Odd Order Products of Conjugate Involutions in Linear Groups over GF(2^a)

Ballantyne, John and Rowley, Peter

2016

MIMS EPrint: **2016.39**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Odd Order Products of Conjugate Involutions in Linear Groups over $GF(2^a)$

John J. Ballantyne and Peter J. Rowley

July 14, 2016

Abstract

Let G be isomorphic to $GL_n(q)$, $SL_n(q)$, $PGL_n(q)$ or $PSL_n(q)$, where $q = 2^a$. If t is an involution lying in a G-conjugacy class X, then for arbitrary n we show that as q becomes large, the proportion of elements of X which have odd-order product with t tends to 1. Furthermore, for n at most 4 we give formulae for the number of elements in X which have odd-order product with t, in terms of q.

1 Introduction

It is well known that for G a classical group defined over the finite field $GF(q)$, where q is a power of a prime p, the proportion of elements of G with order divisible by p tends to zero as q becomes large. Indeed, for G any finite group of Lie-type, Guralnick and Lübeck [11] have produced upper bounds for the number of such elements in G which demonstrate this asymptotic behaviour. This has implications in a number of situations - in particular, when the prime p is 2, its effects are felt in computational group theory. For example, a key technique in the recognition of matrix groups over finite fields is the construction of involution centralizers. A necessary step in this process is the production of the involution in question. However, when working with a finite group of Lie-type defined over a large field of characteristic 2, the generation of elements of even order via a random element approach is effectively impossible. This can be a thorny issue to deal with, although recently Kantor and Kassabov [13] have detailed an ingeneous method of producing an involution in the groups $PGL(2, 2^a)$, and this idea is elaborated upon by Borovik and Yalcinkaya [7].

On the other side of the coin, *given* an involution in a finite group of Lie-type over $GF(2^a)$, the relative lack of even order elements can prove advantageous. For example, when applying the method of Bray [8] to produce elements which centralize a given involution t, it is beneficial to have a supply of conjugates of t which have odd-order product with t, as such elements give rise to a set of elements which are uniformly distributed within $C_G(t)$. Experimental evidence for this benefit when looking to generate $C_G(t)$ can be found in [5], where a variant of Bray's method is discussed.

In this paper we are concerned with a question closely related to the example given immediately above - given an involution t from a linear group G defined over $GF(2^a)$ how many involutions which are G-conjugate to t have odd order product with t? This topic has been recently addressed in [15], where Liebeck demonstrates lower bounds on the number of such involutions in any finite simple group of Lie-type defined over $GF(2^a)$. In the case of classical groups, these bounds depend on the dimension of the group in its natural representation. Our main theorem concerns asymptotic behaviour in the case of linear groups as the size of the field increases.

Theorem 1.1. *Suppose G is isomorphic to $GL_n(q)$, $SL_n(q)$, $PGL_n(q)$ or $PSL_n(q)$, where $q = 2^a$, and suppose that $t \in G$ is an involution. Let X denote the G-conjugacy class of t. Then as a tends to infinity, the proportion of elements of X which have odd-order product with t tends to* 1.

Given the aforementioned work of Guralnick and Lübeck [11], Theorem 1.1 is perhaps not surprising, and indeed it confirms the expectation of Parker and Wilson in [16] in the case of linear groups. Theorem 1.1 does not, however, follow immediately from [11] as *a priori* we do not have knowledge of the distribution in G of elements which arise as products of conjugate involutions.

The topic of this paper also touches upon so-called *fusion graphs*. For a group G and a G-conjugacy class of involutions X, the fusion graph $\mathcal{F}(G, X)$ has X as its vertex set with two distinct involutions $x, y \in X$ joined whenever xy has odd order. Graph theoretic properties such as the diameter of $\mathcal{F}(G, X)$ and its connectivity have been investigated in [2], [3], [6], [4] and [9]. Theorem 1.1 implies for G one of the given linear groups and X any G-conjugacy class of involutions, there is an integer a_0 such that for all $a > a_0$ $\mathcal{F}(G, X)$ has diameter 2.

Our second result gives a precise answer for small linear groups.

Theorem 1.2. *Suppose G is isomorphic to $GL_n(q)$, $SL_n(q)$, $PGL_n(q)$ or $PSL_n(q)$, where $q = 2^a$, and suppose that $t \in G$ is an involution. Let X denote the G-conjugacy class of t, and denote by X_t the set of involutions in X which have odd-order product with t. Then the following hold.*

(i) If $n = 2$, then $|X_t| = q^2 - q + 1$.

(ii) If $n = 3$, then $|X_t| = q^4 - q^3 + 1$.

(iii) Suppose $n = 4$. If $\mathrm{rank}(t) = 1$, then $|X_t| = q^6 - q^5 + 1$, whereas if $\mathrm{rank}(t) = 2$, then $|X_t| = q^4(q^2 - 2q + 2)(q + 1)(q - 1) + 1$.

Our proof of Theorem 1.2, and to a large extent that of Theorem 1.1, relies only on some standard results regarding linear groups and their representation theory, and moreover is constructive in the sense that its methods may be used to produce a set of $C_G(t)$-orbit representatives for the set of conjugates t^g of t for which the product tt^g has odd order. The aforementioned representation theory is developed in Section 2. Underlying this segue into representation theory is

the observation that there is a one-to-one correspondence between the elements of the G-conjugacy class of t which have odd order product with t, and odd order elements of G which are inverted by t. This leads to the notions, for h an element of odd order inverted by t, of h-irreducible and h-reducible modules. In Lemmas 2.7 and 2.8 we obtain results which will enable us to count the number of odd order elements in G which t inverts. Just as important in our enumeration is the profile of $\langle h \rangle$, given in Definition 2.6. Section 3 analyses low dimension linear groups, and establishes Theorem 1.2. Our final section is devoted to proving Theorem 1.1. Here we obtain information regarding the $C_G(t)$-orbits of certain elements of odd order which are inverted by t whose profiles are in a certain sense maximal - see Section 4.1. Then, in Proposition 4.5 we prove a combinatorial result which counts the number of these maximal profiles. Taken together this information is sufficient to give a lower bound on the number of odd order elements which are inverted by t.

Our group theoretic notation is standard, as given for example in [10].

2 Preliminaries

The conclusions of Theorems 1.1 and 1.2 concern subsets of conjugacy classes of certain linear groups. We now make two observations that show it is sufficient to only prove Theorems 1.1 and 1.2 in the case of $GL_n(q)$. Firstly, note that since q is even, any involution in $GL_n(q)$ must have determinant equal to 1. Consequently, any involution conjugacy class of $GL_n(q)$ is contained in $SL_n(q)$, and is an $SL_n(q)$-conjugacy class. Thus our conclusions regarding $GL_n(q)$ will immediately carry over to $SL_n(q)$. Secondly, we observe that as q is even, both $GL_n(q)$ and $SL_n(q)$ have centres of odd-order. Consequently, any conjugacy class of involutions $\overline{X}$ in $PGL_n(q)$ or $PSL_n(q)$ has inverse image which contains an involution conjugacy class X in $GL_n(q)$, respectively $SL_n(q)$. Thus a product $\overline{xy}$ of involutions in $\overline{X}$ has odd-order if, and only if, the product of their preimages xy in X has odd-order. Therefore our conclusions regarding $GL_n(q)$ and $SL_n(q)$ will carry over to the factor groups $PGL_n(q)$ and $PSL_n(q)$.

