Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra ••• (••••) •••–•••
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Finding involutions in finite Lie type groups of odd characteristic ☆

Frank Lübeck [a], Alice C. Niemeyer [b], Cheryl E. Praeger [b,*]

[a] *Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany*
[b] *School of Mathematics and Statistics, The University of Western Australia, 35 Stirling Hwy, Nedlands, WA 6009, Australia*

Received 21 December 2007

Communicated by Andrew Mathas

Abstract

Let G be a finite group of Lie type in odd characteristic defined over a field with q elements. We prove that there is an absolute (and explicit) constant c such that, if G is a classical matrix group of dimension $n \geqslant 2$, then at least $c/\log(n)$ of its elements are such that some power is an involution with fixed point subspace of dimension in the interval $[n/3, 2n/3)$. If G is exceptional, or G is classical of small dimension, then, for each conjugacy class $\mathcal{C}$ of involutions, we find a very good lower bound for the proportion of elements of G for which some power lies in $\mathcal{C}$.

Keywords: Finite groups of Lie type; Proportions of involutions

1. Introduction

In this paper we derive a lower bound for the proportion of elements, in a finite group of Lie type in odd characteristic, for which some power is a special kind of involution. For a finite group H and $I \subset H$ a subset of involutions in H, let

$$\mathrm{P}(H, I) = \left\{ h \in H \;\middle|\; |h| \text{is even}, h^{|h|/2} \in I \right\} \tag{1}$$

☆ Supported by ARC Discovery Project DP0879134.
* Corresponding author.
E-mail address: praeger@maths.uwa.edu.au (C.E. Praeger).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2008.05.009

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Table 1
Table for Theorem 1.1 and Corollary 1.2

S	X	n
$\mathrm{SL}_{\ell+1}(q)$	$\mathrm{GL}_{\ell+1}(q)$	$\ell+1$
$\mathrm{SU}_{\ell+1}(q)$	$\mathrm{GU}_{\ell+1}(q)$	$\ell+1$
$\mathrm{Sp}_{2\ell}(q)$	$\mathrm{GSp}_{2\ell}(q)$	2ℓ
$\mathrm{SO}_{2\ell+1}(q)$	$\mathrm{GO}_{2\ell+1}(q)$	$2\ell+1$
$\mathrm{SO}^{\pm}_{2\ell}(q)$	$\mathrm{GO}^{\pm}_{2\ell}(q)^0$	2ℓ

that is, the set of elements of H which "power up" to an involution in I. We determine lower bounds for the proportion $|\mathrm{P}(H, I)|/|H|$ of such elements for certain groups H which are closely related to the finite simple groups of Lie type in odd characteristic, and certain sets I of involutions.

Our interest in these elements in classical groups was motivated by an algorithmic application originating in work of Leedham-Green and O'Brien [LGO07] which is discussed briefly at the end of this section. They consider the subset I of involutions, in certain finite n-dimensional classical groups H in odd characteristic, that have a fixed point subspace of dimension r, where $\frac{n}{3} \leqslant r < \frac{2n}{3}$. They prove in [LGO07, Theorem 8.1] that there is an explicit constant c such that

$$\frac{|\mathrm{P}(H, I)|}{|H|} > \frac{c}{n}.$$

We consider a wider class of groups and show that there is a lower bound of the form $c/\log n$. We denote by $\mathrm{GSp}_{2\ell}(q)$, $\mathrm{GU}_n(q)$ and $\mathrm{GO}_n(q)$ the general symplectic, unitary, and orthogonal groups, respectively, that is, the groups preserving the relevant forms up to a scalar multiple; $\mathrm{GO}^{\pm}_{2\ell}(q)^0$ denotes the connected general orthogonal group—the index 2 subgroup of $\mathrm{GO}^{\pm}_{2\ell}(q)$ that does not interchange the two $\mathrm{SO}^{\pm}_{2\ell}(q)$-classes of maximal isotropic subspaces.

Theorem 1.1. *Let q be a power of an odd prime and ℓ an integer with $\ell \geqslant 2$. Let S, X, n be as in one of the lines of Table* 1*, so that n is the dimension of the natural representation of X. Let H satisfy $S \leqslant H \leqslant X$ and let $I \subset H$ be the set of involutions which have a fixed point subspace of dimension r with $n/3 \leqslant r < 2n/3$. Then*

$$\frac{|\mathrm{P}(H, I)|}{|H|} \geqslant \frac{1}{5000 \log_2 \ell}.$$

Better bounds for medium rank groups may be obtained, for example, in the case of groups in lines 1–2 of Table 1, by evaluating the expression in (5). We obtain similar bounds for projective groups: note that, for X as in one of the lines of Table 1 and a subgroup Z_0 of the centre $Z(X)$, since the subset I of involutions in Theorem 1.1 contains no central elements, the set $\overline{I} := IZ_0/Z_0$ is a subset of involutions in HZ_0/Z_0.

Corollary 1.2. *Let q, ℓ, H, I be as in Theorem* 1.1 *with S, X, n as in one of the lines of Table* 1*. Let $Z_0 \leqslant Z(X)$, set $\overline{I} := IZ_0/Z_0$ and, for $L \leqslant X$ set $\overline{L} := LZ_0/Z_0$. Then $\overline{S} \leqslant \overline{H} \leqslant \overline{X}$, and $|\mathrm{P}(\overline{H}, \overline{I})|/|\overline{H}| \geqslant 1/(5000 \log_2 \ell)$.*

In a third result we consider groups of Lie type of small rank in odd characteristic (including all exceptional simple types) and I a subset of involutions with any fixed type of centralizer.

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Table 2
Table for Theorem 1.3

Type of X	G_2	${}^2G_2$	${}^3D_4$	F_4	E_6	${}^2E_6$	E_7	E_8
c	.375	.578	.578	.333	.328	.328	.168	.353
Type of X	A_ℓ	${}^2A_\ell$	B_ℓ	C_ℓ	D_ℓ	${}^2D_\ell$		
Values for ℓ	1, 2, 3, 4	2, 3, 4	3, 4	2, 3, 4	4	4		
c	.171	.187	.134	.134	.105	.132		

Theorem 1.3. *Let $X = X_\ell(q)$ be a finite group of Lie type of rank ℓ defined over a field of odd order q, such that X and a positive real number c are as in one of the cases of Table 2. Let I be a conjugacy class of involutions in X. Then $|\mathrm{P}(X, I)|/|X| \geqslant c$.*

In Section 6 we describe precisely the groups X and involution classes we consider, and we explain how we compute a quite precise lower bound for $|\mathrm{P}(X, I)|/|X|$. A table with more details is given in Section 7.

Upper bounds and other groups

Our method to prove Theorem 1.1 does not give upper bounds. We did some numerical experiments for small fixed $q \in \{3, 5, 9, 13\}$ and groups from the theorem up to dimension 1000. We computed many pseudo-random elements and checked if they powered up to an involution with a fixed point space of dimension in the right range. The proportion of these elements is not a monotonic function in the dimension, but the trend was that the proportion was about 25% for small dimensions and went down to about 15% in dimension 1000 (independently of the type of the group and q). Further, statistical tests on the data from the groups H we sampled strongly indicate that $P(H, I)/|H| = O(1/\log(\ell))$. This seems to suggest at least that we cannot expect that there is a lower bound independent of the rank of the group.

From our concrete computations for small rank we also guess that Theorem 1.1 is actually true for any finite group of Lie type G^F corresponding to a simple algebraic group G. But in some cases like the spin groups, or groups of type A_ℓ which are not simply-connected or adjoint we do not have a sufficiently good description of the maximal tori and the involutions they contain, along with the type of the involution centralizers. Detailed information on the tori and involutions is used for the groups mentioned above in our proof.

Algorithmic application

In [LGO07], Leedham-Green and O'Brien introduce a Las Vegas algorithm to find standard generators for a finite simple n-dimensional classical group H in odd characteristic in its natural action. Their algorithm relies on finding an element in the set I of 'strong' involutions, namely involutions having fixed point subspace of dimension r with $r \in [n/3, 2n/3)$, or equivalently (-1)-eigenspace of dimension in the interval $(n/3, 2n/3]$. To do this, they search for elements in $\mathrm{P}(H, I)$ by selection of independent, uniformly distributed random elements.

The complexity of the algorithm of Leedham-Green and O'Brien (see [LGO07, Theorem 1.1]) is currently $O(n\xi + n^4 \log n + n^4 \log q + n\chi)$, where ξ is an upper bound on the number of elementary field operations (that is, additions, multiplications or inversions) required to produce an independent, uniformly distributed random element of H, and χ is an upper bound on the number of elementary field operations required for one application of a discrete log oracle over

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

$\mathbb{F}_q$ or $\mathbb{F}_{q^2}$. In particular this complexity involves a cost of $O(n\xi + n^4 \log n + n^4 \log q)$ to compute a strong involution, see [LGO07, Theorem 8.27]. Using our lower bound reduces the complexity of computing a strong involution by replacing the first factor n by $\log n$. However, the overall complexity of the complete algorithm in [LGO07] remains unchanged because of one other costly procedure involved in it.

Outline of the paper

In Section 2 we explain our strategy for counting elements that power up to involutions in I. This involves detailed information about maximal tori in the groups S, and this information is given in Section 3. Section 4 contains some preliminary results. We prove Theorem 1.1 in Section 5, and in the last subsection (9) we deduce Corollary 1.2 from Theorem 1.1. In Sections 6 and 7 we discuss the small rank counting strategy and results.

2. Setup and strategy

2.1. Setup for the groups

For the proof of Theorem 1.1 we consider finite groups of Lie type as follows.

