zs], we can find a primitive prime divisor ℓ_{2n} of $q^{2n}-1$ and a primitive prime divisor ℓ_{n-1} of $q^{n-1}-1$. It is straightforward to check that T_n^- contains a regular semisimple element x of order divisible by ℓ_{2n}, and likewise $T_{n-1,1}^{+,-}$ contains a regular semisimple element y of order divisible by ℓ_{n-1} (with the projection onto $T_1^- \cong \mathrm{SO}_2^-(q)$ having order $q+1$, which is possible by Lemma 4.1).

Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi(x)\chi(y) \neq 0$. By Proposition 4.2(ii), the pair of tori in question is weakly orthogonal, and hence χ is unipotent, labelled by a minimal symbol

$$S = (X, Y), \quad X = (x_1 < x_2 < \ldots < x_k),\ Y = (y_1 < y_2 < \ldots < y_l).$$

Now, if the denominator of the degree formula in equation (3.6) is not divisible by ℓ_{2n}, then χ has ℓ_{2n}-defect 0, so $\chi(x) = 0$. Similarly, if the denominator of equation (3.6) is not divisible by ℓ_{n-1}, then χ has ℓ_{n-1}-defect 0, and $\chi(y) = 0$. Thus the denominator in equation (3.6) is divisible by both ℓ_{2n} and ℓ_{n-1}.

Observe that if $x_1 = 0$, then by equation (3.3) and the minimality of S, we have

$$n \geq x_k + \sum_{i=1}^{k-1}(i-1) + \sum_{j=1}^{l} j - \frac{(k+l)(k+l-2)}{4} = x_k + \frac{(k-l-2)^2}{4},$$

so $x_k \leq n$, with equality precisely when

$$X = (0, 1, \ldots, k-2, n),\ Y = (1, 2, \ldots, l),\ k = l+2. \tag{4.1}$$

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

On the other hand, if $x_1 \geq 1$, then

$$n \geq x_k + \sum_{i=1}^{k-1} i + \sum_{j=1}^{l} (j-1) - \frac{(k+l)(k+l-2)}{4} = x_k + \frac{(k-l)^2}{4} \geq x_k + 1,$$

so $x_k \leq n-1$. Thus we always have $x_i \leq n$ and, similarly, $y_j \leq n$. Hence, the condition that the denominator of equation (3.6) is divisible by ℓ_{2n} implies that there is an n-cohook n, where we may assume that $n \in X$ and $0 \notin Y$; in particular, equation (4.1) holds. Now, if $l = 0$, then $k = 2$ and $\chi = 1_G$. Assume $l \geq 1$. Since $2|n$, we must also have an $(n-1)$-hook c with $0 \leq c - (n-1) \leq 1$. As $k \geq 3$, we have $0, 1 \in X$ by equation (4.1), so $c \notin X$ – that is, $c \in Y$ and $c - (n-1) \notin Y$. But $1 \in Y$, so $c = n-1 \in Y$. Furthermore, $k - 2 \leq n - 1$, and hence $k \leq n+1$ and $l \leq n-1$ by equation (4.1). It follows that $l = n-1$, so $\chi = \mathsf{St}$, the Steinberg character.

We have shown that 1_G and St are the only two characters in $\mathrm{Irr}(G)$ that are nonzero at both x and y. Now, if $g \in G$ is semisimple, then $g \in x^G \cdot y^G$ by [GT2, Lemma 5.1]. If g is not semisimple, then $\mathsf{St}(g) = 0$, whence

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)} = 1,$$

so $g \in x^G \cdot y^G$ as well.

(ii) The assumption $a \geq 3$ ensures that regular semisimple elements $x \in T^{-,-\epsilon}_{n-a,a}$ and $y \in T^{-,-\epsilon}_{n-a-1,a+1}$ exist. Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi(x)\chi(y) \neq 0$. By Proposition 4.2(ii), the pair of tori in question is weakly orthogonal. Hence, by Proposition 3.2, the number of such characters χ is at most $C_1 = C_1(a)$, and for any such character, $|\chi(x)\chi(y)| \leq C_2 = C_2(a)$ for some explicit functions $C_1(a)$ and $C_2(a)$ of a. Now, choosing $C = \big(481 \log_2(C_1C_2)\big)^2$, for any $g \in G$ with $\mathsf{supp}(g) \geq C$, we have by [LST1, Theorem 1.2.1] that

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)} \right| > 1 - \frac{C_1C_2}{q^{\sqrt{C}/481}} \geq 0,$$

so $g \in x^G \cdot y^G$. □

5. Character estimates in groups of type B_n

In this section, we handle the odd-dimensional orthogonal groups over $\mathbb{F}_q$, for which we also allow q to be even; hence it gives the desired result for symplectic groups in even characteristic. We will need a slight generalisation of the notion of weakly orthogonal tori [MSW], [LST1, Definition 2.2.1]:

Definition 5.1. We say that two $\mathbb{F}$-rational maximal tori T and T' in a connected reductive group $G/\mathbb{F}$ are *centrally orthogonal* if

$$T^*(\mathbb{F}) \cap T'^*(\mathbb{F}) = \mathbf{Z}(G^*(\mathbb{F}))$$

for every choice of dual tori T^* and T'^* in the dual group G^*. This depends only on the types of T and T'.

The following is an analogue of [LST1, Proposition 2.2.2]:

Proposition 5.2. *Let T and T' be centrally orthogonal maximal tori in a connected reductive group $G(\mathbb{F})$, and let $t \in T$ and $t' \in T'$ be regular semisimple elements of $G(\mathbb{F})$. If χ is an irreducible character of $G(\mathbb{F})$ such that $\chi(t)\chi(t') \neq 0$, then there is a (degree 1) character $\alpha \in \mathrm{Irr}(G(\mathbb{F}))$ such that $\chi\alpha$ is unipotent.*

Proof. By [MM, 5.1], if $s \in G(\mathbb{F})$ is semisimple and $\chi(s) \neq 0$, then there exist a maximal torus T and a character $\theta \in \mathrm{Irr}(T(\mathbb{F}))$ such that $R_{T,\theta}(s) \neq 0$, and θ^* belongs to the conjugacy class C_χ. By [DL, 7.2], this implies that s lies in the $G(\mathbb{F})$-conjugacy class of some element of $T(\mathbb{F})$. If $\chi(t)\chi(t') \neq 0$, then there exist $G^*(\mathbb{F})$-conjugate elements θ_1^* and θ_2^* belonging to tori T^* and T'^*, which are dual to tori T and T' containing t and t', respectively. As T^* and T'^* intersect in $\mathbf{Z}(G^*(\mathbb{F}))$, this means $\theta_1^*, \theta_2^* \in \mathbf{Z}(G^*(\mathbb{F}))$, and the statement follows from [DM, Proposition 13.30]. □

Proposition 5.3. *The following statements hold for* $G = \mathrm{SO}_{2n+1}(q)$ *with* $n \geq 3$*:*

(i) *Define* $\kappa := (-1)^n$*. Then the pair of maximal tori* $T_n^{-\kappa}$ *and* $T_{n-1,1}^{\kappa,-}$ *is weakly orthogonal when* $2|q$ *and centrally orthogonal if* $2 \nmid q$.

(ii) *If* $2 \nmid n \geq 5$*, then the pair of maximal tori* T_n^- *and* $T_{n-2,2}^{+,-}$ *is weakly orthogonal when* $2|q$ *and centrally orthogonal if* $2 \nmid q$.

(iii) *If* $2|n \geq 8$*, then the pair of maximal tori* $T_{n-2,2}^{-,-}$ *and* $T_{n-3,3}^{+,+}$ *is weakly orthogonal when* $2|q$ *and centrally orthogonal if* $2 \nmid q$.

Proof. In this case, the dual group G^* is $\mathrm{Sp}(V)$, where $V = \mathbb{F}_q^{2n}$ is endowed with a symplectic form. Consider any g in the intersection of dual tori, and let S denote the spectrum of g on V as a multiset.

In the case of (i), S can be represented as the multiset X and also as the join of multisets $Z \sqcup T$, where

$$\begin{aligned} X &:= \{x, x^q, \ldots, x^{q^{n-1}}, x^{-1}, x^{-q}, \ldots, x^{-q^{n-1}}\}, \\ Z &:= \{z, z^q, \ldots, z^{q^{n-2}}, z^{-1}, z^{-q}, \ldots, z^{-q^{n-2}}\}, \;\; T := \{t, t^{-1}\}, \end{aligned}$$

for some elements $x, z, t \in \bar{\mathbb{F}}_q^\times$ with $x^{q^n+\kappa} = z^{q^{n-1}-\kappa} = t^{q+1} = 1$. Since $|X| = 2n > |Z|$, we may assume that $x \in X \cap T$, whence $x^{q^n+\kappa} = x^{q+1} = 1$. As $(q+1)|(q^n - \kappa)$, it follows that $x^2 = 1 = x^{q-1}$ – that is, $x \in \mathbb{F}_q^\times$. Since we now have $S = X = \{\underbrace{x, x, \ldots, x}_{2n}\}$, we conclude that $g \in \mathbf{Z}(G^*)$.

In the case of (ii), S can be represented as the multisets X and $Z \sqcup T$, where

$$\begin{aligned} X &:= \{x, x^q, \ldots, x^{q^{n-1}}, x^{-1}, x^{-q}, \ldots, x^{-q^{n-1}}\}, \\ Z &:= \{z, z^q, \ldots, z^{q^{n-3}}, \gamma z^{-1}, z^{-q}, \ldots, \gamma z^{-q^{n-3}}\}, \; T := \{t, t^q, t^{-1}, t^{-q}\} \end{aligned}$$

for some elements $x, z, t \in \bar{\mathbb{F}}_q^\times$ with $x^{q^n+1} = z^{q^{n-2}-1} = t^{q^2+1} = 1$. Since $|X| = 2n > |Z|$, we may assume that $x \in X \cap T$, whence $x^{q^n+1} = x^{q^2+1} = 1$. As $2 \nmid n$, it follows that $x^{q+1} = 1 = x^2$, whence $x \in \mathbb{F}_q^\times$, $X = \{\underbrace{x, x, \ldots, x}_{2n}\}$ and $g \in \mathbf{Z}(G^*)$.