Let $G = GL_n(q)$ and t be an involution of G. It is well-known that

$$|G| = q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1).$$

We denote by V the natural n-dimensional module for G over $GF(q^a)$. The *rank* of t is defined to be the dimension of the commutator space $[V,t]$. If $\mathrm{rank}(t) = k$, then

$$|C_G(t)| = q^{k^2+2k(n-2k)}|GL_k(q)||GL_{n-2k}(q)|$$

(see [1], for example).

Lemma 2.1. *Involutions in G are G-conjugate if and only if they have equal rank.*

Following Kleidman and Liebeck [14], by a *subspace decomposition* of V we mean a set of subspaces $V_1, \ldots, V_r$ of V with $r \geq 2$ such that

$$V = V_1 \oplus \cdots \oplus V_r.$$

We write $\mathcal{D} = \{V_1, \ldots, V_r\}$. The *stabilizer in G of $\mathcal{D}$* is the group $N_G(\mathcal{D}) = N_G(\{V_1, \ldots, V_r\})$, which is the subgroup of G which permutes the spaces V_i amongst themselves. The *centralizer in G of $\mathcal{D}$* is the group $C_G(\mathcal{D}) = N_G((V_1, \ldots, V_r))$, which is the subgroup of G leaving each V_i invariant.

Lemma 2.2. *Suppose $\mathcal{D} = \{V_1, V_2\}$ is a decomposition of V, with $\dim V_1 = \dim V_2$. Then there is a unique class of involutions in*

$$N_G(\mathcal{D}) \cong (GL(V_1) \times GL(V_2)) : 2$$

which interchange V_1 and V_2.

Proof. Any involution interchanging V_1 and V_2 must interchange a basis of V_1 with a basis of V_2. Since $GL(V_i)$, $i = 1, 2$, acts transitively on ordered bases of V_i, the lemma follows. □

It is straightforward to see that the involutions in G which are G-conjugate to t and have odd-order product with t are in one-to-one correspondence with the elements of odd-order in G which are inverted by t. We define

$$\mathcal{O}_t = \{g \in G \mid g \text{ has odd order and } g^t = g^{-1}\}.$$

Counting $|\mathcal{O}_t|$, rather than directly counting involutions, allows us to more easily make use of representation theory. Indeed, suppose $H \leq G$ is a subgroup of odd-order which is inverted by t. Since q is even, we may apply Maschke's Theorem to see that

$$V_H = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

where the V_i are irreducible H-modules. Note that, for each i and any $h \in H$,

$$(V_i^t)^h = V_i^{h^{-1}t} = V_i^t,$$

so V_i^t is an irreducible H-module. Thus $V_i \cap V_i^t$ either equals V_i, and so $V_i^t = V_i$, or equals 0. Moreover, since t is an involution, we must have $V_i^{t^2} = V_i$. We may therefore write

$$V_H = W_1 \oplus W_2 \oplus \cdots \oplus W_s$$

where each W_i is an irreducible $\langle H, t\rangle$-module, and as an H-module either W_i is irreducible or is a direct sum of two irreducible summands which are swapped by t. In the former case we say W_i is *H-irreducible*, while in the latter we say W_i is *H-reducible*. If it is the case that $H = \langle h\rangle$ for some element $h \in H$, we may use the notation *h-irreducible* and *h-reducible*, respectively.

Definition 2.3. Suppose $H \leq G$ is a subgroup of odd-order which is inverted by t, and suppose that

$$V_H = W_1 \oplus \cdots \oplus W_k \oplus U_1 \oplus \cdots \oplus U_\ell,$$

where the W_i are H-irreducible and the U_j are H-reducible. For each i, j write w_i, u_j for $\dim W_i$ and $\dim U_j$, respectively, and assume that the W_i and U_j are

ordered so that $w_i \geq w_{i+1}$ and $u_j \geq u_{j+1}$. We define the *profile* of H, $\mathcal{P}(H)$, to be

$$\mathcal{P}(H) = \{w_1, w_2, \ldots, w_k \mid u_1, u_2, \ldots, u_\ell\}.$$

If there happen to be no H-irreducible, respectively H-reducible, spaces in the decomposition of V_H, we reflect this in $\mathcal{P}(H)$ by simply writing 0 in the relevant part of the profile. If h is an element of odd-order which is inverted by t, we define its profile $\mathcal{P}(h)$ to be $\mathcal{P}(\langle h \rangle)$. We shall sometimes employ "exponential notation" when there are multiple copies of a certain dimension.

It follows from the uniqueness of composition series (up to reordering) that the profile is well-defined. Notice that for a given profile $\mathcal{P}(h)$ the entries to the right of the vertical line must be even, since the module is a direct sum of two spaces of equal dimension. Indeed, if $\langle h \rangle$ acts nontrivially on a subspace W_i then the corresponding entry on the left hand side of the profile will also be even, as the following result shows.

Lemma 2.4. *Suppose $h \in \mathcal{O}_t$, with U a non-trivial h-irreducible module. Then* $\dim U = 2\mathrm{rank}(t_U)$.

Proof. Clearly $\dim U \geq 2\mathrm{rank}(t_U)$, so suppose $\dim U > 2\mathrm{rank}(t_U)$. Then $\dim U > 2(\dim U - \dim C_U(t))$, and so $\dim C_U(t) > \dim U/2$. As both t and th leave U invariant we may consider t_U and $(th)_U$ as conjugate involutions in $GL(U)$, and hence

$$\dim C_U(th) = \dim C_U(t) > \dim U/2.$$

Thus $\dim(C_U(t) \cap C_U(th)) \geq 1$. However,

$$C_U(t) \cap C_U(th) \subseteq C_U(t(th)) = C_U(h),$$

and since U is irreducible as a $\langle h \rangle$-module we have $C_U(h) = 0$, a contradiction. Therefore $\dim U = 2\mathrm{rank}(t_U)$. □

We further remark that 1 is the only possible odd entry on the left hand of a profile: this occurs when $\langle h, t \rangle$ acts trivially on the relevant W_i.

In [12], Huppert details many facts regarding *Singer cycles*, that is, elements of $GL_n(q)$ with order $q^n - 1$. Such elements act regularly on the non-zero vectors of V. *Singer cycle subgroups* of $GL_n(q)$ are subgroups generated by Singer cycles. Singer cycle subgroups of $SL_n(q)$ are defined to be those subgroups $S \cap SL_n(q)$, where S is a Singer cycle subgroup of $GL_n(q)$. Since elements of $SL_n(q)$ must have determinant equal to 1, it follows that Singer cycles of $SL_n(q)$ have order $(q^n - 1)/(q - 1)$. All Singer cycle subgroups are conjugate in $GL_n(q)$, respectively $SL_n(q)$.