Let G be a connected reductive algebraic group over an algebraic closure $\bar{\mathbb{F}}_q$ of a finite field $\mathbb{F}_q$ with q elements and such that G is defined over $\mathbb{F}_q$, and let $F : G \to G$ be the corresponding Frobenius morphism. The subgroup $G^F = \{g \in G \mid F(g) = g\}$ of elements of G fixed under F is a finite group of Lie type. We denote by ℓ the semisimple rank of G, that is, the rank of the root system of G.

By [Car93, p. 11], each element $g \in G^F$ has a unique Jordan decomposition $g = su = us$, where $s, u \in G^F$, s is semisimple and u is unipotent. The element s is called the *semisimple part* of g and u is called the *unipotent part* of g. Unipotent elements are p-elements, where p is the characteristic of $\mathbb{F}_q$ and semisimple elements have order prime to p. A subgroup U of G is called *F-stable* if $F(U) = U$. Further, for $g, t \in G$ and U a subgroup of G we denote ${}^gU = gUg^{-1}$ and ${}^gt = gtg^{-1}$.

For more details on groups of Lie type and their basic properties we refer to the overview chapter [Car93, Chapter 1] or the book [Spr98].

For a positive integer n and a prime p we can write $n = p^a m$, such that p does not divide m, for unique integers a and m. Then we denote $(n)_p := p^a$ and $(n)_{p'} := m$, called the *p-part* and *p'-part* of n respectively.

2.2. Strategy of counting

We now assume that q is odd. Let $I \subseteq G^F$ be some union of G^F-conjugacy classes of involutions. To count the elements in the set $\mathrm{P}(G^F, I)$ we adapt methods employed in [IKS95, Section 6] for counting p-singular elements in finite groups of Lie type. (We note that similar methods were used by Lehrer in [Leh92] for exploiting the character theory of Weyl groups to evaluate functions on F-stable maximal tori in Lie type groups. The approach has been developed in a general setting in [NP08].) In addition we apply a result of Erdős and Turán as refined in [BLGN$^+$02, Theorem 2.3].

We begin by noting that an element of G^F lies in $\mathrm{P}(G^F, I)$ if and only if its semisimple part lies in $\mathrm{P}(G^F, I)$, since by our assumption unipotent elements have odd order.

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Lemma 2.1. *Let $s \in G^F$ be semisimple. Then the number of unipotent elements $u \in G^F$ such that $su = us$ is equal to the number of F-stable maximal tori of G containing s.*

Proof. Unipotent elements commuting with s and maximal tori containing s are contained in the connected component of the centralizer of s in G, which is a reductive subgroup of G, see the proof of [Car93, Theorem 3.5.3]. The statement now follows from two theorems of Steinberg which show that both numbers equal $(|C^F|^2)_p$ where p is the defining characteristic of G and C the centralizer of s in G, see [Car93, 3.4.1, 6.6.1]. □

Using similar notation to [IKS95, p. 154], for a fixed semisimple element $s \in G^F$, we define

$$X(s) := \{g \in G^F \mid g = su,\ u \in G^F \text{ unipotent and } su = us\},$$

the set of elements of G^F with semisimple part s, and

$$Y(s) := \{(s, T) \mid T \subset G \text{ an } F\text{-stable maximal torus}, s \in T\}.$$

Lemma 2.1 shows that, for any fixed semisimple $s \in G^F$, there exists some bijection $\varphi_s : X(s) \to Y(s)$.

This shows that there is a bijection

$$\varphi : \mathrm{P}(G^F, I) = \dot{\bigcup_s} X(s) \longrightarrow \dot{\bigcup_s} Y(s), \tag{2}$$

where s runs over the semisimple elements in $\mathrm{P}(G^F, I)$, given by $g = su \mapsto \varphi_s(g)$.

The set $\mathrm{P}(G^F, I)$ is invariant under G^F-conjugacy and so the number of pairs (s, T), for a fixed F-stable maximal torus T, depends only on the G^F-conjugacy class of T, and is equal to $|T \cap \mathrm{P}(G^F, I)|$. Thus

$$|\mathrm{P}(G^F, I)| = \sum_{\mathcal{T}} |\mathcal{T}| . |T_{\mathcal{T}} \cap \mathrm{P}(G^F, I)|, \tag{3}$$

where the sum is over G^F-conjugacy classes $\mathcal{T}$ of F-stable maximal tori in G and $T_{\mathcal{T}}$ denotes a representative from $\mathcal{T}$.

Fix an F-stable maximal torus T and consider the Weyl group $W = N_G(T)/T$. Since T is abelian the image of $t \in T$ under conjugation by $h \in N_G(T)$ depends only on the coset $w = hT \in W$, and we denote this image by ${}^w t$. Elements $w, w' \in W$ are said to be *F-conjugate* if $w' = x^{-1} w F(x)$, for some $x \in W$; note that F-conjugacy is an equivalence relation on W.

Lemma 2.2. *Let G^F, T, W be as above. Then the G^F-conjugacy classes of F-stable maximal tori of G are in bijection with the F-conjugacy classes of the Weyl group W of G as follows. If, for $g \in G$, the torus ${}^g T$ is F-stable, then $w(g) := g^{-1} F(g) T \in W$. Another F-stable maximal torus ${}^h T$, for $h \in G$, is G^F-conjugate to ${}^g T$ if and only if $w(g)$ and $w(h)$ are F-conjugate. Writing $w := w(g)$, the torus $({}^g T)^F$ is mapped under conjugation by g to $T^{Fw^{-1}} := \{t \in T \mid {}^w F(t) = t\}$.*

Proof. See [Car93, 3.3.3]. □

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

If $C \subset W$ is an F-conjugacy class and T_C a corresponding F-stable maximal torus, then [Car93, 3.3.6] shows that the G^F-conjugacy class of T_C contains $|G^F||C|/(|T_C^F||W|)$ elements. Denote by m_C the proportion of elements of T_C^F lying in $\mathrm{P}(G^F, I)$, that is,

$$m_C = \frac{|T_C^F \cap \mathrm{P}(G^F, I)|}{|T_C^F|}. \tag{4}$$

This yields a useful expression for the proportion of elements in $\mathrm{P}(G^F, I)$ in terms of the F-conjugacy classes in W.

Lemma 2.3. *With G, I as above we have*

$$\frac{|\mathrm{P}(G^F, I)|}{|G^F|} = \sum_C m_C \cdot \frac{|C|}{|W|},$$

where the sum on the right hand side is over the F-conjugacy classes $C \subset W$, and m_C is as in (4)*.*

Proof. Let $\mathcal{T}$ be a G^F-conjugacy class of F-stable maximal tori of G corresponding to an F-conjugacy class $C \subset W$, and let $T_C \in \mathcal{T}$. By (3), the contribution to $\frac{|\mathrm{P}(G^F,I)|}{|G^F|}$ from $\mathcal{T}$ is $|\mathcal{T}|\frac{|T_C \cap \mathrm{P}(G^F,I)|}{|G^F|}$. As discussed above, $|\mathcal{T}| = \frac{|G^F||C|}{|T_C^F||W|}$, and the second factor is $m_C \frac{|T_C^F|}{|G^F|}$. Thus the contribution is

$$m_C \frac{|C|}{|W|} \frac{|G^F||T_C^F|}{|T_C^F||G^F|} = m_C \frac{|C|}{|W|}. \qquad \square$$

We obtain lower bounds for this proportion by showing that $m_C \geqslant 1/2$ for certain F-conjugacy classes C, and by estimating the proportion of elements of W in such classes C.

Remark 2.4. We may improve the first assertion of Theorem 5.2 of [IKS95] for finite classical groups using Lemma 2.3 and our discussion in Section 5 on the structure of maximal tori in these groups. Let I be the set of *all* involutions in a finite classical group G in odd characteristic. Then, as we show in Section 5, each maximal torus in G has even order, and hence at least half of its elements are in $\mathrm{P}(G, I)$. Thus $m_C \geqslant 1/2$ for each class C in Lemma 2.3, and so that lemma yields $|\mathrm{P}(G, I)|/|G| \geqslant 1/2$ (whereas [IKS95, Theorem 5.2] states $|\mathrm{P}(G, I)|/|G| \geqslant 1/4$ for these groups).

3. Maximal tori and involutions in classical groups

The aim of this section is to describe the background information we require about the structure of the maximal tori in the groups G^F we consider, and to give a description of the involutions and their centralizers.

For each Dynkin diagram of classical type we choose a group G and for the different types of Frobenius actions on the Dynkin diagram we describe:

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

(i) an F-stable maximal torus T in G and the corresponding Weyl group $W = N_G(T)/T$;
(ii) the roots as maps $T \to \bar{\mathbb{F}}_q^\times$;
(iii) the action of the Weyl group W on T;
(iv) the action of a Frobenius morphism F on T and W.

We also indicate how G is related to various simple algebraic groups with the same Dynkin diagram.

For more details on the following descriptions see [DM91, Chapter 15]. Recall that $\bar{\mathbb{F}}_q$ is an algebraic closure of the finite field $\mathbb{F}_q$. We use the information and notation from Carter [Car93, pp. 39–40] for the simply connected and adjoint types of the finite classical groups.