In the case of (iii), S can be represented as the joins $X \sqcup Y$ and $Z \sqcup T$, where

$$\begin{aligned} X &:= \{x, x^q, \ldots, x^{q^{n-3}}, x^{-1}, x^{-q}, \ldots, x^{-q^{n-3}}\}, \; Y := \{y, y^q, y^{-1}, y^{-q}\}, \\ Z &:= \{z, z^q, \ldots, z^{q^{n-4}}, z^{-1}, z^{-q}, \ldots, z^{-q^{n-4}}\}, \; T := \{t, t^q, t^{q^2}, t^{-1}, t^{-q}, t^{-q^2}\}, \end{aligned}$$

for some $x, y, z, t \in \bar{\mathbb{F}}_q^\times$ with $x^{q^{n-2}+1} = y^{q^2+1} = z^{q^{n-3}-1} = t^{q^3-1} = 1$. Since $|X| = 2n - 4 > |T| = 6$, we may assume that $x \in X \cap Z$, whence $x^{q^{n-2}+1} = x^{q^{n-3}-1} = 1$. As $2|n$, it follows that $x^{q+1} = 1 = x^2$, whence $x \in \mathbb{F}_q^\times$ and $X = \{\underbrace{x, x, \ldots, x}_{2n-4}\}$, $Z = \{\underbrace{x, x, \ldots, x}_{2n-6}\}$. This also implies that $x \in T$, whence $T = \{x, x, x, x, x, x\}$ and $g \in \mathbf{Z}(G^*)$. □

In what follows, for any $n \geq 3$, we note that if $2|q$, then $\mathrm{SO}_{2n+1}(q) \cong \mathrm{Sp}_{2n}(q)$ is simple, whereas if $2 \nmid q$, then $[G, G] = \Omega_{2n+1}(q)$ is simple and has index 2 in $G = \mathrm{SO}_{2n+1}(q)$; let sgn denote the linear character of order 2 of G in the latter case.

Proposition 5.4. *There is an explicit constant* $C \in \mathbb{N}$ *such that the following statements hold for* $G = \mathrm{SO}_{2n+1}(q)$ *with* $2|n \geq C$*:*

(i) *There exist regular semisimple elements* $x \in T_n^- \cap [G,G]$ *and* $y \in T_{n-1,1}^{+,-} \cap [G,G]$ *such that* $x^G \cdot y^G = [G,G] \setminus \{e\}$.

(ii) *If in addition* $2 \nmid q$, *then there exists a regular semisimple element* $y' \in T_{n-1,1}^{+,-} \setminus [G,G]$ *such that* $x^G \cdot (y')^G = G \setminus [G,G]$.

Proof. (a) As $2|n \geq 4$, by [Zs], we can find a primitive prime divisor ℓ_{2n} of $q^{2n}-1$ and a primitive prime divisor ℓ_{n-1} of $q^{n-1}-1$. It is straightforward to check that T_n^- contains a regular semisimple element $x \in [G,G]$ of order ℓ_{2n}, and likewise $T_{n-1,1}^{+,-}$ contains a regular semisimple element $y \in [G,G] \cap \Omega_{2n}^-(q)$ of order divisible by ℓ_{n-1} (with the projection onto $T_1^- \cong \mathrm{SO}_2^-(q)$ having order $q+1$, which is possible by Lemma 4.1). If $2 \nmid q$, then by changing y to have the first projection onto $\mathrm{SO}_{2n-2}^+(q)$ of order ℓ_{n-1}, we obtain a regular semisimple element $y' \in T_{n-1,1}^{+,-} \setminus [G,G]$.

(b) Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi(x)\chi(y) \neq 0$ or $\chi(x)\chi(y') \neq 0$ if $2 \nmid q$. By Proposition 5.3(i), the pair of tori in question is centrally orthogonal, and hence either χ or $\chi \cdot \mathsf{sgn}$ is unipotent by Proposition 5.2. Without loss, we may assume that χ is unipotent, labelled by a minimal symbol

$$S = (X,Y), \;\; X = (x_1 < x_2 < \ldots < x_k), \; Y = (y_1 < y_2 < \ldots < y_l),$$

where $k,l \in \mathbb{Z}_{\geq 0}$ and $2 \nmid (k-l)$. Now, if the denominator of the degree formula in equation (3.6) is not divisible by ℓ_{2n}, then χ has ℓ_{2n}-defect 0, so $\chi(x) = 0$. Similarly, if the denominator of equation (3.6) is not divisible by ℓ_{n-1}, then χ has ℓ_{n-1}-defect 0 and $\chi(y) = 0$, as well as $\chi(y') = 0$ when $2 \nmid q$. Thus the denominator in equation (3.6) is divisible by both ℓ_{2n} and ℓ_{n-1}.

Observe that if $x_1 = 0$, then by equation (3.3) and the minimality of S, we have

$$n \geq x_k + \sum_{i=1}^{k-1}(i-1) + \sum_{j=1}^{l} j - \frac{(k+l-1)^2}{4} = x_k + \frac{(k-l-1)(k-l-3)}{4},$$

so $x_k \leq n$, with equality precisely when

$$X = (0,1,\ldots,k-2,n), \; Y = (1,2,\ldots,l), \;\; k-l = 1 \text{ or } 3. \tag{5.1}$$

On the other hand, if $x_1 \geq 1$, then

$$n \geq x_k + \sum_{i=1}^{k-1} i + \sum_{j=1}^{l}(j-1) - \frac{(k+l-1)^2}{4} = x_k + \frac{(k-l)^2-1}{4} \geq x_k,$$

so $x_k \leq n$, with equality precisely when

$$X = (1,2,\ldots,k-1,n), \; Y = (0,1,\ldots,l-1), \;\; k-l = \pm 1. \tag{5.2}$$

Thus we always have $x_i \leq n$ and similarly $y_j \leq n$. Hence, the condition that the denominator of equation (3.6) is divisible by ℓ_{2n} implies that there is an n-cohook n, whence we may assume that $n = x_k \in X$ and $0 \notin Y$. This rules out the case $x_1 \geq 1$, whence equation (5.1) holds. Now, if $k = 1$, then $l = 0$ and $\chi = 1_G$. If $k = 2$, then $l = 1$, $S = \binom{0,n}{1}$, and $\chi(1) = (q^n-1)(q^n+q)/2(q-1)$; denote this unipotent character by χ_1.

Assume $k \geq 3$. Since $2|n$, we must also have an $(n-1)$-hook c with $0 \leq c-(n-1) \leq 1$. As $k \geq 3$, we have $0,1 \in X$ by equation (5.1), so $c \notin X$ – that is, $c \in Y$ and $c-(n-1) \notin Y$. In particular, $l \geq 1$, and hence $1 \in Y$ and $c = n-1 \in Y$. Furthermore, $k-2 \leq n-1$, and hence $k \leq n+1$ but $l \leq n-1$. By equation (5.1), we have

- either $(k,l) = (n+1,n)$, $S = \binom{0,1,\ldots,n-1,n}{1,2,\ldots,n}$, $\chi = \mathsf{St}$, the Steinberg character, or
- $(k,l) = (n,n-1)$, and $S = \binom{0,1,\ldots,n-2,n}{1,2,\ldots,n-1}$; denote this unipotent character by χ_2.

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

(c) We have shown that, up to tensoring with sgn when $2 \nmid q$, $\chi_0 = 1_G$, St, χ_1 and χ_2 are the only four characters in $\mathrm{Irr}(G)$ that are nonzero at both x and y, respectively at x and y' when $2 \nmid q$. It is clear that

$$\chi_0(x)\chi_0(y) = \chi_0(x)\chi_0(y') = 1, \quad |\mathsf{St}(x)\mathsf{St}(y)| = |\mathsf{St}(x)\mathsf{St}(y')| = 1. \tag{5.3}$$

To bound $|\chi_1(x)\chi_1(y)|$ and $|\chi_1(x)\chi_1(y')|$, we follow the proof of [LST1, Proposition 3.4.1], which relies on the main result of [Lu1]. Recall that χ_1 is labelled by $S = \binom{X}{Y} = \binom{0,n}{1}$. Let $Z_1 = \{0, 1, n\}$ be the set of 'singles' and $Z_2 = X \cap Y = \emptyset$. Then the family $\mathcal{F}(\chi_1)$ consists of all irreducible characters $\psi_{S'}$ of the Weyl group W_n labelled by symbols $S' = \binom{X'}{Y'}$ of defect 1, which contain the same entries (with the same multiplicities) as S does (compare [Lu1, Cor. (5.9)]. For the given $S = \binom{0,n}{1}$ (or in fact for all symbols of odd defect with the same set $Z_1 = \{0, 1, n\}$ of 'singles'), we have the following possibilities for S' and the corresponding pair (λ', μ') of (possibly empty) partitions:

$$\begin{cases} S' = \binom{1,n}{0}, \ (\lambda', \mu') = \big((1, n-1), (\emptyset)\big), \\ S' = \binom{0,n}{1}, \ (\lambda', \mu') = \big((n-1), (1)\big), \\ S' = \binom{0,1}{n}, \ (\lambda', \mu') = \big((\emptyset), (n)\big). \end{cases}$$

Let $w, w' \in \mathsf{W}_n$ correspond to x, respectively to y and y'. Recalling the construction of $\psi_{S'}$ [LST1, (3.2.1)], we find that

$$\psi_{S'}(w) = -1, \ 0, \ -1, \ \psi_{S'}(w') = 0, \ -1, \ -1,$$

respectively. It follows from [Lu1, Cor. (5.9)] that

$$|\chi_1(x)| \leq 1, \ |\chi_1(y)| = |\chi_1(y')| \leq 1. \tag{5.4}$$

To bound the character values for χ_2, we use the Alvis-Curtis duality functor D_G, which sends any irreducible character of G to an irreducible character of G up to a sign (compare [DM, Corollary 8.15]). Using Theorems 1.1 and 1.2 of [Ng], we see that χ_1 is the unique unipotent character of its degree, so, by inspecting [ST, Table 1], χ_1 is a constituent of the rank 3 permutation action of G on singular 1-spaces of its natural module; also, χ_1 is irreducible over $[G, G]$. Hence χ_1 is also a constituent of the permutation character 1_B^G, where B is a Borel subgroup of G, and the same is true for 1_G and St. For each irreducible constituent φ of 1_B^G, there is a polynomial $d_\varphi(X) \in \mathbb{Q}[t]$ in the variable t (the so-called *generic degree*; compare [Ca, §13.5], which depends only on the Weyl group of G but not on q) such that $\varphi(1) = d_\varphi(q)$. According to Theorem (1.7) and Proposition (1.6) of [Cu], D_G permutes the irreducible constituents of 1_B^G. Moreover, there is an integer N such that

$$d_{D_G(\varphi)}(t) = t^N d_\varphi(t^{-1}). \tag{5.5}$$

It is well known (see, for example, Corollary 8.14 and Definition 9.1 of [DM]) that D_G interchanges 1_G and St. Since $\mathsf{St}(1) = q^{n^2}$, (5.5) applied to $\varphi = 1_G$ yields that $N = n^2$. Applying (5.5) to $\varphi = \chi_1$, we now obtain that

$$D_G(\chi_1)(1) = q^{n^2-2n}\chi_1(1). \tag{5.6}$$

Furthermore, in the case of a rational torus T, $D_T(\lambda) = \lambda$ for all $\lambda \in \mathrm{Irr}(T)$; see [DM, Definition 8.8]. Applying this and [DM, Corollary 8.16] to $T = \mathbf{C}_G(x)$, we now see that

$$D_G(\chi)(x) = \pm(D_T \circ \mathrm{Res}_T^G)(\chi)(x) = \pm\chi(x).$$

Similarly, $D_G(\chi)(y) = \pm\chi_1(y)$ and $D_G(\chi)(y') = \pm\chi(y')$. It follows that if χ_2 is nonzero at both x, y (respectively at x, y'), then so is $D_G(\chi_2)$. It follows that either $\chi_2(x)\chi_2(y) \neq 0$, in which case

$\chi_2 = D_G(\chi_1)$ and equation (5.4) yields

$$|\chi_2(x)\chi_2(y)| = |\chi_2(x)\chi_2(y')| \le 1, \tag{5.7}$$

or $\chi_2(x)\chi_2(y) = 0$, in which case equation (5.7) is automatic.