Theorem 2.5. *Suppose G is a subgroup of $GL_n(q)$, with H an abelian normal subgroup of G, and moreover suppose that, as a $GF(q)H$-module, V is the direct sum of s isomorphic irreducible $GF(q)H$-submodules. Set $a = n/s$. Then G is a group of s-dimensional $GF(q^a)$-semilinear transformations. Furthermore, $C_G(H)$ is the subgroup of G consisting of $GF(q^a)$-linear transformations.*

Proof. See Satz 3.11 of [12]. □

If S is a Singer cycle subgroup of $SL_n(q)$ or $GL_n(q)$, then clearly V_S is irreducible. Thus, by Theorem 2.5, S may be considered as a subgroup of $GF(q^n)^*$, and is self-centralizing. Moreover

$$N_{GL_n(q)}(S) \sim S : n.$$

Also by Theorem 2.5, if $h \in SL_n(q)$ has order dividing $q^n - 1$ and $V_{\langle h \rangle}$ is irreducible, then h lies in a Singer cycle subgroup.

For a given profile $\mathcal{P}$, we choose a subgroup $H \leq G$ which is 'maximal' with this profile, in the following way. For a suitable decomposition $\mathcal{D} = \{W_1, \ldots, W_k, U_1, U_1^t, \ldots, U_\ell, U_\ell^t\}$ of V for this profile, we note that

$$C_G(\mathcal{D}) \cong GL(W_1) \times \cdots \times GL(W_k) \times GL(U_1) \times GL(U_1^t) \times \cdots \times GL(U_\ell) \times GL(U_\ell^t).$$

For $1 \leq i \leq k$, within each subgroup $GL(W_i)$ we fix a Singer cycle subgroup S_i which is normalized by t. For $1 \leq j \leq \ell$, within each subgroup $GL(U_j) \times GL(U_j^t)$ we fix a subgroup $\tilde{S}_j$ which is generated by an element (s_j, s_j^{-1}), where s_j is a Singer cycle of $GL(U_j)$. Any subgroup which takes this form we say is *maximal with respect to* $\mathcal{P}$

Lemma 2.6. *Suppose S is a subgroup of G which is maximal with respect to some profile $\mathcal{P}$. Then any element $h \in \mathcal{O}_t$ with profile $\mathcal{P}$ is $C_G(t)$-conjugate into S.*

Proof. Let $\mathcal{D}$ be a suitable decomposition of V_S. First we claim that, without loss of generality, we may assume that h lies in $C_G(\mathcal{D})$. Indeed, since G acts transitively on ordered bases of V, there exists an element $g_1 \in G$ such that h^{g_1} lies in $C_G(\mathcal{D})$ and t^{g_1} lies in $\langle C_G(\mathcal{D}), t \rangle$. Using Lemmas 2.1 and 2.2 we see that there exists $g_2 \in \langle C_G(\mathcal{D}), t \rangle$ such that $t = t^{g_1 g_2}$. Since $h^{g_1 g_2} \in C_G(\mathcal{D})$ our claim holds, so assume that $h \in C_G(\mathcal{D})$.

Since Singer cycle subgroups of $GL_n(q)$ are all conjugate, there exists $g \in C_G(\mathcal{D})$ such that $h \in S^g$. Thus both t and t^g normalize $H = \langle h \rangle$, and so by Theorem 2.5 there exists $n \in N_G(H)$ such that $t^n = t^g$, and consequently $ng^{-1} \in C_G(t)$. Since $h^{ng^{-1}} \in S$, the result holds. □

Lemma 2.7. *Suppose $h \in \mathcal{O}_t$, and that V is an h-irreducible module with* $\dim V = 2k$. *Then*

$$|C_G(t) \cap C_G(h)| = q^k - 1,$$

and

$$[N_G(\langle h \rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2k.$$

Proof. Using Theorem 2.5 we may consider h as a linear transformation of a 1-dimensional $GF(q^{2k})$-vector space, with t acting as a field automorphism of order 2. Moreover, $C_G(h)$ is a Singer cycle subgroup of order $q^{2k} - 1$, and $C_G(h) \cap C_G(t)$ is the centralizer in $GF(q^{2k})^*$ of the field automorphism t, which is $GF(q^k)^*$. Thus $|C_G(h) \cap C_G(t)| = q^k - 1$.

By Theorem 2.5 once more we have that $[N_G(\langle h\rangle) : C_G(h)] = 2k$, with this index coming from the order of the cyclic automorphism group of $GF(q^{2k})$ over $GF(q)$. Since these automorphisms must also commute with the field automorphism t, we see that

$$[N_G(\langle h\rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2k,$$

as required. □

Lemma 2.8. *Suppose $h \in \mathcal{O}_t$, and that V is an h-reducible module with* $\dim V = 2k$. *Then*

$$|C_G(t) \cap C_G(h)| = q^k - 1,$$

and

$$[N_G(\langle h\rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2k.$$

Proof. Write $H = \langle h\rangle$. Since V is h-reducible we may write $V_H = W \oplus W^t$. Note that h_W and h_{W^t} lie in Singer cycle subgroups S_1 and S_2 of $GL(W)$ and $GL(W^t)$, respectively. As $\det(h_W) \neq \det(h_{W^t})$, W and W^t are non-isomorphic H-modules. Consequently they are the unique pair of k-dimensional irreducible H-submodules of V, and since W^g is an irreducible H-module for any $g \in C_G(h)$, it follows that $C_G(h)$ must leave both W and W^t invariant. Hence, using Theorem 2.5, $C_G(h)$ is the subgroup generated by S_1 and S_2. As t clearly swaps W with W^t, an element $g \in C_G(h)$ commutes with t if and only if $g_W = g_{W^t}$, whence $|C_G(h) \cap C_G(t)| = q^k - 1$.

Any element of $N_G(H)$ must either swap W with W^t, or leave each subspace invariant. By Theorem 2.5 we have $[N_{G_W}(H_W) : C_{G_W}(h_W)] = k$, and similarly for the restriction to W^t. As above, for an element $g \in N_G(H)$ to commute with t we require that $g_W = g_{W^t}$. Thus, including t we see that

$$[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2k.$$

□

3 Linear Groups of Small Dimension

In this section we suppose that $G = GL_2(q)$, $GL_3(q)$ or $GL_4(q)$, and derive formulae for the total number of involutions in X which have odd-order product with a fixed involution t. In light of the observations in Section 2, these formulae will also be valid for the groups $SL_n(q)$, $PGL_n(q)$ and $PSL_n(q)$, where $n = 2$, 3 or 4. This analysis will also demonstrate how to construct a set of $C_G(t)$-orbit representatives for $\mathcal{O}_t$, the method of which could be extended to higher dimensions n if desired.

3.1 $GL_2(q)$ and $GL_3(q)$

Let $G = GL_2(q)$, with $t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Let ω be such that $\langle \omega \rangle = GF(q)^*$ and set $h_1 = \begin{pmatrix} 0 & 1 \\ 1 & \omega \end{pmatrix}$ and $h_2 = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$. Recall that $|G| = q(q-1)(q^2-1)$.