3.1. Type A_ℓ

Let $n = \ell + 1$. We consider $G = \mathrm{GL}_n(\bar{\mathbb{F}}_q)$. Its diagonal matrices form a maximal torus T. We write $\mathrm{diag}(a_1, \ldots, a_n)$ for a diagonal matrix with diagonal entries $a_1, \ldots, a_n$. The upper triangular matrices in G form a Borel subgroup and this determines a set of simple roots $\alpha_1, \ldots, \alpha_\ell$. We number them such that $\alpha_i(\mathrm{diag}(a_1, \ldots, a_n)) = a_i a_{i+1}^{-1}$. The Weyl group W can be described by its action on T. Its elements permute the diagonal entries (actually, an element of W is determined by its action on a single element of T that has pairwise distinct entries). The generating reflection along α_i acts on elements $t = \mathrm{diag}(a_1, \ldots, a_n)$ of T by interchanging the coordinates a_i and a_{i+1}, so W is isomorphic to S_n, the symmetric group on n points. In the untwisted case $G^F = \mathrm{GL}_n(q)$ we choose a Frobenius map F such that $F(\mathrm{diag}(a_1, \ldots, a_n)) = \mathrm{diag}(a_1^q, \ldots, a_n^q)$. In the twisted (unitary) case $G^F = \mathrm{GU}_n(q)$ we choose a Frobenius map such that $F(\mathrm{diag}(a_1, \ldots, a_n)) = \mathrm{diag}(a_1^{-q}, \ldots, a_n^{-q})$. In both cases F acts trivially on W, so the F-conjugacy classes are the conjugacy classes and they are parameterized by partitions of n describing the cycle types of the permutations on n points (and on the n diagonal entries of elements in T).

The simply-connected algebraic group of type A_ℓ is $G' = \mathrm{SL}_n(\bar{\mathbb{F}}_q)$, and $T \cap G'$ is a maximal torus of G'. We have $G'^F \cong \mathrm{SL}_n(q)$ in the untwisted case, and $G'^F \cong \mathrm{SU}_n(q)$ in the twisted case.

If Z is the centre of G then $G/Z \cong \mathrm{PGL}_n(\bar{F}_q)$ is the adjoint simple group of type A_ℓ and T/Z is a maximal torus. We have $(G/Z)^F \cong G^F/Z^F$ which is isomorphic to $\mathrm{PGL}_n(q)$ in the untwisted case, and $\mathrm{PGU}_n(q)$ in the twisted case.

There are further simple groups G_d of type A_ℓ corresponding to each non-trivial divisor d of n. These are homomorphic images of G' but there is no easy description of the groups G_d^F in terms of the finite groups mentioned so far. We do not consider these groups in the sequel.

3.2. Type C_ℓ

Here we consider the symplectic groups $G = \mathrm{Sp}_{2\ell}(\bar{\mathbb{F}}_q)$. We choose an ordered basis $(e_1, \ldots, e_\ell, f_\ell, \ldots f_1)$ of a 2ℓ-dimensional $\bar{\mathbb{F}}_q$-vector space, and a symplectic form $\langle , \rangle$ with $\langle e_i, e_j \rangle = \langle f_i, f_j \rangle = 0$ and $\langle e_i, f_j \rangle = \delta_{i,j}$ for $1 \leqslant i, j \leqslant \ell$, where $\delta_{i,j} = 0$ if $i \neq j$ and 1 if $i = j$. Then G is the subgroup of $\mathrm{GL}_{2\ell}(\bar{\mathbb{F}}_q)$ consisting of all matrices that leave this form invariant.

The diagonal matrices in G have the form $t := \mathrm{diag}(a_1, \ldots, a_\ell, a_\ell^{-1}, \ldots, a_1^{-1})$ and they form a maximal torus T. In this setup the upper triangular matrices of G are a Borel subgroup and we number the corresponding simple roots $\alpha_1, \ldots, \alpha_\ell$ such that $\alpha_i(t) = a_i a_{i+1}^{-1}$ for $1 \leqslant i < \ell$ and $\alpha_\ell(t) = a_\ell^2$ (so these are the restrictions of the first ℓ simple roots of $\mathrm{GL}_{2\ell}(\bar{\mathbb{F}}_q)$ to T).

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

The Weyl group $W = N_G(T)/T$ acts naturally on $\{\langle e_i\rangle, \langle f_i\rangle \mid 1 \leqslant i \leqslant \ell\}$ preserving the partition with blocks $\{\langle e_i\rangle, \langle f_i\rangle\}$, for $1 \leqslant i \leqslant \ell$. We identify this set with $\{1, \ldots, \ell, \bar{\ell}, \ldots, \bar{1}\}$, via $\langle e_i\rangle \mapsto i$ and $\langle f_i\rangle \mapsto \bar{i}$, using the convention that $\bar{\bar{i}} = i$. The group $W = S_2 \wr S_\ell$ consists of all the so-called *signed permutations*, that is, permutations w in $S_{2\ell}$ such that $\overline{i^w} = (\bar{i})^w$ for all i.

As in Section 3.1, W can be described by its action on T. The elements of W permute the diagonal entries. The generating reflection along α_i, for $1 \leqslant i < \ell$, interchanges the entries a_i and a_{i+1} and also interchanges the entries a_i^{-1} and a_{i+1}^{-1}. The reflection along α_ℓ interchanges the middle entries a_ℓ and a_ℓ^{-1}. Each element $w \in W$ leaves the set of pairs of entries $\{a_i, a_i^{-1}\}$ invariant, and mapping w to its action on these pairs describes a surjective homomorphism $\pi : W \to S_\ell$ (the symmetric group on these ℓ pairs of entries). The kernel of π is the subgroup of elements which leave all pairs $\{a_i, a_i^{-1}\}$ invariant.

We choose a Frobenius morphism F such that $F(\mathrm{diag}(a_1, \ldots, a_\ell, a_\ell^{-1}, \ldots, a_1^{-1})) = \mathrm{diag}(a_1^q, \ldots, a_\ell^q, a_\ell^{-q}, \ldots, a_1^{-q})$. Then F acts trivially on W and the F-conjugacy classes of W are the conjugacy classes.

To $w \in W$ we associate a pair of partitions (λ, μ) of total sum ℓ as follows. The entries of the partitions are the cycle lengths of $\pi(w) \in S_\ell$. A cycle of $\pi(w)$ of length m is called *positive* if it is the image of two w-cycles of length m, and *negative* if it is the image of one w-cycle of length $2m$. The partitions λ, μ are the multisets of lengths of positive cycles, and negative cycles, respectively. Two elements of W are conjugate if and only if the associated pair of partitions (λ, μ) is the same.

The group $G = \mathrm{Sp}_{2\ell}(\bar{\mathbb{F}}_q)$ is the simply-connected simple group of type C_ℓ. There is a surjective homomorphism (of algebraic groups) $G \to \bar{G}$ to the adjoint simple group $\bar{G}$ of type C_ℓ. It has the centre of G as kernel, and for odd q, the image of G^F has index two in $\bar{G}^F$.

3.3. Type B_ℓ

Here we consider the special orthogonal groups $G = \mathrm{SO}_{2\ell+1}(\bar{\mathbb{F}}_q)$ in a similar manner to the symplectic groups in case C_ℓ. We choose an ordered basis $(e_1, \ldots, e_\ell, e_0, f_\ell, \ldots, f_1)$ of a $(2\ell+1)$-dimensional vector space over $\bar{\mathbb{F}}_q$ and an orthogonal form $\langle,\rangle$ with $\langle e_i, f_j\rangle = \delta_{i,j}$, $\langle e_0, e_0\rangle = 1$ and $\langle e_i, e_j\rangle = \langle f_i, f_j\rangle = 0$, for $0 \leqslant i \leqslant \ell$ and $1 \leqslant j \leqslant \ell$, where $\delta_{i,j} = 0$ if $i \neq j$ and 1 if $i = j$. Then G is the subgroup of $\mathrm{SL}_{2\ell+1}(\bar{\mathbb{F}}_q)$ consisting of all matrices that leave this form invariant. The set of diagonal matrices in G is a maximal torus T and consists of all matrices of the form $\mathrm{diag}(a_1, \ldots, a_\ell, 1, a_\ell^{-1}, \ldots, a_1^{-1})$. The description of the Frobenius morphism F, the Weyl group W, its action on the simple roots, and the action of the generating reflections of W on this torus are almost the same as in the case of the symplectic groups in type C_ℓ, except that we now have $\alpha_\ell(\mathrm{diag}(a_1, \ldots, a_\ell, 1, a_\ell^{-1}, \ldots, a_1^{-1})) = a_\ell$. In particular, we still have $W = S_2 \wr S_\ell$.

Here G is the adjoint simple group of type B_ℓ. There is a surjective homomorphism from the simply-connected groups $\mathrm{Spin}_{2\ell+1}(\bar{\mathbb{F}}_q)$ onto G with kernel of order 2 for odd q. The image of the finite group $\mathrm{Spin}_{2\ell+1}(q)$ in $SO_{2\ell+1}(q)$ has index 2.

3.4. Type D_ℓ

Here we consider $G = \mathrm{SO}_{2\ell}(\bar{\mathbb{F}}_q)$ as a subgroup of $\mathrm{SO}_{2\ell+1}(\bar{\mathbb{F}}_q)$ by 'forgetting' the middle basis vector. This is the group generated by the root subgroups for roots in the subsystem of type D_ℓ of long roots in the root system of type B_ℓ. We use the same maximal torus as in type B_ℓ and the roots and Weyl group action corresponding to the long roots $\alpha_1, \ldots, \alpha_{\ell-1}$ in type B_ℓ. The

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Weyl group W has index 2 in the Weyl group $W(B_\ell)$ of type B_ℓ and an element of the latter is in W if and only if it has an even number of negative cycles. Let $w_\ell \in W(B_\ell)$ be the generating reflection along the short simple root. Then $w_\ell \notin W$ and $W(B_\ell) = W \dot\cup W w_\ell$.

In the untwisted case we take the same Frobenius morphism F as in the case of B_ℓ so F-conjugacy classes coincide with conjugacy classes in W. (A few conjugacy classes of $W(B_\ell)$ contained in W split into two W-classes, but we do not need the details here.) The corresponding finite group is $G^F = \mathrm{SO}^+_{2\ell}(q)$.