(d) Now, if $g \in [G,G]$ is semisimple, then $g \in x^G \cdot y^G$ by [GT2, Lemma 5.1]. Suppose $g \in [G,G]$ is not semisimple. Then $\mathsf{St}(g) = 0$. If $2 \nmid q$, then $\mathsf{sgn}(g) = \mathsf{sgn}(x) = \mathsf{sgn}(y) = 1$. This shows that χ and $\chi \cdot \mathsf{sgn}$ take the same values at x, y and g for any $\chi \in \mathrm{Irr}(G)$. Since the index of any proper subgroup in $[G,G]$ is $> q^{2n-1}$ (see [TZ1, §9]), it follows that $|\chi(g)| \le |G|^{1/2}q^{1/2-n}$, so, choosing n large enough, we obtain from equation (5.6) and equation (5.7) that

$$\frac{|\chi_2(x)\chi_2(y)\chi_2(g)|}{\chi_2(1)} < 0.01.$$

Using Gluck's bound $\dfrac{|\psi(g)|}{\psi(1)} \le 0.95$ [Gl] for any nontrivial $\psi \in \mathrm{Irr}([G,G])$, we obtain

$$\frac{1}{\gcd(2,q-1)}\left|\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)}\right| > 1 - 0.95 - 0.01 = 0.04,$$

so $g \in x^G \cdot y^G$.

Finally, consider the case $2 \nmid q$ and $g \in G \setminus [G,G]$. Then $\mathsf{sgn}(x) = 1$ and $\mathsf{sgn}(g) = \mathsf{sgn}(y') = -1$. Again, by choosing n large enough, we obtain from equation (5.6) and equation (5.7) that

$$\frac{|\chi(x)\chi(y')\chi(g)|}{\chi(1)} < 0.001$$

for $\chi = \chi_2, \chi_2 \cdot \mathsf{sgn}, \mathsf{St}, \mathsf{St}\cdot\mathsf{sgn}$. Next, [GT1, Lemma 2.19] together with Gluck's bound imply that

$$|\psi(g)|/\psi(1) \le (3 + 0.95)/4 = 0.9875$$

for any $\psi \in \mathrm{Irr}(G)$ that is irreducible over $[G,G]$ and of degree > 1. Hence,

$$\frac{1}{2}\left|\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(x)\chi(y')\overline{\chi}(g)}{\chi(1)}\right| > 1 - 0.9875 - 0.002 > 0.01,$$

so $g \in x^G \cdot (y')^G$, as stated. □

Proposition 5.5. *There is an explicit constant $C \ge 5$ such that the following statements hold for $G = \mathrm{SO}_{2n+1}(q)$ with $2 \nmid n \ge C$:*

(i) *There exist regular semisimple elements $x \in T_n^+ \cap [G,G]$ and $y \in T_{n-1,1}^{-,-} \cap [G,G]$ such that $x^G \cdot y^G = [G,G] \setminus \{e\}$.*
(ii) *If in addition $2 \nmid q$, then there exists a regular semisimple element $y' \in T_{n-1,1}^{-,-} \setminus [G,G]$ such that $x^G \cdot (y')^G = G \setminus [G,G]$.*

Proof. (a) As $2 \nmid n \ge 5$, by [Zs], we can find a primitive prime divisor ℓ_{2n-2} of $q^{2n-2} - 1$ and a primitive prime divisor ℓ_n of $q^n - 1$. It is straightforward to check that T_n^+ contains a regular semisimple element $x \in [G,G]$ of order ℓ_n, and likewise $T_{n-1,1}^{-,-}$ contains a regular semisimple element $y \in [G,G] \cap \Omega_{2n}^+(q)$ of order divisible by ℓ_{2n-2} (with the projection onto $T_1^- \cong \mathrm{SO}_2^-(q)$ having order $q+1$, which is possible by Lemma 4.1). If $2 \nmid q$, then by changing y to have the first projection onto $\mathrm{SO}_{2n-2}^-(q)$ of order ℓ_{2n-2}, we obtain a regular semisimple element $y' \in T_{n-1,1}^{-,-} \setminus [G,G]$.

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

(b) Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi(x)\chi(y) \neq 0$ or $\chi(x)\chi(y') \neq 0$ if $2 \nmid q$. By Proposition 5.3(i), the pair of tori in question is centrally orthogonal, and hence either χ or $\chi \cdot \mathsf{sgn}$ is unipotent by Proposition 5.2. Without loss, we may assume that χ is unipotent, labelled by a minimal symbol

$$S = (X, Y), \quad X = (x_1 < x_2 < \ldots < x_k),\ Y = (y_1 < y_2 < \ldots < y_l),$$

where $k, l \in \mathbb{Z}_{\geq 0}$ and $2 \nmid (k - l)$. Now, if the denominator of the degree formula in equation (3.6) is not divisible by ℓ_n, then χ has ℓ_n-defect 0, so $\chi(x) = 0$. Similarly, if the denominator of equation (3.6) is not divisible by ℓ_{2n-2}, then χ has ℓ_{2n-2}-defect 0 and $\chi(y) = 0$, as well as $\chi(y') = 0$ when $2 \nmid q$. Thus the denominator in equation (3.6) is divisible by both ℓ_n and ℓ_{2n-2}.

As mentioned in the proof of Proposition 5.4, we always have that $x_i \leq n$ and $y_j \leq n$. Hence, the condition that the denominator of equation (3.6) is divisible by ℓ_n implies that there is an n-hook n, whence we may assume that $n = x_k \in X$ and $0 \notin X$. This implies $x_1 \geq 1$, whence equation (5.2) holds and $k \geq 1$. Now, if $l = 0$, then $k = 1$ and $\chi = 1_G$. If $l = 1$, then $k = 2$, $S = \binom{1,n}{0}$ and $\chi(1) = (q^n + 1)(q^n - q)/2(q - 1)$; denote this unipotent character by χ_1.

Assume $l \geq 2$. Since $2 \nmid n$, we must also have an $(n-1)$-cohook c with $0 \leq c - (n-1) \leq 1$. Here, $0, 1 \in Y$ by equation (5.2), so $c \notin X$ – that is, $c \in Y$ and $c - (n-1) \notin X$. Also by equation (5.2), $l - 1 \geq c$, so $l \geq n$. Hence $k \geq l - 1 > 2$, whence $1 \in X$, implying $c - (n-1) = 0$ and $c = n - 1 \in Y$. Furthermore, $k - 1 \leq n - 1$, and hence $k \leq n$, and thus $l \leq n + 1$. By equation (5.1), we have

- either $(k, l) = (n, n+1)$, $S = \binom{1,2,\ldots,n-1,n}{0,1,\ldots,n}$, $\chi = \mathsf{St}$, the Steinberg character, or
- $(k, l) = (n-1, n)$, and $S = \binom{1,2,\ldots,n-2,n}{0,1,\ldots,n-1}$; denote this unipotent character by χ_2.

(c) We have shown that, up to tensoring with sgn when $2 \nmid q$, $\chi_0 = 1_G$, St, χ_1 and χ_2 are the only four characters of $\mathrm{Irr}(G)$ that are nonzero at both x and y, respectively at x and y', when $2 \nmid q$. It is clear that equation (5.3) holds. To bound $|\chi_1(x)\chi_1(y)|$, let $w, w' \in \mathsf{W}_n$ correspond to x, respectively to y and y'. Repeating the arguments in the proof of Proposition 5.4, we come up with three possibilities for S' and

$$\psi_{S'}(w) = -1,\ 0,\ 1,\ \psi_{S'}(w') = 0,\ -1,\ 1,$$

respectively. It follows from [Lu1, Cor. (5.9)] that equation (5.4) holds in this case.

Using Theorems 1.1 and 1.2 of [Ng], we see that χ_1 is the unique unipotent character of its degree, so, by inspecting [ST, Table 1], χ_1 is a constituent of the rank 3 permutation action of G on singular 1-spaces of its natural module; also, χ_1 is irreducible over $[G, G]$. Hence χ_1 is also a constituent of the permutation character 1_B^G, where B is a Borel subgroup of G. Now, to bound the character values for χ_2, we again follow the proof of Proposition 5.4, using the Alvis-Curtis duality functor D_G. This shows that equation (5.7) holds in this case as well. To finish the proof, we just repeat part (iv) of the proof of Proposition 5.4 verbatim. □

Proposition 5.6. *There exists an explicit constant $C > 0$ such that the following statements hold for $G = \Omega_{2n+1}(q)$ with $n \geq 8$. Let $H := \mathrm{SO}_{2n+1}(q)$, and consider a pair of maximal tori T and T' in H, where*

(i) *if $2|n$, then $T = T^{-,-}_{n-2,2}$ and $T' = T^{+,+}_{n-3,3}$, and*
(ii) *if $2 \nmid n$, then $T = T^{-}_{n}$ and $T' = T^{+,-}_{n-2,2}$.*

Then there exist regular semisimple elements $x \in T \cap G$ and $y \in T' \cap G$ such that $g \in x^H \cdot y^H$ for every element $g \in G$ with $\mathsf{supp}(g) \geq C$.

Proof. Using Lemma 4.1, we can find regular semisimple elements $x \in T \cap G$ and $y \in T' \cap G$. Suppose $\chi \in \mathrm{Irr}(H)$ is such that $\chi(x)\chi(y) \neq 0$. By Proposition 5.3(ii), (iii) the pair of tori in question is weakly orthogonal when $2|q$ and centrally orthogonal when $2 \nmid q$. Hence, either χ is unipotent or $2 \nmid q$ and $\chi \cdot \mathsf{sgn}$ is unipotent. In the case $2 \nmid q$, note that $\mathsf{sgn}(x) = \mathsf{sgn}(y) = \mathsf{sgn}(g) = 1$ for all $g \in G$. By Proposition 3.2, the number of such characters χ is at most some explicit C_1, and for any such character,

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

$|\chi(x)\chi(y)| \le C_2$ for some explicit C_2. Now, choosing $C = \left(481 \log_2(C_1C_2)\right)^2$, for any $g \in G$ with $\mathsf{supp}(g) \ge C$, we have by [LST1, Theorem 1.2] that

$$\frac{1}{\gcd(2, q-1)}\left|\sum_{\chi \in \mathrm{Irr}(H)} \frac{\chi(x)\chi(y)\overline{\chi}(g)}{\chi(1)}\right| > 1 - \frac{C_1C_2}{q^{\sqrt{C}/481}} \ge 0,$$

so $g \in x^H \cdot y^H$. □

6. The main results on derangements

6.1. Some reductions

In [CC], it is shown that the proportion $\delta(G)$ of derangements in a finite transitive permutation group G of degree n is at least $1/n$. It turns out that if G is simple, the proportion of derangements is bounded away from zero. Indeed, we have the following theorem by Fulman and Guralnick (see [FG3, 1.1] and the references therein).

