Journal of Algebra 421 (2015) 56–101

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Generation of finite classical groups by pairs of elements with large fixed point spaces ☆

Cheryl E. Praeger [a,1], Ákos Seress [2], Şükrü Yalçınkaya [b,*,3]

[a] *Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics M019, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia*
[b] *Nesin Mathematics Village, Şirince, İzmir, Turkey*

ARTICLE INFO

Article history:
Received 7 March 2014
Available online 11 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

Keywords:
Classical groups
Proportion of elements
Group recognition algorithms

ABSTRACT

We study 'good elements' in finite $2n$-dimensional classical groups G: namely t is a 'good element' if $o(t)$ is divisible by a primitive prime divisor of $q^n - 1$ for the relevant field order q, and t fixes pointwise an n-space. The group $\mathrm{SL}_{2n}(q)$ contains such elements, and they are present in $\mathrm{SU}_{2n}(q), \mathrm{Sp}_{2n}(q), \mathrm{SO}^{\varepsilon}_{2n}(q)$, only if n is odd, even, even, respectively. We prove that there is an absolute positive constant c such that two random conjugates of t generate G with probability at least c, if $G \neq \mathrm{SO}^{\varepsilon}_{2n}(2)$ and $G \neq \mathrm{Sp}_{2n}(q)$ with q even. In the exceptional case $G = \mathrm{Sp}_{2n}(q)$ with q even, two conjugates of t never generate G: in this case we prove that two random conjugates of t generate a subgroup $\mathrm{SO}^{\varepsilon}_{2n}(q)$ with probability at least c. The results underpin analysis of new constructive recognition algorithms for classical groups in even characteristic, which succeed where methods utilising involution centralisers are not available.

☆ This research forms part of Discovery Project DP110101153 of the first and second authors funded by the Australian Research Council.
* Corresponding author.
E-mail addresses: cheryl.praeger@uwa.edu.au (C.E. Praeger), sukru.yalcinkaya@istanbul.edu.tr (Ş. Yalçınkaya).
[1] Also affiliated with: King Abdulaziz University, Jeddah, Saudi Arabia.
[2] Our colleague Ákos Seress worked with us intensively on this research project for several years before his death, including the writing of several incomplete drafts of the paper. We completed the writing saddened by his passing. We hope he would be pleased at the outcome.
[3] Current address: İstanbul University, Vezneciler, İstanbul, Turkey.

http://dx.doi.org/10.1016/j.jalgebra.2014.08.020

1. Introduction

Motivated by an algorithmic application [12], we address a problem in statistical group theory related to generating finite classical groups. It involves the notion of a 'good element' in a classical group, defined as follows. Assume that $q = p^e$ is a prime power and $G = X_{2n}(q)$ is a $2n$-dimensional classical group where $X \in \{\mathrm{SL}, \mathrm{Sp}, \mathrm{SU}, \mathrm{SO}^{\varepsilon}\}$, acting naturally on a vector space $V \cong \mathbb{F}_{q^\delta}^{2n}$, where $\delta = 2$ in the unitary case and $\delta = 1$ otherwise. A prime number r is a *primitive prime divisor* of $q^n - 1$ if $r \mid q^n - 1$ but r does not divide $q^i - 1$ for any $i < n$. We often call r a $\mathrm{ppd}(n, q)$*-prime*. By [15], $\mathrm{ppd}(n, q)$-primes exist except when $(n, q) = (6, 2)$ or $(2, p)$, with p a Mersenne prime. We denote the greatest common divisor of the integers a, b by (a, b).

Definition 1. Define $\Phi^X(2, q) := \{(q + 1)/(q - 1, 2)\}$, and for $n \geq 3$, let $\Phi^X(n, q)$ be the set of all integers m such that

(i) m is divisible by some $\mathrm{ppd}(n, q^\delta)$-prime, or $(n, q^\delta) = (6, 2)$ and m is divisible by 9, and

(ii) m divides $\begin{cases} (q^n - 1)/(q - 1) & \text{if } X = \mathrm{SL} \\ (q^n + 1)/(q + 1) & \text{if } X = \mathrm{SU} \text{ and } n \text{ is odd} \\ q^{n/2} + 1 & \text{if } X = \mathrm{Sp} \text{ or } \mathrm{SO}^{\varepsilon} \text{ and } n \text{ is even.} \end{cases}$

We say that $t \in G = X_{2n}(q)$ is a *good element* if $o(t) \in \Phi^X(n, q)$ and t has an n-dimensional fixed point space.

We see in Lemma 3.1 that each good element acts irreducibly on an n-dimensional complement to its fixed point space. Good elements arise algorithmically in new procedures [3,12] to recognise finite d-dimensional classical groups over fields of even order q^δ given as matrix groups on their natural modules. Previously such algorithms were only available in odd characteristic. At a certain point in these algorithms an element t has been constructed with a large fixed point subspace, and acting irreducibly on a complementary subspace, say W. For example it is shown in [13, Corollary 3.5] that with $O(\log d)$ independent random selections one can find, with high probability, an element acting irreducibly on a subspace W of dimension $n = O(\log d)$, some power of which is an element t with these properties and with $|t|$ divisible by a primitive prime divisor of $q^{\delta n} - 1$. The object (see [3, p. 234]) is to find a random conjugate t' of t such that t, t' generate a classical group on a space W' of dimension $2n$ and fix pointwise a complement of W'. A suitable element is then found in $\langle t, t' \rangle$ with the same properties as t. Used recursively, this plays a key role in constructing a small dimensional classical subgroup in at most $\log_2 d$ steps. To the knowledge of the first and third authors, the idea of using good elements to 'double the degree' in this way was first conceived by the second author, and he developed this with Max Neunhöffer into a full recognition algorithm which is available in the recog package in GAP [11] and will be described in a forthcoming paper [12].

We consider a fundamental problem distilled from this process: namely, given a good element t in a finite classical group, determine how likely it is that t together with a random conjugate generate the whole classical group. A broad brush statement of our results is the following.

Theorem 2. *Let t be a good element in $X_{2n}(q)$, where $X \in \{\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon\}$ and if $X = \mathrm{SO}^\varepsilon$ then $q \geq 3$, and let t' be a uniformly distributed random conjugate of t. Then there is an absolute constant $c > 0$ such that,*

(a) $\langle t, t^g\rangle = X_{2n}(q)$ *with probability greater than c, if $(X, q) \neq (\mathrm{Sp}, \mathit{even})$, and*
(b) $\langle t, t^g\rangle \cong \mathrm{SO}^\varepsilon_{2n}(q)$ *with probability greater than c, if $(X, q) = (\mathrm{Sp}, \mathit{even})$.*

The proof and discussion of this theorem in Section 14 show that, for all these groups with $n \geq 9$ the value of c can be taken as 0.042. We believe that this result also holds for $\mathrm{SO}^\varepsilon_{2n}(q)$ with $q = 2$, but our analysis in Section 5 is not sufficiently strong to prove it. For an explanatory comment on the need to treat $(X, q) = (\mathrm{Sp}, \mathit{even})$ separately, see Remark 7(b). The precise problem we address is the following.

Problem 3. Given a good element $t \in G = X_{2n}(q)$ and a uniformly distributed random conjugate t^g of t, estimate from above the following probabilities.

(i) $p_1(X, n, q) := \mathrm{Prob}(\ \langle t, t^g\rangle$ is reducible on $V)$;
(ii) $p(X, n, q) := \mathrm{Prob}(\ \langle t, t^g\rangle \neq G$ and $\langle t, t^g\rangle$ is irreducible$\,)$, where if $X = \mathrm{Sp}$ we assume that q is odd;
(iii) if $X = \mathrm{Sp}$ and q is even, $\tilde{p}(\mathrm{Sp}, n, q) := \mathrm{Prob}(\langle t, t^g\rangle$ is irreducible and lies in a maximal subgroup M of $\mathrm{SO}^\pm_{2n}(q))$ (cf. Lemma 3.3).

Remark 4. First we note that, for $X \neq \mathrm{SL}$, n must satisfy certain parity restrictions in order for $X_{2n}(q)$ to contain good elements, namely, such elements exist if and only if $(X, n) = (\mathrm{SU}, \mathrm{odd}), (\mathrm{Sp}, \mathrm{even})$ or $(\mathrm{SO}^\varepsilon, \mathrm{even})$ (see Lemma 3.1 and Table 2). For the rest of the paper, we assume that these parity restrictions hold. Our main results are upper estimates for the quantities in Problem 3.

Theorem 5. *Let $G = X_{2n}(q)$, where $X \in \{\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon\}$, $q \geq 2$, and $n \geq 2$ if $X =$ SL, SU or Sp, and $n \geq 4$ if $X = \mathrm{SO}^\varepsilon$. Then*

$$p_1(X,n,q) < \begin{cases} \frac{2}{q} + \frac{1}{q^2} - \frac{2}{q^3} - \frac{1}{q^4} + \frac{2}{q^{n^2}} & \text{if } X = \mathrm{SL} \\ \frac{1}{q^2-1} + \frac{3}{2q^{n+2}} & \text{if } X = \mathrm{SU} \\ \frac{1}{q-1} - \frac{1}{q^{n+1}} & \text{if } X = \mathrm{Sp} \\ \frac{1}{(2,q-1)q} + \frac{1}{q(q-1)} + \frac{3}{q^{n/2+1}} & \text{if } X = \mathrm{SO}^+ \\ \frac{1}{(2,q-1)q} + \frac{1}{q(q-1)} + \frac{4}{q^{n/2+1}} & \text{if } X = \mathrm{SO}^-. \end{cases}$$

Theorem 6.

$$p(X,n,q) < \begin{cases} 10.5\, q^{-n^2+n+2} + O(q^{-n^2}) & \text{if } X = \mathrm{SL} \\ 9\, q^{-4(n^2-n)/3+2} + O(q^{-4n^2/3}) & \text{if } X = \mathrm{SU} \\ 3.7\, q^{-n^2/2} + O(q^{-2(n^2-n)/3}) & \text{if } X = \mathrm{Sp} \\ 10.6\, q^{-n^2/2} + O(q^{-2(n^2-n)/3}) & \text{if } X = \mathrm{SO}^\varepsilon \end{cases}$$

and, for q even, $\tilde{p}(\mathrm{Sp},n,q) < 3.7\, q^{-n^2/2} + O(q^{-2(n^2-n)/3})$.

Remark 7. (a) We note that our notation suppresses the order $o(t)$ of t and its G-conjugacy class, since our estimates are uniform across all G-conjugacy classes of good elements.

(b) Our reason for treating the case $X = \mathrm{Sp}$, q even, separately in Problem 3(ii) and (iii) is that, for these groups, if $\langle t, t^g \rangle \neq G$, then this subgroup is either reducible or contained in a subgroup $\mathrm{SO}^{\pm}_{2n}(q)$ (Lemma 3.3).

(c) The bounds in Theorem 5 are valid for all n in the statement, and also for all q. The upper bound for $p_1(\mathrm{SL}, n, 2)$ is less than 0.95 if $n \geq 3$, and in Lemma 5.3 we obtain an upper bound of 0.6 if $n = 2$. For $X = \mathrm{Sp}$, the upper bound is very close to 1 if $q = 2$, and in Lemma 5.7 we give an alternative method of proof for this case (a method which seems too complicated for large q) and prove that $p_1(\mathrm{Sp}, n, 2) < \frac{5}{6}$ for all $n \geq 2$. However we do not have an upper bound for $p_1(\mathrm{SO}^\varepsilon, n, 2)$ which is less than 1. We believe that an approach similar to that used for $p_1(\mathrm{Sp}, n, 2)$ would work, but would require many more subcases and journal pages for a proof.

(d) Although we state asymptotic upper bounds in Theorem 6, explicit (but rather complicated) upper bounds are proved. An explicit upper bound for each case may be obtained by adding the entries in the appropriate column of Table 7. The proof strategy, discussed in Subsection 1.1, involves considering separately several families of maximal subgroups which could contain $\langle t, t^g \rangle$. In all but the last family our results give the correct order of magnitude for the probability contribution, and hold for all $n \geq 3$ (and sometimes also for $n = 2$). Analysis for the last subgroup family, which consists of almost simple groups modulo the scalar matrices and not of geometric type, is less precise; it uses an upper bound [5] due to Häsä on the number of conjugacy classes of these subgroups.

(e) Our results were motivated by the need to justify a crucial part of a new recognition algorithm for finite classical groups, and this application guided our choice to generate the classical group with two random conjugates of a good element. However these results raise the interesting question as to whether two random elements with large fixed point spaces, and acting irreducibly on complementary subspaces, would also generate the classical group with high probability. In the algorithmic context the second random good element is constructed as a random conjugate so the more general context is not needed. Also the estimates we give in the paper would need serious reworking to fit the general situation. However, if true, the following conjecture may have future algorithmic applications.

Conjecture 1. *There is an absolute constant $c > 0$ such that the following holds. Let G be an n-dimensional classical matrix group over a finite field, and let $i, i' \in \{0, \ldots, n\}$ be random and such that $i + i' \leq n$. Let $t, t' \in G$ be random elements with fixed point spaces of dimension i, i', respectively, and such that each of t, t' acts irreducibly on the quotient space modulo the fixed point space.*

1. *If these fixed point spaces intersect trivially and G is not symplectic in even characteristic, then the probability that $\langle t, t' \rangle = G$ is at least c.*
2. *If the fixed point spaces intersect trivially and G is symplectic in even characteristic, then the probability that $\langle t, t' \rangle$ is an orthogonal group of degree n is at least c.*

1.1. Proof strategy

Let $G = X_{2n}(q)$ as in Theorems 5 and 6, and let t, t^g be as in Problem 3. If $\langle t, t^g \rangle \neq G$, then t and t^g belong to some maximal subgroup $M < G$. By Aschbacher's theorem [1], maximal subgroups of G belong to one of nine categories $\mathbf{C}_1, \ldots, \mathbf{C}_9$. Our standard reference is the book of Kleidman and Liebeck [8], where the exact conditions are given on when a subgroup belonging to a category $\mathbf{C}_i$ is maximal in G. We use a modified definition of $\mathbf{C}_1$, namely *we take $\mathbf{C}_1$ to be the set of all subgroups M of G that are maximal with respect to being reducible on V.*

Let $\mathcal{C}$ be a conjugacy class in G of good elements. For a fixed $t \in \mathcal{C}$, set

$$W_1 = \{t^g \mid g \in G,\ \exists M \in \mathbf{C}_1,\ t, t^g \in M\},$$
$$W_2 = \{t^g \mid g \in G,\ \exists M \in \mathbf{C}_i,\ i \neq 1,\ t, t^g \in M,\ \text{and } \langle t, t^g \rangle \text{ irreducible}\}.$$

Then $p_1(X, n, q) = \frac{|W_1|}{|\mathcal{C}|}$ and $p(X, n, q) = \frac{|W_2|}{|\mathcal{C}|}$. We also set

$$\widehat{W_1} = \{(s, s^g) \mid g \in G, \exists M \in \mathbf{C}_1,\ s, s^g \in M \cap \mathcal{C}\},$$
$$\widehat{W_2} = \{(s, s^g) \mid g \in G,\ \exists M \in \mathbf{C}_i,\ i \neq 1,\ s, s^g \in M \cap \mathcal{C},\ \text{and } \langle s, s^g \rangle \text{ irreducible}\}.$$

Since $|W_i|$, $i = 1, 2$, is independent of the choice of $t \in \mathcal{C}$, it follows that $|\widehat{W_i}| = |\mathcal{C}| \cdot |W_i|$ for each $i = 1, 2$. Hence

$$p_1(X, n, q) = \frac{|\widehat{W_1}|}{|\mathcal{C}|^2} \quad \text{and} \quad p(X, n, q) = \frac{|\widehat{W_2}|}{|\mathcal{C}|^2}. \tag{1}$$

Note that

$$|\widehat{W}_1| \le \sum_{M\in\mathbf{C}_1} |M\cap\mathcal{C}|^2 \quad \text{and} \quad |\widehat{W}_2| \le \sum_{i=2}^{9}\sum_{M\in\mathbf{C}_i} |M\cap\mathcal{C}|^2. \tag{2}$$

For each i, we identify a set $\mathcal{S}_i$ of conjugacy classes of subgroups in $\mathbf{C}_i$ that cover all the possible subgroups $\langle t, t^g\rangle$. This set may be smaller than the set of all conjugacy classes in $\mathbf{C}_i$, see for example the analysis for $\mathbf{C}_1$ in Section 5. For each $\mathbf{S}\in\mathcal{S}_i$, let $M(\mathbf{S})$ denote a representative subgroup of $\mathbf{S}$. Then (1) and (2) imply

$$p_1(X,n,q) \le \sum_{\mathbf{S}\in\mathcal{S}_1} \frac{|G|}{|N_G(M(\mathbf{S}))|}\frac{|M(\mathbf{S})\cap\mathcal{C}|^2}{|\mathcal{C}|^2} \quad \text{and} \quad p(X,n,q) \le \sum_{i=2}^{9} p_i(X,n,q) \tag{3}$$

noting that some subgroups in $\mathbf{C}_1$ may not be self-normalising, where each

$$p_i(X,n,q) = \sum_{\mathbf{S}\in\mathcal{S}_i} \frac{|G|}{|M(\mathbf{S})|}\frac{|M(\mathbf{S})\cap\mathcal{C}|^2}{|\mathcal{C}|^2}. \tag{4}$$

For $G = \mathrm{Sp}_{2n}(q)$ with q even, note that, if $\langle t, t^g\rangle$ is irreducible, then it lies in a subgroup $\mathrm{SO}^{\varepsilon}_{2n}(q)$ of G (see Remark 7 and Lemma 3.3). We need to count pairs (t, t^g) such that $\langle t, t^g\rangle$ is irreducible and properly contained in such a subgroup. Thus there exists a subgroup $H \cong \mathrm{SO}^{\varepsilon}_{2n}(q)$ of G such that $\langle t, t^g\rangle$ is contained in one of the maximal subgroups M of $\bigcup_{i=2}^{9} \mathbf{C}^{\varepsilon}_i(H)$, where $\mathbf{C}^{\varepsilon}_i(H)$ is the ith Aschbacher class of maximal subgroups of H, as above.

For each $\varepsilon = \pm$, there is a single G-conjugacy class of subgroups H by [8, Prop. 4.8.6], and hence each H-conjugacy class in $\mathbf{C}^{\varepsilon}_i(H)$ lies in a single G-conjugacy class. The subgroups in $\mathbf{C}^{\varepsilon}_i(H)$ may be contained in maximal subgroups of G lying in the Aschbacher class $\mathbf{C}_i$ for G. However this is not always the case. For example, the stabiliser in H of an orthogonal decomposition of V as a sum of 1-dimensional spaces lies in $\mathbf{C}^{\varepsilon}_2(H)$ but no subgroup of $\mathbf{C}_2$ for G contains it, see Lemma 6.1. Thus we define $\mathbf{C}'_i$ as the union of $\mathbf{C}_i$, for G, together with those subgroups which are conjugate to a maximal subgroup in $\mathbf{C}^{\varepsilon}_2(H)$ (for $\varepsilon = \pm$) but which do not lie in subgroups in $\mathbf{C}_i$. Similarly to our previous strategy, we identify a set $\mathcal{S}'_i$ of conjugacy classes of subgroups in $\mathbf{C}'_i$ that cover all the irreducible $\langle t, t^g\rangle$ contained in subgroups in $\mathbf{C}^{\varepsilon}_2(H)$ (for some $\varepsilon = \pm$), and for each $\mathbf{S}\in\mathcal{S}'_i$, we choose a representative subgroup $M(\mathbf{S})$ of $\mathbf{S}$. Then similar arguments to those above show that

$$\tilde{p}(\mathrm{Sp},n,q) \le \sum_{i=2}^{9} \tilde{p}_i(\mathrm{Sp},n,q), \quad \text{where } \tilde{p}_i(\mathrm{Sp},n,q) = \sum_{\mathbf{S}\in\mathcal{S}'_i} \frac{|G|}{|M(\mathbf{S})|}\frac{|M(\mathbf{S})\cap\mathcal{C}|^2}{|\mathcal{C}|^2}. \tag{5}$$

We prove some preliminary arithmetic results in Section 2, and basic facts about good elements in Section 3. Section 4 contains an analysis of the alternating and symmetric

Table 1
The orders of the classical groups.

G	$\|G\|$
$\mathrm{GL}_n(q)$	$q^{n^2}\Theta(1, n; q)$
$\mathrm{GU}_n(q)$	$q^{n^2}\Theta(1, n; -q)$
$\mathrm{Sp}_{2n}(q)$	$q^{2n^2+n}\Theta(1, n; q^2)$
$\mathrm{O}^{\varepsilon}_{2n}(q)$, $\varepsilon = \pm$	$2q^{2n^2-n}(1 - \varepsilon q^{-n})\Theta(1, n-1; q^2)$
$\mathrm{O}_n(q)$, n odd	$2q^{(n^2/2)-(n/2)}\Theta(1, \frac{n-1}{2}; q^2)$

groups acting on their deleted permutation modules and identifies the good elements that arise and their contribution to the proportions $p_9(X, n, q)$ and $\tilde{p}_9(\mathrm{Sp}, n, q)$. In Sections 5–13 we estimate the probability contributions $p_i(X, n, q)$ and $\tilde{p}_i(\mathrm{Sp}, n, q)$ for $i = 1, \dots, 9$. Theorem 5 is proved in Section 5, and Theorems 2 and 6 are proved in Section 14.

2. Preliminary results

We first note that r is a $\mathrm{ppd}(n, q)$ if and only if q has order n modulo r. Hence $r \equiv 1 \pmod{n}$ and

$$r = kn + 1 \tag{6}$$

for some positive integer k. In particular, we have $r \geq n + 1$.

The following lemma will be used in the computations in Section 7.