For the twisted case we twist that Frobenius morphism with the reflection w_ℓ. Then the F-conjugacy classes of W are all the sets of the form Cw_ℓ, where C is a conjugacy class of $W(B_\ell)$ not contained in W. The surjection $\pi : W(B_\ell) \to S_\ell$ is still surjective when restricted to W or to the coset Ww_ℓ (because w_ℓ is in the kernel). The corresponding finite group is $G^F = \mathrm{SO}^-_{2\ell}(q)$.

The relationship between G and the simply-connected group of type D_ℓ is the same as in type B_ℓ. However here G is not adjoint, and there is a surjection onto the adjoint group of type D_ℓ which has as kernel the centre of G of order 2. For even ℓ there is another type of simple group of type D_ℓ, namely the half spin groups, which are also homomorphic images of the simply-connected groups with kernel of order 2.

3.5. Involutions in classical groups

We can now describe the classes of involutions in the classical groups considered above, and in their central quotients. Since we consider algebraic groups over fields of odd characteristic, the involutions in our groups are semisimple elements. Therefore, involutions are conjugate in the algebraic group G to elements in the torus T of diagonal elements considered above in the various cases of Sections 3.1–3.4. An element in T has order two if it is not trivial and the diagonal entries are all ± 1.

In each case we see that we can sort the $+1$ and -1 entries by conjugation under the action of the Weyl group. This shows that such a class of involutions is parameterized by the dimension of its -1 eigenspace in the given (natural) representation.

The centralizer of such an involution is the intersection of G and the centralizer in the general linear group in which G is embedded. The root system of the connected component of the centralizer is easy to see: it consists of the roots which have the element in their kernel, see [Car93, 3.5.3].

More precisely, we find the following types of centralizers in the algebraic group. In type A_ℓ the centralizers are of type $A_{k-1} + A_{\ell-k}$ if the -1 eigenspace is k-dimensional. In type C_ℓ the centralizers have type $C_k + C_{\ell-k}$, in type B_ℓ we get $B_{\ell-k} + D_k$, and in type D_ℓ it is $D_k + D_{\ell-k}$ for $k \neq 1$ and $D_{\ell-1}$.

If we also consider involutions in the central quotients of the group G considered above, we have to look at elements of T whose square is a scalar matrix. For such elements a few additional types of centralizer occur, namely centralizers of type $A_{\ell-1}$ in groups of type C_ℓ and D_ℓ, and centralizers of type D_ℓ and $B_{\ell-1}$ in groups of type B_ℓ.

Note, that not all types of centralizers mentioned above occur for all ℓ and k (for example, the number of -1 entries in elements of T is always even). And some of the classes mentioned above may not be F-stable for certain Frobenius actions and congruence conditions on q. Much more detailed information about involutions and their centralizers can be found in [GLS99, Chapter 4], but we do not need this here.

We see from this description of centralizers that we could also define the set of involutions I in Theorem 1.1 as those involutions whose centralizers have a composition factor of the same

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

type as G and of rank between $1/3$ and $2/3$ times the rank of G. This description does not refer to a particular representation of G.

4. Preliminary results

In this section we collect some facts for later reference. Recall that, for $i \geqslant 1$, the ith cyclotomic polynomial $\phi_i(X)$ over the rational numbers is recursively defined by the property $X^i - 1 = \prod_{d|i} \phi_d(X)$.

Lemma 4.1. *Let q be odd.*

(a) *Then $\phi_1(q) = q - 1$ and $\phi_2(q) = q + 1$ are divisible by 2 and exactly one of them has 2-part 2, and for $i > 2$,*

$$\big(\phi_i(q)\big)_2 = \begin{cases} 2 & \text{if } i \text{ is a power of } 2, \\ 1 & \text{otherwise.} \end{cases}$$

(b) *In particular*

$$\big(q^n + 1\big)_2 = \begin{cases} 2 & \text{if } n \text{ is even}, \\ (q+1)_2 & \text{if } n \text{ is odd} \end{cases}$$

and if $n = 2^a k$ with k odd and $a \geqslant 1$, then $(q^n - 1)_2 = (q^2 - 1)_2 \cdot 2^{a-1}$.

(c) *For positive integers k, n with $(k)_2 < (n)_2$ we have*

$$\big(q^n - 1\big)_2 > \big(q^k \pm 1\big)_2.$$

Proof. (a) Let n, a, b be positive integers with $n = ab$. Then $q^n - 1 = q^{ab} - 1 = (q^a - 1) \times (q^{a(b-1)} + \cdots + q^a + 1)$. If $a = (n)_2$ the second factor has an odd number of summands, and so is odd. This shows that $(q^n - 1)_2 = (q^a - 1)_2$. So the only integers i for which $\phi_i(q)$ is even are the powers $i = 2^k$ with $k \geqslant 0$. Since for $k > 0$ we have $\phi_{2^k}(X) = X^{2^{k-1}} + 1$, we see that, for $k > 1$, $\phi_{2^k}(q) \equiv 2 \pmod 4$.

(b) For the first part consider $q^{2n} - 1 = (q^n - 1)(q^n + 1)$. Only $\phi_{2(n)_2}(q)$ divides $q^n + 1$ and has a non-trivial 2-part. For the second part we have $(q^n - 1)_2 = (q^{2^a} - 1)_2$ from the proof of part (a), and equality of this expression with $(q^2 - 1)_2 \cdot 2^{a-1}$ follows from the first assertion of (b), just proved.

(c) This follows from part (b) if k is even. Also (b) implies $(q^n - 1)_2 > (q^k + 1)_2$ if k is odd. Finally for k odd, by the proof of (a), $(q^k - 1)_2 = (q - 1)_2 < (q^n - 1)_2$. □

The next statement refers to some concepts defined in Section 3. Recall that the Weyl group of type B_ℓ and C_ℓ is $S_2 \wr S_\ell$, and that the Weyl group W of type D_ℓ is an index 2 subgroup of the Weyl group $W(B_\ell)$ of type B_ℓ that projects onto S_ℓ, namely, $W(B_\ell) = W \,\dot\cup\, W w_\ell$ with w_ℓ as defined in Section 3.4, and $W = W(B_\ell) \cap \mathrm{Alt}_{2\ell}$ (where $\mathrm{Alt}_{2\ell}$ is the alternating group of degree 2ℓ).

Lemma 4.2. *Let n, λ, d be positive integers such that $2 \leqslant d \leqslant n/2$, and let S_n be the symmetric group on n points.*

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

(a) *The proportion* $p_{\neg d}(n)$ *of elements of* S_n *with no cycle of length divisible by* d *satisfies*

$$\frac{1}{4n^{1/d}} < p_{\neg d}(n) < \frac{3}{n^{1/d}}.$$

(b) *If* d *divides* λ*, then the proportion of elements in* S_n *having a cycle of length* λ*, and on the remaining* $n-\lambda$ *points no cycles of length divisible by* d*, is* $p_{\neg d}(n-\lambda)/\lambda$.

(c) *Let* W *be the Weyl group of type* B_n*,* C_n *or* D_n*. If* d *divides* λ*, then the proportion of elements in* W *for which the projection to* S_n *has the properties of part* (b) *is* $p_{\neg d}(n-\lambda)/\lambda$.

(d) *Let* W *be the Weyl group of type* B_n*,* C_n *or* D_n*. Let* C *be a conjugacy class in* S_n *whose elements contain a cycle* τ *of length less than* n*. Let* $\tilde{C}$ *be the preimage of* C *under the surjection* $W \to S_n$*, or in case* D_n *under the surjection* $Ww_n \to S_n$*. In either case the proportion of elements in* $\tilde{C}$ *which have* τ *as a positive cycle is* $1/2$*. Moreover if* W *is of type* B_n *then the proportion of elements in* $\tilde{C}$ *which lie in the reflection subgroup of type* D_n *is* $1/2$.

Proof. (a) From [BLGN$^+$02, Theorem 2.3(b)] we get the more precise lower and upper bounds (the quotient of which converges to 1 for growing n):

$$c(d)\left(\frac{d}{n}\right)^{1/d}\left(1-\frac{1}{n}\right) \leqslant p_{\neg d}(n) \leqslant c(d)\left(\frac{d}{n}\right)^{1/d}\left(1+\frac{2}{n}\right),$$

where $c(d) = \frac{1}{\Gamma(1-1/d)}$.

For $2 \leqslant d \leqslant n/2$ we have $1/2 \leqslant 1-1/d \leqslant 1$ and since the Γ-function $\Gamma(x)$ is decreasing for $0 < x \leqslant 1$ we have $1 \leqslant \Gamma(1-1/d) \leqslant \Gamma(\frac{1}{2}) = \sqrt{\pi} < 2$, hence $\frac{1}{2} < c(d) \leqslant 1$. The real function $x \mapsto x^{1/x}$ has its maximum at $x = e$ and this yields that $1 \leqslant d^{1/d} < 3/2$ for all $d \geqslant 2$. Furthermore, for $n \geqslant 2$ we have $1/2 \leqslant 1-1/n \leqslant 1$ and $1 \leqslant 1+2/n \leqslant 2$.

(b) A λ-subset can be chosen in $\binom{n}{\lambda}$ ways and a λ-cycle on these points in $(\lambda-1)!$ ways; a permutation on the remaining $n-\lambda$ points with no cycles of length divisible by d can be chosen in $(n-\lambda)!\, p_{\neg d}(n-\lambda)$ ways. Thus the number of elements of S_n with the required properties is $n!\, p_{\neg d}(n-\lambda)/\lambda$.

(c) The Weyl group W in this case is $W = S_2 \wr S_n < S_{2n}$, or a subgroup of index 2 that projects onto S_n in the case of D_n. Thus the first assertion follows immediately from part (b).