Suppose $h \in \mathcal{O}_t$. The possible profiles for h are $\{2 \mid 0\}$ and $\{0 \mid 2\}$ (the latter case includes the identity element of G). In view of Lemma 2.6 either V_H is irreducible, or h is $C_G(t)$-conjugate to a diagonal element.

First we consider the case where V_H is irreducible. By Theorem 2.5, in this case h must lie in a Singer cycle subgroup of G, so must have order dividing q^2-1. Since h is inverted by t it necessarily has determinant 1, and so in fact the order of h must divide $q+1$. We may easily check that $H_1 = \langle h_1 \rangle$ has order $q+1$, and $h_1^t = h_1^{-1}$, so by Lemma 2.6 h is $C_G(t)$-conjugate into H_1. Thus we may choose our $C_G(t)$-orbit representatives from H_1.

Note that since $(q+1, q-1) = 1$, all subgroups generated by non-trivial elements of H_1 must act irreducibly on V. By Theorem 2.5 we have $N_G(H_1) \sim H_1 : \langle t \rangle$, and hence

$$[N_G(H_1) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2$$

for all non-trivial $h \in H_1$. Hence every non-trivial element of H_1 is $C_G(t)$-conjugate to exactly one other element of H_1. Also $|C_G(t)| = q(q-1)$, and $|C_G(t) \cap C_G(h)| = q-1$ for all non-trivial $h \in H_1$, by Theorem 2.5. Thus, for $1 \neq h \in H_1$, the $C_G(t)$-orbit containing h consists of q elements. Therefore in total we have $q^2/2$ non-trivial elements of $\mathcal{O}_t$ whose order divides $q+1$.

Now suppose that $V_H = W \oplus W^t$, where W is a 1-dimensional irreducible H-module. Here, h is $C_G(t)$-conjugate to a diagonal element, so its order must divide $q-1$. Clearly we may take our $C_G(t)$-orbit representatives from $H_2 = \langle h_2 \rangle$. In this case, we may easily check that

$$[C_G(t) : C_G(t) \cap C_G(h)] = q-1$$

and

$$[N_G(H_2) \cap C_G(t) : C_G(h) \cap C_G(t)] = 2$$

for all $1 \neq h \in H_2$. Hence, in total we have $(q-2)q/2$ non-trivial elements of $\mathcal{O}_t$ whose order divides $q-1$.

Including the identity element, together this gives

$$\begin{aligned} |\mathcal{O}_t| &= q^2/2 + (q-2)q/2 + 1 \\ &= q^2 - q + 1 \end{aligned}$$

which proves part (i) of Theorem 1.2.

Now let $G = GL_3(q)$, with $t = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The possible profiles for $h \in \mathcal{O}_t$ are $\{2,1 \mid 0\}$, $\{1 \mid 2\}$, with representative elements $h_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}$

and $h_2 = \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$, respectively. We may consider t, h_1 and h_2 to lie naturally in a subgroup $K \times L \leq G$ which is isomorphic to $GL_2(q) \times GL_1(q)$, and observe that the centralizers and normalizers of $\langle t \rangle$, $\langle h_1 \rangle$ and $\langle h_2 \rangle$ will the direct product of those in K (which have been determined above in the $GL_2(q)$ case) with the whole of L. This leads to $q^4/2$ elements in the $C_G(t)$-orbit containing h_1, and $(q^4 - 2q^3)/2$ elements in the $C_G(t)$-orbit containing h_2. Thus, including the identity, we have

$$|\mathcal{O}_t| = q^4 - q^3 + 1.$$

3.2 $GL_4(q)$

Let $G = GL_4(q)$. In the case where $\text{rank}(t) = 1$ we may proceed as in $GL_3(q)$ with the difference that the corresponding subgroup L will be isomorphic to $GL_2(q)$ rather than $GL_1(q)$. The corresponding counts for the $C_G(t)$-orbits are $q^6/2$, $(q^6 - 2q^5)/2$ and 1.

We move on to the case where $\text{rank}(t) = 2$, and take

$$t = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}.$$

For $h \in \mathcal{O}_t$ the possible profiles are $\{4 \mid 0\}$, $\{0 \mid 4\}$, $\{2, 2 \mid 0\}$, $\{2 \mid 2\}$ and $\{0 \mid 2, 2\}$. First suppose that h has profile $\{4 \mid 0\}$, so V_H is irreducible. Then by Theorem 2.5 h must lie in a Singer cycle subgroup S of G, so must have order dividing $(q^4 - 1)/(q - 1) = (q + 1)(q^2 + 1)$, and we may consider h as an element of $GF(q^4)^*$, with t representing a field automorphism of $GF(q^4)$. Since t is an involution, its fixed field is $GF(q^2)$. Therefore, for h to be inverted by t, h must have order coprime to $q^2 - 1$, and hence the order of h must divide $q^2 + 1$. Let H be the unique subgroup of S with order $q^2 + 1$. Since $(q^2 - 1, q^2 + 1) = 1$, no non-trivial element of H may embed into a subgroup $GL_2(q^2)$, and so $\langle h \rangle$ acts irreducibly on V for all $1 \neq h \in H$.

By Lemma 2.6 we may choose our $C_G(t)$-orbit representatives from H. Using Theorem 2.5, for all $1 \neq h \in H$ we have that $N_G(H)/C_G(h)$ is isomorphic to the automorphism group of $GF(q^4)$ over $GF(q)$, and so

$$[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = 4.$$

Moreover $|C_G(t)| = q^5(q - 1)(q^2 - 1)$, and $|C_G(t) \cap C_G(h)| = (q - 1)(q + 1)$ since elements of S are fixed by t if and only if their order divides $q^2 - 1$. Therefore we have

$$\frac{q^2 q^5 (q - 1)(q^2 - 1)}{4(q - 1)(q + 1)} = \frac{q^7 (q - 1)}{4}$$

elements of $\mathcal{O}_t$ in this case.

Next assume that h has profile $\{0 \mid 4\}$, so $V_H = W \oplus W^t$. Since h_W and h_{W^t} lie in subgroups $GL_2(q)$, h must have order dividing $q^2 - 1$. To avoid double-counting we wish only to count such elements h which do not yield a 2-dimensional H-submodule of V which is left invariant by t. Such h are precisely those for which $\det(h_W)$ and $\det(h_{W^t})$ do not equal 1 (since then W and W^t are non-isomorphic as H-modules). Therefore the order of h cannot divide $q + 1$. Moreover, the order of h cannot divide $q - 1$, since then $\langle h \rangle$ would leave a 1-dimensional subspace of V invariant. Hence there are

$$(q^2 - 1) - (q + 1) - (q - 1) + 1 = q^2 - 2q$$

elements of H to consider.

For all relevant $h \in H$ we have $[N_G(H) : C_G(h)] = 4$. Indeed, clearly $t \in N_G(H) \setminus C_G(h)$, and within each $GL_2(q)$ block the index of the centralizer in the normalizer is 2. The restriction on the determinant in G gives the index as claimed. We also have $[C_G(t) : C_G(t) \cap C_G(h)] = (q - 1)(q + 1)$. Indeed, the elements of order dividing $q+1$ which centralize h as they lie in the same Singer cycle subgroup also centralize t, since they embed into the centre of a $GL_2(q^2)$ subgroup which also contains t (using Theorem 2.5 here).