Lemma 2.1. *Let $n, q \geq 2$. Then $f(x) = xq^{2n^2/x}$ is a decreasing function for $1 \leq x \leq n$.*

Proof. Observe that $f'(x) = q^{2n^2/x}(1 - (2n^2 \ln q)/x)$. Now $1 - (2n^2 \ln q)/x < 0$ for $1 \leq x \leq n$ and the result follows. □

For positive integers n, q with $q \geq 2$, set $\Theta(0, n; \pm q) = 1$, and for an integer k satisfying $1 \leq k \leq n$ define

$$\Theta(k, n; q) := \prod_{i=k}^{n}\left(1 - q^{-i}\right) \quad \text{and} \quad \Theta(k, n; -q) := \prod_{i=k}^{n}\left(1 - (-q)^{-i}\right). \tag{7}$$

Then, by [14], the orders of the classical groups can be expressed as in Table 1.

The following technical lemmas will be useful in our computations.

Lemma 2.2. *Assume that k, n, q are integers satisfying $1 \leq k \leq n$ and $q \geq 2$.*

(i) *Then*

$$1 - \frac{1}{q} - \frac{1}{q^2} < \Theta(k, n; q) < 1$$

$$1 < \Theta(k, n; -q) \le 1 + \frac{1}{q^k} \quad \textit{if } k \textit{ is odd,}$$

$$1 - \frac{1}{q^k} < \Theta(k, n; -q) < 1 \quad \textit{if } k \textit{ is even.}$$

(ii) *Moreover if* $k < n$*, then*

$$1 < \frac{\Theta(k+1, n; q)}{\Theta(1, n-k; q)} < \left(1 - \frac{1}{q} - \frac{1}{q^2}\right)^{-1}$$

$$\frac{1 - q^{-k-1}}{1 + q^{-1}} < \frac{\Theta(k+1, n; -q)}{\Theta(1, n-k; -q)} < 1 \quad \textit{if } k \textit{ is odd,}$$

$$\frac{1}{1 + q^{-1}} < \frac{\Theta(k+1, n; -q)}{\Theta(1, n-k; -q)} < 1 + \frac{1}{q^{k+1}} \quad \textit{if } k \textit{ is even,}$$

(iii) *and if* n *is even,* $n \ge 4$ *then*

$$\frac{1 - q^{-2} - q^{-4}}{1 - q^{-n}} < \frac{\Theta(1, \frac{n}{2} - 1; q^2)}{\Theta(\frac{n}{2}, n-1; q^2)} < \frac{1}{1 - q^{-n}}.$$

Proof. The inequalities in (i) and the lower bound for the first line of (ii) are the content of [10, Lemma 3.5] and [14, Lemmas 3.1 and 3.2]. The upper bound for the first line of (ii) follows from two applications of the first line of (i). Similarly the second and third lines of (ii) follow from multiple applications of the second and third lines of (i). For part (iii), observe that $\frac{\Theta(1,n/2-1;q^2)}{\Theta(n/2,n-1;q^2)} = \frac{\Theta(1,n/2;q^2)}{(1-q^{-n})\Theta(n/2,n-1;q^2)}$, and apply the first line of part (ii). □

Lemma 2.3. *Assume that* n, m, q *are integers with* $1 \le m < n$*. Then*

(i) $\frac{\Theta(1,n;-q)}{\Theta(1,m;-q)} \le \begin{cases} 1 & \textit{if } m \textit{ is odd} \\ 1 + q^{-m-1} & \textit{if } m \textit{ is even.} \end{cases}$

(ii) $\frac{\Theta(1,m;-q)}{\Theta(1,n;-q)} \le \begin{cases} 1 & \textit{if } m \textit{ is even} \\ \frac{1}{1-q^{-m-1}} & \textit{if } m \textit{ is odd.} \end{cases}$

Proof. (i) Assume first that n is odd. For m odd, we have $\frac{\Theta(1,n;-q)}{\Theta(1,m;-q)} = (1 - q^{-m-1})(1 + q^{-m-2}) \cdots (1 + q^{-n})$. It is clear that, for any $s \ge 1$, the product $(1 - q^{-s})(1 + q^{-s-1}) \le 1$. Hence the result follows. If m is even, then $\frac{\Theta(1,n;-q)}{\Theta(1,m;-q)} = (1 + q^{-m-1})(1 - q^{-m-2}) \cdots (1 + q^{-n})$. Our previous argument shows that $(1 - q^{-m-2}) \cdots (1 + q^{-n}) \le 1$ and the result follows.

Assume now that n is even. Then $\frac{\Theta(1,n;-q)}{\Theta(1,m;-q)} = \frac{\Theta(1,n-1;-q)}{\Theta(1,m;-q)}(1 - q^{-n})$. Hence the result follows from the above computations.

Table 2
Tori and centralizers for good elements in classical groups.

G	Parity of n	$\|T\|$	$\|C_G(t)\|$
$\mathrm{SL}_{2n}(q)$	any	$(q^n-1)/(q-1)$	$(q^n-1)\|\mathrm{SL}_n(q)\|$
$\mathrm{SU}_{2n}(q)$	odd	$(q^n+1)/(q+1)$	$(q^n+1)\|\mathrm{SU}_n(q)\|$
$\mathrm{Sp}_{2n}(q)$	even	$q^{n/2}+1$	$(q^{n/2}+1)\|\mathrm{Sp}_n(q)\|$
$\mathrm{SO}^{\varepsilon}_{2n}(q)$, $\varepsilon=\pm$	even	$q^{n/2}+1$	$(q^{n/2}+1)\|\mathrm{SO}^{-\varepsilon}_n(q)\|$

(ii) In this case observe that the product $(1+q^{-s})(1-q^{-s-1})\geq 1$ for any $s\geq 1$, $q\geq 2$. Then the results follow from similar computations to part (i). $\square$

3. Good elements in classical groups

Let G be a classical group isomorphic to $\mathrm{SL}_{2n}(q)$, $\mathrm{SU}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$ or $\mathrm{SO}^{\varepsilon}_{2n}(q)$, and let V denote the underlying vector space $V=V(2n,q^{\delta})$ where $\delta=1$ for $\mathrm{SL}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$ and $\mathrm{SO}^{\varepsilon}_{2n}(q)$, and $\delta=2$ for $\mathrm{SU}_{2n}(q)$. We assume that $n\geq 2$ if $G\cong\mathrm{SL}_{2n}(q)$, $\mathrm{SU}_{2n}(q)$ or $\mathrm{Sp}_{2n}(q)$, and $n\geq 4$ if $G\cong\mathrm{SO}^{\varepsilon}_{2n}(q)$.

Lemma 3.1. *Suppose that t is a good element in $G=X_{2n}(q)$ with fixed point subspace U.*

- (i) *Then t preserves a decomposition $V=U\oplus W$, such that t acts irreducibly on W, if $X\neq\mathrm{SL}$ then U and W are non-degenerate, and if $X=\mathrm{SO}^{\varepsilon}$ then W has minus type;*
- (ii) *t lies in a unique cyclic torus T such that T preserves $V=U\oplus W$, T has fixed point subspace U, $C_G(t)=C_G(T)$, and $|T|$, $|C_G(t)|$, and the parity of n are as in Table 2. Also $|N_G(T)|=n|C_G(T)|$ and the number of G-conjugates of t contained in T is n.*
- (iii) *Conversely for G of type X, for n as in Table 2 and each $m\in\Phi^X(n,q)$, G contains $\varphi(m)/n$ conjugacy classes of good elements of order m where φ is the Euler phi function.*

Proof. (i) The good element t acts on the n-dimensional quotient V/U and since $o(t)\in\Phi^X(n,q)$, it follows that t is irreducible on V/U. By Definition 1, t is semisimple, and so by Maschke's Theorem, there exists a t-invariant complement W for U. Hence t preserves the decomposition $V=U\oplus W$ with t irreducible on W. Moreover W is uniquely determined by t. Suppose now that $X\neq\mathrm{SL}$. Then, for $u\in U$ and $w\in W$, we have $(u,w)=(u^t,w^t)=(u,w^t)$, so $(u,w^t-w)=0$. Notice that $t-\mathrm{I}$ is nonsingular on W, so $\{w^t-w\mid w\in W\}=W$. Therefore $u\in W^{\perp}$ for each $u\in U$, so $U\subseteq W^{\perp}$. Since the dimension of $U^{\perp}$ is n, we have $W=U^{\perp}$, so both U and W are nondegenerate. If $X=\mathrm{SO}^{\varepsilon}$ then W is of minus type since the group induced by G_W on W contains the irreducible element $t|_W$.

(ii) By [6, Satz II.7.3], the centraliser of $t|_W$ in $\mathrm{GL}(W)$ is a cyclic torus $\hat{T}$ of order q^n-1, and it follows, on identifying $\mathrm{GL}(W)$ with a subgroup of $\mathrm{GL}(V)$ fixing U pointwise, that $T := \hat{T} \cap G$ is the unique cyclic torus containing t such that T preserves $V = U \oplus W$ and T has fixed point subspace U. Now $N_{\mathrm{GL}(V)}(\hat{T})$ leaves both U and W invariant, and it follows from [6, Satz II.7.3] that $N_{\mathrm{GL}(V)}(\hat{T}) = \mathrm{GL}(U) \times N_{\mathrm{GL}(W)}(\hat{T})$ with $N_{\mathrm{GL}(W)}(\hat{T}) = \hat{T}.n$, and $C_{\mathrm{GL}(V)}(t) = C_{\mathrm{GL}(V)}(\hat{T})$. Part (ii) and the entries in Table 2 now follow for the case $X = \mathrm{SL}$ on intersecting with $\mathrm{SL}(V)$.

Assume now that $X \neq \mathrm{SL}$, so $U = W^\perp$, and $t|_W$ is an irreducible element of order $o(t)$ in the classical group $H(W)$ induced on W by the setwise stabiliser of W in G. It follows that the parity of n is as in Table 2, and that W is of minus-type if $X = \mathrm{SO}^\varepsilon$ (so in this case U is of type $-\varepsilon$). Now $C_G(T) = C_G(t) \le C := H(U) \times C_{H(W)}(T)$, where $H(U)$ is the classical group induced on U by the setwise stabiliser of U in G, and $C_{H(W)}(T)$ is a torus containing T of order $q^n+1, q^{n/2}+1, q^{n/2}+1$ for $X = \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon$, respectively. For $X = \mathrm{Sp}, \mathrm{SO}^\varepsilon$, we have $C_{H(W)}(T) = T$ of order $q^{n/2}+1$, while $T = C_{H(W)}(T) \cap G$ has index $q+1$ in $C_{H(W)}(T)$ for $X = \mathrm{SU}$. Hence $|T|$ and $|C_G(t)|$ are as in Table 2, for these cases also.

In each case, all tori of $H(W)$ of order $|T|$ are conjugate in $H(W)$, and hence all tori of G of order $|T|$ and with an n-dimensional fixed point space are conjugate in G. For all types, $|N_G(T)| = n|C_G(T)|$ (see [8, Props. 4.3.6, 4.3.10] and the last paragraph of the proof of [8, Lemma 4.3.15] for type SO^ε). In all cases $N_G(T)$ acts by conjugation on the good elements contained in T with orbits of length n. Thus T contains n good elements that are $N_G(T)$-conjugate to t. On the other hand, if t' is a G-conjugate of t and $t' \in T$, then, by the uniqueness of T, an element of G conjugating t' to t lies in $N_G(T)$. It follows that T contains exactly n of the G-conjugates of t, and these elements form a single orbit under the action of $N_G(T)$.

(iii) Conversely, suppose that n is as in Table 2. Let T be a cyclic torus with an n-dimensional fixed point subspace and order as in Table 2. If $n > 2$, then all elements of T of order divisible by a $\mathrm{ppd}(n, q^\delta)$-prime are good elements, if $(n, q^\delta) = (6, 2)$, then all elements of T of order 9 are good elements, and if $n = 2$, then all elements of T of order $(q+1)/(q-1, 2)$ are good elements. Let $m \in \Phi^G(n, q)$. Then T contains good elements of order m, namely the $\varphi(m)$ generators of its unique subgroup of order m where φ is the Euler phi function. We have shown that, from each G-conjugacy class of good elements, exactly n lie in T and form a single $N_G(T)$-class. Hence there are exactly $\varphi(m)/n$ conjugacy classes of good elements of order m in G. □

This result leads to the following estimates for the quantity $|C_G(t)|^2/|G|$, for a good element t in G.

Corollary 3.2. *Let $G = X_{2n}(q)$ and let $t \in G$ be a good element. Then*

$$\frac{|C_G(t)|^2}{|G|} \le \begin{cases} \frac{(q^n-1)^2}{(q-1)q^{2n^2}} \le \frac{1}{q^{2n^2-2n}} & \textit{if } X = \mathrm{SL} \\ \frac{(q^n+1)^2}{q^{2n^2+1}} \le \frac{8}{16q^{2n^2-2n}} & \textit{if } X = \mathrm{SU} \\ \frac{25}{16}q^{-n^2+n} & \textit{if } X = \mathrm{Sp} \\ \frac{25}{9}q^{-n^2+n} & \textit{if } X = \mathrm{SO}^\varepsilon. \end{cases}$$

Proof. We use the data from Tables 1 and 2, the inequalities from Lemma 2.2, and that $q \ge 2$. First let $X = \mathrm{SL}$. Then

$$\begin{aligned} \frac{|C_G(t)|^2}{|G|} &= \frac{(q^n-1)^2|\mathrm{SL}_n(q)|^2}{|\mathrm{SL}_{2n}(q)|} = \frac{(q^n-1)^2 q^{2n^2}\Theta(1,n;q)^2}{(q-1)q^{4n^2}\Theta(1,2n;q)} \\ &< \frac{(q^n-1)^2\Theta(1,n;q)}{(q-1)q^{2n^2}\Theta(n+1,2n;q)} \\ &< \frac{(q^n-1)^2}{(q-1)q^{2n^2}} < \frac{1}{q^{2n^2-2n}} \end{aligned}$$

applying Lemma 2.2(ii). Next, for $X = \mathrm{SU}$, we use also that $n \ge 3$ and n is odd (from Table 2), as well as Lemma 2.2(ii).

$$\begin{aligned} \frac{|C_G(t)|^2}{|G|} &= \frac{(q^n+1)^2|\mathrm{SU}_n(q)|^2}{|\mathrm{SU}_{2n}(q)|} = \frac{(q^n+1)^2 q^{2n^2}\Theta(1,n;-q)^2}{(q+1)q^{4n^2}\Theta(1,2n;-q)} \\ &= \frac{(q^n+1)^2\Theta(1,n;-q)}{(q+1)q^{2n^2}\Theta(n+1,2n;-q)} < \frac{(q^n+1)^2(1+q^{-1})}{(q+1)q^{2n^2}} \\ &= \frac{(q^n+1)^2}{q^{2n^2+1}} \le \frac{9}{16q^{2n^2-2n}}. \end{aligned}$$

For $X = \mathrm{Sp}$, we have n even and we use Lemma 2.2(ii) as for the SL-case.

$$\begin{aligned} \frac{|C_G(t)|^2}{|G|} &= \frac{(q^{n/2}+1)^2|\mathrm{Sp}_n(q)|^2}{|\mathrm{Sp}_{2n}(q)|} = \frac{(q^{n/2}+1)^2 q^{n^2+n}\Theta(1,n/2;q^2)^2}{q^{2n^2+n}\Theta(1,n;q^2)} \\ &= \frac{(1+q^{-n/2})^2\Theta(1,n/2;q^2)}{q^{n^2-n}\Theta(n/2+1,n;q^2)} < \frac{(1+q^{-n/2})^2}{q^{n^2-n}}. \end{aligned}$$

If $n = 2$, then a direct computation gives $\frac{|C_G(t)|^2}{|G|} < \frac{6}{5}q^{-n^2+n}$, while if $n \ge 4$, then the last expression above is at most $\frac{25}{16}q^{-n^2+n}$. Finally, if $X = \mathrm{SO}^\varepsilon$, then $n \ge 4$ and n is even. Hence, using Lemma 2.2(iii),

$$\begin{aligned} \frac{|C_G(t)|^2}{|G|} &= \frac{(q^{n/2}+1)^2|\mathrm{SO}_n^{-\varepsilon}(q)|^2}{|\mathrm{SO}_{2n}^{\varepsilon}(q)|} \\ &= \frac{(q^{n/2}+1)^2 q^{n^2-n}(1+\varepsilon q^{-n/2})^2\Theta(1,n/2-1;q^2)^2}{q^{2n^2-n}(1-\varepsilon q^{-n})\Theta(1,n-1;q^2)} \end{aligned}$$

$$= \frac{(1+q^{-n/2})^2(1+\varepsilon q^{-n/2})^2\Theta(1,n/2-1;q^2)}{q^{n^2-n}(1-\varepsilon q^{-n})\Theta(n/2,n-1;q^2)}$$

$$< \frac{(1+q^{-n/2})^2(1+2/(q^{n/2}-1))}{q^{n^2-n}(1-q^{-n})}. \tag{8}$$

Using $q \geq 2$ and $n \geq 4$ this quantity is at most $(\frac{25}{16} \cdot \frac{16}{15} \cdot \frac{5}{3})q^{-n^2+n} = \frac{25}{9}q^{-n^2+n}$. □

Next we analyse the irreducible subgroups $\langle t, t^g \rangle$ mentioned in Remark 7(d).

Lemma 3.3. *Let $G \cong \mathrm{Sp}_{2n}(q)$ where q, n are even. Let $m \in \Phi^{\mathrm{Sp}}(n,q)$ and $t \in G$ be a good element of order m. Then for $g \in G$, either $\langle t, t^g \rangle$ is reducible on V, or $\langle t, t^g \rangle \leq \mathrm{SO}^{\pm}_{2n}(q)$.*

Proof. Note that $\mathrm{PSp}_{2n}(q) \cong \Omega_{2n+1}(q)$. Let $\hat{V}$ be the associated orthogonal space of dimension $2n+1$ for G with nonsingular 1-dimensional radical R and $V = \hat{V}/R$. Then t acts irreducibly on a non-degenerate n-dimensional subspace $\hat{W}$ of $\hat{V}$ and fixes pointwise an $(n+1)$-dimensional subspace $\hat{U}$. In particular $\hat{W} = [\hat{V}, t] = \langle vt - v \mid v \in \hat{V} \rangle$ has dimension n. Take an element $g \in G$. Then similarly $[\hat{V}, t^g]$ is non-degenerate of dimension n. Thus $Y := [\hat{V}, t] + [\hat{V}, t^g]$ has dimension at most $2n$ and is left invariant by $\langle t, t^g \rangle$. If $Y \cap Y^{\perp} \nleq R$, then $\langle t, t^g \rangle$ leaves invariant the non-zero totally isotropic subspace $((Y \cap Y^{\perp}) + R)/R$ of V. If $Y \cap Y^{\perp} \leq R$ and $Y + R \neq \hat{V}$, then $(Y+R)/R$ is a non-degenerate proper subspace of V invariant under $\langle t, t^g \rangle$. Finally if $Y \cap Y^{\perp} \leq R$ and $Y + R = \hat{V}$, then Y is a hyperplane of $\hat{V}$ not containing R, and the stabilisers in G of such hyperplanes are $\mathrm{SO}^{\pm}_{2n}(q)$. □

We finish this section with a result about subspaces invariant under a good element.

Lemma 3.4. *Let $t \in \mathrm{SL}_{2n}(q)$ be a good element preserving a decomposition $V = U \oplus W$ as in Lemma 3.1, and let Z be an arbitrary t-invariant subspace of V. Then either $Z \subseteq U$ or $W \subseteq Z$.*

Proof. Let $u + w \in Z \setminus \{0\}$ with $u \in U$ and $w \in W$. If for all such vectors the component w is zero, then $Z \subseteq U$. Suppose on the other hand that $w \neq 0$ for some vector in Z. Then Z contains $(u+w)t^j = u + wt^j$, and hence also $wt^j - w$, for each $j = 1, \dots, n-1$. Since $t|_W$ is irreducible, the vectors $w, wt, \dots, wt^{n-1}$ are linearly independent, and hence $wt - w, \dots, wt^{n-1} - w$ generate an $(n-1)$-dimensional subspace of $Z \cap W$. Since $n \geq 2$, $Z \cap W$ is t-invariant, and $t|_W$ is irreducible, it follows that $W \subseteq Z$. □

4. Alternating and symmetric groups

In this section we identify good elements that act on the deleted permutation module of an alternating or symmetric group (Lemma 4.5). We use the following notation and definitions. We denote the symmetric group on n letters by S_n. Let $V = \mathbb{F}_q^{\ell}$, $q = p^k$, and let $M = S_\ell$ act on V by permuting the coordinates naturally. In this section only we follow the usage of [9, Section 4] and use U, W to denote the following subspaces of V.

$$W := \left\{(x_1, \dots, x_\ell) \in V \,\middle|\, \sum x_i = 0\right\} \quad \text{and} \quad E := \langle e \rangle, \quad \text{where } e = (1, 1, \dots, 1).$$

Then W and E are the only non-zero proper S_ℓ-invariant subspaces of V. Moreover, E is contained in W if and only if p divides ℓ. Defining $U := W/(W \cap E)$, we have

$$\dim(U) = \begin{cases} \ell - 1 & \text{if } p \text{ does not divide } \ell \\ \ell - 2 & \text{if } p \mid \ell. \end{cases}$$

The quotient space U is called the *fully deleted permutation module.*

Let $\mathcal{B} = \{e_1, \dots, e_\ell\}$ be the standard basis for V. Then $v_i = e_i - e_{i+1} + W \cap E$, for $1 \le i \le m$, forms a basis $\mathcal{B}' = \{v_1, \dots, v_m\}$ for U, where $m = \ell - 2$ or $\ell - 1$ depending on whether p divides ℓ, or p does not divide ℓ, respectively. If p is an odd prime, then for $n \ge 3$, by [9, Section 4],

(a) S_{2n+1} is contained in $\mathrm{PO}^{\varepsilon}_{2n}(p)$ if $p \nmid 2n + 1$;
(b) S_{2n+2} is contained in $\mathrm{PO}^{\varepsilon}_{2n}(p)$ if $p \mid n + 1$.