(d) We define maps f, f' on each such $\tilde{C}$. Let $w \in \tilde{C}$, let σ be the corresponding element of C, and let τ be a cycle of length less than n. In particular, σ has at least two cycles. Let i be the least entry in the cycle τ, and define $f(w) = (i, \bar{i})w$. Then $f(w)$ also projects to σ and all cycles of σ have the same sign for $f(w)$ as for w, except for the cycle τ which has changed sign. In the case of B_n or C_n, this implies that $f(w) \in \tilde{C}$. Moreover f is bijective and f interchanges the elements for which τ is a positive cycle with those for which it is a negative cycle, proving the first assertion of (d) for types B_n and C_n.

Now suppose that W is of type D_n so that $W' = W \dot{\cup} Ww_n$ and $W = W' \cap \mathrm{Alt}_{2n}$, where W' is the Weyl group of type B_n. Let C_1, C_2 be the preimages of C in W, Ww_n, respectively. Then f maps even permutations to odd permutations, and vice versa, and hence f interchanges C_1 and C_2, which implies the last assertion of (d). Choose k to lie in a cycle of σ different from τ, and for $w \in C_1 \cup C_2$ define $f'(w) = (k, \bar{k})f(w)$. Then $f'(w)$ also projects to σ and f' maps even permutations to even permutations. Hence f' fixes C_1 and C_2 setwise. Moreover, f' still interchanges the elements of $C_1 \cup C_2$ for which τ is a positive cycle with those for which it is a

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

negative cycle. Thus f interchanges the set of elements of C_i (where $i = 1, 2$) for which τ is a positive cycle with those for which it is a negative cycle. This proves the first assertion of (d) for type D_n. □

Lemma 4.3. *Let H be a finite group, I a union of conjugacy classes of involutions in H and $Z \leqslant Z(H)$ a subgroup of the centre of H with $I \cap Z = \emptyset$. Then*

$$\frac{|\mathrm{P}(H/Z, IZ/Z)|}{|H/Z|} \geqslant \frac{|\mathrm{P}(H, I)|}{|H|}.$$

Proof. Note that every element of IZ/Z is an involution because $I \cap Z = \emptyset$. The canonical homomorphism $H \to H/Z$ maps elements $h \in \mathrm{P}(H, I)$ (that is $h^k \in I$ for some k) to cosets $hI \in \mathrm{P}(H/Z, IZ/Z)$. Moreover, the image of $\mathrm{P}(H, I)$ contains at least $|\mathrm{P}(H, I)|/|Z|$ elements. So, $|\mathrm{P}(H, I)|/|Z| \leqslant |\mathrm{P}(H/Z, IZ/Z)|$ and the statement follows on dividing by $|H/Z|$. □

Lemma 4.4. *Let S be one of the groups $\mathrm{Sp}_{2\ell}(q)$, $\mathrm{SO}_{2\ell+1}(q)$ or $\mathrm{SO}^{\pm}_{2\ell}(q)$, and let X be the corresponding group of matrices which map the defining bilinear form to a scalar multiple of itself, namely $\mathrm{GSp}_{2\ell}(q)$, $\mathrm{GO}_{2\ell+1}(q)$ or $\mathrm{GO}^{\pm}_{2\ell}(q)^0$, respectively. Let Z be the centre of X and let $S \leqslant H \leqslant G$. Then the index of $S(H \cap Z)$ in H divides* 4.

We prove in fact that $|H : S(H \cap Z)| \leqslant 2$ except in the case where $S = \mathrm{SO}^{\pm}_{2\ell}(q)$ or $\mathrm{SO}_{2\ell+1}(q)$ with q odd, H contains $\mathrm{O}^{\pm}_{2\ell}(q)$ or $\mathrm{O}^{\pm}_{2\ell}(q)$ respectively, and some element of H multiplies the form by a non-square scalar. In this latter case, the index is 4.

Proof. Define the epimorphism $\pi : X \to \mathbb{F}_q^{\#}$ by $g \mapsto c$ if g maps the form defining S to c times this form. Let K denote the kernel of π. Then K contains S, and $K = S$ if either q is even or $S = \mathrm{Sp}_{2\ell}(q)$. In all other cases $|K : S| = 2$ (see for example, [KL90, p. 24, 2.5.11, 2.6.1]). The centre Z consists of the scalar matrices $\{a \cdot \mathrm{id} \mid a \in \mathbb{F}_q^{\#}\}$, and we have $\pi(a \cdot \mathrm{id}) = a^2$.

Let $S \leqslant H \leqslant X$. If $\pi(H)$ consists of squares in $\mathbb{F}_q^{\#}$ then $H \cap Z$ contains representatives of all cosets in $H/(H \cap K)$, and hence $H = (H \cap K)(H \cap Z)$ containing $S(H \cap Z)$ as a subgroup of index at most 2. Suppose then that $\pi(H)$ contains a non-square, so that q is odd and $(H \cap K)(H \cap Z)$ has index 2 in H. If $S = H \cap K$ then again $|H : S(H \cap Z)| \leqslant 2$, while if $S \neq H \cap K$ then S is a special orthogonal group, H contains the full orthogonal group, and $|H : S(H \cap Z)| = 4$. □

5. Proof of Theorem 1.1

(i) *Maximal tori in* $\mathrm{GL}_n(q)$ *and* $\mathrm{GU}_n(q)$

As introduced in Section 3.1, let $G = \mathrm{GL}_n(\bar{\mathbb{F}}_q)$, F the Frobenius morphism of G, T the maximal torus of G, and W the Weyl group of G. The Frobenius map F raises diagonal entries in elements of T to the εqth power, where $\varepsilon = 1$ in the untwisted case $G^F = \mathrm{GL}_n(q)$ and $\varepsilon = -1$ in the twisted case $G^F = \mathrm{GU}_n(q)$. Let $w \in W$.

By Lemma 2.2, the maximal tori of G^F corresponding to the (F-)conjugacy class of w are isomorphic to $T^{Fw^{-1}} = \{t \in T \mid {}^wF(t) = t\}$. We determine the structure of this group as follows. Let $t = \mathrm{diag}(a_1, \ldots, a_n) \in T^{Fw^{-1}}$. For each cycle $(i_1, \ldots, i_\lambda)$ of w, w permutes cyclically the diagonal entries $b_1 := a_{i_1}, b_2 := a_{i_2}, \ldots, b_\lambda := a_{i_\lambda}$ of t. The condition ${}^wF(t) = t$ yields for these

diagonal entries the equations $b_2 = b_1^{\varepsilon q}, \ldots, b_\lambda = b_{\lambda-1}^{\varepsilon q}$ and $b_1 = b_\lambda^{\varepsilon q}$. Therefore, $b_1^{(\varepsilon q)^\lambda - 1} = 1$ and $b_i = b_{i-1}^{\varepsilon q}$ for $1 < i \leqslant \lambda$. Since distinct cycles of w act on disjoint sets of entries we get the following structure of $T^{Fw^{-1}}$: if $(\lambda_1, \ldots, \lambda_r)$ is the partition of n describing the cycle lengths of w, then $T^{Fw^{-1}}$ is a direct product of cyclic groups of orders $q^{\lambda_i} - \varepsilon^{\lambda_i}$, for $1 \leqslant i \leqslant r$.

Note that, in the description of the w-action on $t \in T^{Fw^{-1}}$, if the cycle length λ is even then the corresponding cyclic direct factor of $T^{Fw^{-1}}$ has order $q^\lambda - 1$, and the involution in this direct factor has entry -1 precisely in positions $i_1, \ldots, i_\lambda$.

(ii) *Maximal tori with $m_C \geqslant 1/2$ in $\mathrm{GL}_n(q)$ and $\mathrm{GU}_n(q)$*

Let a be a positive integer (which we specify in step (iv) below) and let $M(a) \subset W$ be the following union of conjugacy classes of W. An element $w \in W$ is in $M(a)$ if and only if it contains a cycle of length $2^a k$, for some integer k such that $n/3 < 2^a k \leqslant 2n/3$, and no other cycle has length divisible by 2^a.

A maximal torus of G^F corresponding to $w \in M(a)$ has the form $C \times A$, where C is cyclic of order $q^{2^a k} - 1$, and A is non-trivial and is a direct product of cyclic groups of orders $q^r \pm 1$ for certain integers r with $(r)_2 < (2^a k)_2$. By Lemma 4.1(c) and (a), $(q^r \pm 1)_2 < (q^{2^a k} - 1)_2$.

Now consider the subsets $\{x\} \times A \subset C \times A$ such that $|x|$ has maximal 2-part. There are $|C|/2$ such elements x. Since all elements in A have 2-part of smaller order, all such elements power up to the involution $(z, 1) \in C \times A$, where z is the unique involution of C. As we have seen above such an involution has -1 as an eigenvalue with multiplicity $2^a k$, so its centralizer in G is of type $\mathrm{GL}_{2^a k}(\bar{\mathbb{F}}_q) \times \mathrm{GL}_{n-2^a k}(\bar{\mathbb{F}}_q)$. Hence $(z, 1)$ is an involution in our set I.

In other words, using the notation m_C introduced after Lemma 2.2, if C is a conjugacy class of W contained in $M(a)$ then $m_C \geqslant 1/2$.