Theorem 6.1. *There exists an absolute constant $\epsilon > 0$ such that if G is a finite simple transitive permutation group and $\mathcal{D} = \mathcal{D}(G) \subset G$ is the set of derangements in G, then*

$$|\mathcal{D}| \ge \epsilon |G|.$$

This confirms a conjecture of Boston and Shalev.

In fact, it is shown in [FG3] that $\epsilon = 0.016$ will do, provided $|G| \gg 0$.

Clearly, Theorem A holds in the case G is a cyclic group of odd prime order. Its proof for nonabelian simple groups will occupy the rest of the section.

It is also clear that the set $\mathcal{D}$ is a normal subset whose size is bounded below by Theorem 6.1. More generally, products of normal subsets in simple groups are the main subject of [LST2], which we now briefly describe.

Let $\epsilon > 0$ be a constant. Let G be a nonabelian finite simple group and S and T normal subsets of G such that $|S|$, $|T| > \epsilon|G|$. We are particularly interested in the following questions:

Question 1. Does every element in $G \setminus \{e\}$ lie in ST if $|G|$ is sufficiently large?

Question 2. Does the ratio between the number of representations of each $g \in G \setminus \{e\}$ and $\frac{|S|\,|T|}{|G|}$ tend uniformly to 1 as $|G| \to \infty$?

The main results of [LST2] are summarised below. An affirmative answer to Question 2 implies an affirmative answer to Question 1 (and, of course, the same holds in the special case $S = T$).

Theorem 6.2. [LST2, Theorem A]

(i) *The answers to Questions 1 and 2 are negative if G is allowed to range over all finite simple groups or even just over the alternating groups, or just over all projective special linear groups.*
(ii) *In the $S = T$ case, the answer to Question 2 is still negative for alternating groups.*
(iii) *In the $S = T$ case, the answer to Question 1 is positive for alternating groups.*
(iv) *If G is a group of Lie type of bounded rank, then the answers to Questions 1 and 2 are both positive.*

As shown in Theorem 6.2(i), the answer to Question 1 is in the negative if one varies over all (sufficiently large) finite simple groups. However, one can still prove the following result, where $m(G)$ denotes the smallest degree of a nontrivial complex character of a finite group G, $\mathbf{U}_G$ the uniform distribution on G and, for any element $g \in G$ and subsets $A, B, C \subseteq G$, $\mathbf{P}_{A,B,C}(g)$ denotes the probability that $xyz = g$, where $x \in A$, $y \in B$ and $z \in C$ are randomly chosen, uniformly and independently. Furthermore, the $L^\infty(f)$ norm of a distribution f on G is $|G| \cdot \max_{x \in G} |f(x)|$.

Corollary 6.3. [LST2, Corollary 7.2] *For finite groups G and subsets $A, B, C \subseteq G$ satisfying*

$$m(G)|A|\,|B|\,|C|/|G|^3 \to \infty$$

as $|G| \to \infty$, we have

$$\|\mathbf{P}_{A,B,C} - \mathbf{U}_G\|_{L^\infty} \to 0 \text{ as } |G| \to \infty.$$

In particular, we have $ABC = G$ for $|G| \gg 0$.

These two conclusions hold when G is a finite simple group and $A, B, C \subseteq G$ are subsets of sizes $\geq \epsilon|G| > 0$ for any fixed $\epsilon > 0$.

An extensive discussion of the motivation behind Question 1 and Question 2, in particular the connections of them and Corollary 6.3 to results of Gowers and others [Go], [NP], [PS], is given in the Introduction of [LST2].

Clearly, Theorem 6.1 and Corollary 6.3 give an immediate proof of the easier three-derangement result:

Proposition 6.4. *For all sufficiently large transitive simple permutation groups G, every permutation in G is a product of three derangements.*

We now prove some preliminary results that reduce the proof of Theorem A to the case G is a simple group of Lie type of unbounded rank.

Let G be as above, and let $H < G$ be a point stabiliser. Recall that $\mathcal{D}(G,H)$ denotes the set of derangements of G in its action on the left cosets of H and that $\mathcal{D}(G,H) = G \setminus \cup_{g \in G} H^g$. Thus, if $M < G$ is a maximal subgroup containing H, then $\mathcal{D}(G,M) \subseteq \mathcal{D}(G,H)$. Hence $\mathcal{D}(G,M)^2 = G$ implies $\mathcal{D}(G,H)^2 = G$. This reduces Theorem A to the primitive case where H is a maximal subgroup of G.

Clearly, $\mathcal{D}(G,H)$ is a normal subset of G and $\mathcal{D}(G,H) = \mathcal{D}(G,H)^{-1}$. Assuming $|G|$ is sufficiently large, by Theorem 6.1, we have $|\mathcal{D}(G,H)| > \epsilon|G|$ with $\epsilon = 0.016$. Combining with Theorem 6.2(iii), (iv), this implies the following.

Corollary 6.5. *Theorem A holds for sufficiently large alternating groups and for finite simple groups of Lie type of bounded rank over fields of sufficiently large size.*

In fact, the conclusion of Theorem A holds for **all** (simple) alternating groups; see Theorem B.

Since almost simple sporadic groups have bounded order, it remains to deal with classical groups of unbounded rank. For any such group $\tilde{G}$, let $\mathcal{Y}(\tilde{G})$ denote the union of all irreducible subgroups of $\tilde{G}$ (if q is even and $\tilde{G} = \mathrm{Sp}_{2r}(q)$, we exclude the subgroups $\mathrm{GO}^{\pm}_{2r}(q)$ from $\mathcal{Y}(\tilde{G})$). We use [FG3, Theorem 1.7] (extending [Sh1]), which states the following:

Theorem 6.6. *Let $\tilde{G}$ be a classical group of rank r acting faithfully on its natural module V. Then*

$$\frac{|\mathcal{Y}(\tilde{G})|}{|\tilde{G}|} \to 0 \text{ as } r \to \infty.$$

Corollary 6.7. *Theorem A holds for all simple classical groups G over $\mathbb{F}_q$ of sufficiently large rank, provided the point-stabiliser H is irreducible and not $\mathrm{GO}^{\pm}_n(q)$ when $G = \mathrm{Sp}_n(q)$ with $2|q$.*

Proof. By the above theorem, we have

$$|\mathcal{Y}(G)|/|G| < 1/2$$

for $n \gg 0$. Since $\cup_{g \in G} H^g \subseteq \mathcal{Y}(G)$, it follows that $|\mathcal{D}(G,H)| > |G|/2$ and therefore $\mathcal{D}(G,H)^2 = G$. □

Theorem 6.8. *There are absolute constants C_1, C_2 such that the following holds. Let G be a finite simple classical group in dimension n over $\mathbb{F}_q$, acting as a primitive permutation group with point-stabiliser H.*

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

If q is even, assume $(G,H) \neq (\mathrm{Sp}_n(q), \mathrm{GO}_n^{\pm}(q))$. Suppose $n \geq C_1$ and the action is not a subspace action on subspaces of dimension $k \leq C_2$. Then G satisfies Theorem A.

Proof. Relying on Corollary 6.7, we may assume that H is reducible: namely, G acts in a subspace action, say on subspaces (nondegenerate or totally singular for $G \neq \mathrm{PSL}_n(q)$) of dimension k, with $1 \leq k \leq n/2$. Theorems 6.4, 9.4, 9.10, 9.17 and 9.30 of [FG2] show that, as $k \to \infty$, the proportion of derangements in G tends to 1. The result follows as before. □

6.2. *Completion of the proof of Theorem A*

In view of Corollary 6.5, it remains to prove Theorem A for finite simple classical groups $G = \mathrm{Cl}(V)$ in subspace actions where $\dim(V)$ is sufficiently large. Let $\tilde{G}$ denote the central extension of G for which V is a faithful linear representation, and let $\tilde{H}$ denote the inverse image in $\tilde{G}$ of a point stabiliser H of G. Also let Π denote the transitive permutation representation with H a point stabiliser. We show that if $\dim(V)$ is sufficiently large, there exist elements $\tilde{x}, \tilde{y} \in \tilde{G}$ that are derangements on $\tilde{G}/\tilde{H}$ and such that every element in $G \setminus \{1\}$ is the product of a conjugate of x and a conjugate of y, where x (respectively, y) is the image of $\tilde{x}$ (respectively, $\tilde{y}$) in G. Since x^{-1} is also a derangement, the identity element 1 is also a product of two derangements. We proceed by cases.

6.2.1. The case $\tilde{G} = \mathrm{SL}_n(q)$ with $n \geq 98$

Here $\tilde{H}$ is the stabiliser of an m-dimensional subspace V' of $V = \mathbb{F}_q^n$. First we consider the case where $1 < m < n-1$. Fixing an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$, we obtain an embedding of the norm-1 elements of $\mathbb{F}_{q^n}$ in $\mathrm{SL}_n(q)$. Let $\tilde{x}$ denote the image of a multiplicative generator of the group of norm-1 elements. Let $\tilde{y}$ denote the image in $\mathrm{SL}_n(q) > \mathrm{GL}_{n-1}(q)$ of a generator of $\mathbb{F}_{q^{n-1}}^{\times}$. Thus $\tilde{x}$ and $\tilde{y}$ are regular elements of the tori $T = T_n$ and $T' = T_{n-1,1}$ of $\mathrm{SL}_n(q)$ in [MSW, Table 2.1]. As the characteristic polynomial of $\tilde{x}$ is irreducible over $\mathbb{F}_q$ and that of $\tilde{y}$ has an irreducible factor of degree $n-1$, it follows that neither $\tilde{x}$ nor $\tilde{y}$ can fix an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ of dimension m, so x and y are indeed derangements. By [MSW, Theorem 2.1], the product of the conjugacy classes of x and y covers all nontrivial elements of G.

Assume now that $m = 1$ or $m = n-1$. Then we note that the elements t and t' constructed in Theorem 2.4 are both derangements in Π, so the statement follows from Theorem 2.4.

6.2.2. The case $\tilde{G} = \mathrm{SU}_n(q)$ with $n \geq 5$

Since H is maximal, we have that $\tilde{H}$ is the stabiliser of an m-dimensional subspace V' of $V = \mathbb{F}_{q^2}^n$, $1 \leq m \leq n-1$, where V' is either totally singular, or nondegenerate. The existence of the Hermitian form allows us to assume that $1 \leq m \leq n/2$. Applying Theorem 6.8, we may further assume that $m \leq c_2$ is bounded and that $m \leq n/2 - 1$. Let $\tilde{x}$ and $\tilde{y}$ be elements of $\tilde{G}$ of order $\frac{q^n-(-1)^n}{q+1}$ and $q^{n-1} - (-1)^{n-1}$, respectively, so they are regular semisimple elements of tori $T = T_n$ and $T' = T_{n-1,1}$, respectively. Assume that V' is not a nondegenerate 1-space. Then both $\tilde{x}$ and $\tilde{y}$ are derangements in Π. By [MSW, Theorem 2.2], the product of the conjugacy classes of x and y covers all nontrivial elements of G, and the statement follows.