If $p = 2$, then

(c) S_{2n+2} is contained in $\begin{cases} \mathrm{O}^{+}_{2n}(2) & \text{if } n \equiv 3 \pmod 4, \\ \mathrm{O}^{-}_{2n}(2) & \text{if } n \equiv 1 \pmod 4, \\ \mathrm{Sp}_{2n}(2) & \text{if } n \text{ is even;} \end{cases}$

(d) S_{2n+1} is contained in $\begin{cases} \mathrm{O}^{+}_{2n}(2) & \text{if } n \equiv 0 \pmod 4, \\ \mathrm{O}^{-}_{2n}(2) & \text{if } n \equiv 2 \pmod 4. \end{cases}$

We note that, if $X_{2n}(p)$ is one of the orthogonal groups in (a)–(d) above, then $S_{2n+1} \times Z$ or $S_{2n+2} \times Z$, as appropriate, is a maximal $\mathcal{C}_9$-subgroup where Z is the centre of $X_{2n}(p)$ and $|Z| = (p - 1, 2)$. We use this notation throughout this section to examine good elements in these groups.

Lemma 4.1. *Suppose that $S_\ell \times Z$ lies in an orthogonal group $X_{2n}(p)$ as above, where $n \ge 3$ and $\ell \in \{2n + 1, 2n + 2\}$. If $S_\ell \times Z$ contains a good element t, then the largest prime r dividing $o(t)$ is $r = n + 1$ or $r = 2n + 1$, and r is a* ppd(n, p)*-prime.*

Proof. By Definition 1, the order of t is divisible by a ppd(n, p)-prime, say r, and by (6), $r = kn + 1$ for some $k \ge 1$. Since $\ell < 3n + 1$, the only possibilities are $k = 1$ or $k = 2$. If $s > r$ and s is a prime dividing $o(t)$, then $s + r \le \ell \le 2n + 2 \le 2r$, which is a contradiction. □

Table 3
Conditions for $v \in W$ to be fixed by ag in Lemma 4.2.

a	p	Conditions on the k_i	Conditions on the a_i and b
1	odd	$I_1 = 0$	$b = 0$ if $p \nmid \ell$
1	2	$I_1 = 0$, I_2 even	$b = 0$ if $p \nmid \ell$
1	2	$I_1 = 0$, I_2 odd	$b = 0$
1	–	$I_1 > 0$	$b = 0$ and $\sum_{i=1}^s k_i a_i = 0$
−1	odd	–	$a_i = b/2$ for each odd k_i, and $b = 0$ if $p \nmid \ell$

Recall that $\mathcal{B} = \{e_1, \ldots, e_\ell\}$ is the standard basis for $V = \mathbb{F}_p^\ell$. Let $k_1, \ldots, k_s$ be positive integers with $\sum_{i=1}^s k_i = \ell$ and, for $1 \le i \le s$, let $\ell_i := \sum_{j<i} k_j$ (so $\ell_1 = 0$). For an integer j, let $\delta_j = 0$ if j is even and $\delta_j = 1$ if j is odd. For $1 \le i \le s$ and $a_i, b \in \mathbb{F}_p$, define

$$v(i, a_i, 1, b) = \sum_{j=1}^{k_i} \big(a_i + (j-1)b\big) e_{\ell_i + j},$$

$$v(i, a_i, -1, b) = \sum_{j=1}^{k_i} \big((-1)^{j-1} a_i + \delta_{j-1} b\big) e_{\ell_i + j}. \tag{9}$$

Lemma 4.2. *Using the notation $V, W, E = \langle e \rangle, s, e_i, k_i, \ell_i$ as above, let $w_i = (\ell_i + 1, \ldots, \ell_i + k_i)$ for each $i \le s$, and let $g = w_1 \cdots w_s \in S_\ell$. Let $v \in V$ and $a = \pm 1$. Then $v + W \cap E$ is fixed by ag if and only if there exist $a_1, \ldots, a_s, b \in \mathbb{F}_q$ such that $v = \sum_{i=1}^s v(i, a_i, a, b)$, with $b = 0$ if $W \cap E = 0$, and for each $i \le s$,*

$$\big(1 + a + \cdots + a^{k_i - 1}\big)\big((a-1)a_i + b\big) = 0. \tag{10}$$

Moreover the vector $v = \sum_{i=1}^s v(i, a_i, a, b)$ lies in W if and only if

$$\sum_{i=1}^s k_i a_i + \left(\sum_{i=1}^s \binom{k_i}{2}\right) b = 0 \quad \text{if } a = 1$$

$$\sum_{i=1}^s \delta_{k_i} a_i + \left(\sum_{i=1}^s \left\lfloor \frac{k_i}{2} \right\rfloor\right) b = 0 \quad \text{if } a = -1. \tag{11}$$

Also both conditions, '$v \in W$' and '$v + W \cap E$ is fixed by ag', hold if and only if the elements a_i, b and the numbers $I_1 = \#\{i \mid p \nmid k_i\}$ and $I_2 = \#\{i \mid k_i \equiv 2 \pmod 4\}$ are as in one of the rows of Table 3.

Proof. The coset $v + W \cap E$ is fixed by ag if and only if $avg = v - be$ for some $b \in \mathbb{F}_q$, with $b = 0$ if $W \cap E = 0$. In order for this equation to hold, for each i the coefficient a_i of e_{ℓ_i+1} in v determines the coefficients of e_{ℓ_i+j} for $2 \le j \le k_i$ recursively (equating coefficients of these basis vectors on both sides of the equation): namely, the coefficient of e_{ℓ_i+2} is $aa_i + b, \ldots,$ the coefficient of $e_{\ell_i+k_i}$ is $a^{k_i-1}a_i + (1 + a + \cdots + a^{k_i-2})b$, that is to say, the coefficient of e_{ℓ_i+j} is $a_i + (j-1)b$ if $a = 1$ and $(-1)^{j-1}a_i + \delta_{j-1}b$ if $a = -1$. Thus the components of v over the cycle w_i add to $v(i, a_i, a, b)$. Moreover, equating the coefficients of e_{ℓ_i+1} on both sides of the equation yields $(a^{k_i} - 1)a_i + (1 + a + \cdots + a^{k_i-1})b = 0$, or equivalently, $(1+a+\cdots+a^{k_i-1})((a-1)a_i+b) = 0$. Conversely, if this equation holds for each i and $v = \sum_{i=1}^{s} v(i, a_i, a, b)$, then it is straightforward to check that $avg = v - be$, and hence ag fixes $v + W \cap E$. This proves the first assertion.

It is easy to see that the coefficients of the standard basis elements in $v = \sum_{i=1}^{s} v(i, a_i, a, b)$ add up to 0 (that is to say, $v \in W$) if and only if Eqs. (11) hold.

Next we examine more carefully the combined conditions: '$v \in W$' and '$v + W \cap E$ is fixed by ag', for $v = \sum_{i=1}^{s} v(i, a_i, a, b)$. By the arguments above, these two conditions hold if and only if both (10) hold for each i and also the equations in (11) hold. Note also that $b = 0$ if $W \cap E = 0$, equivalently, if $p \nmid \ell$

Suppose that $a = 1$. Assume first that p divides k_i for each i, that is $I_1 = 0$. Then (10) holds for each i and the final condition becomes $(\sum_{i=1}^{s} \binom{k_i}{2})b = 0$. If p is odd, then this holds since p divides each $\binom{k_i}{2}$, and row 1 of Table 3 holds. Similarly if $p = 2$ and the number of i such that $k_i \equiv 2 \pmod 4$ is even, that is, I_2 is even, then the final condition holds, and we have row 2 of Table 3. On the other hand, if $p = 2$ and I_2 is odd, then the final condition holds if and only if $b = 0$, as in row 3 of Table 3. Now assume that $I_1 > 0$, say $p \nmid k_{i_1}$. Then (10) holds for i_1 if and only if $b = 0$. With $b = 0$ we see that (10) holds for each i, and the final condition becomes $\sum_{i=1}^{s} k_i a_i = 0$, as in row 4 of Table 3.

Now consider the case $a = -1 \neq 1$, so p is odd. If k_i is even, then the first factor on the left hand side of (10) is zero, and hence (10) holds. On the other hand if k_i is odd, then (10) holds if and only if $a_i = b/2$. Thus (10) holds for all i if and only if $a_i = b/2$ whenever k_i is odd, Under these conditions, (11) becomes

$$0 = \sum_{i \text{ with } k_i \text{ odd}} a_i + \left(\sum_{i=1}^{s} \left\lfloor \frac{k_i}{2} \right\rfloor\right) b = 2^{-1}\left(\sum_{i=1}^{s} k_i\right) b = 2^{-1}\ell b$$

which, since p is odd, is equivalent to '$b = 0$ if $p \nmid \ell$', as in row 5 of Table 3. □

Now we are ready to compute the dimensions of fixed point spaces for elements of $Z \times S_\ell$ in the fully deleted permutation module U.

Lemma 4.3. *Suppose that $p \mid 2n+2$. Let $g = w_1 \cdots w_s \in S_{2n+2}$ be as in Lemma 4.2 so $w_i = (\ell_i + 1, \ldots, \ell_i + k_i)$ for each i. Let $I_3 = \#\{i \mid k_i \text{ odd}\}$. Then $\dim(\mathrm{Fix}_U(\pm g))$ is given in Table 4.*

Proof. Note that $E < W$ since p divides $\ell = 2n+2$, so $U = W/E$. Let g be as given and $a = \pm 1$, let I_1, I_2 be as in Lemma 4.2, and I_3 be as in the statement. By Lemma 4.2 the fixed vectors of ag in U are the cosets $v + E$ with $v = \sum_{i=1}^{s} v(i, a_i, a, b)$ where the a_i and b satisfy the appropriate line of Table 3. Note that since ag fixes E, either all or no vectors in a coset are of this form. Also note the assumption that p divides $\ell = 2n+2$.

Table 4
Fixed point dimensions for $\pm g$ in Lemma 4.3.

a	p	$\dim(\mathrm{Fix}_U(ag))$	Conditions on the k_i
1	odd	s	$p \mid k_i$ for all i
1	odd	$s-2$	$p \nmid k_i$ for some i
−1	odd	$s-I_3$	
1	2	s	all k_i even, and n odd
1	2	$s-1$	all k_i even, and n even
1	2	$s-2$	some k_i odd

Suppose first that p is odd and $a = 1$. If $p \mid k_i$ for all i (line 1 of Table 3), then the a_i and b are arbitrary giving p^{s+1} vectors forming p^s cosets, so $\dim(\mathrm{Fix}_U(g)) = s$, as in line 1 of Table 4. On the other hand if $p \nmid k_i$ for some i (line 4 of Table 3), then we require $b = 0$ and $\sum_{i\in I_1} k_i a_i = 0$, giving p^{s-2} cosets and dimension $s-2$ as in line 2 of Table 4. If p is odd and $a = -1$ (line 5 of Table 3), then b is arbitrary since $p \mid \ell$, and the requirements are that $a_i = b/2$ for each odd k_i, giving p^{s-I_3} cosets and dimension $s - I_3$, as in line 3 of Table 4.

Now consider $p = 2$ so $a = 1$. If all the k_i are even (lines 2 and 3 of Table 3), then we obtain dimension s or $s-1$ according as I_2 is even or odd, respectively, and this is equivalent to $\ell = 2n + 2 \equiv 0$ or $2 \pmod 4$, respectively, that is, n being odd or even, respectively, as in line 4 or 5 of Table 4, respectively. □

Lemma 4.4. *Suppose that* $p \nmid 2n + 1$. *Let* $g = w_1 \cdots w_s \in S_{2n+1}$ *be as in Lemma 4.2 so* $w_i = (\ell_i + 1, \ldots, \ell_i + k_i)$ *for each* i. *Then* $\dim(\mathrm{Fix}_U(g)) = s - 1$, *and for* p *odd,* $\dim(\mathrm{Fix}_U(-g)) = s - I_3$ *with* $I_3 = \#\{i \mid k_i \text{ odd}\}$.

Proof. Since $p \nmid 2n+1$, $W \cap E = 0$ and so $U = W/(W \cap E) \cong W$. Also $p \nmid 2n+1$ implies that not all cycle lengths in g are divisible by p, so by Lemma 4.2, $I_1 > 0$ and the fixed vectors of g in W are the sums $\sum_{i=1}^{s} v(i, a_i, 1, 0)$ with $\sum_{i\in I_1} k_i a_i = 0$, so the dimension of the fixed point subspace of g on U is $s - 1$. For p odd, the fixed vectors of $-g$ are the sums $\sum_{i=1}^{s} v(i, a_i, -1, 0)$ with $a_i = 0$ for each odd k_i, giving fixed point subspace of dimension $s - I_3$. □

Lemma 4.5. *Let* $G \cong \mathrm{SO}^{\pm}_{2n}(p)$ *or* $\mathrm{Sp}_{2n}(2)$ *and suppose that* $M \cong Z \times S_\ell < G$, *where* $\ell = 2n + 1$ *or* $2n + 2$, $\ell \geq 5$, *and* $|Z| = (2, q - 1)$, *and that* M *contains a good element. Then* $n \geq 4, n+1$ *is prime, and the good elements in* M *lie in* S_ℓ *and have cycle structure* $(n + 1)^1 1^{\ell-n-1}$.

Proof. Recall that by Lemma 3.1, G contains good elements if and only if n is even. If $n = 2$, then $G = \mathrm{SO}^-_4(2) \cong A_5$ or $G = \mathrm{Sp}_4(2) \cong A_6$ so M is not a proper subgroup of G. Hence $n \geq 4$. Let $t = ag \in M$ be a good element, with $a \in \mathbb{F}_p^*$, $g \in S_\ell$. As $|Z| = (p-1, 2)$, $a = \pm 1$. Let $c(g)$ denote the number of cycles in the disjoint cycle decomposition of g. By Lemma 4.1, g has a cycle of prime length $r \geq n + 1$, implying that $c(g) \leq n + \mu$, with $\mu := \ell - 2n \in \{1, 2\}$. Note that $c(g) = n + \mu$ if and only if $r = n + 1$ and the cycle structure of g is $(n+1)^1 1^{n+\mu-1}$, that is, the asserted cycle structure.

By Lemmas 4.3 and 4.4, $n = \dim(\mathrm{Fix}_U(ag)) \le c(g)$. If g has no cycles of length 1, then $c(g) \le 1 + \lfloor (n + 1/2) \rfloor < n$, which is a contradiction. Hence g has at least one cycle of length 1, and then the same lemmas imply that $\dim(\mathrm{Fix}_U(ag)) \le c(g) - \mu$ (note that in line 3 of Table 4 we have $I_3 \ge 2$ since there are cycles of odd lengths $1, r$). Thus $n = \dim(\mathrm{Fix}_U(ag)) \le c(g) - \mu \le n$, and equality must hold. By the previous paragraph, g has the required cycle structure and so $r = n + 1$ is prime.

If $a = 1$, then there is nothing more to prove since in this case $t = g \in S_\ell$. Assume then that p is odd and $a = -1$, so $t = -g$. We have proved that $\dim(\mathrm{Fix}_U(-g)) = c(g) - \mu = n$. However line 3 of Table 4 gives $\dim(\mathrm{Fix}_U(-g)) = c(g) - I_3$, where I_3 is the number of odd k_i. Hence $I_3 = \mu \le 2$. However, since g has cycle structure $(n+1)^1 1^{n+\mu-1}$, the parameter $I_3 = n + \mu > 2$, which is a contradiction. □

Using this information we obtain an estimate for the contribution of these subgroups to the probabilities $p_9(X, n, q)$ and $\tilde{p}_9(\mathrm{Sp}, n, q)$ (our estimate is reasonable only for $n \ge 5$).

Lemma 4.6. *Let $p_9^{(1)}(X, n, q)$ (for $X = \mathrm{Sp}$ or SO^ε) and $\tilde{p}_9^{(1)}(\mathrm{Sp}, n, q)$ denote the contributions to $p_9(X, n, q)$ and $\tilde{p}_9(\mathrm{Sp}, n, q)$ from maximal subgroups $Z \times S_\ell$ or $Z \times A_\ell$, where $\ell = 2n + 1$ or $2n + 2$, and $|Z| = (2, q - 1)$. Then $p_9^{(1)}(X, n, q) < q^{-n^2+4n+3}$ and $\tilde{p}_9^{(1)}(\mathrm{Sp}, n, q) < q^{-n^2+4n+3}$.*

Proof. Suppose that $G = X_{2n}(q)$ contains a maximal subgroup $M \cong Z \times S_\ell$ or $Z \times A_\ell$, with $\ell = 2n + 1$ or $2n + 2$ and $X = \mathrm{SO}^\varepsilon$ or Sp, as in (a)–(d) above. We may assume that G contains good elements so, by Lemma 4.5, $n \ge 4$ and $n + 1$ is prime. Moreover if $n = 4$ then the claimed upper bound holds (it is greater than 1, so useless). Thus we may assume that $n \ge 6$ and $\ell \ge 2n + 1 \ge 13$.

We claim that the number of G-conjugacy classes of such subgroups M is 1. By [7, Lemma 1.7.1], the number of G-conjugacy classes of such subgroups M is at most the number of L-conjugacy classes, where $L := \mathrm{GL}_{2n}(q)$. There is a unique irreducible representation of A_ℓ of degree $2n$ in characteristic p (see for example [8, Prop. 5.3.5]). Thus for M, N two maximal subgroups of G of this type, the derived subgroups M', N' (both isomorphic to A_ℓ) are conjugate in L. Hence there is a single G-conjugacy class of subgroups $M' \cong A_\ell$, and a single G-conjugacy class of subgroups $M = N_G(M')$.

By Lemma 4.5, the good elements $t \in M \cap \mathcal{C}$ all lie in S_ℓ and have cycle type $(n+1)^1 1^{\ell-n-1}$. All such elements are conjugate in M. Thus by (4) and (5), the contributions to $p_9(X, n, q)$ are

$$p_9^{(1)}(X, n, q) = \frac{|C_G(t)|^2}{|G|} \frac{|M|}{|C_M(t)|^2} = \frac{|C_G(t)|^2}{|G|} \frac{\ell!(2, q-1)}{(n+1)^2(\ell - n - 1)!^2},$$

and similarly for $\tilde{p}_9^{(1)}(\mathrm{Sp}, n, q)$. By Corollary 3.2, $\frac{|C_G(t)|^2}{|G|} \leq \frac{25}{9} q^{-n^2+n}$. Also the second factor is $\frac{\binom{2n+2}{n+1}(2,q-1)}{(n+1)^2}$ or $\frac{\binom{2n+1}{n}(2,q-1)}{n+1}$ as $\ell = 2n+2$ or $2n+1$, respectively, and the former is greater. Observing that $\binom{2n+2}{n+1} \leq (2e)^{n+1} < q^{3n+3}$, we see that

$$p_9^{(1)}(X, n, q) \leq \frac{50}{9q^{n^2-n}} \frac{(2e)^{n+1}}{(n+1)^2} < \frac{1}{q^{n^2-4n-3}}.$$

The same argument shows that $\tilde{p}_9^{(1)}(\mathrm{Sp}, n, q) < 1/q^{n^2-4n-3}$. □

5. $\mathbf{C_1}$: Subspace stabilisers and Theorem 5

Here $G = X_{2n}(q)$, and we consider subgroups M that are maximal subject to being reducible on V.

If $G = \mathrm{SL}_{2n}(q)$, then each such subgroup $M \cong P_i$, the stabiliser of some i-dimensional subspace Z, and has the form $M = Q_M L_M$ where Q_M is the unipotent radical of M and $L_M = (\mathrm{GL}_i(q) \times \mathrm{GL}_{2n-i}(q)) \cap G$ is the stabiliser of some decomposition $V = Z \oplus Y$ and is called a *Levi factor* of M. Also M is isomorphic under an outer automorphism of G to P_{2n-i}.

For $G = X_{2n}(q)$ with $X \neq \mathrm{SL}$, a maximal reducible subgroup M preserving a proper nontrivial subspace Z also leaves invariant $Z \cap Z^\perp$. By maximality, $Z \cap Z^\perp$ is either 0 or Z, that is, Z is either nondegenerate, or totally isotropic. In the former case, M is the direct product of classical groups induced on Z and $Z^\perp$, and we may assume that $i = \dim(Z) \leq n$ since $M = N_i$ is also the stabiliser of $Z^\perp$ of dimension $2n - i$. We note that, if $i = n$, then M may not be maximal, since there may exist elements of G interchanging Z and $Z^\perp$. In the latter case, M is a maximal parabolic subgroup P_i, the stabiliser of a totally isotropic i-dimensional subspace Z of V (where $i \leq n$), and M has the form $M = Q_M L_M$, where Q_M is the unipotent radical and L_M is $\mathrm{GL}_i(q^\delta) \times G_{2n-2i}(q)$, a *Levi factor* of M, with $G_{2n-2i}(q)$ a classical group induced by L_M on $Z^\perp/Z$ [8, Lemma 4.1.12].

Often, if t, t^g are good elements generating a reducible subgroup, then they fix more than one subspace. For our estimates, we wish to avoid 'double counting' such pairs as far as possible. Thus first we identify, in Lemmas 5.2 and 5.1, the maximal reducible subgroups we need to consider. Throughout the section, $\mathcal{C}$ denotes the G-conjugacy class of good elements containing t.

Lemma 5.1. *Let t, t^g be good elements in $\mathrm{SL}_{2n}(q)$ such that $\langle t, t^g\rangle$ is reducible on V, and let $V = U \oplus W$ be the decomposition preserved by t as in Lemma 3.1. Then $\langle t, t^g\rangle \leq M$ for one of the following subgroups M.*

(i) *$M = P_{2n-1}$ preserving a $(2n-1)$-space containing $W + W^g$; or*
(ii) *$M \cong P_1$ preserving a 1-space contained in $U \cap U^g$; or*
(iii) *$M = P_n$ preserving either $U = W^g$ or $W = U^g$.*

Proof. Let Z be a proper nontrivial subspace preserved by $\langle t, t^g \rangle$, and note that t^g preserves $V = U^g \oplus W^g$. Since t leaves Z invariant, it follows from Lemma 3.4 that either $Z \subseteq U$ or $W \subseteq Z$, and similarly either $Z \subseteq U^g$ or $W^g \subseteq Z$. Suppose first that both $W \subseteq Z$ and $W^g \subseteq Z$. Since $V = U \oplus W$, each coset of Z is of the form $Z + u$ for some $u \in U$. Since t fixes u, t also fixes the coset $Z + u$. Similarly $Z + u = Z + (u')^g$ for some $u' \in U$ and is therefore fixed by t^g. It follows that $\langle t, t^g \rangle$ fixes each coset of Z setwise, and hence $\langle t, t^g \rangle$ fixes a $(2n-1)$-dimensional subspace Z' containing Z. Thus $\langle t, t^g \rangle$ lies in $M \cong P_{2n-1}$.