(iii) *Estimating $|\mathrm{P}(G^F, I)|/|G^F|$ for $\mathrm{GL}_n(q)$ and $\mathrm{GU}_n(q)$*

We now obtain a lower bound for this proportion using Lemma 2.3 and considering only the contributions from conjugacy classes of W contained in the subset $M(a)$ defined in (ii). For any positive integer a this yields:

$$\frac{|\mathrm{P}(G^F, I)|}{|G^F|} \geqslant \frac{1}{2} \cdot \frac{|M(a)|}{|W|}. \tag{5}$$

By Lemma 4.2(b),

$$\frac{|M(a)|}{|W|} = \sum_k \frac{p_{\neg 2^a}(n - 2^a k)}{2^a k}, \tag{6}$$

where the sum is over all k such that $n/3 < 2^a k \leqslant 2n/3$.

By Lemma 4.2(a) and using $2^a k \leqslant 2n/3$ we see that

$$\frac{p_{\neg 2^a}(n - 2^a k)}{2^a k} \geqslant \frac{3}{2n} p_{\neg 2^a}\left(n - 2^a k\right) > \frac{3}{2n} \cdot \frac{1}{4} \cdot \frac{1}{(n - 2^a k)^{1/2^a}} > \frac{3}{8n} \cdot \frac{1}{n^{1/2^a}}.$$

The number of summands in (6) is at least $(2n/3 - n/3)/2^a - 1 = n/(3 \cdot 2^a) - 1$. If $(13/4) \cdot 2^a \leqslant n$, then this number is at least $n/(39 \cdot 2^a)$.

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Using these lower bounds for the summands in (5) we get

$$\frac{|\mathrm{P}(G^F, I)|}{|G^F|} > \frac{1}{2}\cdot\frac{3}{8}\cdot\frac{1}{n}\cdot\frac{1}{n^{1/2^a}}\cdot\frac{n}{39\cdot 2^a} = \frac{1}{208}\cdot\frac{1}{2^a\cdot n^{1/2^a}}, \tag{7}$$

where a is any positive integer such that $(13/4)\cdot 2^a \leqslant n$.

(iv) *Proof of Theorem 1.1 for* $\mathrm{GL}_n(q)$ *and* $\mathrm{GU}_n(q)$

If for growing n we evaluate the right hand side of (7) for $a \sim \log_2\log_2 n$ we see that $|\mathrm{P}(G^F, I)|/|G^F| > c/\log_2(n)$ for some constant c.

To get the explicit constant stated in Theorem 1.1 we must look a bit more closely. Set $f(a) = 2^a n^{1/2^a}$. Considering $\log_2 f(a) = a + (\log_2 n)/2^a$ as a function on real numbers $a \geqslant 1$, and computing its derivative, we find that this function has a minimum at $a_0 = \log_2\ln 2 + \log_2\log_2 n$.

Now let c be the real number with $-1/2 \leqslant c < 1/2$ such that $a_0 + c$ is an integer. We evaluate $\log_2 f(a_0 + c) = \log_2\ln 2 + \log_2\log_2 n + c + (\log_2 n)/(\ln 2\cdot\log_2 n\cdot 2^c)$. Thus

$$f(a_0 + c) = \ln 2\cdot 2^c\cdot\log_2 n\cdot 2^{1/(2^c\ln 2)} = \ln 2\cdot 2^c\cdot e^{(1/2^c)}\cdot\log_2 n < 3\log_2 n \tag{8}$$

(the factor $2^c\cdot e^{(1/2^c)}$ is maximal for $c = -1/2$ which yields the last inequality).

Computing $a = a_0 + c$ for some small values of n one can check that, for $n \geqslant 7$, we have $a \geqslant 1$ and $(13/4)\cdot 2^a \leqslant n$. For large n these properties clearly hold. So, for $n \geqslant 7$, we have found an a such that the last factor on the right hand side of (7) is greater than $1/(3\log_2 n)$ and so

$$\frac{|\mathrm{P}(G^F, I)|}{|G^F|} > \frac{1}{208}\cdot\frac{1}{3\log_2 n} = \frac{1}{624\log_2 n}. \tag{9}$$

Note that G is of type A_ℓ with $n = \ell + 1$, and that for $n > 2$ we have $1/(\log_2 n) > 1/(2\log_2 \ell)$.

For $n < 7$ we can easily check the statement of Theorem 1.1 by considering one appropriate class of maximal tori directly. For example, if $n = 6$ consider the G^F-conjugacy class of maximal tori parameterized by the conjugacy class C of elements in W with cycle type $(4, 1, 1)$. A corresponding maximal torus is a direct product of a cyclic group of order $q^4 - 1$ and two cyclic groups of orders $q \pm 1$. Thus the 2-part of the order of the large cyclic factor is at least 4 times the 2-part of $q \pm 1$, that is $m_C \geqslant 3/4$. Furthermore $|C|/|W| = 1/8$. The theorem for this case follows by applying Lemma 2.3 to this single summand which is large enough.

(v) *Proof for* $\mathrm{SL}_n(q) \leqslant H \leqslant \mathrm{GL}_n(q)$ *and* $\mathrm{SU}_n(q) \leqslant H \leqslant \mathrm{GU}_n(q)$

We first consider, as in step (i) above, the cyclic subgroups of the groups $T^{Fw^{-1}}$ corresponding to a cycle of w of length λ. The corresponding diagonal entries of the element $t \in T^{Fw^{-1}}$ are of the form $b_1, b_1^{\varepsilon q}, \ldots, b_1^{(\varepsilon q)^{\lambda-1}}$, where $b_1^{q^\lambda - \varepsilon^\lambda} = 1$. The product of these diagonal entries is b_1^k where $k = 1 + \varepsilon q + \cdots + (\varepsilon q)^{\lambda-1} = \varepsilon^{\lambda-1}\cdot(q^\lambda - \varepsilon^\lambda)/(q - \varepsilon)$. In particular, if $b_1 \in \bar{\mathbb{F}}_q^\#$ has order $q^\lambda - \varepsilon^\lambda$ then this product has order $q - \varepsilon$ and hence is a generator of $\det(G^F)$.

In step (ii) we counted subsets of $T^{Fw^{-1}}$ of the form $\{(x, y) \in C \times A \mid y \in A\}$ for certain $x \in C$. Each such subset is invariant under multiplication by elements from A. Since A is not trivial we have just seen that A contains elements with any possible determinant. Therefore, the

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

sets we counted have the same number of elements in each coset of $\mathrm{SL}_n(q)$ within $\mathrm{GL}_n(q)$ in the untwisted case, and each coset of $\mathrm{SU}_n(q)$ within $\mathrm{GU}_n(q)$ in the twisted case.

Now consider the elements of G^F which are mapped under φ, as defined in Eq. (2), to the pairs (T, s) with s in one of the subsets $\{x\} \times A$ as above. These elements are also equally distributed into the cosets with constant determinant because unipotent elements have determinant 1.

This shows that the lower bound from step (iv) also holds for all groups H satisfying $\mathrm{SL}_n(q) \leqslant H \leqslant \mathrm{GL}_n(q)$ or $\mathrm{SU}_n(q) \leqslant H \leqslant \mathrm{GU}_n(q)$.

(vi) *F-stable maximal tori in* $\mathrm{Sp}_{2\ell}(q)$, $\mathrm{SO}_{2\ell+1}(q)$, *and* $\mathrm{SO}^{\pm}_{2\ell}(q)$

First let $G = \mathrm{Sp}_{2\ell}(\bar{\mathbb{F}}_q)$. The description of maximal tori in G^F is very similar to that given in step (i), this time using the description of the Weyl group W and its action on the torus of diagonal matrices given in Section 3.2.

Consider the action of an element $w \in W$ on some element $t \in T^{Fw^{-1}}$, say $t = \mathrm{diag}(a_1, \ldots, a_\ell, a_\ell^{-1}, \ldots, a_1^{-1})$. If the element $\pi(w) \in S_\ell$ has a positive cycle $\tau = (i_1, i_2, \ldots, i_\lambda)$ of length λ, then w permutes λ independent diagonal entries of t cyclically, say $b_1, b_2, \ldots, b_\lambda$, and in the same way permutes cyclically their inverses $b_1^{-1}, b_2^{-1}, \ldots, b_\lambda^{-1}$. (Here each $b_j = a_{i_j}^{\pm 1}$.) The equation ${}^wF(t) = t$ restricted to these diagonal entries describes a cyclic subgroup of order $q^\lambda - 1$, just as in the case of $\mathrm{GL}_n(q)$. If τ is a negative cycle of $\pi(w)$ then w permutes the 2λ entries $b_1, b_2, \ldots, b_\lambda, b_1^{-1}, \ldots, b_\lambda^{-1}$ cyclically. In this case we have $b_1^{-1} = b_\lambda^q = \cdots = b_1^{q^\lambda}$, so the corresponding cyclic subgroup of $T^{Fw^{-1}}$ has order $q^\lambda + 1$.

Again, the involution in the cyclic subgroup of $T^{Fw^{-1}}$ corresponding to the cycle τ has entry -1 precisely in positions i_j and $2\ell + 1 - i_j$, for $1 \leqslant j \leqslant \lambda$.

The same description holds for the groups $\mathrm{SO}_{2\ell+1}(q)$ described in Section 3.3 of type B_ℓ, and the groups $\mathrm{SO}^{\pm}_{2\ell}(q)$ described in Section 3.4 of type D_ℓ or ${}^2D_\ell$.

(vii) *Proof of Theorem 1.1 for* $\mathrm{Sp}_{2\ell}(q)$, $\mathrm{SO}_{2\ell+1}(q)$, *and* $\mathrm{SO}^{\pm}_{2\ell}(q)$

We can carry over steps (ii)–(iv), now with ℓ instead of n, almost exactly. The variation is that, in this case, we define $M(a)$ as the subset of elements of W with a *positive* cycle of length $2^a k$, such that k is odd and $\ell/3 < 2^a k \leqslant 2\ell/3$, and no other (positive or negative) cycle has length divisible by 2^a.