Suppose now that V' is a nondegenerate 1-space. If $q > 2$, then we again note that the elements t and t' constructed in Theorem 2.4 are both derangements in Π, so the statement follows from Theorem 2.4. Assume now that $q = 2$. Consider the case $g \in \tilde{G} = \mathrm{SU}_n(2)$ is a transvection. Then we can put g in a factor $A = \mathrm{SU}_4(2)$ of a standard subgroup

$$A \times B = \mathrm{SU}_4(2) \times \mathrm{SU}_{n-4}(2)$$

of $\tilde{G}$. Direct calculation with [GAP] shows that g is a product $g = xy$ of two elements of order 5 in A. If n is large, we choose $z \in B$ a regular semisimple element of type T_{n-4}, a maximal torus in B. Now we note that $g = (xz)(yz^{-1})$ and both xz, yz^{-1} are derangements. We also note that any non-unipotent element

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

of support 1 in $\mathrm{SU}_n(2)$ is semisimple, and hence by [GT2, Lemma 5.1] it is a product of two regular semisimple elements of type T_n, which are derangements. It remains to consider the case $\mathsf{supp}(g) \geq 2$, in which case the statement follows from Theorem 2.6, since the elements t and t' constructed therein are derangements in Π.

6.2.3. The case $\tilde{G} = \Omega_{2n+1}(q)$ or $\mathrm{Sp}_{2n}(q)$ with $n \geq 5$

Let $\tilde{x}$ and $\tilde{y}$ be elements of order q^n+1 and q^n-1 generating tori of type $T = T_n^-$ and $T' = T_n^+$, respectively. Thus the Frob_q orbit of any eigenvalue of $\tilde{x}$ (respectively, $\tilde{y}$) in the natural representation consists of a $2n$-cycle (respectively, two n-cycles) together with an additional fixed point if G is of type B_n. As in Section 6.2.2, we may assume that $\tilde{H}$ is the stabiliser of an m-dimensional subspace V', which is either totally singular or nondegenerate and has bounded dimension by Theorem 6.8. For C_n, therefore, the theorem follows from [MSW, Theorem 2.3], while for B_n it holds by [MSW, Theorem 2.4] unless V' is a nondegenerate 1-space. Likewise, we must still consider the cases $(\tilde{G}, \tilde{H}) = (\mathrm{Sp}_{2n}(q), \mathrm{GO}_{2n}^{\pm}(q))$ when $2|q$.

In both of the remaining actions, we can view $\tilde{G} = [\Gamma, \Gamma]$, where $\Gamma = \mathrm{SO}(V)$ and $V = \mathbb{F}_q^{2n+1}$ when $2 \nmid q$ and $\Gamma = \mathrm{Sp}(V) \cong \mathrm{SO}_{2n+1}(q)$ and $V = \mathbb{F}_q^{2n}$ when $2|q$. Then Π is the restriction to $\tilde{G}$ of the transitive permutation action of Γ with point stabiliser $\mathrm{GO}_{2n}^{\epsilon}(q)$ for a fixed $\epsilon = \pm$. First we consider the case $\epsilon 1 = (-1)^n$. By Propositions 5.4 and 5.5, if n is large enough, we can find in $\tilde{G}$ regular semisimple elements x_1 of type $T_n^{-\epsilon}$ and y_1 of type $T_{n-1,1}^{\epsilon,-}$ such that $x_1^{\Gamma} \cdot y_1^{\Gamma} = \tilde{G} \setminus \{e\}$. Since both x_1 and y_1 are derangements in Π, the statement follows in this case.

Assume now that $\epsilon 1 \neq (-1)^n$. By Proposition 5.6, we can find in $\tilde{G}$ regular semisimple elements x_2 of type $T_{n-2,2}^{-,-}$ and y_2 of type $T_{n-3,3}^{+,+}$ when $2|n$, x_2 of type T_n^- and y_2 of type $T_{n-2,2}^{+,-}$ when $2 \nmid n$, such that $x_2^{\Gamma} \cdot y_2^{\Gamma}$ contains any element $g \in \tilde{G}$ of large enough support, say $\mathsf{supp}(g) \geq B$. Since both x_2 and y_2 are derangements in Π, the statement again follows in this case. Now we consider the case $\mathsf{supp}(g) < B < n-3$, and let λ be the primary eigenvalue of g on V (compare [LST1, Proposition 4.1.2]); note that $\lambda = \pm 1$. By [LST1, Lemma 6.3.4], we can decompose $V = U \perp W$ as an orthogonal sum of g-invariant nondegenerate subspaces, with $\dim(U) = 6$; U has type $+$ if $2 \nmid q$ and $g|_U = \lambda \cdot 1_U$. Define

$$\begin{cases} I(W) = J(W) = \mathrm{Sp}(W) \cong \mathrm{Sp}_{2n-6}(q), & \text{when } 2|q, \\ I(W) = \mathrm{SO}(W) \cong \mathrm{SO}_{2n-5}(q),\ J(W) = \Omega(W) \cong \Omega_{2n-5}(q), & \text{when } 2 \nmid q. \end{cases}$$

Likewise, we define

$$J(U) = \begin{cases} \mathrm{Sp}(U) \cong \mathrm{Sp}_6(q), & \text{when } 2|q, \\ \Omega(U) \cong \Omega_6^+(q), & \text{when } 2 \nmid q. \end{cases}$$

Since $\epsilon 1 = (-1)^{n-3}$, we can consider regular semisimple elements $x_3 \in T_{n-3}^{-\epsilon} \cap J(W)$ and $y_3 \in T_{n-4,1}^{\epsilon,-} \cap J(W)$ constructed in Propositions 5.4 and 5.5 for $J(W)$. If $2 \nmid q$, we will also consider the regular semisimple element $y_3' \in T_{n-4,1}^{\epsilon,-} \setminus J(W)$ constructed in Propositions 5.4 and 5.5 for $I(W) \cong \mathrm{SO}_{2n-5}(q)$. Also fix a regular semisimple element $z \in T_3^+$ of $J(U)$.

If $2|q$ or $\lambda = 1$, then we can write $g = \mathrm{diag}(1_U, h)$ with $h \in J(W)$. By Propositions 5.4 and 5.5, when n is large enough, $h = x_3^u y_3^v$ for some $u, v \in I(W)$, whence $g = (zx_3)^u (z^{-1}y_3)^v$ is a product of two derangements.

Finally, assume that $2 \nmid q$ and $\lambda = -1$; write $g = \mathrm{diag}(-1_U, h)$ with $h \in I(W)$. If $q \equiv 1 (\mathrm{mod}\ 4)$, then $1 = (-1)^{3(q-1)/2}$, so $-1_U \in J(U) \cong \Omega_6^+(q)$ by [KL, Proposition 2.5.13], whence $h \in J(W)$ and, as in the previous case, $g = ((-1_U)zx_3)^u (z^{-1}y_3)^v$ is a product of two derangements. If $q \equiv 3$ $(\mathrm{mod}\ 4)$, then $-1 = (-1)^{3(q-1)/2}$ and $-1_U \in I(U) \setminus J(U)$. In this case, $h \in I(W) \setminus J(W)$, so by Propositions 5.4 and 5.5, when n is large enough, we can write $h = x_3^{u'} (y_3')^{v'}$ for some $u', v' \in I(W)$. Now $g = ((-1_U)zx_3)^{u'} (z^{-1}y_3')^{v'}$ is again a product of two derangements in Π.

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

6.2.4. The case $\tilde{G} = \Omega^-_{2n}(q)$ with $n \geq 4$

Here we choose, in accordance with Lemma 4.1, regular semisimple elements $\tilde{x}$ of type T and $\tilde{y}$ of type T', where $T = T^-_n$ is a maximal torus of order $q^n + 1$ and $T' = T^{-,+}_{n-1,1}$ is a maximal torus whose full preimage in $\mathrm{Spin}^-_{2n}(q)$ has order $(q^{n-1}+1)(q-1)$. (Similarly, in what follows, while specifying the order of tori in question, we will instead list the order of their full preimages in the corresponding group of simply connected type.) Then the characteristic polynomial of $\tilde{x}$ is irreducible, while that of $\tilde{y}$ factors into two linear factors and an irreducible factor of degree $2n-2$. Again, $\tilde{H}$ is the stabiliser of an m-dimensional subspace V', totally singular (with $m \leq n-1$ bounded by Theorem 6.8), or nondegenerate. Now [MSW, Theorem 2.5] implies the theorem, unless $\dim(V') = 1$ or V' is a nondegenerate 2-space of type $+$.

Consider the remaining three actions. Assume first that $2|n$. Then note that the elements x_1, y_1 of types T^-_n and $T^{+,-}_{n-1,1}$ constructed in the proof of Proposition 4.3(i) are both derangements in Π, whence the statement follows from Proposition 4.3(i). Hence we may assume that $2 \nmid n \geq 13$. In this case, note that the elements x_2, y_2 of types $T^{-,+}_{n-5,5}$ and $T^{-,+}_{n-6,6}$ constructed in the proof of Proposition 4.3(ii) with $(a, \epsilon) = (5, -)$ are both derangements in Π. Hence, there exists some absolute constant B such that if $\mathsf{supp}(g) \geq B$, then the statement follows from Proposition 4.3(ii). Now we consider the case $\mathsf{supp}(g) < B < n-3$, and let λ be the primary eigenvalue of g on V (compare [LST1, Proposition 4.1.2]). By [LST1, Lemma 6.3.4], we can decompose $V = U \perp W$ as an orthogonal sum of g-invariant subspaces, with $\dim(U) = 6$, U of type $+$ and $g|_U = \lambda \cdot 1_U$. As $2|(n-3) \geq 10$, we can find regular semisimple elements $x_3 \in T^-_{n-3}$ and $y_3 \in T^{-,+}_{n-4,1}$ constructed in the proof of Proposition 4.3(i) for $\Omega(W) \cong \Omega^-_{2n-6}(q)$. Also fix a regular semisimple element $z \in T^+_3$ of $\Omega(U) \cong \Omega^+_6(q)$. If $2|q$ or $\lambda = 1$, then we can write $g = \mathrm{diag}(1_U, h)$ with $h \in \Omega^-_{2n-6}(q)$. By Proposition 4.3(i), $h = x_3^u y_3^v$ for some $u, v \in \Omega(W)$, whence $g = (zx_3)^u (z^{-1}y_3)^v$ is a product of two derangements. Finally, assume that $2 \nmid q$ and $\lambda = -1$. If $q \equiv 3 \pmod 4$, then $-1 = (-1)^{n(q-1)/2}$, so $-1_V \in \Omega^-_{2n}(q) = \tilde{G}$ by [KL, Proposition 2.5.13], whence we can replace g by $(-1_V)g$ and appeal to the previous case. If $q \equiv 1 \pmod 4$, then $1 = (-1)^{3(q-1)/2}$ and $-1_U \in \Omega(U) \cong \Omega^+_6(q)$. In this case, we can write $g = \mathrm{diag}(-1_U, h)$ with $h \in \Omega^-_{2n-6}(q)$. Again, by Proposition 4.3(i), $h = x_3^u y_3^v$ for some $u, v \in \Omega(W)$, whence $g = ((-1_U)zx_3)^u (z^{-1}y_3)^v$ is a product of two derangements in Π.