Suppose next that $Z \subseteq U$ and $W^g \subseteq Z$. Then $Z = U = W^g$ and $\langle t, t^g \rangle$ lies in $M \cong P_n$. Similarly if $Z \subseteq U^g$ and $W \subseteq Z$, then $Z = U^g = W$ and again $\langle t, t^g \rangle$ lies in $M \cong P_n$. From now on we may assume that $Z \subseteq U \cap U^g$. Since $Z \neq 0$, the group $\langle t, t^g \rangle$ fixes Z pointwise and hence lies in $M \cong P_1$. □

Lemma 5.2. *Let t, t^g be good elements in $X_{2n}(q)$, where $X \neq \mathrm{SL}$, such that $\langle t, t^g \rangle$ is reducible on V, and let $V = U \oplus W$ be the decomposition preserved by t as in Lemma 3.1. Then $\langle t, t^g \rangle \leq M$ for one of the following subgroups M.*

- (i) *$M \cong P_1$, preserving a 1-space contained in $U \cap U^g$; or*
- (ii) *$M \cong N_1$ preserving a non-degenerate 1-space contained in $U \cap U^g$, and $X = \mathrm{SU}$ or SO^ε; or*
- (iii) *$M \cong N_n$, preserving the non-degenerate subspaces $U = W^g$ and $W = U^g$, and $X = \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^+$, where if $X = \mathrm{SO}^+$, then U, W have minus type.*

Moreover, for M in parts (i) and (ii), $M \cap \mathcal{C}$ is a single M-conjugacy class, while in part (iii), $M \cap \mathcal{C}$ is a union of two M-conjugacy classes and t, t^g are not M-conjugate.

Proof. Let Z be a proper nontrivial subspace preserved by $\langle t, t^g \rangle$. Since also $Z \cap Z^\perp$ is preserved we may assume that Z is either totally isotropic or nondegenerate.

Suppose first that Z is totally isotropic of dimension $i \leq n$, and let $M = Q_M L_M \cong P_i$ be the maximal parabolic subgroup stabilising Z, as above. We claim that $i \leq n/2$. Let $m = o(t)$. If $i = n$, then $L_M = \mathrm{GL}_n(q^\delta)$ does contain elements of order m but each such element fixes no non-zero vector of V and hence is not a good element. Thus P_n contains no good elements, so $i < n$. If $n/2 < i < n$, then neither $\mathrm{GL}_i(q^\delta)$ nor $G_{2n-2i}(q)$ contains elements of order m, and hence in this case also P_i does not contain any good elements. This proves the claim. Since $i \leq n/2$ it follows from Lemma 3.4 that $Z \subseteq U \cap U^g$ is fixed pointwise by $\langle t, t^g \rangle$. Thus $\langle t, t^g \rangle$ is contained in a parabolic subgroup P_1 stabilising a 1-subspace of $U \cap U^g$ as in part (a).

Now suppose that Z is nondegenerate. Since $\langle t, t^g \rangle$ also preserves $Z^\perp$ we may assume that $i := \dim(Z) \leq n$. Then it follows from Lemma 3.4 that either (i) Z is contained in $U \cap U^g$ and hence is fixed pointwise by $\langle t, t^g \rangle$ (possibly interchanging Z and $Z^\perp$ if $i = n$), or (ii) $i = n$ and, interchanging Z and $Z^\perp$ if necessary, $Z = U = W^g$ and $Z^\perp = W = U^g$.

Consider case (i). If Z contains an isotropic vector v, then $\langle t, t^g \rangle$ is contained in the stabiliser of $\langle v \rangle$, a parabolic subgroup P_1, as in part (a). If Z contains no isotropic vectors, then either $i = 1$ and $X = \mathrm{SU}$ or SO^ε, or $i = 2$, $X = \mathrm{SO}^\varepsilon$, and Z is of minus type. In either case $\langle t, t^g \rangle$ preserves a 1-subspace of Z and part (b) holds.

Finally suppose that $i = n$, $Z = U = W^g$ and $Z^\perp = W = U^g$. Here, if $X = \mathrm{SO}^\varepsilon$, then U, W must both have minus type (to admit the actions of t, t^g) and so we have $\varepsilon = +$.

In part (a) or (b), M is the stabiliser of a 1-space Z and in both cases $W + W^g \subseteq Z^\perp$. It follows from the structure of M that the cyclic tori T, T^g containing t, t^g, respectively, (as defined in Lemma 3.1) are conjugate in M. Also $|N_M(T)| = n|C_M(T)|$, and hence $M \cap \mathcal{C}$ is a single M-conjugacy class. On the other hand, in part (c), there are two M-conjugacy classes of tori which are G-conjugate to T, but we still have that $|N_M(T)| = n|C_M(T)|$, so the n elements of $T \cap \mathcal{C}$ are still conjugate in $N_M(T)$. Thus $M \cap \mathcal{C}$ is a union of two M-conjugacy classes, and since exactly one of t, t^g fixes U pointwise, and U is M-invariant, these elements lie in different M-classes in $M \cap \mathcal{C}$. □

In general, if M is a maximal subgroup of G containing an element $t \in \mathcal{C}$, and such that $M \cap \mathcal{C}$ is an M-conjugacy class (which occurs in particular in parts (i) and (ii) of Lemma 5.2), then the contribution from the conjugacy class of M to the estimates for the quantities in (3) is given by:

$$\frac{|G|}{|M|} \frac{|M \cap \mathcal{C}|^2}{|\mathcal{C}|^2} = \frac{|M|}{|G|} \frac{|C_G(t)|^2}{|C_M(t)|^2}. \tag{12}$$

5.1. Linear groups

Here $G \cong \mathrm{SL}_{2n}(q)$, $n \geq 2$, $q \geq 2$. We use the first expression for the probability $p_1(\mathrm{SL}, n, q)$, namely $\frac{|W_1|}{|\mathcal{C}|}$ where, for a fixed $t \in \mathcal{C}$, W_1 is the subset of $\mathcal{C}$ of elements t^g such that $\langle t, t^g \rangle$ is reducible. Directly estimating this quantity gives a more accurate upper bound which is valid for all q (whereas using the approximation from (2) leads to an upper bound greater than 1 for $q = 2$). We deal separately with the cases of Lemma 5.1.

Lemma 5.3. *If $X = \mathrm{SL}_{2n}(q)$ with $n \geq 2$, then*

$$p_1(\mathrm{SL}, n, q) < \frac{2}{q} + \frac{1}{q^2} - \frac{2}{q^3} - \frac{1}{q^4} + \frac{2}{q^{n^2}}$$

and moreover $p_1(\mathrm{SL}, 2, 2) < 0.6$.

Proof. We are given a good element $t \in \mathcal{C}$ together with its decomposition $V = U \oplus W$, where U is the fixed point space of t, and t is irreducible on W. We need to count conjugates t^g such that $H := \langle t, t^g \rangle$ is reducible on V. Let $V = U' \oplus W'$ be the analogous decomposition for t^g. Note that, the conjugacy class $\mathcal{C}$ is partitioned according to the subspace W' on which the elements act irreducibly, and each n-space contributes the same number of t^g to $\mathcal{C}$. This number is q^{n^2} (the number of choices for the complement U' of W') times the number $\frac{|\mathrm{GL}_n(q)|}{q^n-1}$ of possibilities for $t^g|_{W'}$. For $G \cong \mathrm{SL}_{2n}(q)$, $\mathcal{C}$ is also a conjugacy class of $\mathrm{GL}_{2n}(q)$, so

$$|\mathcal{C}| = \frac{|G|}{|C_G(t)|} = \frac{|\mathrm{GL}_{2n}(q)|}{|\mathrm{GL}_n(q)|(q^n-1)} \tag{13}$$

and the proportion of t^g in $\mathcal{C}$ corresponding to a fixed n-space W' is therefore $q^{n^2}\frac{|\mathrm{GL}_n(q)|^2}{|\mathrm{GL}_{2n}(q)|}$.

Consider Lemma 5.1(i) where H fixes a hyperplane containing $W+W'$. The elements t^g involved here are those where $W+W' \neq V$, or equivalently, where $W' \cap W \neq 0$. Hence the proportion of such t^g is equal to $1-\mathsf{p}$ where p is the proportion of n-spaces W' such that $W' \cap W = 0$. Since the number of complements to W is q^{n^2}, this proportion is

$$\mathsf{p} = \frac{|\mathrm{GL}_n(q)|^2 q^{2n^2}}{|\mathrm{GL}_{2n}(q)|} = \frac{\theta(1,n;q)^2}{\theta(1,2n;q)} = \frac{\theta(1,n;q)}{\theta(n+1,2n;q)}$$

and by Lemma 2.2(ii) with $(n,2n)$ for (k,n), this is greater than $1-q^{-1}-q^{-2}$.

Next, for the contribution from Lemma 5.1(ii), we observe that $\mathcal{C}$ is partitioned according to the ordered pair U', W', with equal proportions of t^g for each given pair U', W'. The n-space pairs U', W' we must consider for Lemma 5.1(ii) are those for which $W'+W=V$, $U' \cap W' = 0$, and $U \cap U' \neq 0$ hold. We have shown that the proportion satisfying the condition on W that $W'+W=V$ is equal to $\mathsf{p} = \frac{\theta(1,n;q)}{\theta(n+1,2n;q)}$. We must multiply this by the proportion of U' satisfying $U' \cap W' = 0$, and $U \cap U' \neq 0$, for given W' with $W+W'=V$. An upper bound for this proportion is the proportion of U' satisfying $U \cap U' \neq 0$ without requiring that U' be disjoint from the given W': and this is $1-\mathsf{p}$. Hence the contribution from Lemma 5.1(ii) is at most $\mathsf{p}(1-\mathsf{p})$. Adding the contributions from Lemma 5.1 parts (i) and (ii) we get a contribution of at most

$$(1-\mathsf{p}) + \mathsf{p}(1-\mathsf{p}) = 1-\mathsf{p}^2 < 1-\left(1-\frac{1}{q}-\frac{1}{q^2}\right)^2 = \frac{2}{q}+\frac{1}{q^2}-\frac{2}{q^3}-\frac{1}{q^4}.$$

Now consider the contribution from Lemma 5.1(iii). The elements t^g in $\mathcal{C}$ we need to consider are those where either $U'=W$ or $W'=U$. Arguing as in the first paragraph of the proof, each of these possibilities occurs with probability $q^{n^2}\frac{|\mathrm{GL}_n(q)|^2}{|\mathrm{GL}_{2n}(q)|} = q^{-n^2}\frac{\theta(1,n;q)^2}{\theta(1,2n;q)}$, which by Lemma 2.2 is less than q^{-n^2}.

This proves the general upper bound for $p_1(\mathrm{SL},n,q)$. For $q \geq 3$, this upper bound is less than 0.72 for all $n \geq 2$, and for $q=2$, the upper bound is $\frac{15}{16}+\frac{2}{q^{n^2}}$ which, for $n \geq 3$, is less than 0.95. An exact computation for $n=q=2$ gives $\mathsf{p}=16/35$, so that $p_1(\mathrm{SL},2,2) < 0.6$. □

5.2. Reducible subgroups with $X \neq \mathrm{SL}$

Throughout this subsection, t is a good element in a G-conjugacy class $\mathcal{C}$, and t lies in one of the subgroups M in Lemma 5.2. We deal uniformly, for all types $X \neq \mathrm{SL}$, with the groups in parts (i), (ii) and (iii) of Lemma 5.2 in three separate lemmas. We recall the parity restrictions on n given by Lemma 3.1.

Lemma 5.4. *For $X = \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon$, the contribution to $p_1(X,n,q)$ from the subgroups in Lemma 5.2(i) satisfies*

$$\text{‘contribution’} < \begin{cases} \frac{1}{q(q^2-1)} - \frac{3}{4q^{n+2}} & \text{if } X = \mathrm{SU} \\ \frac{1}{q-1} - \frac{2}{q^{n+1}} & \text{if } X = \mathrm{Sp} \\ \frac{1}{q(q-1)} - \frac{2}{q^{n/2+1}} + \frac{8}{3q^n} & \text{if } X = \mathrm{SO}^+ \\ \frac{1}{q(q-1)} + \frac{4}{q^{n/2+1}} & \text{if } X = \mathrm{SO}^-. \end{cases}$$

Proof. Let $G = X_{2n}(q)$, and let $M = P_1$ be a maximal subgroup stabilising a totally isotropic 1-space Z as in Lemma 5.1(i). These subgroups form a single G-conjugacy class. Moreover, by Lemma 5.1, $M \cap \mathcal{C}$ is a single M-conjugacy class and its elements fix Z pointwise. Thus the contribution to $p_1(X,n,q)$ is given by (12).

Suppose first that $X = \mathrm{SU}$, so n is odd. Then by [8, Props. 4.1.4, 4.1.18] $M \cong q^{4n-3}.(\mathrm{SL}_1(q^2) \times \mathrm{SU}_{2n-2}(q)).(q^2-1)$. Also $|C_M(t)| = (q^n+1)(q^2-1)q^{2n-3}|\mathrm{SL}_1(q^2)| \times |\mathrm{SU}_{n-2}(q)|$. Thus using (12) and Tables 1 and 2, the contribution to $p_1(X,n,q)$ is

$$\begin{aligned} \frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} &= \frac{(1+q^{-n})^2(1-q^{-n+1})^2}{(1-q^{-2n})(1+q^{-2n+1})(1-q^{-2})}\frac{1}{q^3} \\ &= \frac{(1+q^{-n})(1-q^{-n+1})^2}{(1-q^{-n})(1+q^{-2n+1})q(q^2-1)}. \end{aligned}$$

Now $D := (1-q^{-n})(1+q^{-2n+1}) = 1 - q^{-n} + q^{-2n+1} - q^{-3n+1} < 1$, and

$$\begin{aligned} N &:= \left(1+\frac{1}{q^n}\right)\left(1-\frac{1}{q^{n-1}}\right)^2 = 1 - \frac{2}{q^{n-1}} + \frac{1}{q^n} + \frac{1}{q^{2n-2}} - \frac{2}{q^{2n-1}} + \frac{1}{q^{3n-2}} \\ &= D - \frac{2}{q^{n-1}} + \frac{2}{q^n} + \frac{1}{q^{2n-2}} - \frac{3}{q^{2n-1}} + \frac{1}{q^{3n-2}} + \frac{1}{q^{3n-1}} \\ &< D - \frac{2}{q^{n-1}}\left(1 - \frac{1}{q} - \frac{1}{2q^{n-1}}\right) \le D - \frac{3}{4q^{n-1}} \end{aligned}$$

where the last inequality used $n \ge 3, q \ge 2$. Thus the contribution is at most

$$\frac{D - \frac{3}{4}q^{-n+1}}{Dq(q^2-1)} = \frac{1}{q(q^2-1)} - \frac{3}{4Dq^n(q^2-1)} < \frac{1}{q(q^2-1)} - \frac{3}{4q^{n+2}}.$$

Suppose next that $X = \mathrm{Sp}$, so n is even. Then by [8, Prop. 4.1.19], $M \cong q^{2n-1}.(\mathrm{GL}_1(q) \times \mathrm{Sp}_{2n-2}(q))$. Also $|C_M(t)| = q^{n-1}(q^{n/2+1})|\mathrm{Sp}_{n-2}(q)||\mathrm{GL}_1(q)|$. Thus, using (12) and Tables 1 and 2, the contribution to $p_1(X,n,q)$ is

$$\begin{aligned}\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} &= \frac{(1-q^{-n})^2}{(1-q^{-2n})(1-q^{-1})q} = \frac{(1-q^{-n})}{(1+q^{-n})(q-1)} \\ &= \frac{1}{q-1} - \frac{2}{(q^n+1)(q-1)} \le \frac{1}{q-1} - \frac{2}{q^{n+1}}.\end{aligned}$$

Finally suppose that $X = \mathrm{SO}^\varepsilon$, so n is even and $n \ge 4$. Then by [8, Prop. 4.1.20] $M \cong q^{2n-2}(\mathrm{GL}_1(q) \times \mathrm{SO}^\varepsilon_{2n-2}(q))$. Also $|C_M(t)| = q^{n-2}(q^{n/2}+1)|\mathrm{SO}^{-\varepsilon}_{n-2}(q)||\mathrm{GL}_1(q)|$ Thus, using (12) and Tables 1 and 2 the contribution to $p_1(X,n,q)$ is

$$\begin{aligned}\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} &= \frac{1}{q^2}\frac{(1-\varepsilon q^{-n+1})(1+\varepsilon q^{-n/2})^2}{(1-\varepsilon q^{-n})(1+\varepsilon q^{-n/2+1})^2}\frac{(1-q^{-n+2})^2}{(1-q^{-2n+2})(1-q^{-1})} \\ &= \frac{1}{q(q-1)}Y(\varepsilon)\end{aligned}$$

where $Y(\varepsilon) = \frac{(1-\varepsilon q^{-n+1})(1+\varepsilon q^{-n/2})^2}{(1-\varepsilon q^{-n})(1+\varepsilon q^{-n/2+1})^2}\frac{(1-q^{-n+2})^2}{(1-q^{-2n+2})}$.

Suppose first that $\varepsilon = +$. Then

$$\begin{aligned}Y(+) &= \frac{(1-q^{-n+1})(1+q^{-n/2})^2}{(1-q^{-n})(1+q^{-n/2+1})^2}\frac{(1-q^{-n+2})^2}{(1-q^{-2n+2})} \\ &= \frac{(1+q^{-n/2})(1-q^{-n/2+1})^2}{(1-q^{-n/2})(1+q^{-n+1})} \\ &< \frac{1-2q^{-n/2+1}+q^{-n/2}-2q^{-n+1}+q^{-n+2}+q^{-3n/2-2}}{1-q^{-n/2}} \\ &< 1+\frac{-2q^{-n/2}(q-1)+q^{-n+2}}{1-q^{-n/2}}\end{aligned}$$

so the contribution is

$$\frac{Y(+)}{q(q-1)} < \frac{1}{q(q-1)} - \frac{2}{q^{n/2+1}} + \frac{8}{3q^n}$$

where for the last term we used the conditions $q \ge 2, n \ge 4$. Similarly if $\varepsilon = -$,

$$\begin{aligned}Y(-) &= \frac{(1+q^{-n+1})(1-q^{-n/2})^2}{(1+q^{-n})(1-q^{-n/2+1})^2}\frac{(1-q^{-n+2})^2}{(1-q^{-2n+2})} \\ &= \frac{(1-q^{-n/2})^2(1+q^{-n/2+1})^2}{(1+q^{-n})(1-q^{-n+1})}\end{aligned}$$

$$< \frac{1 + 2q^{-n/2+1} - 2q^{-n/2} + q^{-n+2}}{1 - q^{-n+1}}$$
$$= 1 + \frac{2q^{-n/2}(q-1) + q^{-n+2} + q^{-n+1}}{1 - q^{-n+1}}$$

so the contribution is

$$\frac{Y(-)}{q(q-1)} < \frac{1}{q(q-1)} + \frac{2}{q^{n/2+1}(1-q^{-n+1})} + \frac{q+1}{q^n(q-1)(1-q^{-n+1})}$$
$$\leq \frac{1}{q(q-1)} + \frac{4}{q^{n/2+1}}$$

again using $q \geq 2, n \geq 4$. □

Lemma 5.5. *Let $X = \mathrm{SU}, \mathrm{SO}^+, \mathrm{SO}^-$, the contribution to $p_1(X, n, q)$ from the subgroups in Lemma 5.2*(ii) *is at most*

$$\frac{1}{q(q+1)} + \frac{2}{q^{n+2}}, \quad \frac{1}{(2,q-1)q} + \frac{8}{3q^{n/2+1}}, \quad \frac{1}{(2,q-1)q},$$

respectively.

Proof. Let $G = X_{2n}(q)$, and consider a subgroup $M = N_1$ stabilising a non-degenerate 1-space Z as in Lemma 5.1(ii). By that lemma, $M \cap \mathcal{C}$ is a single M-conjugacy class, and its elements fix Z pointwise. Thus the contribution to $p_1(X, n, q)$ is given by (12).

Suppose first that $X = \mathrm{SU}$. Then $M \cong (\mathrm{SU}_1(q) \times \mathrm{SU}_{2n-1}(q))(q+1)$, and $|C_M(t)| = (q^n+1)(q+1)|\mathrm{SU}_{n-1}(q)|$. Thus, using (12) and Tables 1 and 2, the contribution (recalling that n is odd and at least 3) is

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{(1+q^{-n})^2}{(1-q^{-2n})(1+q^{-1})}\frac{1}{q^2}$$
$$= \frac{(1+q^{-n})}{(1-q^{-n})(1+q^{-1})}\frac{1}{q^2} = \frac{1}{q(q+1)}\left(1 + \frac{2}{q^n-1}\right)$$
$$< \frac{1}{q(q+1)} + \frac{2}{q^{n+2}}.$$

Now suppose that $X = \mathrm{SO}^\varepsilon$. Then $M \cong (\mathrm{O}_1(q) \times \mathrm{O}_{2n-1}(q)) \cap \mathrm{SO}^\varepsilon_{2n}(q)$, and $|C_M(t)| = (q^{n/2}+1)|\mathrm{O}_{n-1}(q)|$.