In the description of $|M(a)|/|W|$ in Eq. (6) we now use Lemma 4.2(c) and (d) which give an additional factor $1/2$ (because we only consider positive cycles of length $2^a k$). The rest of the argument remains the same, so that we get, for $\ell \geqslant 7$,

$$\frac{|\mathrm{P}(G^F, I)|}{|G^F|} > \frac{1}{1248 \log_2 \ell}. \tag{10}$$

That this inequality also holds for values of ℓ up to 6 can be checked by considering appropriate single classes of tori as discussed at the end of step (iv).

(viii) *Proof for groups H satisfying* $\mathrm{Sp}_{2\ell}(q) \leqslant H \leqslant \mathrm{GSp}_{2\ell}(q)$, *or* $\mathrm{SO}_{2\ell+1}(q) \leqslant H \leqslant \mathrm{GO}_{2\ell+1}(q)$, *or* $\mathrm{SO}^{\pm}{}_{2\ell}(q) \leqslant H \leqslant \mathrm{GO}_{2\ell}{}^{\pm}(q)^0$

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

Set $S := G^F = \mathrm{Sp}_{2\ell}(q)$, $\mathrm{SO}_{2\ell+1}(q)$, or $\mathrm{SO}^{\pm}_{2\ell}(q)$, and let X be the corresponding group as in Lemma 4.4 and $Z := Z(X)$, so that $S \leqslant H \leqslant X$. As in Lemma 4.4 we can write H, or a subgroup of H of index at most 4, as $S(H \cap Z) = \{gz \mid g \in S^F \text{ and } z \in H \cap Z\}$. Note that in the proof of Theorem 1.1 for the groups S we only counted elements $g \in S$ with $(|g|)_2 \geqslant (q^2-1)_2$. For such an element g, and for all $z \in H \cap Z$, the product gz powers up to the same involution as g does because z has 2-part at most $(q-1)_2$. In particular, $P(S(H \cap Z), I)/|S(H \cap Z)| = P(S, I)/|S|$ and, therefore,

$$\begin{aligned}\frac{P(H,I)}{|H|} &\geqslant \frac{P(S(H\cap Z),I)}{|S(H\cap Z)|}\frac{1}{|H : S(H\cap Z)|}\\ &= \frac{P(S,I)}{|S|}\frac{1}{|H : S(H\cap Z)}\\ &\geqslant \frac{P(S,I)}{4|S|}.\end{aligned}$$

This completes the proof of Theorem 1.1.

(ix) *Proof of Corollary 1.2*

The information given by Lemma 4.3 is sufficient to enable us to deduce Corollary 1.2 from Theorem 1.1. Let H, I be as in Theorem 1.1 with X, S as in one of the lines of Table 1. Let $Z_0 \leqslant Z(X)$, so that $\overline{S} \leqslant \overline{H} \leqslant \overline{X}$ where $\overline{L} = LZ_0/Z_0$ for $L \leqslant X$. Now $\overline{H} \cong H/(H \cap Z_0)$, $H \cap Z_0 \leqslant Z(H)$ and $(H \cap Z_0) \cap I = \emptyset$. The assertion of Corollary 1.2 now follows from Lemma 4.3 and Theorem 1.1.

6. Method of computation for small rank cases

For the small rank cases in Theorem 1.1 we did computer calculations using the tools provided by the CHEVIE [GHL+96] system.

To describe them we use the notation and descriptions from [Car93, 1.9, 1.11, 1.19, 3.1]. In CHEVIE a series of groups of Lie type G^F is specified by a root datum $(X, \Phi, Y, \Phi^\vee)$ (as defined on [Car93, p. 19]) with respect to some F-stable maximal torus $T \leqslant G$ and a matrix F_0 which describes the induced action of the Frobenius map on the lattice Y. For elements w in the Weyl group W we also write w for its action induced on Y. Maximal tori of G are isomorphic to $Y \otimes_{\mathbb{Z}} \mathbb{Q}_{p'}/\mathbb{Z}$, where $\mathbb{Q}_{p'}$ is the subgroup of the additive group of rational numbers consisting of those rationals with denominators not divisible by the characteristic p of $\mathbb{F}_q$.

In this setup the equation ${}^w F(t) = t$, for $t \in T$, translates to a matrix equation $(qF_0w^{-1} - \mathrm{id}_Y)t = 0$ where the torus elements t are written as tuples with $\mathrm{rank}(Y)$ entries in $\mathbb{Q}_{p'}/\mathbb{Z}$ with respect to the chosen basis of Y. We compute transformation matrices L and R such that $L(qF_0w^{-1} - \mathrm{id}_Y)R$ has diagonal form. Then it is easy to describe the solutions, and hence also the structure of $T^{Fw^{-1}}$, as a product of cyclic groups. By multiplication with R we also get the solutions in the original basis.

Finding the involutions: All involutions have conjugates contained in T, and the G-conjugacy classes of involutions are parameterized by the W-orbits on the involutions in T, see [Car93, 3.7.1]. In our setup we can write down all the involutions in T as all the non-zero tuples with entries $0, 1/2 \in \mathbb{Q}_{p'}/\mathbb{Z}$. CHEVIE can compute the W-orbits on this set and, for a representative

in each orbit, the stabilizer in W and the system of roots having a representative in the kernel. This determines the G-classes of involutions together with the Lie types of their centralizers, see [Car93, 3.5.3].

It turns out that we can compute the diagonalisation above generically, that is, without specializing q, if we distinguish a finite number of congruence classes for q (modulo $\ell+1$ in type A_ℓ, modulo 3 in type E_6 and modulo 2 or 4 in types B_ℓ, C_ℓ, E_7 and D_ℓ, and nothing to distinguish in the remaining cases). The direct factors which describe the maximal tori $T^{Fw^{-1}}$ always have orders a rational number times a product of cyclotomic polynomials evaluated at q. For our estimates we further distinguish the cases when q is congruent to 1 or 3 modulo 4 or, equivalently, when $q-1$ or $q+1$, respectively, is divisible by 4 or some higher power of 2. We only consider involutions which are non-trivial in the direct components with the maximal number of factors $q-1$ or $q+1$, respectively, in their orders (since depending on q the orders of the other direct factors can have an arbitrarily smaller 2-part).

Consider a direct product of cyclic groups $C_1 \times \cdots \times C_r$. The proportion of its elements which power up to the involution which is of order 2 in components $C_1, \ldots, C_s$ and trivial on $C_{s+1}, \ldots, C_r$ can be computed by counting, for each possible 2-part 2^k, the elements in $C_1, \ldots, C_s$ for which the order has 2-part equal to 2^k, and the elements in $C_{s+1}, \ldots, C_r$ for which the order has 2-part less than 2^k. This can be done using the following lemma.

Lemma 6.1. *If C is a cyclic group of even order $2^k \cdot m$ with m odd, and if $0 \leqslant a < k$, then the proportion of elements in C for which the order has 2-part equal to 2^{k-a}, and the proportion of elements for which the order has 2-part less than 2^{k-a}, are both $1/2^{a+1}$.*

Proof. Let $C = \langle c \rangle$. Then each odd power of c has order with 2-part equal to 2^k, and each even power of c has order with smaller 2-part. This proves the result for $a = 0$. We now use induction on k. The case $k = 1$ is covered by the case $a = 0$. For $k > 1$ and $a > 0$, we use the inductive hypothesis for the group $\langle c^2 \rangle$. □

For particular values of q we can always consider all cyclic factors for all classes of tori and so compute the exact values of $|\mathrm{P}(G^F, I)|$, using Lemma 2.3.

7. Tables for small rank cases

The following table contains the detailed results for some small rank cases computed as described in Section 6. We cover classical types up to rank 4. (We have done the computations for all simple G of rank at most 8, but we do not print all the results.) And we cover all exceptional simple types.

The first column describes the type of the group G^F. We give the type of the root system, prepended by the order of the Frobenius action on the Dynkin diagram if not trivial. A further index indicates the isomorphism type of the algebraic group G within its isogeny class. It is *sc* or *ad* for the simply connected or adjoint group, respectively. In type D_ℓ there is also *SO* for the special orthogonal groups and for even ℓ there is *HS* for the half spin groups. In type A_ℓ there is one isomorphism type for each divisor d of $\ell+1$. If d is not 1 (corresponding to the simply connected groups) or $\ell+1$ (corresponding to the adjoint groups), we indicate the group by d as an index.

The second column lists the classes of involutions in G by specifying the types of their centralizers. A component T_1 specifies a one-dimensional torus in the centre of the connected

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

component of the centralizer. If the centralizer is not connected we specify the order of the component group after a 'dot.' In some cases there are several classes with the same type of centralizer, but we do not want to give the precise root datum and the representatives used in the computations. For the classical types we did not try to identify the classes in terms of the natural representation.

The third column specifies a congruence condition on q for which the lower bound of the proportion of elements in G^F powering to an involution in the given class was computed. The lower bound b_I for this proportion is given in the fourth column.

Although we need to distinguish different congruence classes of q, depending on the type of G, during the computations, we often find the same lower bounds in different cases, this simplifies the third column. (Even in cases where we find the same lower bound for $q \equiv 1$ or 3 mod 4, the contribution from specific classes of tori can be different.)

We leave out a few lines corresponding to classes of involutions in G which are not F-stable (and so the proportion in the last column is 0).