6.2.5. The case $\tilde{G} = \Omega^+_{2n}(q)$ with $2 \nmid n \geq 5$

We again choose regular semisimple elements $\tilde{x}$ and $\tilde{y}$ of type T and T', where the maximal tori $T = T^+_n$ and $T' = T^{-,-}_{n-1,1}$ have order $q^n - 1$ and $(q^{n-1}+1)(q+1)$, using Lemma 4.1. Here, the characteristic polynomial of $\tilde{x}$ factors into two irreducibles of degree n while the characteristic polynomial of $\tilde{y}$ factors into irreducibles of degree $2n-2$ and 2. Now, Theorem 6.8 and [MSW, Theorem 2.6] imply the theorem unless $\tilde{H}$ is the stabiliser of a nondegenerate 2-space V' of type $-$. (Note that the case V' is nondegenerate 1-dimensional does not occur since we choose $\tilde{y}$ to have the second irreducible factor of degree 2 in its characteristic polynomial; compare Lemma 4.1.)

Consider the remaining action on nondegenerate 2-spaces of type $-$, assuming $n \geq 9$. Note that the elements x_1, y_1 of types $T^{-,-}_{n-3,3}$ and $T^{-,-}_{n-4,4}$ constructed in the proof of Proposition 4.3(ii) with $(a, \epsilon) = (3, +)$ are both derangements in Π. Hence, there exists some absolute constant B such that if $\mathsf{supp}(g) \geq B$, then the statement follows from Proposition 4.3(ii). Now we consider the case $\mathsf{supp}(g) < B < n-3$, and let λ be the primary eigenvalue of g on V. Applying [LST1, Lemma 6.3.4], we can decompose $V = U \perp W$ as an orthogonal sum of g-invariant subspaces, with $\dim(U) = 6$, U of type $-$ and $g|_U = \lambda \cdot 1_U$. As $2|(n-3) \geq 6$, we can find regular semisimple elements $x_2 \in T^-_{n-3}$ and $y_2 \in T^{-,+}_{n-4,1}$ in $\Omega(W) \cong \Omega^-_{2n-6}(q)$. Also fix a regular semisimple element $z \in T^-_3$ of $\Omega(U) \cong \Omega^-_6(q)$. If $2|q$ or if $\lambda = 1$, then we can write $g = \mathrm{diag}(1_U, h)$ with $h \in \Omega^-_{2n-6}(q)$. By [MSW, Theorem 2.5], $h = x_2^u y_2^v$ for some $u, v \in \Omega(W)$, whence $g = (zx_2)^u (z^{-1}y_2)^v$ is a product of two derangements. Finally, assume that $2 \nmid q$ and $\lambda = -1$. If $q \equiv 1 \pmod 4$, then $1 = (-1)^{n(q-1)/2}$, so $-1_V \in \Omega^+_{2n}(q) = \tilde{G}$, whence we can replace g by $(-1_V)g$ and return to the previous case. If $q \equiv 3 \pmod 4$, then $-1 = (-1)^{3(q-1)/2}$ and $-1_U \in \Omega(U) \cong \Omega^-_6(q)$. In this case, we can write $g = \mathrm{diag}(-1_U, h)$ with $h \in \Omega^-_{2n-6)}(q)$. Again, by

[MSW, Theorem 2.5], $h = x_3^u y_3^v$ for some $u, v \in \Omega(W)$, whence $g = ((-1_U)zx_3)^u(z^{-1}y_3)^v$ is a product of two derangements.

6.2.6. The case $\tilde{G} = \Omega^+_{2n}(q)$ with $2|n \geq 6$

Now we choose regular semisimple elements $\tilde{x}$ and $\tilde{y}$ of type T and T', where the maximal tori $T = T^{+,+}_{n-1,1}$ and $T' = T^{-,-}_{n-1,1}$ have order $(q^{n-1}-1)(q-1)$ and $(q^{n-1}+1)(q+1)$, again using Lemma 4.1. By [GT3, Theorem 2.7], $\tilde{x}^{\tilde{G}} \cdot \tilde{y}^{\tilde{G}}$ contains all noncentral elements of $\tilde{G}$. Hence the theorem follows, unless $\tilde{H}$ is the stabiliser of an m-dimensional subspace V', where either V' is nondegenerate and $m = 1, 2$ (with $m = 1$ only when $q \leq 3$) or V' is totally singular and $m = 1$.

If V' is a nondegenerate 2-space of type $-$, we then choose $\tilde{y}'$ regular semisimple of type $T'_2 = T^{-,-}_{n-2,2}$, a maximal torus of order $(q^{n-2}+1)(q^2+1)$ as in [LST1, §7.1]. As $\tilde{x}$ and $\tilde{y}'$ are both derangements in Π, the theorem now follows from [LST1, §7.2] and [GM2, Theorem 7.6].

In the remaining cases, note that, as shown in the proof of [MSW, Theorem 2.7], there exists a regular semisimple element $\tilde{x}'$ of type T'_1, a maximal torus of order $(q^{n/2}+(-1)^{n/2})^2$, such that there are exactly three irreducible characters of $\tilde{G}$ that are nonzero at both $\tilde{x}'$ and $\tilde{y}$: namely, $1_{\tilde{G}}$, St and one more character ρ: $|\mathsf{St}(\tilde{x}')\mathsf{St}(\tilde{y})| = 1$ and $|\rho(\tilde{x}')\rho(\tilde{y})| = 2$. The imposed condition on V' ensures that $\tilde{x}'$ and $\tilde{y}$ are both derangements in Π. Consider any $g \in \tilde{G} \setminus \mathbf{Z}(\tilde{G})$. If g is semisimple, then $g \in (\tilde{x}')^{\tilde{G}} \cdot (\tilde{y})^{\tilde{G}}$ by [GT2, Lemma 5.1]. The same conclusion holds if g is nonsemisimple but has large enough support $\mathsf{supp}(g) > B$ with $q^{\sqrt{B}} \geq 2^{481}$ – indeed, in this case $|\rho(g)/\rho(1)| \leq q^{-\sqrt{\mathsf{supp}(g)}/481} < 1/2$, so

$$\left|\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(\tilde{x}')\chi(\tilde{y})\overline{\chi}(g)}{\chi(1)}\right| > 1 - \left|\frac{\rho(\tilde{x}')\rho(\tilde{y})\overline{\rho}(g)}{\rho(1)}\right| > 1 - 1 = 0.$$

It therefore remains to consider the case q is bounded and $\mathsf{supp}(g) \leq B$, in which case we may assume $n > B+6$, so g acting on the natural module $\mathbb{F}_q^{2n}$ has a primary eigenvalue $\lambda = \pm 1$ by [LST1, Proposition 4.1.2]. In the case $2 \nmid q$, the condition $2|n$ implies by [KL, Proposition 2.5.13] that $-1 \in \Omega^+_{2n}(q) = \tilde{G}$. Hence we can multiply g by a suitable central element of $\tilde{G}$ to ensure that $\lambda = 1$. Now, using [LST1, Lemma 6.3.4] and the assumption $n > B + 6$, we can find a g-invariant decomposition $V = U \perp W$, where $\dim U = 10$, g acts trivially on U and U is nondegenerate of type $+$, whence W is nondegenerate of type $+$ of dimension $2n - 10$. By [MSW, Theorem 2.6], we can find regular semisimple elements $\tilde{u}$ and $\tilde{v}$ of type a maximal torus of order $q^{n-5} - 1$ and a maximal torus of order $(q^{n-6}+1)(q+1)$ in $H := \Omega^+_{2n-10}(q)$ such that the W-component h of g is $\tilde{u}^{h_1} \cdot \tilde{v}^{h_2}$ for some $h_1, h_2 \in H$. We also fix a regular semisimple element $\tilde{z} \in \Omega^+_{10}(q)$ of type a maximal torus of order $(q^3+1)(q^2+1)$. Now it is clear that $g = (\tilde{z}\tilde{u})^{h_1}(\tilde{z}^{-1}\tilde{v})^{h_2}$ and both $\tilde{z}\tilde{u}$ and $\tilde{z}^{-1}\tilde{v}$ are derangements in Π.

Thus we have completed the proof of Theorem A.

6.3. A probabilistic result on derangements

Recall that, for a permutation group G and an element $g \in G$, $\mathbf{P}_{\mathcal{D}(G),\mathcal{D}(G)}(g)$ denotes the probability that two independently chosen random derangements $s, t \in \mathcal{D}(G)$ satisfy $st = g$.

Proposition 6.9. *Let G be a finite simple transitive permutation group.*

(i) $\mathbf{P}_{\mathcal{D}(G),\mathcal{D}(G)}$ *converges to the uniform distribution on G in the L^1 norm as $|G| \to \infty$. Hence the random walk on G with respect to its derangements as a generating set has mixing time two.*

(ii) *If G is a group of Lie type of bounded rank, then* $\mathbf{P}_{\mathcal{D}(G),\mathcal{D}(G)}$ *converges to the uniform distribution on G in the L^∞ norm as $|G| \to \infty$.*

Proof. By [Sh2, Theorem 2.5], if G is a finite simple group and $x, y \in G$ are randomly chosen, then almost surely $\mathbf{P}_{x^G,y^G}$ converges to the uniform distribution $\mathbf{U}_G$ in the L^1 norm as $|G| \to \infty$. Hence the same holds for randomly chosen $x, y \in T$, where T is any normal subset of G of proportion bounded away from 0. By Theorem 6.1 of Fulman and Guralnick we may apply this to $T = \mathcal{D}(G)$. This implies part (i).

Part (ii) follows from part (iv) of [LST2, Theorem A]. □

We note that, by Corollary 6.9 of [LS], if $T \subseteq \mathsf{A}_n$ is a normal subset of size at least $e^{-(1/2-\delta)n}|\mathsf{A}_n|$ for some fixed $\delta > 0$, then, as $n \to \infty$, the mixing time of the random walk on A_n with respect to the generating set T is two. This provides an alternative proof of part (i) for alternating groups.

We also note that part (ii) above does not hold for alternating groups; indeed, this follows from Theorem 6.2(ii) and its proof in [LST2].

7. Products of derangements in alternating groups

In this section, we prove Theorem B. First we need the following technical result:

Proposition 7.1. *Let H be a proper subgroup of A_n such that one of the following conditions holds:*

(i) $n \in \{5, 7, 11, 12, 13, 14, 15, 16\}$ *and H contains an ℓ-cycle for the two largest odd integers $\ell \leq n$.*
(ii) $n \geq 17$ *and H contains an ℓ-cycle for the three largest odd integers $\ell \leq n$.*

Then $2|n$ and $H \cong \mathsf{A}_{n-1}$, a point stabiliser in the natural action of A_n on $\Delta := \{1, 2, \ldots, n\}$.