Thus, using (12) and Tables 1 and 2, the contribution (recalling that n is even and at least 4) is

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{(1+\varepsilon q^{-n/2})^2}{(2,q-1)(1-\varepsilon q^{-n})}\frac{1}{q}.$$

If $\varepsilon = +$, then this is

$$\frac{(1+q^{-n/2})^2}{(2,q-1)q(1-q^{-n})} = \frac{(1+q^{-n/2})}{(2,q-1)q(1-q^{-n/2})} \le \frac{1}{(2,q-1)q} + \frac{8}{3q^{n/2+1}}.$$

If $\varepsilon = -$, then this is

$$\frac{(1-q^{-n/2})^2}{(2,q-1)q(1+q^{-n})} < \frac{1}{(2,q-1)q}. \qquad \square$$

Lemma 5.6. *For $X = \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^+$, the contribution to $p_1(X,n,q)$ from the subgroups in Lemma 5.2(iii) is less than $\frac{c}{q^{\delta n^2}}$, where $c = \frac{3}{2}, 1, \frac{16}{9}$, respectively.*

Proof. Let $G = X_{2n}(q)$, and consider a subgroup $M = N_n$ stabilising a non-degenerate n-space Z as in Lemma 5.1(iii). Then M is a direct product of the classical groups induced on $Z, Z^\perp$, and there is one conjugacy class of such subgroups with size $|G|/2|M|$. Also $M \cap \mathcal{C}$ is a union of two M-conjugacy classes interchanged by $N_G(M)$. The pairs (t, t^g) in M we need to count are those where exactly one of t or t^g fixes Z pointwise and the other fixes $Z^\perp$ pointwise. The number of pairs (t, t^g) with t fixing Z pointwise is $|M : C_M(t)|^2$, and the same number of pairs arises with t^g fixing Z pointwise. Thus the contribution to $p_1(X,n,q)$ from these subgroups is

$$\frac{|G|}{2|M|}\frac{2|M|^2}{|C_M(t)|^2}\frac{1}{|\mathcal{C}|^2} = \frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2}.$$

For $X = \mathrm{SU}, \mathrm{Sp}$, using Tables 1 and 2, this quantity is equal to

$$\frac{1}{q^{2n^2}}\frac{\Theta(1,n;-q)^2}{\Theta(1,2n;-q)}, \qquad \frac{1}{q^{n^2}}\frac{\Theta(1,n/2;q^2)^2}{\Theta(1,n;q^2)},$$

respectively, and since $\frac{\Theta(1,n;-q)^2}{\Theta(1,2n;-q)} < 1 + \frac{1}{q} \le \frac{3}{2}$ and $\frac{\Theta(1,n/2;q^2)^2}{\Theta(1,n;q^2)} = \frac{\Theta(1,n/2;q^2)}{\Theta(n/2+1,n;q^2)} < 1$, by Lemma 2.2(ii), the result follows for these cases. Now suppose that $X = \mathrm{SO}^+$. By Lemma 5.2, Z has minus type, so $|C_M(t)| = |C_G(t)| = (q^{n/2}+1)|\mathrm{SO}_n^-(q)|$. By Tables 1 and 2 and Lemma 2.2 (recall n is even here), this contribution is

$$\begin{aligned}\frac{|\mathrm{O}_n^-(q)|^2}{(2,q-1)|\mathrm{SO}_{2n}^+(q)|} &= \frac{q^{n^2-n}(1+q^{-n/2})^2\Theta(1,n/2-1;q^2)^2}{(2,q-1)q^{2n^2-n}(1-q^{-n})\Theta(1,n-1;q^2)} \\ &\le \frac{(q^{n/2}+1)}{q^{n^2}(q^{n/2}-1)}\frac{\Theta(1,n/2-1;q^2)}{\Theta(n/2,n-1;q^2)} < \frac{(q^{n/2}+1)}{q^{n^2}(q^{n/2}-1)(1-q^{-n})} \\ &\le \frac{16}{9q^{-n^2}}\end{aligned}$$

where we use $n \ge 4$, $q \ge 2$ in the last inequality. $\square$

5.3. Proof of Theorem 5

The cases where $p_1(X,n,q) = 0$ follow from Lemma 3.1, and the upper bound for $X = \mathrm{SL}$ is proved in Lemma 5.3. Suppose now that $X \neq \mathrm{SL}$ and $G = X_{2n}(q)$ contains good elements. We add the contributions to $p_1(X,n,q)$ from Lemmas 5.4, 5.5 and 5.6. The results for $X = \mathrm{Sp}$ and $X = \mathrm{SO}^\varepsilon$ are straightforward; for $X = \mathrm{SU}$ we note that $\frac{1}{q(q^2-1)} + \frac{1}{q(q+1)} = \frac{1}{q^2-1}$.

5.4. Symplectic groups over $\mathbb{F}_2$

We note that, if $X = \mathrm{Sp}$, $q = 2$ then the upper bound in Theorem 5 is very close to 1 for large n. We give, in Lemma 5.7 an alternative argument that obtains an upper bound $\frac{5}{6}$, using a similar, but more complicated approach to that in Lemma 5.3. Direct computation shows that $p_1(\mathrm{Sp},2,2) = \frac{1}{2}$. We give proof details for $n \geq 4$ (recall that n is even).

Lemma 5.7. *For $n \geq 2$, $p_1(\mathrm{Sp},n,2) < \frac{5}{6}$.*

Proof. As noted above we may assume that $n \geq 4$. By Lemmas 5.2 and 5.6, we have $p_1(\mathrm{Sp},n,2) < \mathsf{p} + \frac{1}{2^{n^2}}$, where $\mathsf{p} = \frac{N}{|\mathcal{C}|}$ with N the number of elements $t^g \in \mathcal{C}$ such that the fixed point subspace U' of t^g intersects U nontrivially. Note that U' determines the decomposition $V = U' \oplus W'$ for t^g since $W' = (U')^\perp$. Moreover, for a given U', the number of $t^g \in \mathcal{C}$ with fixed point space U' is equal to $\frac{|\mathrm{Sp}_n(2)|}{2^{n/2}+1}$. Thus $N = \frac{|\mathcal{U}|.|\mathrm{Sp}_n(2)|}{2^{n/2}+1}$, where $\mathcal{U}$ is the set of nondegenerate n-spaces U' such that $U' \cap U \neq 0$. Since $|\mathcal{C}| = \frac{|\mathrm{Sp}_{2n}(2)|}{|\mathrm{Sp}_n(2)|\,(2^{n/2}+1)}$, this implies that $\mathsf{p} = \frac{|\mathcal{U}||\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}$.

For $i = 1,2,3$, let $\mathcal{T}_i$ be the set of i-subsets of non-zero vectors from U; for $T \subseteq U^\#$ let $\mathcal{U}(T) = \{U' \in \mathcal{U} \mid T \subseteq U' \cap U\}$; and let $N_i = \sum_{T\in\mathcal{T}_i} |\mathcal{U}(T)|$. Then $\mathcal{U} = \bigcup_{T\in\mathcal{T}_1} \mathcal{U}(T)$, and by the pigeon hole principle, $|\mathcal{U}| \leq N_1 - N_2 + N_3$. Thus

$$\mathsf{p} \leq \mathsf{p}_1 - \mathsf{p}_2 + \mathsf{p}_3, \quad \text{where } \mathsf{p}_i = \frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|} N_i = \frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|} \sum_{T\in\mathcal{T}_i} |\mathcal{U}(T)|.$$

We use the following facts in our estimation of the p_i. These are easily derived from $|\mathrm{Sp}_{2n}(2)| = 2^{2n^2+n}\theta(1,n;2^2)$.

1. For $i = 1,2,3$, $\frac{|\mathrm{Sp}_{2n-2i}(2)|\,|\mathrm{Sp}_n(2)|}{|\mathrm{Sp}_{2n}(2)|\,|\mathrm{Sp}_{n-2i}(2)|} = 2^{-2in} \prod_{j=0}^{i-1} (1 + 2^{-n+j})^{-1}$.
2. The number of nondegenerate 2-subspaces of U is $\frac{2^{2n-2}(1-2^{-n})}{3}$.
3. For $i = 2,3$, the number of totally isotropic i-subspaces of U is $\prod_{j=0}^{i-1} \frac{2^{n-j}-2^j}{2^i-2^j}$.

Claim: $\mathsf{p}_1 = \frac{1-2^{-n}}{1+2^{-n}} = 1 - \frac{2}{2^n+1}$. We note that $|\mathcal{U}(T)|$ depends only on the structure of $\langle T\rangle$. In this case $\mathrm{Sp}(U)$ acts transitively on the $\mathcal{U}(T)$ for $T \in \mathcal{T}_1$, and hence $N_1 =$

$(2^n-1)|\mathcal{U}(\{v\})|$ for any chosen $v \in U^{\#}$. To construct $U' \in \mathcal{U}(\{v\})$, we first choose $x \in V \setminus v^{\perp}$. The number of such x is $2^{2n}-2^{2n-1}=2^{2n-1}$. Then we form U' as $\langle v,x\rangle \perp U_0$ where U_0 is any nondegenerate $(n-2)$-subspace of $\langle v,x\rangle^{\perp}$. Given v, x, the number of such U_0 is $\frac{|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}$. Hence the number of pairs (x, U_0) is $\frac{2^{2n-1}\,|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}$. On the other hand, for a given $U' \in \mathcal{U}(\{v\})$, the number of $x \in U' \setminus v^{\perp}$ is 2^{n-1}, and given x, the subspace U_0 is uniquely determined as $U_0 = U \cap \langle v,x\rangle^{\perp}$. It follows that $|\mathcal{U}(\{v\})| = \frac{2^n\,|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}$, and hence that

$$\mathsf{p}_1 = \frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}\cdot\frac{2^n(2^n-1)|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|} = \frac{2^{2n}(1-2^{-n})|\mathrm{Sp}_{2n-2}(2)||\mathrm{Sp}_n(2)|}{|\mathrm{Sp}_{2n}(2)||\mathrm{Sp}_{n-2}(2)|}$$

which is equal to $\frac{1-2^{-n}}{1+2^{-n}}$, using fact 1 above.

Claim: $\mathsf{p}_2 = \frac{(1-2^{-n})^2}{2(1+2^{-n})(1+2^{-n+1})} > \frac{1}{2}\mathsf{p}_1 - \frac{1.5}{2^n+1}$. For $T \in \mathcal{T}_2$, the subspace $\langle T\rangle$ has dimension 2, and $|\mathcal{U}(T)|$ depends only on whether $\langle T\rangle$ is nondegenerate or totally singular. Consider the former case. The number of pairs T for which $\langle T\rangle$ is nondegenerate is equal to the number of nondegenerate 2-subspaces of U times the number 3 of unordered bases for a 2-space. So by fact 2 above, the number of such T is $2^{2n-2}(1-2^{-n})$. Each U' containing such a T has the form $\langle T\rangle \perp U_0$ for a nondegenerate $(n-2)$-subspace U_0 of $T^{\perp}$, and the number of choices for U_0 is $\frac{|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}$. Thus the contribution to p_2 is

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}\cdot\frac{|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}\cdot 2^{2n-2}\big(1-2^{-n}\big)$$

which is equal to $\frac{1-2^{-n}}{4(1+2^{-n})}$, using fact 1. Now consider the case where $\langle T\rangle$ is totally isotropic. The number of pairs T of this type is equal to the number of totally isotropic 2-subspaces of U times the number 3 of unordered bases for a 2-space. So using fact 3 above, the number of such T is $(2^n-1)(2^{n-2}-1)$. Each U' containing such a $T=\{v_1,v_2\}$ has the form $\langle T,x_1,x_2\rangle \perp U_0$, where $x_1 \in v_2^{\perp} \setminus T^{\perp}$, $x_2 \in \langle v_1,x_1\rangle^{\perp} \setminus \langle T,x_1\rangle^{\perp}$, and U_0 is a nondegenerate $(n-4)$-subspace of $\langle T,x_1,x_2\rangle^{\perp}$. The number of such x_1 is 2^{2n-2}; given x_1, the number of such x_2 is 2^{2n-3}; and given x_1, x_2, the number of such U_0 is $\frac{|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$. Hence the number of triples (x_1,x_2,U_0) is $\frac{2^{4n-5}\,|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$. Each $U' \in \mathcal{U}(T)$ corresponds to several triples as follows: there are 2^{n-2} elements $x_1 \in U' \cap v_2^{\perp}$, given x_1 there are 2^{n-3} elements $x_2 \in U' \cap \langle v_1,x_1\rangle^{\perp}$; and given x_1, x_2, the subspace $U_0 = U' \cap \langle T,x_1,x_2\rangle^{\perp}$ is uniquely determined. Thus $|\mathcal{U}(T)| = \frac{2^{2n}\,|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$, and the contribution to p_2 is

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}\cdot\frac{2^{2n}|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}\cdot\big(2^n-1\big)\big(2^{n-2}-1\big)$$

which is equal to $\frac{(1-2^{-n})(1-2^{-n+2})}{4(1+2^{-n})(1+2^{-n+1})}$, using fact 1. Adding these two contributions gives the expression for p_2 above, proving the claim.

Claim: $\mathsf{p}_3 < \frac{1}{3}\mathsf{p}_1$. For $T \in \mathcal{T}_3$, the space $X := \langle T\rangle$ may be (i) a 3-space which is not totally isotropic, (ii) a totally isotropic 3-space, (iii) a nondegenerate 2-space, or (iv) a totally isotropic 2-space. We consider these cases separately. In cases (i) and (ii), $T = \{v_1, v_2, v_3\}$ is a basis for X, and we require n at least 4, 6 respectively.

(i) In this case the radical R of X has dimension 1, and both R and X/R are determined by T. We can enumerate the possible triples T by first choosing R (in $2^n - 1$ ways) and then choosing a nondegenerate 2-subspace X' of $(U \cap R^\perp)/R$; on noting that the preimage of X' in $R^\perp$ is a suitable 3-space X, we then choose T as one of the 28 bases of X. The number of such T is therefore $\frac{28(2^n-1)|\mathrm{Sp}_{n-2}(2)|}{|\mathrm{Sp}_{n-4}(2)|\,|\mathrm{Sp}_2(2)|}$. For each of these triples T, we can write the space it generates as $X = R \perp X_0$ for a nondegenerate 2-space X_0 (there are 4 choices of X_0 in X). We extend X to U' by first choosing $x \in X_0^\perp \setminus (R \perp X_0)^\perp$ (in 2^{2n-3} ways), and then choosing a nondegenerate $(n-4)$-subspace X_1 of $\langle X, x\rangle^\perp$ (in $\frac{|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$ ways), yielding $U' = \langle X, x\rangle \perp X_1$. For each such T, U', the number of X_0, x, X_1 is $4 \cdot 2^{n-3}$ since $x \in (U' \cap X_0^\perp) \setminus (U' \cap X^\perp)$ and $X_1 = U' \cap \langle X, x\rangle^\perp$. Thus $|\mathcal{U}(T)| = \frac{2^n|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$, and the contribution to p_3 from these T is

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|} \cdot \frac{28(2^n-1)|\mathrm{Sp}_{n-2}(2)|}{|\mathrm{Sp}_{n-4}(2)|\,|\mathrm{Sp}_2(2)|} \cdot \frac{2^n|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$$
$$= \frac{|\mathrm{Sp}_n(2)||\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_{2n}(2)||\mathrm{Sp}_{n-4}(2)|} \cdot \frac{|\mathrm{Sp}_{n-2}(2)|}{|\mathrm{Sp}_{n-4}(2)||\mathrm{Sp}_2(2)|} \cdot 7 \cdot 2^{2n+2}\bigl(1 - 2^{-n}\bigr)$$

which, using facts 1 and 2 is equal to $\frac{7(1-2^{-n})(1-2^{-n+2})}{48(1+2^{-n})(1+2^{-n+1})} < \frac{7}{48}\mathsf{p}_1$.

(ii) The number of triples T of this type is equal to the number of totally isotropic 3-subspaces X of U times the number 28 of unordered bases of a 3-space. So using fact 3, the number of such T is $\frac{2^{3n-4}(1-2^n)(1-2^{-n+2})(1-2^{-n+4})}{3}$. Each U' containing such a $T = \{v_1, v_2, v_3\}$ has the form $\langle T, x_1, x_2, x_3\rangle \perp U_0$, where $x_1 \in \langle v_2, v_3\rangle^\perp \setminus T^\perp$, $x_2 \in \langle v_1, v_3, x_1\rangle^\perp \setminus \langle T, x_1\rangle^\perp$, $x_3 \in \langle v_1, v_2, x_1, x_2\rangle^\perp \setminus \langle T, x_1, x_2\rangle^\perp$, and U_0 is a nondegenerate $(n-6)$-subspace of $\langle T, x_1, x_2, x_3\rangle^\perp$. The number of such x_1, x_2, x_3 is $2^{2n-3} \cdot 2^{2n-4} \cdot 2^{2n-5}$, and given x_1, x_2, x_3 the number of such U_0 is $\frac{|\mathrm{Sp}_{2n-6}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-6}(2)|}$. Hence the number of tuples (x_1, x_2, x_3, U_0) is $\frac{2^{6n-12}\,|\mathrm{Sp}_{2n-6}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-6}(2)|}$. Each $U' \in \mathcal{U}(T)$ corresponds to several tuples as follows: there are $2^{n-3} \cdot 2^{n-4} \cdot 2^{n-5}$ triples of elements x_1, x_2, x_3 in U', and then $U_0 = U' \cap \langle T, x_1, x_2\rangle^\perp$ is uniquely determined. Thus $|\mathcal{U}(T)| = \frac{2^{3n}\,|\mathrm{Sp}_{2n-6}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-6}(2)|}$, and the contribution to p_3 is

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|} \cdot \frac{2^{3n}|\mathrm{Sp}_{2n-6}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-6}(2)|} \cdot \frac{2^{3n-4}(1-2^n)(1-2^{-n+2})(1-2^{-n+4})}{3}$$

which, using fact 1, is equal to $\frac{(1-2^{-n})(1-2^{-n+2})(1-2^{-n+4})}{48(1+2^{-n})(1+2^{-n+1})(1+2^{-n+2})} < \frac{1}{48}\mathsf{p}_1$.

(iii)–(iv) In the last two cases, the triple T is the set of non-zero vectors in $\langle T\rangle$, so the number of triples T is the number of nondegenerate or totally isotropic 2-subspaces of U, respectively. In case (iii) each $U' \in \mathcal{U}(T)$ is of the form $\langle T\rangle \perp U_0$ for a nondegenerate $(n-2)$-subspace U_0 of $T^\perp$, and the contribution to p_3 from these triples is therefore

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}\cdot\frac{|\mathrm{Sp}_n(2)|}{|\mathrm{Sp}_{n-2}(2)|\,|\mathrm{Sp}_2(2)|}\cdot\frac{|\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-2}(2)|}$$
$$=\frac{|\mathrm{Sp}_n(2)||\mathrm{Sp}_{2n-2}(2)|}{|\mathrm{Sp}_{2n}(2)||\mathrm{Sp}_{n-2}(2)|}\cdot\frac{|\mathrm{Sp}_n(2)|}{|\mathrm{Sp}_{n-2}(2)|\,|\mathrm{Sp}_2(2)|}$$

which is equal to $\frac{1-2^{-n}}{12(1+2^{-n})}=\frac{1}{12}\mathsf{p}_1$, using facts 1 and 2.

In case (iv), by our argument for the previous claim, $|\mathcal{U}(T)|=\frac{2^{2n}\,|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$, and so the contribution to p_3 is

$$\frac{|\mathrm{Sp}_n(2)|^2}{|\mathrm{Sp}_{2n}(2)|}\cdot\frac{2^{2n-2}(1-2^{-n})(1-2^{-n+2})}{3}\cdot\frac{2^{2n}\,|\mathrm{Sp}_{2n-4}(2)|}{|\mathrm{Sp}_n(2)|\,|\mathrm{Sp}_{n-4}(2)|}$$

which is equal to $\frac{(1-2^{-n})(1-2^{-n+2})}{12(1+2^{-n})(1+2^{-n+1})}<\frac{1}{12}\mathsf{p}_1$, using fact 1.

Finally we conclude that $\mathsf{p}\le\mathsf{p}_1-\mathsf{p}_2+\mathsf{p}_3<\frac{5}{6}\mathsf{p}_1+\frac{1.5}{2^n+1}=\frac{5}{6}-\frac{1}{6(2^n+1)}$, and hence that $p_1(\mathrm{Sp},n,2)<\frac{5}{6}-\frac{1}{6(2^n+1)}+\frac{1}{2^{n^2}}$ which is less than $\frac{5}{6}$ for $n\ge 3$. □

6. $\mathbf{C}_2$: Stabilisers of direct sum decompositions

The maximal subgroups M of $G=X_{2n}(q)$ $(q\ge 3)$ in the Aschbacher class $\mathbf{C}_2$ are stabilisers of direct decompositions $V=V_1\oplus\cdots\oplus V_\ell$ with each V_i of dimension $d:=2n/\ell$ and $\ell\ge 2$. Thus $M\le\hat{M}:=\mathrm{GL}_d(q^\delta)\wr S_\ell$. Suppose that $M\cap\mathcal{C}\ne\emptyset$ for a G-conjugacy class $\mathcal{C}$ of good elements and let $t\in M\cap\mathcal{C}$ and $g\in G$ be such that $\langle t,t^g\rangle\le M$ and $\langle t,t^g\rangle$ is irreducible on V. If $(n,q)\ne(2,2^a-1)$ for any a, and $(n,q)\ne(6,2)$, let r be a ppd(n,q^δ)-prime dividing $o(t)$, and recall that $r\ge n+1$. *In this section we will assume that $\langle t,t^g\rangle$ cannot be written over a proper subfield: those subgroups not satisfying this condition are contained in $\mathbf{C}_5$-subgroups and will be treated in Section 9*. First we restrict d,ℓ,r,X. (Note that the excluded prime powers of the form $q=2^a-1$ are precisely the Mersenne primes.)

Lemma 6.1. *Suppose that $(n,q)\ne(2,5)$, or $(2,2^a-1)$ for any a. Then $d=1$, $\ell=2n\ge 8$, $(n,q)\ne(6,2)$, $r=n+1$, and $X\in\{\mathrm{SL},\mathrm{SO}^+\}$. Moreover, if $X=\mathrm{SO}^+$, then q is an odd prime.*

Proof. Suppose first that $d=1$ so $\ell=2n$. Then $q^\delta>2$, since otherwise $M\cong S_{2n}$ which is not irreducible on V, contradicting the fact that $\langle t,t^g\rangle$ is irreducible and contained in M. In particular $(n,q)\ne(6,2)$ (for if n is even, then $X\ne\mathrm{SU}$ and so $\delta=1$). Similarly if $n=2$, then $\delta=1$ since $\mathrm{SU}_4(q)$ does not contain good elements, so $q>2$; in this case, $|M|$ divides $24(q-1)^4$, and M contains an element of order $o(t)=(q+1)/(2,q-1)$. If q is even, then this implies that $q=q^\delta=2$, which is a contradiction, so q is odd.