$A_1(q)_{ad}$	$T_1.2$	–	0.6250
$A_1(q)_{sc}$	A_1	–	0.6250
$A_2(q)_{ad}$	$A_1 + T_1$	1 mod 4	0.5937
		3 mod 4	0.5625
$A_2(q)_{sc}$	$A_1 + T_1$	1 mod 4	0.5937
		3 mod 4	0.5625
${}^2A_2(q)_{ad}$	$A_1 + T_1$	1 mod 4	0.5625
		3 mod 4	0.5937
${}^2A_2(q)_{sc}$	$A_1 + T_1$	1 mod 4	0.5625
		3 mod 4	0.5937
$C_2(q)_{ad}$	$(A_1 + A_1).2$	–	0.4140
	$(\tilde{A}_1 + T_1).2$	–	0.3281
$C_2(q)_{sc}$	C_2	–	0.4140
	$A_1 + A_1$	–	0.3281
$G_2(q)$	$A_1 + \tilde{A}_1$	–	0.5781
${}^2G_2(\sqrt{3^{2m+1}})$	$A_1 + \tilde{A}_1$	–	0.3750
$A_3(q)_{ad}$	$A_2 + T_1$	1 mod 4	0.3515
		3 mod 4	0.1875
	$(A_1 + A_1 + T_1).2$	1 mod 4	0.4785
		3 mod 4	0.5742
$A_3(q)_{sc}$	$A_1 + A_1 + T_1$	1 mod 4	0.2382
		3 mod 4	0.2890
	A_3	1 mod 4	0.5917
		3 mod 4	0.4726
$A_3(q)_2$	$(A_1 + A_1 + T_1).2$	1 mod 4	0.2128
		3 mod 4	0.2812
	$(A_1 + A_1 + T_1).2$	1 mod 4	0.2441
		3 mod 4	0.2734
	A_3	1 mod 4	0.3574
		3 mod 4	0.1718
${}^2A_3(q)_{ad}$	$A_2 + T_1$	1 mod 4	0.1875
		3 mod 4	0.3515

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

	$(A_1 + A_1 + T_1).2$	1 mod 4	0.5742
		3 mod 4	0.4785
${}^2A_3(q)_{sc}$	$A_1 + A_1 + T_1$	1 mod 4	0.2890
		3 mod 4	0.2382
	A_3	1 mod 4	0.4726
		3 mod 4	0.5917
${}^2A_3(q)_2$	$(A_1 + A_1 + T_1).2$	1 mod 4	0.2812
		3 mod 4	0.2128
	$(A_1 + A_1 + T_1).2$	1 mod 4	0.2734
		3 mod 4	0.2441
	A_3	1 mod 4	0.1718
		3 mod 4	0.3574
$B_3(q)_{ad}$	$(C_2 + T_1).2$	–	0.2470
	$(\tilde{A}_1 + A_1 + A_1).2$	–	0.2587
	$A_3.2$	–	0.2646
$B_3(q)_{sc}$	$\tilde{A}_1 + A_1 + A_1$	–	0.2636
	B_3	–	0.5322
$C_3(q)_{ad}$	$C_2 + A_1$	–	0.5263
	$(\tilde{A}_2 + T_1).2$	–	0.2695
$C_3(q)_{sc}$	$C_2 + A_1$	–	0.2587
	$C_2 + A_1$	–	0.2470
	C_3	–	0.2646
$A_4(q)_{ad}$	$A_3 + T_1$	1 mod 4	0.3999
		3 mod 4	0.3613
	$A_2 + A_1 + T_1$	1 mod 4	0.3505
		3 mod 4	0.3476
$A_4(q)_{sc}$	$A_2 + A_1 + T_1$	1 mod 4	0.3505
		3 mod 4	0.3476
	$A_3 + T_1$	1 mod 4	0.3999
		3 mod 4	0.3613
${}^2A_4(q)_{ad}$	$A_3 + T_1$	1 mod 4	0.3613
		3 mod 4	0.3999
	$A_2 + A_1 + T_1$	1 mod 4	0.3476
		3 mod 4	0.3505
${}^2A_4(q)_{sc}$	$A_2 + A_1 + T_1$	1 mod 4	0.3476
		3 mod 4	0.3505
	$A_3 + T_1$	1 mod 4	0.3613
		3 mod 4	0.3999
$B_4(q)_{ad}$	$(B_3 + T_1).2$	–	0.2210
	$(C_2 + A_1 + A_1).2$	–	0.2080
	$(A_3 + \tilde{A}_1).2$	–	0.1341
	$D_4.2$	–	0.2510
$B_4(q)_{sc}$	$C_2 + A_1 + A_1$	–	0.1881
	D_4	–	0.2443
	B_4	–	0.4060
$C_4(q)_{ad}$	$C_3 + A_1$	–	0.3338

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

	$(C_2+C_2).2$	–	0.2803
	$(\tilde{A}_3+T_1).2$	–	0.2243
$C_4(q)_{sc}$	C_2+C_2	–	0.2080
	C_4	–	0.2510
	C_3+A_1	–	0.2210
	C_3+A_1	–	0.1341
$D_4(q)_{ad}$	$(A_3+T_1).2$	–	0.2243
	$(A_1+A_1+A_1+A_1).4$	–	0.2007
	$(A_3+T_1).2$	–	0.2243
	$(A_3+T_1).2$	–	0.2243
$D_4(q)_{sc}$	$A_1+A_1+A_1+A_1$	–	0.1408
	D_4	–	0.2443
	D_4	–	0.2443
	D_4	–	0.2443
$D_4(q)_{SO}$	$(A_1+A_1+A_1+A_1).2$	–	0.1807
	$(A_3+T_1).2$	–	0.2185
	$(A_3+T_1).2$	–	0.1052
	D_4	–	0.3693
${}^2D_4(q)_{ad}$	$(A_3+T_1).2$	–	0.4433
	$(A_1+A_1+A_1+A_1).4$	–	0.3598
${}^2D_4(q)_{sc}$	$A_1+A_1+A_1+A_1$	–	0.2353
	D_4	–	0.5678
${}^2D_4(q)_{SO}$	$(A_1+A_1+A_1+A_1).2$	–	0.2353
	$(A_3+T_1).2$	–	0.2236
	$(A_3+T_1).2$	–	0.1630
	D_4	–	0.1328
	$(A_1+A_1+A_1+A_1).4$	–	0.5781
${}^3D_4(q)_{sc}$	$A_1+A_1+A_1+A_1$	–	0.5781
$F_4(q)$	B_4	–	0.4060
	C_3+A_1	–	0.3338
$E_6(q)_{sc}$	A_5+A_1	1 mod 4	0.3288
		3 mod 4	0.3289
	D_5+T_1	1 mod 4	0.4053
		3 mod 4	0.3845
${}^2E_6(q)_{ad}$	D_5+T_1	1 mod 4	0.3845
		3 mod 4	0.4053
	A_5+A_1	1 mod 4	0.3289
		3 mod 4	0.3288
${}^2E_6(q)_{sc}$	A_5+A_1	1 mod 4	0.3289
		3 mod 4	0.3288
	D_5+T_1	1 mod 4	0.3845
		3 mod 4	0.4053
$E_7(q)_{ad}$	$(E_6+T_1).2$	–	0.1842
	D_6+A_1	–	0.4508
	$A_7.2$	–	0.1686
$E_7(q)_{sc}$	D_6+A_1	–	0.2669
	D_6+A_1	–	0.2155

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009

	E_7	–	0.3211
$E_8(q)$	$E_7 + A_1$	–	0.3537
	D_8	–	0.3651

Acknowledgments

We thank Samuel Müller for statistical advice. We also thank an anonymous referee for helpful comments.

References

[BLGN+02] Robert Beals, Charles R. Leedham-Green, Alice C. Niemeyer, Cheryl E. Praeger, Ákos Seress, Permutations with restricted cycle structure and an algorithmic application, Combin. Probab. Comput. 11 (5) (2002) 447–464.

[Car93] Roger W. Carter, Finite Groups of Lie Type, Wiley Classics Lib., John Wiley & Sons Ltd., Chichester, 1993, Conjugacy classes and complex characters, reprint of the 1985 original, A Wiley–Interscience Publication.

[DM91] François Digne, Jean Michel, Representations of Finite Groups of Lie Type, London Math. Soc. Stud. Texts, vol. 21, Cambridge University Press, Cambridge, 1991.

[GHL+96] Meinolf Geck, Gerhard Hiss, Frank Lübeck, Gunter Malle, Götz Pfeiffer, CHEVIE—A system for computing and processing generic character tables, Appl. Algebra Engrg. Comm. Comput. 7 (3) (1996) 175–210, Computational methods in Lie theory, Essen, 1994, http://www.math.rwth-aachen.de/~CHEVIE.

[GLS99] Daniel Gorenstein, Richard Lyons, Ronald Solomon, The Classification of the Finite Simple Groups, Number 4. Part II. Chapters 1–4, Math. Surveys Monogr., vol. 40, American Mathematical Society, Providence, RI, 1999.

[IKS95] I.M. Isaacs, W.M. Kantor, N. Spaltenstein, On the probability that a group element is p-singular, J. Algebra 176 (1) (1995) 139–181.

[KL90] Peter Kleidman, Martin Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 129, Cambridge University Press, Cambridge, 1990.

[Leh92] G.I. Lehrer, Rational tori, semisimple orbits and the topology of hyperplane complements, Comment. Math. Helv. 67 (2) (1992) 226–251.

[LGO07] C.R. Leedham-Green, E.A. O'Brien, Constructive recognition of classical groups in odd characteristic, preprint, 2007.

[NP08] A.C. Niemeyer, C.E. Praeger, Proportions of elements in finite simple groups of Lie type: A method and an application to p-singular elements, preprint, 2008.

[Spr98] T.A. Springer, Linear Algebraic Groups, second ed., Progr. Math., vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998.

Please cite this article in press as: F. Lübeck et al., Finding involutions in finite Lie type groups of odd characteristic, J. Algebra (2008), doi:10.1016/j.jalgebra.2008.05.009