Proof. We proceed by induction on n, with the induction base verifying the cases where $n \leq 13$. Set

$$\mathcal{L}_n := \{\ell \in \mathbb{Z} \mid 2 \nmid \ell, \lfloor 3n/4 \rfloor \leq \ell \leq n\}.$$

(a) If $n = 5$, then 15 divides $|H|$, so $H = \mathsf{A}_5$ by [CCNPW]. Similarly, if $n = 7$, then 35 divides $|H|$, so $H = \mathsf{A}_7$ by [CCNPW]. Suppose $n = 11$. As 11 divides $|H|$, using [CCNPW], we see that H is contained in a maximal subgroup $X \cong \mathrm{M}_{11}$ of A_{11}. But this is a contradiction since X contains no element of order 9, whereas H contains a 9-cycle. Next assume that $n = 12$. Then H contains an 11-cycle and a 9-cycle. Using [CCNPW], we again see that H is contained in a maximal subgroup Y of A_{12}, with $Y \cong \mathrm{M}_{12}$ or $Y \cong \mathsf{A}_{11}$, a point stabiliser. The former case is ruled out since M_{12} contains no element of order 9. In the latter case, we must have $H = \mathsf{A}_{11}$ by the $n = 11$ result. If $n = 13$, then $11 \cdot 13$ divides $|H|$, so $H = \mathsf{A}_{13}$ by [CCNPW].

(b) For the induction step, assume $n \geq 14$. First we consider the case H is intransitive on Δ. If $2 \nmid n$, then H contains an n-cycle, so it is transitive on Δ: a contradiction. Hence $2|n$. Then we may assume that H contains the $(n-1)$-cycle $g = (1, 2, \ldots, n-1)$. It follows that $\{1, 2, \ldots, n-1\}$ and $\{n\}$ are the two H-orbits on Δ, so $H \leq \mathrm{Stab}_{\mathsf{A}_n}(n) \cong \mathsf{A}_{n-1}$. If in addition $n \geq 18$, then $n-1, n-3, n-5$ are the three largest members of $\mathcal{L}_n$, and at the same time they are also the three largest members of $\mathcal{L}_{n-1}$. Applying the induction hypothesis to $n-1$, we obtain that $H = \mathrm{Stab}_{\mathsf{A}_n}(n)$, as stated. Suppose $n = 16$. Then $H \leq \mathsf{A}_{15}$, and it contains a 15-cycle and a 13-cycle. It follows that H is transitive on $\Delta' := \{1, 2, \ldots, 15\}$, and in fact it acts primitively on Δ'. Now, using [GAP], we can check that A_{15} and S_{15} are the only primitive subgroups of S_{15} that have order divisible by 13. It follows that $H = \mathsf{A}_{15}$.

(c) We may now assume that H is transitive on Δ. Suppose that H is imprimitive: H preserves a partition $\Delta = \Delta_1 \sqcup \Delta_2 \sqcup \ldots \sqcup \Delta_b$ with $1 < |\Delta_i| = a = n/b < n$. If $2|n$, then we may assume that H contains the $(n-1)$-cycle $g = (1, 2, \ldots, n-1)$ and that $n \in \Delta_b$. Then g fixes Δ_b and so must fix the set $\Delta_b \setminus \{n\}$ of size $a - 1 < n - 1$, a contradiction. Next, consider the case $2 \nmid n$. Then we may assume that H contains the $(n-2)$-cycle $h = (1, 2, \ldots, n-2)$ and that $n \in \Delta_b$. Note that $a > 1$ divides n, which is odd, and hence $n/3 \geq a \geq 3$. Now h fixes Δ_b and so must fix the set $\Delta_b \setminus \{n\}$ of size $a - 1$ with $2 \leq a - 1 < n - 2$, again a contradiction.

(d) Now we consider the remaining case, where H is primitive on Δ.

If $n = 14$, then $11 \cdot 13$ divides $|H|$. Using [GAP], we can check that $H = \mathsf{A}_n$. Similarly, if $15 \leq n \leq 17$, then A_n is the only primitive subgroup of A_n that has order divisible by 13, whence $H = \mathsf{A}_n$.

From now on, we may assume $n \geq 18$ and let $H_1 := \mathrm{Stab}_H(1) \leq \mathsf{A}_{n-1}$. First we consider the case $2|n$. Then H contains an $(n-1)$-cycle g, an $(n-3)$-cycle h and an $(n-5)$-cycle k. Since H is transitive on Δ, we may replace g by an H-conjugate so that $g(1) = 1$, and similarly $h(1) = 1$ and $k(1) = 1$. Thus $H_1 \leq \mathsf{A}_{n-1}$ contains g, h and k, and $n-1, n-3, n-5$ are the first three members of $\mathcal{L}_{n-1}$. By the induction hypothesis applied to H_1, we have $H_1 = \mathsf{A}_{n-1}$. As H is transitive on Δ, it follows that $H = \mathsf{A}_n$.

(e) Now we may assume that $2 \nmid n \geq 19$. Arguing as above, we may assume that H_1 contains an $(n-2)$-cycle $s = (3, 4, \ldots, n)$. Assume in addition that H_1 is intransitive on $\{2, 3, \ldots, n\}$. Since H_1 contains s, it follows that $\{1\}$, $\{2\}$ and $\{3, 4, \ldots, n\}$ are the 3 H_1-orbits on Δ. Note that $H_2 := \mathrm{Stab}_H(2)$ now contains H_1 and $|H_2| = |H|/n = |H_1|$, whence $H_2 = H_1$. We claim that for any $i \in \Delta$, there is a unique $i^\star \in \Delta \setminus \{i\}$ such that

$$\mathrm{Stab}_H(i) = \mathrm{Stab}_H(i^\star). \tag{7.1}$$

(Indeed, using transitivity of H, we can find $x \in H$ such that $i = x(1)$, whence equation (7.1) holds for $i^\star := x(2)$. Conversely, if $\mathrm{Stab}_H(i) = \mathrm{Stab}_H(j)$ for some $j \neq i$, then conjugating the equality by x, we see that $H_1 = \mathrm{Stab}_H(1)$ fixes $x^{-1}(j) \neq x^{-1}(i) = 1$. The orbit structure of H_1 on Δ then shows that $x^{-1}(j) = 2$, so $j = x(2) = i^\star$, and the claim follows.) We also note that the uniqueness of $i^\star$ and equation (7.1) imply that $(i^\star)^\star = i$. Hence, the set Δ is partitioned into pairs $\{j_1, j_1^\star\}, \ldots, \{j_m, j_m^\star\}$, which is impossible since $2 \nmid n$.

We have shown that H_1 is transitive on $\{2, 3, \ldots, n\}$, so H is doubly transitive on Δ. In particular, H has a unique minimal normal subgroup S, which is either elementary abelian or a nonabelian simple group; see [Cam, Proposition 5.2]. Suppose we are in the former case. Then one may identify Δ with the vector space $\mathbb{F}_p^d$ for some prime p with $p^d = n$, S with the group of translations $t_v : u \mapsto u + v$ on $\mathbb{F}_p^d$, $1 \in \Delta$ with the zero vector in $\mathbb{F}_p^d$ and H_1 with a subgroup of $\mathrm{GL}(\mathbb{F}_p^d)$. Since $2 \nmid n$, $p > 2$, so H_1 is imprimitive on $\mathbb{F}_p^d \setminus \{0\}$ (indeed, it permutes the sets of nonzero vectors of $(p^d-1)/(p-1)$ $\mathbb{F}_p$-lines). On the other hand, the presence of the $(n-2)$-cycle $s \in H_1$ shows (as in (iii)) that the transitive subgroup H_1 must be primitive on $\mathbb{F}_p^d \setminus \{0\}$, a contradiction.

We have shown that S is simple, nonabelian. Now we can use the list of (H, S, n) as given in [Cam]. The possibility $(H, S, n) = (\mathrm{M}_{23}, \mathrm{M}_{23}, 23)$ is ruled out since H must contain the element s of order 21. Next, if $(S, n) = ({}^2B_2(q), q^2+1)$ with $q = 2^{2f+1} \geq 8$, then $S \lhd H \leq \mathrm{Aut}(S) = S \cdot C_{2f+1}$. This is impossible, since H contains the element s of order $q^2 - 1$. Similarly, if $(S, n) = (\mathrm{PSU}_3(q), q^3+1)$ with $q = 2^e \geq 4$, then $S \lhd H \leq \mathrm{Aut}(S) = \mathrm{PGU}_3(q) \cdot C_{2e}$. This is again impossible, since H contains the element s of order $q^3 - 1$. Next, if $(S, n) = (\mathrm{SL}_2(q), q+1)$ with $q = 2^e \geq 8$, then $S \lhd H \leq \mathrm{Aut}(S) = \mathrm{SL}_2(q) \cdot C_e$. This is again impossible since H contains the element of order $n - 4 = q - 3$.

As H is a proper subgroup of A_n, there remains only one possibility that

$$(S, n) = (\mathrm{PSL}_d(q), (q^d-1)/(q-1))$$

with $d \geq 3$, and we may assume that S and H act on the $(q^d-1)/(q-1)$ lines of the vector space $\mathbb{F}_q^d = \langle e_1, e_2, \ldots, e_d \rangle_{\mathbb{F}_q}$. Since H is doubly transitive, we may assume that the two fixed points of the $(n-2)$-cycle s are $\langle e_1 \rangle_{\mathbb{F}_q}$ and $\langle e_2 \rangle_{\mathbb{F}_q}$. In this case, s acts on the set of $q+1$ $\mathbb{F}_q$-lines of $\langle e_1, e_2 \rangle_{\mathbb{F}_q}$, fixing two of them. This is again impossible, since s permutes cyclically the other $n-2$ $\mathbb{F}_q$-lines. □

Proof of Theorem B.

(a) Fix a symbol $\alpha \in \Omega$, and consider the point stabiliser $H := \mathrm{Stab}_G(\alpha)$. We also consider the natural permutation action of G on $\Delta := \{1, 2, \ldots, n\}$. The cases $5 \leq n \leq 10$ can be checked directly using [GAP], so we will assume that $n \geq 11$.

In the notation of Proposition 7.1, suppose first that there is some $\ell \in \mathcal{L}_n$ such that H does **not** contain any ℓ-cycle. In other words, any ℓ-cycle in $G = \mathsf{A}_n$ is a derangement on Ω. By the main result of [B], the choice of ℓ ensures that every element in G is a product of two ℓ-cycles and hence a product of two derangements (on Ω).

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press

It remains to consider the case where H contains an ℓ-cycle for any $\ell \in \mathcal{L}_n$. By Proposition 7.1, this implies that $2|n$ and $H = \mathrm{Stab}_G(1)$, and thus $\Omega = \Delta$. We will now show that every element $g \in G$ is a product of two derangements on Δ. (Presumably this also follows from [Xu], but for the reader's convenience, we give a short, direct proof.)