Hence we have

$$\frac{(q^2 - 2q)q^5(q - 1)(q^2 - 1)}{4(q - 1)(q + 1)} = \frac{(q^2 - 2q)q^5(q - 1)}{4}$$

elements of $\mathcal{O}_t$ in this case.

Now suppose that h has profile $\{2, 2 \mid 0\}$, so $V_H = W \oplus U$, where W and U are 2-dimensional irreducible H-modules which are also left invariant by t. By Lemma 2.6 we may choose our $C_G(t)$-orbit representatives to lie in a unique block diagonal subgroup S generated by Singer cycle subgroups of $SL(W)$ and $SL(U)$. Thus $|S| = (q + 1)^2$. Since h should act irreducibly on both W and U, neither block should equal the 2×2 identity element, so we have q^2 elements of S to consider. There are now two subcases.

Firstly, suppose that W and U are isomorphic H-modules. This occurs if and only if $h_W = h_U^{\pm 1}$ as elements of $GL_2(q)$. In this case, h embeds as a central element in a subgroup $GL_2(q^2)$ of G which also contains t. By Theorem 2.5, t acts as a field automorphism on $C_G(h)$. Hence $C_G(h) \cap C_G(t)$ is the centralizer of a field automorphism in $GL_2(q^2) \cap G$. There are $2q$ elements to consider, and by Theorem 2.5, for any such h we have

$$[N_G(\langle h \rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 4.$$

This yields

$$\frac{2qq^5(q - 1)(q^2 - 1)}{4q(q - 1)(q^2 - 1)} = \frac{q^5}{2}$$

elements of $\mathcal{O}_t$.

The second possibility is that W and U are non-isomorphic H-modules. There are $q^2 - 2q$ such elements of S, and for each such h we have

$$|C_G(h) \cap C_G(t)| = (q - 1)^2,$$

given by elements of the form

$$\begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \lambda^{-1} & \\ & & & \lambda^{-1} \end{pmatrix}$$

where $\lambda \in GF(q)^*$, along with the centre of G. Each such element h is $C_G(t)$-conjugate to exactly seven other elements of S. Indeed, we may invert h_U and h_W individually, and we may also swap the blocks h_U and h_W. Since $h_U \neq h_W^{\pm 1}$, swapping blocks will yield a element of S distinct from those given by inverting h_U or h_W. Thus we have

$$\frac{(q^2-2q)q^5(q-1)(q^2-1)}{8(q-1)^2} = \frac{(q^2-2q)q^5(q+1)}{8}$$

elements of $\mathcal{O}_t$.

Now suppose that h has profile $\{2 \mid 2\}$, so $V_H = W \oplus U \oplus U^t$ where W is a 2-dimensional irreducible H-module which is also t-invariant, and U is a 1-dimensional H-module. By Lemma 2.6 we may choose our $C_G(t)$-orbit representatives to lie in the subgroup S of G which is generated by

$$\begin{pmatrix} 0 & 1 & & \\ 1 & \omega & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & \omega & 0 \\ & & 0 & \omega^{-1} \end{pmatrix},$$

where $\langle \omega \rangle = GF(q)^*$. Since $(q-1, q+1) = 1$, S is cyclic. For the moment we do not wish to consider those elements of S where a 2×2 block equals the identity block, so there are

$$(q+1)(q-1) - (q+1) - (q-1) + 1 = q^2 - 2q$$

elements to consider. For each such h we have $|C_G(t) \cap C_G(h)| = (q-1)^2$ (given by diagonal elements as in the previous case), and

$$[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = 4$$

(given by inversion within each 2×2 block). Thus we have

$$\frac{(q^2-2q)q^5(q-1)(q^2-1)}{4(q-1)^2} = \frac{q^5(q^2-2q)(q+1)}{4}$$

elements of $\mathcal{O}_t$.

Now suppose that h acts trivially on U and U^t. Here we may argue as in the $GL_3(q)$ case dealt with above, except that the corresponding subgroup L is isomorphic to $GL_2(q)$ and t projects to an involution in L, rather than the identity element. This results in

$$\frac{q^5(q+1)}{2}$$

elements of $\mathcal{O}_t$.

The next case to consider it that where h has profile $\{0 \mid 2, 2\}$. By Lemma 2.6 we may assume that h lies in a subgroup S of G which is generated by

$$\begin{pmatrix} \omega & 0 & & \\ 0 & \omega^{-1} & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & \omega & 0 \\ & & 0 & \omega^{-1} \end{pmatrix},$$

where $\langle \omega \rangle = GF(q)^*$. Clearly S has order $(q-1)^2$ - however, we do not wish to consider elements of S for which either 2×2 block equals I_2, so there are $(q-2)^2$ elements of S with the required profile.

Firstly suppose that h contains no 2×2 identity block on its main diagonal. Then there are two subcases to consider. Firstly, suppose that $h \in S$ embeds as a central element in a subgroup $GL_2(q^2)$ which also contains t acting as a field automorphism of order 2. This occurs if and only if h takes the form

$$\begin{pmatrix} \lambda & 0 & & \\ 0 & \lambda^{-1} & & \\ & & \lambda & 0 \\ & & 0 & \lambda^{-1} \end{pmatrix}$$

or

$$\begin{pmatrix} \lambda & 0 & & \\ 0 & \lambda^{-1} & & \\ & & \lambda^{-1} & 0 \\ & & 0 & \lambda \end{pmatrix}$$

for some $\lambda \in GF(q)$. In this case $C_G(h) \cap C_G(t)$ is the centralizer of a field automorphism in $GL_2(q^2) \cap G$, which is $GL_2(q)$. There are $2(q-2)$ such elements h, and for each we have

$$[N_G(\langle h \rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 4.$$

This yields

$$\frac{2(q-2)q^5(q-1)(q^2-1)}{4q(q-1)(q^2-1)} = \frac{q^4(q-2)}{2}$$

elements of $\mathcal{O}_t$.

The second subcase is that $h \in S$ does not embed as a central element in a $GL_2(q^2)$ subgroup which also contains t acting as a field automorphism of order 2. There are $(q-2)^2 - 2(q-2)$ such elements h of S, and for such an h we have $|C_G(h) \cap C_G(t)| = (q-1)^2$, since $C_G(h) \cap C_G(t)$ is the set consisting of elements of the form

$$\begin{pmatrix} \lambda & 0 & & \\ 0 & \lambda & & \\ & & \lambda^{-1} & 0 \\ & & 0 & \lambda^{-1} \end{pmatrix}$$

for some $\lambda \in GF(q)$, along with the centre of G. For each such h we have

$$[N_G(\langle h \rangle) \cap C_G(t) : C_G(h) \cap C_G(t)] = 8,$$

as we can easily take elements of $C_G(t)$ which invert either 2×2 block of h we choose, or swap the two blocks. Hence we have

$$\frac{((q-2)^2 - 2(q-2))q^5(q-1)(q^2-1)}{8(q-1)^2} = \frac{((q-2)^2 - 2(q-2))q^5(q+1)}{8}$$

elements of $\mathcal{O}_t$.