Now t induces a permutation of $\{V_1, V_2, V_3, V_4\}$ of order $s \leq 4$, and $t^s \in \mathrm{GL}_1(q)^4$ has order at most $(o(t), q-1) \leq 2$. Thus $o(t) = s$ or $2s$, and $q+1 = 2s$ or $4s$, respectively, so $q \in \{3, 5, 7, 11\}$. Our assumptions imply that $q = 11$ so $o(t) = 2s = 6$. However then the fixed point space of t^3 (which is t-invariant and contains the fixed point space of t) has dimension $0, 1$ or 3, a contradiction. Thus $n > 2$ and $o(t)$ is divisible by a ppd(n, q^δ)-prime r, as defined above. This implies that $r \leq \ell$ so $r = n+1 > 3$, and in particular n is even, so $X \neq \mathrm{SU}$ and $\delta = 1$ (see Table 2). Also $\ell = 2n \geq 8$. By [8, Table 4.2A], $X \neq \mathrm{Sp}$, since in the case Sp, the V_i are non-degenerate. Suppose that $X = \mathrm{SO}^\varepsilon$. Then q must be prime since otherwise M can be written over a proper subfield (see [8, p. 100, Remarks on the conditions]). Then, since $q = q^\delta > 2$, q is odd. Then [8, Prop. 4.2.15(O)] implies that $\varepsilon = +$.

Now we assume that $d \geq 2$. If $(n, q) = (6, 2)$, then $X \neq \mathrm{SU}$ so $q = q^\delta = 2$ (since n is even) and $o(t) = 9$. It follows that S_ℓ contains an element of order 9, which is impossible since $\ell = 2n/d \leq n = 6$. By our assumptions on (n, q) it now follows that $o(t)$ is divisible by a ppd(n, q^δ)-prime r as defined above. Now $\ell \leq n < r$. Let $t_0 := t^{o(t)/r}$. Then $t_0 \in \mathrm{GL}_d(q^\delta)^\ell$ fixes each V_i setwise. Since r is a ppd(n, q^δ)-prime, it follows that $d = n$ and $\ell = 2$. Moreover, we may assume that t_0 acts irreducibly on V_1 and fixes V_2 pointwise. Then also t must fix V_1 pointwise and hence leaves V_1 and V_2 invariant. Similarly t^g leaves each of V_1 and V_2 invariant, which implies that $\langle t, t^g\rangle$ is reducible, a contradiction. □

We prove the following estimates. Note that Z_m denotes a cyclic group of order m.

Lemma 6.2. *Suppose that $(n, q) \neq (2, 5)$, or $(2, 2^a - 1)$ for any a.*

(i) *Then $p_2(X, n, q) = 0$ if $X = \mathrm{SU}, \mathrm{Sp}$ or SO^-, and*

$$p_2(X, n, q) < \begin{cases} \frac{1}{q^{n^2}} & \text{if } X = \mathrm{SL} \\ \frac{1}{2q^{n^2-3n}} & \text{if } X = \mathrm{SO}^+. \end{cases}$$

(ii) $\tilde{p}_2(\mathrm{Sp}, n, q) = 0$.

Proof. Suppose that $G \cap \mathcal{C} \neq \emptyset$. Then, by Lemma 6.1, in all cases $o(t)$ is divisible by a ppd(n, q)-prime $r = n+1$, and the subgroups $\langle t, t^g\rangle$ to be considered lie in a conjugate of the subgroup $N = \mathrm{GL}_1(q) \wr S_{2n}$ of $\mathrm{GL}(V)$, permuting the $2n$ coordinate vectors $e_1, \ldots, e_{2n}$. The Sylow r-subgroups of N are cyclic, so $t^{o(t)/r}$ can be conjugated by some $x \in G$ to a permutation matrix s that permutes the first $n+1$ coordinate vectors $e_1, \ldots, e_{n+1}$ and fixes the last $n-1$ coordinate vectors $e_{n+2}, \ldots, e_{2n}$. Thus the fixed point space of s has basis $e_1 + \cdots + e_{n+1}$, $e_{n+2}, \ldots, e_{2n}$, and this must also be a basis of the fixed point space of t^x. Now t^x must induce an r-cycle in S_{2n} (since t^x centralises the r-cycle $(t^{o(t)/r})^x$), and so $t^x = ys$ where $y = (y_i) \in (\mathbb{F}_q^*)^{2n}$ and, without loss of generality, $s = (1, 2, \ldots, r) \in S_{2n}$. Since t^x fixes e_i, for $i > r$, we have $y_i = 1$, for

$i > r$. Also, since t^x fixes $\sum_{i=1}^r e_i$, it follows that $y_i = 1$ for $i \leq r$ also. Thus $t^x = s \in S_{2n}$. It follows that $|C_N(t)| = (q-1)^n(n-1)!(n+1)$. Also, the cyclic torus T^x containing t^x, given by Lemma 3.1, satisfies $T^x \cap N \leq Z_{q-1} \times \langle t^x \rangle$ and since $r = n+1$ is prime, $N_N(T^x \cap N)/C_N(T^x \cap N) \cong Z_n$. It follows that $N \cap \mathcal{C}$ is a single N-conjugacy class. (Indeed this argument shows that in all the cases below $M \cap \mathcal{C}$ is a single M-conjugacy class, so that $p_2(X, n, q)$ is given by (4).)

Suppose first that $X = \mathrm{SL}$. Then the maximal $\mathbf{C}_2$ subgroups M containing the groups $\langle t, t^g \rangle$ form a single G-conjugacy class, have index $q-1$ in some conjugate of N, and $|C_M(t)| = |C_N(t)|/(q-1)$. Thus $p_2(\mathrm{SL}, n, q)$ is equal to

$$\begin{aligned}\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} &= \frac{(q-1)^{2n-1}(2n)!}{q^{n(2n-1)}\prod_{i=2}^{2n}(q^i-1)}\frac{(q^n-1)^2q^{n(n-1)}\prod_{i=2}^{n}(q^i-1)^2}{(n-1)!^2(q-1)^{2n-2}(n+1)^2} \\ &< \frac{(2n)!}{(n-1)!^2(n+1)^2}\frac{\prod_{i=1}^{n}(q^i-1)}{q^{n^2-2n}\prod_{i=n+1}^{2n}(q^i-1)}.\end{aligned}$$

Since $\frac{q^i-1}{q^{n+i}-1} < \frac{1}{q^n}$ for each $i \geq 1$, and $\frac{(2n)!}{(n-1)!^2(n+1)^2} = \frac{(2n)!}{(n)!^2}\frac{n^2}{(n+1)^2} < \binom{2n}{n} < 4^n$, we have $p_2(\mathrm{SL}, n, q) < 4^n/q^{2n^2-2n}$. Since $n \geq 4$, by Lemma 6.1, we have $q^{n^2} \geq q^{4n} \geq 4^n q^{2n}$, so $p_2(\mathrm{SL}, n, q) < 1/q^{n^2}$.

Now suppose that $X = \mathrm{SO}^+$, with q an odd prime and $n \geq 4$ even, as in Lemma 6.1. Then $M \cong (O_1(q) \wr S_{2n}) \cap \mathrm{SO}^+_{2n}(q)$, where $O_1(q) = \{\pm 1\}$, so $|M| = 2^{2n-1}(2n)!$ and $|C_M(t)| = 2^{n-1}(n-1)!(n+1)$. By [8, Prop. 4.2.15], the number of G-conjugacy classes of such subgroups M is $c \leq 4$. Thus $p_2(\mathrm{SO}^+, n, q)$ is equal to

$$\begin{aligned}c\,\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} &= \frac{c2^{2n-1}(2n)!}{|\mathrm{SO}^+_{2n}(q)|}\frac{(q^{n/2}+1)^2|\mathrm{SO}^-_n(q)|^2}{(n-1)!^2 2^{2n-2}(n+1)^2} \\ &\leq \frac{8(2n)!}{(n-1)!^2(n+1)^2}\frac{(q^{n/2}+1)^2|\mathrm{SO}^-_n(q)|^2}{|\mathrm{SO}^+_{2n}(q)|}.\end{aligned}$$

As above, $\frac{(2n)!}{(n-1)!^2(n+1)^2} = \frac{(2n-2)!}{(n-1)!^2}\frac{2n(2n-1)}{(n+1)^2} < 4^n$. Moreover, by Table 1 and Lemma 2.2(iii),

$$\begin{aligned}\frac{(q^{n/2}+1)^2|\mathrm{SO}^-_n(q)|^2}{|\mathrm{SO}^+_{2n}(q)|} &= \frac{(q^{n/2}+1)^2q^{n^2-n}(1-q^{-n/2})^2\Theta(1,n/2-1;q^2)^2}{q^{2n^2-n}(1-q^{-n})\Theta(1,n-1;q^2)} \\ &< \frac{(q^{n/2}+1)^2(1-q^{-n/2})^2}{q^{n^2}(1-q^{-n})^2} = \frac{1}{q^{n^2-n}}.\end{aligned}$$

Thus $p_2(\mathrm{SO}^+, n, q) < \frac{8.4^n}{q^{n^2-n}}$ which is less than $\frac{1}{2q^{n^2-3n}}$ since $n \geq 4$ and $q \geq 3$. This proves part (i).

Finally consider $X = \mathrm{Sp}$ with q even, and the proportion $\tilde{p}_2(\mathrm{Sp}, n, q)$ given by (5). By Lemma 6.1 there are no subgroups containing good elements since q is even. Hence $\tilde{p}_2(\mathrm{Sp}, n, q) = 0$. □

Table 5
$\mathbf{C}_3$ subgroups containing good elements.

X	M	c	Conditions
SL	$(\mathrm{GL}_{2d}(q^s).s) \cap \mathrm{SL}_{2n}(q)$	1	
SU	$(\mathrm{GU}_{2d}(q^s).s) \cap \mathrm{SU}_{2n}(q)$	1	d, s odd
Sp	$\mathrm{Sp}_{2d}(q^s).s$	1	d even
Sp	$\mathrm{GU}_n(q).2$	1	$s = 2$ and d, q odd
SO^ε	$(\mathrm{O}^\varepsilon_{2d}(q^s).s) \cap \mathrm{SO}^\varepsilon_{2n}(q)$	1 or $(s, 2)$	d even,
SO^+	$\mathrm{GU}_n(q) \cap \mathrm{SO}^+_{2n}(q)$	2	$s = 2$ and d odd

7. $\mathbf{C}_3$: Stabilisers of extension fields

Let M be a maximal subgroup of $G = X_{2n}(q)$ belonging to Aschbacher class $\mathbf{C}_3$, where $n \geq 3$. Then M preserves on V the structure of an $\mathbb{F}_{q^{\delta s}}$-space of dimension $2n/s$, for some prime s, so $M \leq \mathrm{GL}_{2n/s}(q^{\delta s}).s < \mathrm{GL}(V)$. Let $\mathcal{C}$ be a class of good elements, and suppose that $M \cap \mathcal{C} \neq \emptyset$. Let $t \in M \cap \mathcal{C}$ and, if $n \neq 2$ and $(n, q) \neq (6, 2)$, let r be a $\mathrm{ppd}(n, q^\delta)$-prime dividing $o(t)$. First we derive some basic facts about $M \cap \mathcal{C}$ and identify the possibilities for M using [8, Table 4.3.A].

Lemma 7.1. *Suppose that $(n, q) \neq (2, 3), (2, 7)$. The dimension $n = ds$, for some d, $M \cap \mathcal{C} \subseteq G \cap \mathrm{GL}_{2d}(q^{\delta s})$, and the number c of G-conjugacy classes for M and the possible structure of M are given in Table 5. Also either $M \cap \mathcal{C}$ is a single M-conjugacy class, or line 6 of Table 5 holds with q odd and $M \cap \mathcal{C}$ is a union of at most two equal-sized M-conjugacy classes.*

Proof. If $o(t)$ is divisible by a $\mathrm{ppd}(n, q^\delta)$-prime r, then, by Lemma 3.1, the element $t_0 := t^{o(t)/r}$ of order r lies in a cyclic torus T of G of order dividing $q^{\delta n} - 1$ such that $T \subset M \cap \mathrm{GL}_{2n/s}(q^{\delta s})$ and T has an n-dimensional $\mathbb{F}_q$-fixed point subspace in V. In particular the group $\mathrm{GL}_{2n/s}(q^{\delta s})$ has non-cyclic Sylow r-subgroups, and this is true if and only if s divides n. Let $d := n/s$. If the good element t does not lie in $M_0 := G \cap \mathrm{GL}_{2d}(q^{\delta s})$, then t induces a nontrivial field automorphism of M_0, and in particular t does not centralise $\langle t \rangle \cap M_0$, which is a contradiction. Thus $t \in M_0$ and hence $M \cap \mathcal{C} \subset M_0$. A similar argument shows that $t \in M_0$ in the cases $n = 2$ and $(n, q) = (6, 2)$. The possibilities for M are given in [8, Table 4.3.A] (note that n is even if $X = \mathrm{SO}^\varepsilon$, so line 6 of [8, Table 4.3.A] is not possible, and in line 6 of Table 5 we must have $\varepsilon = +$). Also the values for c come from the various results in [8, Section 4.3] (the value for c in line 5 depends on ε).

In all cases the cyclic torus T containing t, defined in Lemma 3.1, is contained in M_0, and all cyclic tori of M of order $|T|$ are conjugate in M_0. In all cases, except possibly line 6, we have $N_M(T) = N_{M_0}(T).s = C_{M_0}(T).n$ and it follows that the n conjugates of t in T (see Lemma 3.1) are conjugate in $N_M(T)$. Thus $M \cap \mathcal{C}$ is a single M-conjugacy class. In line 6, possibly $N_M(T) = N_{M_0}(T).s = C_{M_0}(T).[n/2]$ and $M \cap \mathcal{C}$ splits into two equal sized M-conjugacy classes.

Finally we verify the conditions column of Table 5. If $X = \mathrm{SU}$, then n is odd so both d, s are odd also. In line 3, the fixed point subspace of t is a nondegenerate d-dimensional $\mathbb{F}_{q^s}$-space, and hence d is even. In lines 4 and 6, $s = 2$ and a cyclic torus of M_0 with d-dimensional $\mathbb{F}_{q^2}$-fixed point subspace has order $q^d - (-1)^d$, and since t lies in such a torus it follows that d is odd. (In line 4, the condition q odd follows from [8, Table 4.3.A].) In line 5, since M contains T with $r \mid |T|$ acting irreducibly on a d/s-dimensional $\mathbb{F}_{q^s}$-subspace, d must be even. □

Now we consider all these cases to estimate $p_3(X, n, q)$ and $\tilde{p}_3(\mathrm{Sp}, n, q)$.

Lemma 7.2. *Suppose that* $(n, q) \neq (2, 3), (2, 7)$.

(i) *Then*

$$p_3(X,n,q) < \begin{cases} \frac{3.6}{q^{n^2}} & \text{if } X = \mathrm{SL} \\ \frac{5}{q^{4n^2/3}} & \text{if } X = \mathrm{SU} \\ \frac{3.7}{q^{n^2/2}} & \text{if } X = \mathrm{Sp} \\ \frac{10.6}{q^{n^2/2}} & \text{if } X = \mathrm{SO}^{\varepsilon}. \end{cases}$$

(ii) $\tilde{p}_3(\mathrm{Sp}, n, q) \leq \frac{3.7}{q^{n^2/2}}$.

Proof. *Cases* $X = \mathrm{SL}$ *and* SU. Here there is a unique class of subgroups M for each prime divisor s of n, as in line 1 or 2, respectively, of Table 5, and

$$\left|C_M(t)\right| = \begin{cases} ((q^s)^{n/s} - 1)|\mathrm{SL}_{n/s}(q^s)|\frac{(q^s-1)}{(q-1)} & \text{if } X = \mathrm{SL} \\ (q^n + 1)|\mathrm{GU}_{n/s}(q^s)|(\frac{1}{q+1}) & \text{if } X = \mathrm{SU}. \end{cases}$$

First let $X = \mathrm{SL}$. By Tables 1 and 2, we have

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{\Theta(1, \frac{2n}{s}; q^s)\Theta(1, n; q)^2}{\Theta(1, 2n; q)\Theta(1, \frac{n}{s}; q^s)^2}\frac{s}{q^{2n^2(1-1/s)}}.$$

By Lemma 2.2(ii), $\frac{\Theta(1,n;q)^2}{\Theta(1,2n;q)} \leq 1$, so

$$\frac{\Theta(1, \frac{2n}{s}; q^s)\Theta(1, n; q)^2}{\Theta(1, 2n; q)\Theta(1, \frac{n}{s}; q^s)^2} \leq \frac{\Theta(\frac{n}{s} + 1, \frac{2n}{s}; q^s)}{\Theta(1, \frac{n}{s}; q^s)} \leq \frac{16}{11}$$

where the second inequality follows from Lemma 2.2(ii) since $q^s \geq 4$, so

$$p_3(\mathrm{SL}, n, q) \leq \frac{16}{11}\sum_{s|n,\ s\ \text{prime}} \frac{s}{q^{2n^2(1-1/s)}} = \frac{16}{11q^{2n^2}}\sum_{s|n,\ s\ \text{prime}} sq^{2n^2/s}.$$

Since the number of different prime divisors of n is at most $\log n$, by Lemma 2.1 we have $p_3(\mathrm{SL}, n, q) \leq \frac{32}{11q^{n^2}} + \frac{48\log n}{11q^{4n^2/3}}$. If the second term arises, then $n \geq 3$ and since $\frac{\log n}{q^{n^2/3}} \leq \frac{\log n}{2^{n^2/3}} \leq \frac{\log 3}{2^3} < 0.138$, it follows that $p_3(\mathrm{SL}, n, q) \leq \frac{3.6}{q^{n^2}}$.

Now let $X = \mathrm{SU}$, so n, s are odd. By Tables 1 and 2, we have

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{\Theta(1, \frac{2n}{s}; -q^s)\Theta(1, n; -q)^2}{\Theta(1, 2n; -q)\Theta(1, \frac{n}{s}; -q^s)^2}\frac{s}{q^{2n^2-2n^2/s}}.$$

Since n/s is odd, by Lemma 2.3(i), $\frac{\Theta(1, \frac{2n}{s}; -q^s)}{\Theta(1, \frac{n}{s}; -q^s)} \leq 1$, and by Lemma 2.2, $\Theta(1, \frac{n}{s}; -q^s) > 1$. Also, by Lemma 2.2,

$$\frac{\Theta(1, n; -q)^2}{\Theta(1, 2n; -q)} = \frac{\Theta(1, n; -q)}{\Theta(n+1, 2n; -q)} < \frac{(1+q^{-1})}{(1-q^{-n-1})} \leq \frac{8}{5}.$$

Thus $\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} < \frac{8}{5}\frac{sq^{2n^2/s}}{q^{2n^2}}$. Arguing as in the SL-case, and noting that here $s \geq 3$, we obtain

$$p_3(\mathrm{SU}, n, q) \leq \frac{24}{5q^{4n^2/3}} + \frac{8\log n}{q^{8n^2/5}} = \frac{1}{q^{4n^2/3}}\left(\frac{24}{5} + \frac{8\log n}{q^{4n^2/15}}\right) < \frac{5}{q^{4n^2/3}}.$$

Note that if the second term is present, then $n \geq 5$.

In preparation for the case $X = \mathrm{Sp}$, we consider next the contribution from line 4 of Table 5. Since the arguments for this line are the same as those for line 6, we deal with both these lines together.

Case of lines 4 *and* 6 *of Table 5.* We note that $n \equiv 2 \pmod 4$ (since d is odd). We do not restrict q to be odd in line 4 as we need the estimates for q even when dealing with $\tilde{p}_3(\mathrm{Sp}, n, q)$. There are one or two G-conjugacy classes of these subgroups M for $X = \mathrm{Sp}, \mathrm{SO}^+$, respectively; also $M \cap \mathcal{C}$ is either a single M-class, or possibly a union of two equal sized M-classes when $X = \mathrm{SO}^+$. Thus the contribution to $p_3(X, n, q)$ is given by (12) when $X = \mathrm{Sp}$, and this must be modified a bit for $X = \mathrm{SO}^+$. In both cases, by Table 2, $|C_M(t)| = (q^{n/2}+1)|\mathrm{GU}_{n/2}(q)|$.

First let $X = \mathrm{Sp}$. Then by Tables 1 and 2 and by Lemma 2.2(ii) (since $n/2$ is odd), the contribution is

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)^2|} = \frac{2\Theta(1, n; -q)\Theta(1, \frac{n}{2}; q^2)^2}{\Theta(1, n; q^2)\Theta(1, \frac{n}{2}; -q)^2}\frac{1}{q^{n^2/2}} < \frac{2}{q^{n^2/2}}. \tag{14}$$

Now let $X = \mathrm{SO}^+$. We require one factor of 2 since there are two G-conjugacy classes, and an additional factor of 4 because there may be two M-conjugacy classes in $M \cap \mathcal{C}$. Thus the contribution in this case (noting that $n \equiv 2 \pmod 4$) and applying Lemma 2.2(ii) and (iii)) is at most

$$
\begin{aligned}
8\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)^2|} &= \frac{\Theta(1,n;-q)\Theta(1,\frac{n}{2}-1;q^2)^2}{\Theta(1,n-1;q^2)\Theta(1,\frac{n}{2};-q)^2}\frac{(1+q^{-n/2})^2}{(1-q^{-n})}\frac{8}{q^{n^2/2}} \\
&\le \frac{8}{(1-q^{-n/2})^2 q^{n^2/2}} < \frac{10.5}{q^{n^2/2}}
\end{aligned}
\tag{15}
$$

using $q^n \ge 2^6$.