(b) We will again proceed by induction on n, with the induction base $5 \leq n \leq 10$ already checked.

(b1) For the induction step, suppose that g fixes at least 2 points in Δ, say $g(i) = i$ for $i = 1, 2$. Since $n \geq 11$, we have $n-2 \geq \lfloor 3n/4 \rfloor$. Viewing $g \in \mathsf{A}_{n-2}$, by the main result of [B], we have that $g = x_1x_2$ is a product of two $(n-2)$-cycles $x_1, x_2 \in \mathsf{S}_{n-2}$. It follows that $g = \tilde{x}_1\tilde{x}_2$, with $\tilde{x}_1 = x_1(1,2)$ and $\tilde{x}_2 = x_2(1,2)$ being derangements in A_n.

(b2) Suppose now that $g = g_1g_2 \in \mathsf{A}_m \times \mathsf{A}_{n-m}$ with $5 \leq m \leq n/2$. By the induction hypothesis, $g_i = y_iz_i$, with $y_1, z_1 \in \mathsf{A}_m$ and $y_2, z_2 \in \mathsf{A}_{n-m}$ being derangements. It follows that $g = (y_1y_2)(z_1z_2)$, with $y_1y_2 \in \mathsf{A}_n$ and $z_1z_2 \in \mathsf{A}_n$ being derangements. In particular, we are done if, in the decomposition of g into disjoint cycles, g contains a cycle of odd length c, where $5 \leq c \leq n-5$. We are also done if $c = 3$: indeed, if $g = (1,2,3)h$ with $h \in \mathsf{A}_{n-3}$ disjoint from $(1,2,3)$, then we can write $h = h_1h_2$, with $h_i \in \mathsf{A}_{n-3}$ being derangements, so $g = ((1,3,2)h_1) \cdot ((1,3,2)h_2)$ is a product of two derangements. Together with (b1), we are also done in the case $c = n-3$.

(b3) Suppose g contains at least two cycles t_1, t_2 of even length d_1, d_2 in its disjoint cycle decomposition. If $6 \leq d_1 + d_2 \leq n-6$, we are done by the previous step (b2), by taking $g_1 := t_1t_2$. We are also done if $d_1 + d_2 = 4$: indeed, if $g = (1,2)(3,4)h$ with $h \in \mathsf{A}_{n-4}$ disjoint from $(1,2)(3,4)$, then we can write $h = h_1h_2$, with $h_i \in \mathsf{A}_{n-4}$ being derangements, so $g = ((1,3)(2,4)h_1) \cdot ((1,4)(2,3)h_2)$ is a product of two derangements.

(b4) The above steps leave only the following two cases for the disjoint cycle decomposition of g (up to conjugation):

- $g = g_1g_2$, where g_1 is an a-cycle, g_2 is an $(n-a)$-cycle and $2|a$. Here, if $4 \leq a \leq n-4$, then $g = g^2 \cdot g^{-1}$, with g^2 and g^{-1} being derangements. In the remaining case, say $g = (1,2,\ldots,n-2)(n-1,n)$, setting $h = (1,2,\ldots,n-3,n-1)(n-2,n)$, we see that gh consists of two disjoint $n/2$-cycles and is therefore a derangement, while $g = (gh)(h^{-1})$.
- $g = (1,2,\ldots,n-1)$. Setting $h = (1,n-3)(2,3,\ldots,n-4,n-2,n-1,n) \in \mathsf{A}_n$, we see that

$$gh = (1,n-2)(2,4,6,\ldots,n-4,n-1,n,3,5,\ldots,n-3)$$

is a derangement, while $g = (gh)(h^{-1})$. □

Acknowledgements. The authors are grateful to the referee for the careful reading and many helpful comments that greatly improved the exposition of the paper.

Conflicts of Interest. None.

Financial support. Michael Larsen was partially supported by the NSF (grants DMS-1702152 and DMS-2001349). Aner Shalev was partially supported by ISF grant 686/17 and the Vinik Chair of mathematics, which he holds. Pham Tiep was partially supported by the NSF (grants DMS-1840702 and DMS-2200850), the Simons Foundation, the Joshua Barlaz Chair in Mathematics and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton). Part of this work was done while AS and PT participated in the program 'Groups, Representations and Applications: New Perspectives' at the Isaac Newton Institute for Mathematical Sciences in 2020. This work was supported by EPSRC grant number EP/R014604/1. All three authors were partially supported by BSF grants 2016072 and 2020037.

References

[Al] D. Alvis, Duality and character values of finite groups of Lie-type, *J. Algebra* **74** (1982), 211–222.
[B] E. Bertram, Even permutations as a product of two conjugate cycles, *J. Comb. Theory Ser. A* **12** (1972), 368–380.

[BG] T.C. Burness and M. Giudici, '*Classical Groups, Derangements and Primes*', Australian Mathematical Society Lecture Series, **25**, Cambridge University Press, Cambridge, 2016. xviii+346 pp.

[Cam] P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.* **13** (1981), 1–22.

[CC] P.J. Cameron and A.M. Cohen, On the number of fixed point free elements in a permutation group. A collection of contributions in honour of Jack van Lint. *Discrete Math.* **106 /** 107 (1992), 135–138.

[Ca] R. Carter, '*Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*', Wiley, Chichester, 1985.

[CCNPW] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, '*ATLAS of Finite Groups*', Clarendon Press, Oxford, 1985.

[Cu] C.W. Curtis, Truncation and duality in the character ring of a finite group of Lie type, *J. Algebra* **62** (1980), 320–332.

[DL] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Ann. of Math.* **103** (1976), 103–161.

[DM] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, London Mathematical Society Student Texts **21**, Cambridge University Press, 1991.

[D] J.D. Dixon, Random sets which invariably generate the symmetric group, *Discrete Math.* **105** (1992), 25–39.

[EFG] S. Eberhard, K. Ford and B. Green, Invariable generation of the symmetric group, *Duke Math. J.* **166** (2017), 1573–1590.

[En] V. Ennola, On the characters of the finite unitary groups, *Ann. Acad. Scient. Fenn. A I*, no. 323 (**1963**).

[FKS] B. Fein, W.M. Kantor and M. Schacher, Relative Brauer groups. II, *J. Reine Angew. Math.* **328** (1981), 39–57.

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

[FG1] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.

[FG2] J. Fulman and R. Guralnick, Derangements in subspace actions of finite classical groups, *Trans. Amer. Math. Soc.* **369** (2017), 2521–2572.

[FG3] J. Fulman and R. Guralnick, Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture, *Trans. Amer. Math. Soc.* **370** (2018), 4601–4622.

[GAP] The GAP group , '**GAP** - Groups, Algorithms, and Programming', Version 4.8.7, 2017, http://www.gap-system.org.

[Gl] D. Gluck, Character value estimates for nonsemisimple elements, *J. Algebra* **155** (1993), 221–237.

[Go] W.T. Gowers, Quasirandom groups, *Combin. Probab. Comput.* **17** (2008), 363–387.

[GLT] R.M. Guralnick, M. Larsen and P.H. Tiep, Character levels and character bounds, *Forum of Math. Pi* **8** (2020), e2, 81 pages.

[GLBST] R.M. Guralnick, M.W. Liebeck, E.A. O'Brien, A. Shalev and P.H. Tiep, Surjective word maps and Burnside's $p^a q^b$ theorem, *Invent. Math.* **213** (2018), 589–695.

[GM1] R.M. Guralnick and G. Malle, Simple groups admit Beauville structures, *J. Lond. Math. Soc.* **85** (2012), 694–721.

[GM2] R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[GT1] R.M. Guralnick and P.H. Tiep, A problem of Kollár and Larsen on finite linear groups and crepant resolutions, *J. Europ. Math. Soc.* **14** (2012), 605–657.

[GT2] R.M. Guralnick and P.H. Tiep, Lifting in Frattini covers and a characterization of finite solvable groups, *J. Reine Angew. Math.* **708** (2015), 49–72.

[GT3] R.M. Guralnick and P.H. Tiep, Effective results on the Waring problem for finite simple groups, *Amer. J. Math.* **137** (2015), 1401–1430.

[GW] R.M. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* **101** (1997), 255–287.

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

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

[LS] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Invent. Math.* **174** (2008), 645–687.

[LST1] M. Larsen, A. Shalev and P.H. Tiep, The Waring problem for finite simple groups, *Ann. of Math.* **174** (2011), 1885–1950.

[LST2] M. Larsen, A. Shalev and P.H. Tiep, Products of normal subsets, (submitted).

[LTT] M. Larsen, J. Taylor, and P.H. Tiep, Character bounds for regular semisimple elements and asymptotic results on Thompson's conjecture, (submitted).

[LM] F. Lübeck and G. Malle, Murnaghan-Nakayama rule for values of unipotent characters in classical groups, *Represent. Theory* **20** (2016), 139–161.

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

[Lu1] G. Lusztig, Unipotent characters of the symplectic and odd orthogonal groups over a finite field, *Invent. Math.* **64** (1981), 263–296.

[Lu2] G. Lusztig, *'Characters of a Reductive Group over a Finite Field'*, Annals of Mathematics Studies **107**, Princeton University Press, 1984.

[Ma1] G. Malle, Unipotente Grade imprimitiver komplexer Spiegelungsgruppen, *J. Algebra* **177** (1995), 768–826.

[Ma2] G. Malle, Almost irreducible tensor squares, *Comm. Algebra* **27** (1999), 1033–1051.

[MM] G. Malle and B.H. Matzat, *'Inverse Galois Theory'*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[MSW] G. Malle, J. Saxl, and T. Weigel, Generation of classical groups. *Geom. Dedicata* **49** (1994), 85–116.

[Mc] E. McKemmie, Invariable generation of finite classical groups, *J. Algebra* **585** (2021), 592–615.

[Ng] H.N. Nguyen, Low-dimensional complex characters of the symplectic and orthogonal groups, *Comm. Algebra* **38** (2010), 1157–1197.

[NP] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Europ. Math. Soc.* **13** (2011), 1063–1077.

[Ol] J.B. Olsson, Remarks on symbols, hooks and degrees of unipotent characters, *J. Combin. Theory Ser. A* **42** (1986), 223–238.

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

[PS] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type, *J. Amer. Math. Soc.* **29** (2016), 95–146.

[Sh1] A. Shalev, A theorem on random matrices and some applications, *J. Algebra* **199** (1998), 124–141.

[Sh2] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), 3075–3086.

[ST] P. Sin and P.H. Tiep, Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551–606.

[TZ1] P.H. Tiep and A.E. Zalesskii, Some characterizations of the Weil representations of the symplectic and unitary groups, *J. Algebra* **192** (1997), 130–165.

[TZ2] P.H. Tiep and A.E. Zalesskii, Unipotent elements of finite groups of Lie type and realization fields of their complex representations, *J. Algebra* **271** (2004), 327–390.

[Xu] C.-H. Xu, The commutators of the alternating group, *Sci. Sinica* **14** (1965), 339–342.

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284.

https://doi.org/10.1017/fms.2022.69 Published online by Cambridge University Press