Now suppose that exactly one of the 2×2 blocks on the main diagonal of h equals I_2. Again we may argue in a similar way to the $GL_3(q)$ case, with minor modifications, and obtain

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

elements of $\mathcal{O}_t$. The final possibility to consider is that both 2×2 blocks on the main diagonal of h equal I_2. However, this of course just yields the identity element, and adds 1 to the count.

Adding all these contributions together yields that

$$|\mathcal{O}_t| = q^4(q^2 - 2q + 2)(q+1)(q-1) + 1,$$

which completes the proof of Theorem 1.2.

4 Proof of Theorem 1.1

Suppose $G = GL_n(q)$, $q = 2^a$ and t is an involution of G. Set $X = t^G$, and let V be the natural $GF(q)G$-module. Here we write $X \sim q^R$ to mean that X is a polynomial in q with leading term q^R. We begin by considering the case where $\mathrm{rank}(t) = n/2$, and set $k = n/2$.

4.1 The case where $\mathrm{rank}(t) = n/2$.

We wish to consider certain subgroups of G having profiles which are in some sense maximal. We write $\mathrm{Prof}(t)$ for the set of all possible profiles which arise from subgroups of odd-order which are inverted by t. We then define

$$\mathrm{MProf}(t) = \{\mathcal{P} = \{n_1, \ldots, n_r | n_{r+1}, \ldots, n_s\} \mid n_i \geq 2 \text{ for } 1 \leq i \leq r\}.$$

Subgroups with profiles in MProf will contain elements which, when block diagonalized, contain no trivial Jordan blocks. Now, for a given $\mathcal{P} \in \mathrm{MProf}$, we choose a subgroup $H \leq G$ which is maximal with respect to $\mathcal{P}$. We repeat the definition of such subgroups from Section 2. For a suitable decomposition

$$\mathcal{D} = \{W_1, \ldots, W_r, U_{r+1}, U_{r+1}^t, \ldots, U_s, U_s^t\}$$

of V for this profile, we recall that

$$C_G(\mathcal{D}) \cong GL(W_1)\times\cdots\times GL(W_r)\times GL(U_{r+1})\times GL(U_{r+1}^t)\times\cdots\times GL(U_s)\times GL(U_s^t).$$

For $1 \leq i \leq r$, within each subgroup $GL(W_i)$ we fix a Singer cycle subgroup S_i which is normalized by t and for $r+1 \leq j \leq s$, within each subgroup $GL(U_j) \times GL(U_j^t)$ we fix a subgroup $\tilde{S}_j$ which is generated by an element (s_j, s_j^{-1}), where s_j is a Singer cycle of $GL(U_j)$.

For each $\mathcal{P} \in \mathrm{MProf}$ we choose an H which is maximal with respect to $\mathcal{P}$, and collect these together to form a set of representative subgroups $\mathcal{H}$. The $C_G(t)$-orbit representatives we wish to consider will lie in these subgroups.

Definition 4.1. Let H be a subgroup of G which is maximal with respect to some $\mathcal{P} \in \mathrm{MProf}(t)$. Let

$$\mathcal{D} = \{W_1, \ldots, W_r, U_{r+1}, U_{r+1}^t, \ldots, U_s, U_s^t\}$$

be a suitable decomposition of V for this profile. We define the subset $\mathcal{O}_t(H)$ of H to consist of all elements $h \in H$ which satisfy the following three properties.

(i) $h \in \mathcal{O}_t$,

(ii) each W_i is irreducible when considered as an $\langle h\rangle$-module,

(iii) no two spaces in $\{W_i, U_j \oplus U_j^t \mid 1 \leq i \leq r, r+1 \leq j \leq s\}$ are isomorphic as $\langle h\rangle$-modules.

Lemma 4.2. *For q sufficiently large, $|\mathcal{O}_t(H)| \sim q^k$.*

Proof. Since $|\mathcal{O}_t(H)| < |X| \sim q^k$, it suffices to show that for sufficiently large q, the size of the subsets consisting of elements of H which satisfy conditions (i), (ii) and (iii), respectively, are each expressible as a polynomial in q with leading term q^k.

First we consider those elements of H which satisfy (i). Set $k_i = n_i/2$. For $1 \leq i \leq r$, $g \in S_i$ is inverted by t if, and only if, g lies outside the 'fixed field' of t, which has order $q^{k_i} - 1$. Thus we require that g has order coprime to $q^{k_i} - 1$. Since $q^{n_i} - 1 = (q^{k_i} - 1)(q^{k_i} + 1)$, there are $q^{k_1} + 1$ such elements. For $r+1 \leq i \leq m$, $\tilde{S}_i$ is isomorphic to a Singer cycle subgroup of $GL_{n_i}(q)$, so $|\tilde{S}_i| = q^{k_i} - 1$, and all elements are inverted by t. Consequently the number of elements of H which satisfy (i) is given by a polynomial with leading term $q^{k_1+\cdots+k_s} = q^k$.

Now consider those elements of H which satisfy (ii). To guarantee the spaces V_i are irreducible as $\langle h\rangle$-modules, we may take the projections of h to each V_i to have order $q^{k_i} + 1$ for $1 \leq i \leq r$, and $q^{k_i} - 1$ for $r+1 \leq i \leq s$. Since in a subgroup of order $q^{k_i} + 1$, respectively $q^{k_i} - 1$, the number of such elements is given by a polynomial with leading term q^{k_i}, the number of elements of H which satisfy (ii) is given by a polynomial with leading term q^k.

Finally, consider those elements of H which satisfy (iii). Note that V_i and V_j are isomorphic as $\langle h\rangle$-modules if, and only if, $\dim V_i = \dim V_j = n_i$ and

the projections h_i and h_j of h to V_i and V_j, respectively, are conjugate when considered as elements of $GL_{n_i}(q)$. Since $N_{GL_{n_i}(q)}(S_i) \cong S_i : n_i$, there are n_i conjugates of h_i in $GL_{n_i}(q)$. This number does not depend on q, so for q sufficiently large there are q^{k_i} choices of h_j. Hence the number of elements of H which satisfy (iii) is given by a polynomial with leading term q^k.