Case $X = \mathrm{Sp}$. It remains to deal with line 3 of Table 5. There is a unique class of subgroups M for each prime divisor s of n, such that n/s is even (so $s = 2$ arises only if $n \equiv 0 \pmod 4$), and $M \cap \mathcal{C}$ is a single M-conjugacy class. Here $|C_M(t)| = ((q^s)^{\frac{n}{2s}} + 1)|\mathrm{Sp}_{n/s}(q^s)|$, and by Tables 1 and 2, the contribution from these groups is

$$
\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{\Theta(1,\frac{n}{s};q^{2s})\Theta(1,\frac{n}{2};q^2)^2}{\Theta(1,n;q^2)\Theta(1,\frac{n}{2s};q^{2s})^2}\frac{s}{q^{n^2-n^2/s}}.
$$

By Lemma 2.2(ii),

$$
\frac{\Theta(1,\frac{n}{s};q^{2s})\Theta(1,\frac{n}{2};q^2)^2}{\Theta(1,n;q^2)\Theta(1,\frac{n}{2s};q^{2s})^2} < \frac{\Theta(\frac{n}{2s}+1,\frac{n}{s};q^{2s})}{\Theta(1,\frac{n}{2s};q^{2s})} < \frac{16}{11}
$$

so that the contribution from all of these subgroups is at most $\frac{16}{11}\sum_s \frac{s}{q^{n^2(1-1/s)}}$. If $n \equiv 0 \pmod 4$ so that $s = 2$ is allowed, this is less than $\frac{32}{11q^{n^2/2}} + \frac{48\log n}{11q^{2n^2/3}} = \frac{1}{q^{n^2/2}}(\frac{32}{11} + \frac{48\log n}{11q^{n^2/6}}) < \frac{3}{q^{n^2/2}}$ noting that $n \ge 12$ if the second term is present. If $n \equiv 2 \pmod 4$, then the contribution is at most $\frac{48\log n}{11q^{2n^2/3}} \le \frac{1}{q^{n^2/2}}\frac{48\log 3}{11\, 2^{3^2/6}} < \frac{1.7}{q^{n^2/2}}$. Combining with (14) in the case $n \equiv 2 \pmod 4$, we see that, for all n, we have $p_3(\mathrm{Sp},n,q) < \frac{3.7}{q^{n^2/2}}$.

Case $X = \mathrm{SO}^\varepsilon$. It remains to deal with line 5 of Table 5. There are at most $(s,2)$ G-conjugacy classes of subgroups M for each prime divisor s of n, such that n/s is even (so $s = 2$ arises only if $n \equiv 0 \pmod 4$), and $M \cap \mathcal{C}$ is a single M-conjugacy class. Here $|M| = s|\mathrm{SO}^\varepsilon_{2n/s}(q^s)|$ and $|C_M(t)| = ((q^s)^{\frac{n}{2s}} + 1)|\mathrm{SO}^{-\varepsilon}_{n/s}(q^s)|$, so by Tables 1 and 2, this contribution is at most

$$
(2,s)\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} = \frac{\Theta(1,\frac{n}{s}-1;q^{2s})\Theta(1,\frac{n}{2}-1;q^2)^2}{\Theta(1,n-1;q^2)\Theta(1,\frac{n}{2s}-1;q^{2s})^2}\frac{(2,s)s}{q^{n^2(1-1/s)}}.
$$

Now

$$
\frac{\Theta(1,\frac{n}{s}-1;q^{2s})\Theta(1,\frac{n}{2}-1;q^2)^2}{\Theta(1,n-1;q^2)\Theta(1,\frac{n}{2s}-1;q^{2s})^2} = \frac{\Theta(\frac{n}{2s}+1,\frac{n}{s}-1;q^{2s})\Theta(1,\frac{n}{2}-1;q^2)}{\Theta(1,\frac{n}{2s}-1;q^{2s})\Theta(\frac{n}{2}+1,n-1;q^2)}
$$

and, by Lemma 2.2(ii) and (iii), we have $\frac{\Theta(1,\frac{n}{2}-1;q^2)}{\Theta(\frac{n}{2}+1,n-1;q^2)} < (1-q^{-n})^{-1}$, and

$$
(2,s)\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} < \frac{1-q^{-ns}}{(1-q^{-2s}-q^{-4s})(1-q^{-n})}\frac{(2,s)s}{q^{n^2(1-1/s)}} = \frac{\nu s}{q^{n^2(1-1/s)}}.
$$

If $s = 2$, then $q^s \geq 4$ and $n \geq 4$ (since n/s is even), so $\nu \leq 2.143$ if $s = 2$; and if $s \geq 3$, then $n \geq 2s \geq 6$ and $\nu < 1.09$. Thus the contribution from all of these subgroups is at most $\frac{4.286}{q^{n^2/2}} + \sum_{s>2} \frac{(1.09)s}{q^{n^2(1-1/s)}}$, where the first term is present only if $n \equiv 0 \pmod 4$, and the second term sums to at most $\frac{3.3 \log n}{q^{2n^2/3}}$ (arguing as above). We note that the latter function is $\frac{3.3}{q^{n^2/2}} \frac{\log n}{q^{n^2/6}}$, and $\frac{\log n}{q^{n^2/6}} \leq \frac{\log n}{2^{n^2/6}} \leq \frac{\log n_0}{2^{n_0^2/6}}$ if $n \geq n_0$. If $n = 4, 8$, then the only term is for $s = 2$ so the contribution is less than $\frac{4.3}{q^{n^2/2}}$. If $n \equiv 0 \pmod 4$ and $n \geq 12$, then the second term is at most $\frac{3.3}{q^{n^2/2}} \frac{\log 12}{2^{24}} < \frac{0.001}{q^{n^2/2}}$, so the contribution again is at most $\frac{4.3}{q^{n^2/2}}$. In $n \equiv 2 \pmod 4$ and $n \geq 6$, then the contribution is the second term and is at most $\frac{3.3}{q^{n^2/2}} \frac{\log 6}{2^6} < \frac{0.1}{q^{n^2/2}}$. Combining with (15) in the case where $\varepsilon = +$ and $n \equiv 2 \pmod 4$, we see that, for all n, $p_3(\mathrm{SO}^\varepsilon, n, q) < \frac{10.6}{q^{n^2/2}}$.

Case $\tilde{p}_3(\mathrm{Sp}, n, q)$. Here $X = \mathrm{Sp}$ and q is even. By Lemma 7.1, the subgroups to be considered are those in line 4 of Table 5 (which cover those in line 5 for $\varepsilon = \pm$), and in the case $n \equiv 2 \pmod 4$ also those in line 6 (which do not lift to maximal subgroups in $\mathbf{C}_3$ for G). The contribution $\tilde{p}_3(\mathrm{Sp}, n, q)$, as given by (5), is therefore equal to the estimate given in the case Sp above. Thus $\tilde{p}_3(\mathrm{Sp}, n, q) < \frac{3.7}{q^{n^2/2}}$. □

8. $\mathbf{C}_4$: Stabilisers of tensor products

We deal with maximal subgroups in $\mathbf{C}_4$ for $n \geq 3$.

Lemma 8.1. *Suppose that $n \geq 3$. Then, for all X, $p_4(X, n, q) = \tilde{p}_4(\mathrm{Sp}, n, q) = 0$.*

Proof. By [8, Table 4.4.A], for all X, if M is a maximal $\mathbf{C}_4$-subgroup in $G = X_{2n}(q)$, then M is the stabiliser in G of a tensor decomposition $V = U \otimes W$ with $\dim(U) \geq \dim(W) \geq 2$, and $M \leq \mathrm{GL}(U) \otimes \mathrm{GL}(W)$. Thus, since $n \geq 3$, M contains elements of order belonging to $\Phi^X(n, q)$ if and only if $\dim(U) = n, \dim(W) = 2$. Let t be an element of such a subgroup with $o(t) \in \Phi^X(n, q)$, say $t = t_U \otimes t_W$, with $t_U \in \mathrm{GL}(U), t_W \in \mathrm{GL}(W)$. Then $t^{q^2-1} = t' \otimes 1$ with order $o(t') \in \Phi^X(n, q)$. Let $\{w_1, w_2\}$ be a basis for W, and for $j = 1, 2$, let $V_j := \langle u \otimes w_j \mid u \in U \rangle$. Then each V_j is $(t' \otimes 1)$-invariant and $t' \otimes 1$ acts irreducibly on it. Moreover, $V = V_1 \oplus V_2$, and hence $t' \otimes 1$ does not fix an n-dimensional subspace of V pointwise, and so is not a good element. It follows that M does not contain good elements. □

9. $\mathbf{C}_5$: Stabilisers of subfields

Let M be a maximal subgroup of $G = X_{2n}(q)$ belonging to Aschbacher class $\mathbf{C}_5$. By [8, Table 4.5.A], M is a cyclic extension of $X'_{2n}(q_0)$, for some type X', and M stabilises

Table 6
$\mathbf{C}_5$ subgroups containing good elements.

X	$c \le$	Conditions on s
SL	$q-1$	
SU	$q+1$	s odd
Sp	1	s odd
SO^ε	1	s odd

$\mathbb{F}_{q^\delta} V_0$, where $q^\delta = q_0^s$ for some prime s, and $V_0 := V(2n, q_0)$ is an $\mathbb{F}_{q_0}$-subspace of V. Let $\mathcal{C}$ be a class of good elements, suppose that $M \cap \mathcal{C} \ne \emptyset$ and let $t \in M \cap \mathcal{C}$. First we derive some basic facts about r, $M \cap \mathcal{C}$ and M.

Lemma 9.1. *The integer $n \ge 3$, $s \nmid n$ and $o(t)$ is divisible by a $\mathrm{ppd}(n, q^\delta)$-prime r which is also a $\mathrm{ppd}(n, q_0)$-prime. Moreover the type $X' = X$, $M \cap \mathcal{C}$ is a single M-conjugacy class, and the number c of G-conjugacy classes of subgroups M is at most the quantity given in Table 6.*

Proof. Suppose that $n = 2$, so $o(t) = \frac{q+1}{(2,q-1)}$. We claim that $o(t)$ is not a 2-power. Suppose to the contrary that it is a 2-power, say $q = q_0^s = 2^a - 1 > 3$. Hence $q_0^s \equiv 3 \pmod 4$, so s is odd and $2^a = q_0^s + 1$ is divisible by $q_0 + 1$. This means that $q_0 + 1 = 2^b$, for some $b < a$, and $2^{a-b} = \frac{q_0^s+1}{q_0+1} = 1 - q_0 + \cdots + q_0^{s-1} \equiv s \pmod{2^b}$, which is a contradiction since s is odd. This proves the claim. Thus, $o(t)$ is divisible by a $\mathrm{ppd}(2s, q_0)$-prime, say r, and since $r \ge 2s + 1 \ge 5$ it follows that r divides $|\mathrm{SL}_4(q_0)|$. This implies that $s = 2$ and that all elements of M of order r lie in Singer cycles of $\mathrm{SL}_4(q_0)$ and hence are fixed point free on V, which is a contradiction. Thus $n \ge 3$, and since $q > 2$, it follows that $o(t)$ is divisible by a $\mathrm{ppd}(n, q^\delta)$-prime r.

We note that $r \nmid |Z(G)|$. Therefore r divides $|X'_{2n}(q_0)|$, and hence r is a $\mathrm{ppd}(k, q_0)$-prime, for some $k \le 2n$. Now $r \mid (q_0^k - 1)$, which implies that $r \mid (q^{\delta k} - 1)$, so k is a multiple of n. If $k = 2n$, then an element t_0 of order r in $\langle t \rangle$ lies in a Singer cycle of $\mathrm{GL}_{2n}(q_0)$ acting fixed point freely on $\mathbb{F}_{q^\delta} V_0$, and hence t has no fixed points in V, which is a contradiction. Thus r is a $\mathrm{ppd}(n, q_0)$-prime. Moreover, $s \nmid n$ since otherwise $q^{\delta n/s} - 1 = q_0^n - 1$ is divisible by r, which contradicts the definition of r.

By [8, Table 4.5.A], either $X' = X$ or (i) $X = \mathrm{SU}$, $s = 2$, and $X' = \mathrm{SO}^\varepsilon$ (with q odd) or $X' = \mathrm{Sp}$, or (ii) $X = \mathrm{SO}^\varepsilon$ and $X' = \mathrm{SO}^{\varepsilon'}$, where $\varepsilon = (\varepsilon')^s$. In case (i), $s = 2$ and r divides $q_0^n - 1 = q^{\delta n/2} - 1$, which is a contradiction as in the previous paragraph. In case (ii), n is even by Table 2, so s is odd since $s \nmid n$. Thus $(\varepsilon')^s = \varepsilon'$ and so $\varepsilon = \varepsilon'$ and $X' = X$. For the same reason s is odd if $X = \mathrm{Sp}$; also s is odd if $X = \mathrm{SU}$ by [8, Table 4.5.A].

In each case $|N_M(\langle t \rangle) : C_M(t)| = n$, and $N_M(\langle t \rangle)$ is transitive by conjugation on the $\mathcal{C} \cap \langle t \rangle$, so $M \cap \mathcal{C}$ is a single M-conjugacy class. Finally the values of c follow from [8, Props. 4.5.3, 4.5.4, 4.5.10]. □

Lemma 9.2. *We have*

(i)

$$p_5(X,n,q) < \begin{cases} 8q^{-n^2+n+2} & \text{if } X = \mathrm{SL} \\ 8q^{-4(n^2-n)/3+2} & \text{if } X = \mathrm{SU} \\ 3q^{-2(n^2-n)/3} & \text{if } X = \mathrm{Sp} \\ 4q^{-2(n^2-n)/3} & \text{if } X = \mathrm{SO}^{\varepsilon}. \end{cases}$$

(ii) $\tilde{p}_5(\mathrm{Sp},n,q) \le 3q^{-2(n^2-n)/3}$.

Proof. *Case* $X = \mathrm{SL}$. We refer to and use the notation of Lemma 9.1. Here $M \cong (Z_{q-1}.\mathrm{GL}_{2n}(q_0)) \cap \mathrm{SL}_{2n}(q)$, and considering the scalars in M we have $|M| = |\mathrm{SL}_{2n}(q_0)|\frac{(2n,q-1)}{(2n,q_0-1)} \le |\mathrm{SL}_{2n}(q_0)|\frac{q-1}{q_0-1}$. Also $|C_M(t)| \ge (q_0^n - 1)|\mathrm{SL}_n(q_0)|$. By Tables 1 and 2,

$$\frac{|M|}{|C_M(t)|^2} \le \frac{(q-1)q_0^{4n^2}\Theta(1,2n;q_0)}{(q_0^n-1)^2 q_0^{2n^2}\Theta(1,n;q_0)^2} \le \frac{4(q-1)q_0^{2n^2}}{(q_0^n-1)^2}$$

since $\frac{\Theta(n+1,2n;q_0)}{\Theta(1,n;q_0)} \le \frac{1}{1-q_0^{-1}-q_0^{-2}} \le 4$, by Lemma 2.2. Applying Corollary 3.2 and noting that there are $c \le q-1$ classes of subgroups for each s, we see that the contribution to $p_5(\mathrm{SL},n,q)$ of subgroups with a fixed s is at most

$$c\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} \le \frac{4(q-1)(q^n-1)^2}{(q_0^n-1)^2 q^{2n^2(1-1/s)}}.$$

In particular, if $s = 2$, then a direct computation shows that this contribution is at most $\frac{8}{q^{n^2-n-2}} - \frac{4}{q^{n^2-n-1}}$. For $s \ge 3$, using the fact that $\frac{(q^n-1)^2}{(q_0^n-1)^2} \le 2q^{2n(1-1/s)}$ we see that the contribution for s is less than $\frac{8(q-1)}{q^{(2n^2-2n)(1-1/s)}}$. Now summing over all odd primes gives a contribution less than

$$\frac{8(q-1)}{q^{4(n^2-n)/3}}\sum_{j\ge 0} q^{-j} < \frac{8}{q^{4(n^2-n)/3-1}},$$

and combining with the contribution for $s = 2$ yields $p_5(\mathrm{SL},n,q) < 8q^{-n^2+n+2}$.

Case $X = \mathrm{SU}$. Here $|M| \le |\mathrm{SU}_{2n}(q_0)|\frac{q+1}{q_0+1}$, and $|C_M(t)| \ge (q_0^n + 1)|\mathrm{SU}_n(q_0)|$. Using Tables 1 and 2,

$$\frac{|M|}{|C_M(t)|^2} \le \frac{(q+1)q_0^{4n^2}\Theta(1,2n;-q_0)}{(q_0^n+1)^2 q_0^{2n^2}\Theta(1,n;-q_0)^2} \le \frac{(q+1)q_0^{2n^2}}{(q_0^n+1)^2}$$

since $\frac{\Theta(n+1,2n;-q_0)}{\Theta(1,n;-q_0)} < 1$ by Lemma 2.2. Applying Corollary 3.2 and noting that there are $c \le q+1$ classes of subgroups for each s, we see that the contribution to $p_5(\mathrm{SU}, n, q)$ of subgroups with a fixed s is at most

$$c\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} \le \frac{(q+1)^2(q^n+1)^2}{(q_0^n+1)^2 q^{2n^2(1-1/s)}} < \frac{4}{q^{(2n^2-2n)(1-1/s)-2}}$$

using the fact that $\frac{(q+1)(q^n+1)}{(q_0^n+1)} \le 2q^{n(1-1/s)+1}$. Now we add over s, and note that $s \ge 3$ since n is odd (Table 2). A cruder estimate than in the SL-case gives

$$p_5(\mathrm{SU}, n, q) < \frac{4}{q^{4(n^2-n)/3-2}} \sum_{j\ge 0} q^{-j} \le \frac{8}{q^{4(n^2-n)/3-2}}.$$

Case $X = \mathrm{Sp}$ and part (ii). Here s is odd, $M = \mathrm{Sp}_{2n}(q_0)$, and $|C_M(t)| = (q_0^{n/2}+1) \cdot |\mathrm{Sp}_n(q_0)|$. Using Tables 1 and 2,

$$\frac{|M|}{|C_M(t)|^2} = \frac{q_0^{2n^2+n}\Theta(1,n;q_0^2)}{(q_0^{n/2}+1)^2 q_0^{n^2+n}\Theta(1,n/2;q_0^2)^2} \le \frac{16q_0^{n^2-n}}{11}$$

since by Lemma 2.2, $\frac{\Theta(n/2+1,n;q_0^2)}{\Theta(1,n/2;q_0^2)} < 16/11$ (note $q_0^2 \ge 4$). Applying Corollary 3.2 and noting that there is a unique class of subgroups for each s, we see that the contribution to $p_5(\mathrm{Sp}, n, q)$ from subgroups with a fixed s is at most

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} \le \frac{25}{11q^{(n^2-n)(1-1/s)}} < \frac{2.3}{q^{(n^2-n)(1-1/s)}}.$$

Adding over $s \ge 3$, we obtain $p_5(\mathrm{Sp}, n, q) < 2.3\, q^{-2(n^2-n)/3}\sum_{j\ge 0} q^{-j}$, and since $\sum_{j\ge 0} q^{-j} = 1/(1-q^{-1}) \le 8/7$ (since $q \ge 8$), this is less than $3q^{-2(n^2-n)/3}$. We note here that, by the proof of Lemma 9.1, if q is even, then every maximal $\mathbf{C}_5$-subgroup of $\mathrm{SO}_{2n}^{\varepsilon}(q)$ containing good elements is contained in a maximal $\mathbf{C}_5$-subgroup of $\mathrm{Sp}_{2n}(q)$, and it follows that $\tilde{p}_5(\mathrm{Sp}, n, q) < 3q^{-2(n^2-n)/3}$, as in part (ii).

Case $X = \mathrm{SO}^{\varepsilon}$. Again s is odd, and here $M = \mathrm{SO}_{2n}^{\varepsilon}(q_0)$, and $|C_M(t)| = (q_0^{n/2}+1) \cdot |\mathrm{SO}_n^{-\varepsilon}(q_0)|$. Using Tables 1 and 2,

$$\frac{|M|}{|C_M(t)|^2} = \frac{q_0^{2n^2-n}(1-\varepsilon q_0^{-n})\Theta(1,n-1;q_0^2)}{(q_0^{n/2}+1)^2 q_0^{n^2-n}(1+\varepsilon q_0^{-n/2})^2\Theta(1,n/2-1;q_0^2)^2} \le \frac{17}{9}\cdot\frac{16q_0^{n^2-n}}{11}$$

since by Lemma 2.2, $\frac{\Theta(n/2,n-1;q_0^2)}{\Theta(1,n/2-1;q_0^2)} < 16/11$ (note $q_0^2 \ge 4$). By Corollary 3.2, and using the inequality (8), since $q = q_0^s \ge 8$ we have $|C_G(t)|^2/|G| < 1.1q^{-n^2+n}$. Noting that there is a unique class of subgroups for each s, we see that the contribution to $p_5(\mathrm{SO}^{\varepsilon}, n, q)$ of subgroups with a fixed s is at most

$$\frac{|M|}{|G|}\frac{|C_G(t)|^2}{|C_M(t)|^2} \le \frac{17 \times 16 \times 1.1}{99\, q^{(n^2-n)(1-1/s)}} < \frac{3.1}{q^{(n^2-n)(1-1/s)}}.$$

Adding over $s \ge 3$, as in the Sp-case we obtain $p_5(\mathrm{SO}^\varepsilon, n, q) < 4q^{-2(n^2-n)/3}$. □

10. $\mathbf{C}_6$: Normalisers of symplectic-type groups

A maximal subgroup M of $G = X_{2n}(q)$ belonging to Aschbacher class $\mathbf{C}_6$, is contained in $(Z(G) \circ R).\mathrm{Sp}_{2d}(2)$, where $R = 2^{1+2d}$ is an extraspecial 2-group. Moreover $2n = 2^d$, q is odd, and R is absolutely irreducible on V (see [8, Section 4.6, especially Table 4.6.B]). We deal with all cases where a good element is not a 2-element (which can happen only when $n = 2$ and $q = 2^a - 1$ for some $a > 1$). It turns out that, with a single exception, these maximal groups do not contain good elements.

Lemma 10.1. *Suppose that $(n, q) \neq (2, 2^a - 1)$ for any a. Then either*

(i) $p_6(X, n, q) = \tilde{p}_6(\mathrm{Sp}, n, q) = 0$, *or*
(ii) $(X, n, q) = (\mathrm{SL}, 2, 5)$, $M = (Z_4 \circ 2^{1+6}).\mathrm{Sp}_6(2)'$ *contains good elements of order* 3, *and* $p_6(\mathrm{SL}, 2, 5) < \frac{1}{48} < 0.021$.