It follows that $|\mathcal{O}_t(H)| \sim q^k$ for q sufficiently large. □

Lemma 4.3. *Suppose $h \in \mathcal{O}_t(H)$. Then $|C_G(h) \cap C_G(t)| \sim q^k$.*

Proof. Suppose h has profile

$$\{n_1^{m_1}, n_2^{m_2}, \ldots, n_r^{m_r} | n_{r+1}^{m_{r+1}}, \ldots, n_s^{m_s}\}.$$

Since no two irreducible summands of V_H are isomorphic as $\langle h \rangle$-modules we have that $C_G(h)$ leaves each irreducible direct summand of V_H invariant. Now we apply Lemmas 2.7 and 2.8, setting $k_i = n_i/2$, to see that

$$\begin{aligned} |C_G(h) \cap C_G(t)| &= (q^{k_1} - 1)^{m_1}(q^{k_2} - 1)^{m_2} \cdots (q^{k_s} - 1)^{m_s} \\ &\sim q^{k_1 m_1 + k_2 m_2 + \cdots + k_s m_s} \\ &= q^k. \end{aligned}$$

□

Lemma 4.4. *Suppose H has profile*

$$\mathcal{P}(H) = \{n_1^{m_1}, n_2^{m_2}, \ldots, n_r^{m_r} | n_{r+1}^{m_{r+1}}, \ldots, n_s^{m_s}\}.$$

Then for any $h \in \mathcal{O}_t(H)$,

$$[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = n_1^{m_1} n_2^{m_2} \cdots n_s^{m_s} m_1! m_2! \cdots m_s!.$$

Proof. Certainly $N_G(H) \leq N_G(\mathcal{D})$. First considering $N_G(H) \cap C_G(\mathcal{D})$, and restricting to individual direct summands, by Lemmas 2.7 and 2.8 we have that

$$[N_G(H) \cap C_G(\mathcal{D}) \cap C_G(t) : C_G(h) \cap C_G(\mathcal{D}) \cap C_G(t)] = n_1^{m_1} n_2^{m_2} \cdots n_s^{m_s}.$$

Additionally we have elements from $(N_G(H) \cap C_G(t)) \setminus C_G(\mathcal{D})$ which permute summands which are isomorphic as $\langle H, t \rangle$-modules. Since two summands from $\mathcal{D}$ are $\langle H, t \rangle$-isomorphic precisely when they have equal dimension and are of the same type, we find that

$$[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = n_1^{m_1} n_2^{m_2} \cdots n_s^{m_s} m_1! m_2! \cdots m_s!$$

as required. □

In view of Lemma 4.4, for H with profile $\mathcal{P} = \{n_1^{m_1}, n_2^{m_2}, \ldots, n_r^{m_r} | n_{r+1}^{m_{r+1}}, \ldots, n_s^{m_s}\}$ we define the integer $n(H)$ to be

$$n(H) = n_1^{m_1} n_2^{m_2} \cdots n_s^{m_s} m_1! m_2! \cdots m_s!$$

Now, for each $H \in \mathcal{H}$, we count the elements of $\mathcal{O}_t$ which are $C_G(t)$-conjugate into $\mathcal{O}_t(H)$. For $h \in \mathcal{O}_t(H)$, by Lemma 4.3 the length of the $C_G(t)$-orbit containing h is $[C_G(t) : C_G(t) \cap C_G(h)] \sim q^{2k^2}/q^k$. Moreover, by Lemma 4.2 the size of $\mathcal{O}_t(H) \sim q^k$. Note that no element $h \in \mathcal{O}_t(H)$ can be $C_G(t)$-conjugate to any $h' \in \mathcal{O}_t(H')$, where $H' \in \mathcal{H}$ but $H' \neq H$, since h and h' will have different profiles. However, some elements of $\mathcal{O}_t(H)$ will be $C_G(t)$-conjugate to each other, so to compensate for this we divide the length of each orbit by $[N_G(H) \cap C_G(t) : C_G(h) \cap C_G(t)] = n(H)$, using Lemma 4.4. Putting this together, we see that

$$|\mathcal{O}_t| \geq \sum_{H \in \mathcal{H}} \frac{q^k q^{2k^2}}{n(H) q^k} = q^{2k^2} \sum_{H \in \mathcal{H}} \frac{1}{n(H)}.$$

Since $|X| \sim q^{2k^2}$, we complete the proof of Theorem 1.1 for the case where $\mathrm{rank}(t) = n/2$ by showing that

$$\sum_{H \in \mathcal{H}} \frac{1}{n(H)} = 1.$$

As this is a purely combinatorial result, we state it as such.

Proposition 4.5. *Let n be even, and suppose $\lambda = (\lambda_1, \lambda_2)$ is a partition of n into two parts of even length. Suppose further that $\mu = (\mu_1^{m_1}, \mu_2^{m_2}, \ldots, \mu_r^{m_r})$ and $\nu = (\nu_1^{\ell_1}, \nu_2^{\ell_2}, \ldots, \nu_s^{\ell_s})$ are partitions into even length parts of λ_1 and λ_2, respectively. For a given n, denote by $\mathcal{T}_n$ the set of all possible triples (λ, μ, ν). For $t \in \mathcal{T}_n$, we define k_t to be*

$$k_t = \mu_1^{m_1} \mu_2^{m_2} \cdots \mu_r^{m_r} \nu_1^{\ell_1} \nu_2^{\ell_2} \cdots \nu_s^{\ell_s} m_1! m_2! \cdots m_r! \ell_1! \ell_2! \cdots \ell_s!.$$

Then for all even n we have

$$\sum_{t \in \mathcal{T}_n} \frac{1}{k_t} = 1.$$

As preparation for the proof of Proposition 4.5 we give two lemmas.

Lemma 4.6. *For $n \geq k$,*

$$\sum_{k=0}^{n} \binom{2n-2k}{n-k} \binom{2k}{k} = 2^{2n}.$$

Lemma 4.7. *If n is even, then the number of elements of $\mathrm{Sym}(n)$ which consist of only even length cycles is*

$$(n-1)^2 (n-3)^2 \cdots 5^2 3^2.$$

Proof. Assume that $\mathrm{Sym}(n)$ acts canonically on the set $\{1, 2, \ldots, n\}$, and let $\sigma \in \mathrm{Sym}(n)$ be an element consisting of only even length cycles. There are $n-1$ possibilities for 1σ, since $1\sigma = 1$ would yield a 1-cycle in σ. Without

loss of generality say $1\sigma = 2$. There are now $n-1$ possibilities for 2σ, since $2\sigma = 2$ is impossible. If $2\sigma \neq 1$, then without loss say $2\sigma = 3$. There are now $n-3$ possibilities for 3σ, since we require $3\sigma \notin \{1,2,3\}$. Without loss assume $3\sigma = 4$. Now there are $n-3$ possibilities for 4σ, since we require $4\sigma \notin \{2,3,4\}$. Continuing, we see that there are

$$(n-1)^2(n-3)^3 \cdots 5^2 3^2$$

choices for elements having only even length cycles, as in the statement of the lemma. □

Proof of Proposition 4.5. First write

$$k_t = \lambda_1!\lambda_2! \left(\frac{\mu_1^{m_1} \cdots \mu_r^{m_r} m_1! \cdots m_r!}{\lambda_1!} \right) \left(\frac{\nu_1^{\ell_1} \cdots \nu_s^{\ell_s} \ell_1! \cdots \ell_s!}{\lambda_2!} \right),$$

and notice that

$$\frac{\lambda_1!}{\mu_1^{m_1} \cdots \mu_r^{m_r} m_1! \cdots m_r!},$$

for example, is the index in $\mathrm{Sym}(\lambda_1)$ of the centralizer of an element with cycle type $\mu = (\mu^{m_1}, \ldots, \mu_r^{m_r})$. Denote by C_μ the number of elements in $\mathrm{Sym}(\lambda_1)$ with cycle type μ, and by C_ν the number of elements in $\mathrm{Sym}(\lambda_2)$ with cycle type ν. Then

$$k_t = \frac{\lambda_1!\lambda_2!}{C_\mu C_\nu}.$$

Consequently, we have

$$\begin{aligned} \sum_{t \in \mathcal{T}_n} \frac{1}{k_t} &= \sum_\lambda \left(\left(\sum_\mu \frac{C_\mu}{\lambda_1!} \right) \left(\sum_\nu \frac{C_\nu}{\lambda_2!} \right) \right) \\ &= \sum_\lambda \frac{1}{\lambda_1!\lambda_2!} \left(\sum_\mu C_\mu \right) \left(\sum_\nu C_\nu \right). \end{aligned}$$

Next, observe that $\sum_\mu C_\mu$ is equal to the number of elements of $\mathrm{Sym}(\lambda_1)$ which consist of only even length cycles (similarly for the sum over all ν). We may therefore apply Lemma 4.7 to get

$$\sum_{t \in \mathcal{T}_n} \frac{1}{k_t} = \sum_\lambda \frac{1}{\lambda_1!\lambda_2!} \left((\lambda_1 - 1)^2 (\lambda_1 - 3)^2 \cdots 5^2 3^2 \right) \left((\lambda_2 - 1)^2 (\lambda_2 - 3)^2 \cdots 5^2 3^2 \right).$$

Since both λ_1 and λ_2 are even we may write $\lambda_1 = 2d_1$ and $\lambda_2 = 2d_2$ for some integers d_1 and d_2. Now, using the fact that

$$\prod_{i=1}^{r} (2i-1) = \frac{(2r)!}{2^r r!}$$

for any integer $r \geq 1$, we have

$$\begin{aligned}\sum_{t\in\mathcal{T}_n}\frac{1}{k_t} &= \sum_{\lambda}\frac{1}{(2d_1)!(2d_2)!}\left(\frac{(2d_1)!(2d_1)!}{2^{d_1}d_1!2^{d_1}d_1!}\right)\left(\frac{(2d_2)!(2d_2)!}{2^{d_2}d_2!2^{d_2}d_2!}\right)\\ &= \sum_{\lambda}\frac{(2d_1)!(2d_2)!}{2^{d_1+d_2}2^{d_1+d_2}d_1!d_1!d_2!d_2!}.\end{aligned}$$

Since $2(d_1+d_2)=n$ and $\frac{(2d_1)!}{d_1!d_1!}=\binom{2d_1}{d_1}$ (similarly for d_2), the above becomes

$$\sum_{t\in\mathcal{T}_n}\frac{1}{k_t}=\frac{1}{2^n}\sum_{\lambda}\binom{2d_1}{d_1}\binom{2d_2}{d_2}.$$

Writing $n=2n'$, then $2d_2=2n'-2d_1$, so we have

$$\begin{aligned}\sum_{\lambda}\binom{2d_1}{d_1}\binom{2n'-2d_1}{n'-d_1} &= \sum_{d_1=0}^{n'}\binom{2d_1}{d_1}\binom{2n'-2d_1}{n'-d_1}\\ &= 2^{2n'}\\ &= 2^n,\end{aligned}$$

where the second equality follows from Lemma 4.6. Thus

$$\sum_{t\in\mathcal{T}_n}\frac{1}{k_t}=1,$$

as claimed. □

The proof of Theorem 1.1 for the case where $\mathrm{rank}(t)=n/2$ is now complete.

4.2 The case where $\mathrm{rank}(t) < n/2$

Now assume that $\mathrm{rank}(t)=k<n/2$. We may consider t to lie naturally in a subgroup $K\times L\leq G$ which is isomorphic to $GL_{2k}(q)\times GL_{n-2k}(q)$. Within K, we may consider t to be an involution with maximal rank. Therefore in K we choose a set of subgroups $\mathcal{H}$ in the same way as in Section 4.1 from which to choose our $C_G(t)$-orbit representatives. By Lemma 4.2 we again have that $\mathcal{O}_t(H)\sim q^k$ for all $H\in\mathcal{H}$. For $h\in\mathcal{O}_t(H)$ we have

$$\begin{aligned}[C_G(t):C_G(t)\cap C_G(h)] &= \frac{q^{k^2+2k(n-2k)}|GL_k(q)||GL_{n-2k}(q)|}{q^k|GL_{n-2k}(q)|}\\ &= \frac{q^{k^2+2k(n-2k)}|GL_k(q)|}{q^k},\end{aligned}$$

and

$$[N_G(H)\cap C_G(t):C_G(h)\cap C_G(t)]=n(H)$$

(considering H as a subgroup of K when we write $n(H)$). Therefore, arguing as previously we have that

$$|\mathcal{O}_t| \geq q^{k^2+2k(n-2k)}|GL_k(q)| \sum_{H \in \mathcal{H}} \frac{1}{n(H)},$$

and since $q^{k^2+2k(n-2k)}|GL_k(q)| \sim q^{2k(n-k)}$ and $|X| \sim q^{2k(n-k)}$, the result follows by Proposition 4.5.

References

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

[2] J. Ballantyne: *Local fusion graphs of finite groups*, PhD. Thesis, University of Manchester, 2011.

[3] J. Ballantyne: *On local fusion graphs of finite Coxeter groups*, J. Group Theory 16 (2013), no. 4, 595-617.

[4] J. Ballantyne, N. Greer, P. Rowley: *Local fusion graphs for symmetric groups*, J. Group Theory 16 (2013), no. 1, 35-49.

[5] J. Ballantyne, P. Rowley: *A note on computing involution centralizers*, J. Symbolic Comput. 54 (2013), 1–8.

[6] J. Ballantyne, P. Rowley: *Local fusion graphs and sporadic simple groups*, Electron. J. Combin. 22 (2015), no. 3, Paper 3.18, 13 pp.

[7] A. Borovik, S. Yalcnkaya: *Adjoint representations of black box groups* $\mathrm{PSL}_2(\mathbb{F}_q)$, arXiv:1502.06374.

[8] J. N. Bray: *An improved method for generating the centralizer of an involution*, Arch. Math. 74 (2000), 241–245.

[9] A. Devillers, M. Giudici: *Involution graphs where the product of two adjacent vertices has order three*, J. Aust. Math. Soc. 85 (2008), no. 3, 305-322.

[10] D. Gorenstein: *Finite groups*, Second edition. Chelsea Publishing Co., New York, 1980. xvii+519 pp.

[11] R. Guralnick, F. Lübeck: *On p-singular elements in Chevalley groups in characteristic p*, (English summary) Groups and computation, III (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

[12] B. Huppert: *Endliche Gruppen. I*, (German) Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967 xii+793 pp.

[13] W. M. Kantor, M. Kassabov: *Black box groups isomorphic to* $PGL(2, 2^e)$, J. Algebra 421 (2015), 16–26.

[14] P. Kleidman, M. Liebeck: *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990. x+303 pp.

[15] M. W. Liebeck: *On products of involutions in finite groups of Lie type in even characteristic*, J. Algebra 421 (2015), 431–437.

[16] C. Parker, R. Wilson: *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra 324 (2010), no. 5, 885–915.