Proof. Suppose that M, as above, contains a good element t, and let $V = U \oplus W$ be as in Lemma 3.1. Let r be a $\mathrm{ppd}(n, q^\delta)$-prime dividing $o(t)$ if $n \ge 3$, or $r = o(t) = (q+1)/2$ if $n = 2$. By the conditions on n, q, the integer r is not a power of 2.

Since R is irreducible on V, for each non-zero $v \in V$, the R-orbit vR spans V and in particular $|vR| \ge 2n$. Also $|vR|$ divides $|R| = 2^{1+2d} = 8n^2$. It follows that r does not divide $|vR|$, and so vR contains a fixed vector of t, that is, $U \cap vR \neq \emptyset$. Thus the number of R-orbits on non-zero vectors is at most $|U| - 1 = q^{\delta n} - 1$. However each of these R-orbits has length at most $|R|$, and so $q^{2\delta n} - 1 = |V| - 1 \le 8n^2(q^{\delta n} - 1)$. Hence $3^{\delta n} < q^{\delta n} + 1 \le 8n^2$, which implies that $(n, q^\delta, r) = (4, 3, 5), (2, 5, 3)$ (since $(n, q) = (2, 3)$ is excluded from the analysis).

If $(n, q^\delta, r) = (4, 3, 5)$, then M must contain a good element t_0 of order 5 (some power of t). Since $r = 5 = 2^2 + 1$, $\langle t_0 \rangle$ projects to a cyclic torus of order 5 of $\mathrm{Sp}_6(2)$, and hence t_0 leaves invariant a tensor decomposition $V = V_1 \otimes V_2$ with $\dim(V_1) = 2, \dim(V_2) = 4$, contradicting Lemma 8.1.

Thus $(n, q^\delta, r) = (2, 5, 3)$. Here $X = \mathrm{SL}$, and the subgroup M of $\mathrm{SL}_4(5)$ was constructed and examined using GAP [4]. The group M has two conjugacy classes of elements of order 3, and one of them consists of good elements (the other contains fixed point free elements). This computation showed that $\frac{|G|}{|M|}\frac{|M \cap \mathcal{C}|^2}{|\mathcal{C}|^2} = \frac{256}{50\,375} < \frac{1}{196}$. By [8, Prop. 4.6.5], there are four G-conjugacy classes of such maximal subgroups M, and hence $p_6(\mathrm{SL}, 2, 5) < \frac{1}{48}$. □

11. $\mathbf{C}_7$: Stabilisers of tensor powers

A maximal subgroup M of $X_{2n}(q)$ belonging to the Aschbacher class $\mathbf{C}_7$ is the stabiliser of a tensor power decomposition $V = V_1 \otimes \cdots \otimes V_\ell$, where $\dim(V_i) = d$ for all i and $2n = d^\ell$, for some $\ell \geq 2$; and so M is contained in a group of the shape $(\mathrm{GL}_d(q) \wr S_\ell) \cap \mathrm{SL}_{2n}(q)$ or $(\mathrm{GU}_d(q) \wr S_\ell) \cap \mathrm{SU}_{2n}(q)$. We show that M contains no good elements if $n \geq 3$.

Lemma 11.1. *$p_7(X, n, q) = 0$, for any X, q, and any $n \geq 3$, and $\tilde{p}_7(\mathrm{Sp}, n, q) = 0$.*

Proof. Suppose to the contrary that M, as above, contains a good element t, and let $V = U \oplus W$ be as in Lemma 3.1. Let r be a $\mathrm{ppd}(n, q^\delta)$-prime dividing $o(t)$, and note in particular that $r \geq n+1$. Since $2^n \geq 2n = d^\ell \geq 2^\ell$, we obtain $n \geq \ell$, and in particular $r > \ell$. Hence r divides the order of an element in $\mathrm{GL}_d(q)$ or $\mathrm{GU}_d(q)$. By definition of r, this implies that $d \geq n$, and the only possibility is $n = d = \ell = 2$, which contradicts $n \geq 3$. □

12. $\mathbf{C}_8$: Classical subgroups

By [8, Table 4.8.A], if $G = X_{2n}(q)$ has maximal subgroups belonging to $\mathbf{C}_8$, then either $X = \mathrm{SL}$, or q is even, $X = \mathrm{Sp}$, and $M \cong \mathrm{SO}^\varepsilon_{2n}(q)$. We do not consider the latter case for estimating $p_8(X, n, q)$ since we assume that q is odd if $X = \mathrm{Sp}$. Also we note that $\tilde{p}_8(\mathrm{Sp}, n, q) = 0$ since the subgroups $\mathrm{SO}^\varepsilon_{2n}(q)$ have no proper maximal $\mathbf{C}_8$ subgroups. We establish the following estimates.

Lemma 12.1.

(i) *$p_8(X, n, q) = 0$ if $X = \mathrm{SU}$ or SO^ε, or if $(X, q) = (\mathrm{Sp}, odd)$, and $p_8(\mathrm{SL}, n, q) < 2.7q^{-n^2+n+2}$.*
(ii) *$\tilde{p}_8(\mathrm{Sp}, n, q) = 0$.*

Proof. Part (ii) follows from our comments above. Also, for part (i), by our comments above, the only case to consider is $X = \mathrm{SL}$, so let $G = \mathrm{SL}_{2n}(q)$. Suppose that M is a maximal $\mathbf{C}_8$-subgroup of G containing a good element t from the G-conjugacy class $\mathcal{C}$, and that there are c conjugacy classes of such subgroups M. Then, using the results in [8, Section 4.8], especially [8, Table 4.8.A], and Lemma 3.1, the cases we need to consider are

(a) $M = Z_{(2n,q-1)} \circ \mathrm{Sp}_{2n}(q)$, $c = (q-1, n)$, and n is even;
(b) $M = Z_{(2n,q-1)} \circ \mathrm{SU}_{2n}(q_0)$, $c \leq q-1$, $q = q_0^2$, and n is odd;
(c) $M = Z_{(2n,q-1)} \circ \mathrm{SO}^\varepsilon_{2n}(q)$, $c \leq q-1$, q is odd, and n is even.

Moreover, in all cases the n conjugates of t in the cyclic torus T of Lemma 3.1 are still $N_M(T)$-conjugate, and hence $M \cap \mathcal{C}$ is a single M-conjugacy class. Thus by (4) and (12), the contribution to $p_8(\mathrm{SL}, n, q)$ from each type of subgroup M is at most $\frac{(q-1)|M|}{|G|} \frac{|C_G(t)|^2}{|C_M(t)|^2}$, which by Corollary 3.2 is at most $\frac{(q^n-1)^2}{q^{2n^2}} \frac{|M|}{|C_M(t)|^2}$.

Case (a). By Tables 1 and 2, and noting that $|M| \le (q-1)|\mathrm{Sp}_{2n}(q)|$ and that $\frac{\Theta(n/2+1,n;q^2)}{\Theta(1,n/2;q^2)} \le (1-q^{-2}-q^{-4})^{-1} \le \frac{16}{11}$ (or less than $\frac{9}{8}$ if q is odd), by Lemma 2.2, the contribution is at most

$$\frac{(q^n-1)^2}{q^{2n^2}} \frac{(q-1)q^{2n^2+n}\Theta(1,n;q^2)}{(q^{n/2}+1)^2 q^{n^2+n}\Theta(1,n/2;q^2)^2} < \frac{16(q^{n/2}-1)^2}{11q^{n^2-1}} \le \frac{8}{11q^{n^2-n-2}}$$

or less than $\frac{9}{8q^{n^2-n-1}} \le \frac{3}{8q^{n^2-n-2}}$ if q is odd.

Case (b). By Tables 1 and 2, and noting that $|M| \le (q_0-1)|\mathrm{SU}_{2n}(q_0)|$ and that $\frac{\Theta(n+1,2n;-q_0)}{\Theta(1,n;-q_0)} < 1$, by Lemma 2.2, the contribution is at most

$$\frac{(q^n-1)^2}{q^{2n^2-1}} \frac{(q-1)q_0^{4n^2}\Theta(1,2n;-q_0)}{(q_0^n+1)^2 q_0^{2n^2}\Theta(1,n;-q_0)^2} < \frac{1}{q^{n^2-n-2}}.$$

Case (c). By Tables 1 and 2, and noting that $|M| \le (q-1)|\mathrm{SO}^{\varepsilon}_{2n}(q)|$, and (using Lemma 2.2(iii)) that $\frac{\Theta(n/2,n-1;q^2)}{\Theta(1,n/2-1;q^2)} \le (1-q^{-2}-q^{-4})^{-1} < \frac{9}{8}$ (since q is odd), the contribution for type ε is at most

$$\begin{aligned} &\frac{(q^n-1)^2}{q^{2n^2-1}} \frac{(q-1)q^{2n^2-n}(1-\varepsilon q^{-n})\Theta(1,n-1;q^2)}{(q^{n/2}+1)^2 q^{n^2-n}(1+\varepsilon q^{-n/2})^2\Theta(1,n/2-1;q^2)^2} \\ &\le \frac{9(q^{n/2}-1)^2(1-\varepsilon q^{-n})}{8q^{n^2-2}(1+\varepsilon q^{-n/2})^2} \le \frac{9(q^n-\varepsilon)}{8q^{n^2-2}} \end{aligned}$$

and hence, summing over ε, the contribution in this case is at most $\frac{9}{4q^{n^2-n-2}}$.

Collecting these results we see that $p_8(\mathrm{SL}, n, q) \le kq^{-n^2+n+2}$, where $k = 1$ if n is odd, $k = \frac{8}{11}$ if both n and q are even, and $k = \frac{21}{8} < 2.7$ if n is even and q is odd. □

13. $\mathbf{C}_9$: Nearly simple subgroups

Let $G = X_{2n}(q)$ and let M be a maximal subgroup of G belonging to the Aschbacher Class $\mathbf{C}_9$ for G, or if $(X, q) = (\mathrm{Sp}, \mathit{even})$, a maximal subgroup in Aschbacher Class $\mathbf{C}_9$ for $\mathrm{SO}^{\varepsilon}_{2n}(q)$. By [9, Theorem 4.2], one of the following holds.

(1) $M \cong Z \times S_\ell$ where $\ell = 2n+1$ or $2n+2$, $Z = Z(G) \le Z_2$, and $X = \mathrm{SO}^{\varepsilon}$ or Sp as in (a)–(d) of Section 4;
(2) $|M| < q^{6\delta n}$.

We obtain the following estimates for the $\mathbf{C}_9$-probabilities.

Lemma 13.1. *For $n \geq 9$,*

(i) $p_9(X,n,q) < 6q^{-2n^2+10.6n}$ *if* $X = \mathrm{SL}$;
(ii) $p_9(X,n,q) < 6q^{-2n^2+16.6n}$ *if* $X = \mathrm{SU}$;
(iii) $p_9(X,n,q) < 9q^{-n^2+9.6n}$ *if* $X = \mathrm{Sp}$ *(with q odd) or* SO^ε;
(iv) $\tilde{p}_9(\mathrm{Sp},n,q) < 9q^{-n^2+9.6n}$ *for q even.*

Proof. Let $G = X_{2n}(q)$ and let M be a maximal $\mathbf{C}_9$-subgroup of G, or of $\mathrm{SO}^\varepsilon_{2n}(q)$ if $X = \mathrm{Sp}$ and q is even. Suppose that $\mathcal{C}$ is a conjugacy class of good elements with $M \cap \mathcal{C} \neq \emptyset$. By Lemma 4.6, the contributions from groups in case (1) to the $\mathbf{C}_9$-probabilities satisfy $p_9^{(1)}(X,n,q) < q^{-n^2+4n+3}$ and $\tilde{p}_9^{(1)}(\mathrm{Sp},n,q) < q^{-n^2+4n+3}$.

We deal now with the groups in case (2), using the following upper bound for the number $c(G)$ of conjugacy classes of $\mathbf{C}_9$-subgroups in G proved in [5, Theorem 1.1]:

$$c(G) < N(n,q) := 2(2n)^{5.2} + 2n \log_2 \log_2 q. \tag{16}$$

Let $\mathcal{S}$ be the set of G-conjugacy classes of maximal $\mathbf{C}_9$-subgroups in case (2). For these groups M, we use the trivial upper bound $|M \cap \mathcal{C}| \leq |M| < q^{6\delta n}$, so, by (4), the contribution $p_9^{(2)}(X,n,q)$ to $p_9(X,n,q)$ from all groups in case (2) is at most

$$\begin{aligned} p_9^{(2)}(X,n,q) &\leq \sum_{\mathbf{S}\in\mathcal{S}} \frac{|G|}{|M(\mathbf{S})|}\frac{|M(\mathbf{S}) \cap \mathcal{C}|^2}{|\mathcal{C}|^2} \leq \frac{|G|}{|\mathcal{C}|^2}\sum_{\mathbf{S}\in\mathcal{S}} \big|M(\mathbf{S})\big| \\ &\leq \frac{|C_G(t)|^2}{|G|} N(n,q) q^{6\delta n}. \end{aligned} \tag{17}$$

Note that, for all $n \geq 9$ and $q \geq 2$, we have $2n \leq q^{n/2}$ so $2(2n)^{5.2} \leq 2q^{2.6n}$ and $2n \log_2 \log_2 q \leq q^n$. Thus $N(n,q) < 3q^{2.6n}$. We use the upper bounds from Corollary 3.2. If $X = \mathrm{SL}$ or SU, then $\frac{|C_G(t)|^2}{|G|} \leq 2q^{-2n^2+2n}$, and so

$$p_9(\mathrm{SL},n,q) = p_9^{(2)}(\mathrm{SL},n,q) < \frac{6}{q^{2n^2-10.6n}}$$

and

$$p_9(\mathrm{SU},n,q) = p_9^{(2)}(\mathrm{SU},n,q) < \frac{6}{q^{2n^2-16.6n}}.$$

If $X = \mathrm{Sp}$ or SO^ε, then $\frac{|C_G(t)|^2}{|G|} \leq \frac{25}{9} q^{-n^2+n}$, and so

$$p_9^{(2)}(X,n,q) < \frac{25}{3q^{n^2-9.6n}}.$$

Table 7
Upper bounds for $p_i(X, n, q)$ and $\tilde{p}_i(\mathrm{Sp}, n, q)$.

i	$p_i(\mathrm{SL}, n, q)$	$p_i(\mathrm{SU}, n, q)$	$p_i(\mathrm{Sp}, n, q)$	$p_i(\mathrm{SO}^\varepsilon, n, q)$	$\tilde{p}_i(\mathrm{Sp}, n, q)$
2	q^{-n^2}	0	0	$q^{-n^2+3n}/2$	0
3	$3.6q^{-n^2}$	$5q^{-4n^2/3}$	$3.7q^{-n^2/2}$	$10.6q^{-n^2/2}$	$3.7q^{-n^2/2}$
4	0	0	0	0	0
5	$8q^{-n^2+n+2}$	$8q^{-4(n^2-n)/3+2}$	$3q^{-2(n^2-n)/3}$	$4q^{-2(n^2-n)/3}$	$3q^{-2(n^2-n)/3}$
6	$1/48$	0	0	0	0
7	0	0	0	0	0
8	$2.7q^{-n^2+n+2}$	0	0	0	0
9	$6q^{-2n^2+10.6n}$	$6q^{-2n^2+16.6n}$	$9q^{-n^2+9.6n}$	$9q^{-n^2+9.6n}$	$9q^{-n^2+9.6n}$

Table 8
Conditions on n, q for the upper bounds in Table 7 to hold.

i	$p_i(X, n, q)$ and $\tilde{p}_i(\mathrm{Sp}, n, q)$
1	all n, q
2	$(n, q) \neq (2, 5), (2, 2^a - 1)$
3	$(n, q) \neq (2, 3), (2, 7)$
4	$n \geq 3$
5	$n \geq 3$
6	$(n, q) \neq (2, 2^a - 1)$
7	$n \geq 3$
8	$n \geq 3$ if $X = \mathrm{SL}$
9	$n \geq 9$

Thus, for $X = \mathrm{Sp}, \mathrm{SO}^\varepsilon$, adding to the estimate $p_9^{(1)}(X, n, q)$ we have $p_9(X, n, q) = p_9^{(1)}(X, n, q) + p_9^{(2)}(X, n, q) < 9q^{-n^2+9.6n}$. Similarly $\tilde{p}_9(\mathrm{Sp}, n, q)$ is less than $9q^{-n^2+9.6n}$. $\square$

14. Proofs of Theorems 2 and 6

We draw together results of the previous sections, namely Lemmas 6.2, 7.2, 8.1, 9.2, 10.1, 11.1, 12.1, 13.1. Although most of the results hold for smaller n, let us assume that $n \geq 9$ for $X = \mathrm{SL}, \mathrm{SU}$, and let $n \geq 10$ for $X = \mathrm{Sp}, \mathrm{SO}^\varepsilon$. Then, using (3) and (5), the probabilities $p(X, n, q) \leq \sum_{i=2}^{9} p_i(X, n, q)$, $\tilde{p}(\mathrm{Sp}, n, q) \leq \sum_{i=2}^{9} \tilde{p}_i(X, n, q)$, and upper bounds for the $p_i(X, n, q)$ and $\tilde{p}_i(\mathrm{Sp}, n, q)$ are obtained in the results mentioned above. We summarise these in Table 7 on page 99. We give in Table 8 a summary, for each i, of the conditions on n, q needed for the upper bounds on $p_i(X, n, q)$ and $\tilde{p}_i(\mathrm{Sp}, n, q)$ to hold. Recall that throughout the paper we assume that $n \geq 2$ if $X = \mathrm{SL}, \mathrm{SU}$ or Sp and $n \geq 4$ if $X = \mathrm{SO}^\varepsilon$. Moreover, if $i = 5$, then $n \geq 3$ by Lemma 9.1. Theorem 6 follows immediately from Tables 7, 8.

To prove Theorem 2, we note that Theorem 5 yields a positive lower bound p_1 for the probability that $\langle t, t' \rangle$ is irreducible, where t is a good element in $G = X_{2n}(q)$ and t' is a random conjugate of t. Note that we must make an exception of the groups $\mathrm{SO}_{2n}^\varepsilon(2)$ since Theorem 5 gives an upper bound for $p_1(\mathrm{SO}^\varepsilon, n, 2)$ greater than 1; thus in dealing with the groups $\mathrm{SO}_{2n}^\varepsilon(q)$ we take $q \geq 3$. Then for $n \geq 9$, adding the terms in the appropriate column of Table 7 gives an upper bound p_2 for the probability that $\langle t, t' \rangle$ is irreducible and contained in a maximal subgroup of G, or in the case $G = \mathrm{Sp}_{2n}(q)$ with q even, contained in a maximal subgroup of a subgroup $\mathrm{SO}^\varepsilon(q)$. Moreover $p_2 < p_1$ for all $n \geq 9$. Thus taking the minimum of the values for $p_1 - p_2$ over all classical types and all $n \geq 9$, (apart from the case of $\mathrm{SO}^\varepsilon_{2n}(2)$), we obtain a positive constant c which, provided $n \geq 9$, is a lower bound for the probability that $\langle t, t' \rangle$ is equal to G or, if $G = \mathrm{Sp}_{2n}(q)$ with q even, is equal to a subgroup $\mathrm{SO}^\varepsilon(q)$.

By Theorem 5, Table 7, and Lemma 5.7, for all $n \geq 9$ the smallest values of $p_1 - p_2$, for the types $X = \mathrm{SL}, \mathrm{SU}, \mathrm{Sp}$ (q even or odd), SO^ε ($q \geq 3$), occur for the parameters $(n, q) = (9, 2), (9, 2), (12, 2)$ and $(10, 3)$, respectively, and these minimum values are 0.042, 0.6, 0.15 and 0.5, respectively. Hence, whenever the parameter $n \geq 9$, one can take the absolute constant c in Theorem 2 to be $c = 0.042$.

The actual constant c in Theorem 2 must be modified to take account of the families of groups with $n \leq 8$, where an upper bound for $p_9(X, n, q)$ is not given in Lemma 13.1. In these cases, information about the $\mathbf{C}_9$-subgroups of G is available in the tables in [2], and c can be taken as a minimum of 0.042 and the smallest value of $p_1 - p_2$ for these low dimensional groups.

Acknowledgments

We thank Martin Liebeck for very helpful discussions which led us to refine our methods in the proof of Theorem 5 for $\mathrm{SL}_{2n}(q)$. This enabled us to obtain a useful upper bound in the case $q = 2$. We thank an anonymous referee for suggesting to us a form of Conjecture 1, and for other helpful comments which improved the exposition. We thank Max Neunhöffer for advice regarding the new recognition algorithms in his GAP package.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math. 76 (3) (1984) 469–514.

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

[3] H. Dietrich, C.R. Leedham-Green, F. Lübeck, E.A. O'Brien, Constructive recognition of classical groups in even characteristic, J. Algebra 391 (2013) 227–255.

[4] GAP-Group, GAP – Groups, Algorithms, and Programming, version 4.7.2, http://www.gap-system.org, 2013.

[5] J. Häsä, Growth of cross-characteristic representations of finite quasisimple groups of Lie type, J. Algebra 407 (2014) 275–306.

[6] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.

[7] P. Kleidman, The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups, J. Algebra 110 (1) (1987) 173–242.

[8] P. Kleidman, M. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, Cambridge, 1990.

[9] M.W. Liebeck, On the orders of maximal subgroups of the finite classical groups, Proc. Lond. Math. Soc. (3) 50 (3) (1985) 426–446.

[10] P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields, J. Lond. Math. Soc. 52 (1995) 263–284.

[11] M. Neunhöeffer, GAP package recog, version 1.2, http://www-groups.mcs.st-and.ac.uk/~neunhoef/Computer/Software/Gap/recog.html, 28 May 2012.
[12] M. Neunhoeffer, Á. Seress, Constructive recognition of $SL_n(q)$, in preparation.
[13] A.C. Niemeyer, C.E. Praeger, Elements in finite classical groups whose powers have large 1-eigenspaces, Discrete Math. Theor. Comput. Sci. (2014), to appear, arXiv:1405.2385.
[14] C. Praeger, Á Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions, J. Group Theory 14 (2011) 521–545.
[15] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1) (1892) 265–284.