On products of involutions in finite groups of Lie type in even characteristic

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2AZ, UK

Dedicated to the memory of Ákos Seress

Abstract

Let G be a finite simple group of Lie type in characteristic 2, and $t \in G$ an involution. We provide a lower bound for the proportion of elements $g \in G$ such that tt^g has odd order. This has applications to the theory of recognition algorithms for such groups.

1 Introduction

Many algorithms involving finite simple groups depend on the ability to construct involution centralizers. The standard method for doing this was given by Bray [2]: let G be a simple group and $t \in G$ an involution. For a conjugate t^g of t, let n be the order of $tt^g = [t, g]$. If n is odd, then $g[t, g]^{(n-1)/2}$ centralizes t; moroever, if g is uniformly distributed among elements of G for which $[t, g]$ has odd order, then the corresponding element $g[t, g]^{(n-1)/2}$ is uniformly distributed among elements of $C_G(t)$. Since few random elements are required to generate $C_G(t)$, this leads to a construction of this centralizer, provided there is a good proportion of elements g for which $[t, g]$ has odd order. Lower bounds for such proportions were obtained for groups of Lie type in odd characteristic in [9, Theorems 1,2], and for long root elements in characteristic 2 in [7, 3.9]. In this note we obtain lower bounds for all involutions in finite groups of Lie type in characteristic 2.

Our first result deals with the case of classical groups. It is useful for the recognition algorithm developed in [5].

Theorem 1 *Let G be a finite classical simple group with natural module of dimension d over a field of characteristic 2, let $t \in G$ be an involution, and let $r = \mathrm{rank}(t+1)$. Then the proportion of $g \in G$ such that $[t,g]$ has odd order is at least c/r, where c is a positive absolute constant; in particular it is at least $2c/d$.*

The proof shows that $c = \frac{1}{64}$ suffices, and more care would improve this value. However, computational evidence indicates that a stronger result may be true with $2c/d$ replaced by a positive absolute constant independent of d.

For the exceptional groups of Lie type, we prove:

Theorem 2 *There is a positive absolute constant b such that if G is a finite simple exceptional group of Lie type over a field of characteristic 2, and $t \in G$ is an involution, then the proportion of $g \in G$ such that $[t,g]$ has odd order is at least b.*

The proof shows that $b = \frac{1}{100}$ suffices (see the Remark at the end of the paper). Again, this is undoubtedly far from best possible.

Acknowledgement I would like to thank the referee for suggesting the inclusion of Theorem 2 and a number of other helpful remarks.

2 Proof of Theorem 1

The proof of Theorem 1 is based on a simple idea – embedding any given involution of G in a suitable dihedral subgroup. For simplicity we break the proof up into four lemmas, each dealing with one family of classical groups.

Lemma 2.1 *Theorem 1 holds when $G = PSL_d(q)$ (q even).*

Proof. Let $G = PSL_d(q)$ with q even. Since two involutions in G are conjugate in G if and only if they are conjugate in $PGL_d(q)$, it suffices to prove the result with G replaced by $GL_d(q)$, which is a little more convenient notation-wise.

Let $t \in G = GL_d(q)$ be an involution, and take t to have Jordan canonical form $\mathrm{diag}(J_2^r, J_1^{d-2r})$, where J_i denotes an $i \times i$ unipotent Jordan block matrix. Let U (respectively, W) be the subspace spanned by bases for the J_2-blocks (respectively, J_1-blocks), so that $GL(U) \times GL(W) = GL_{2r}(q) \times GL_{d-2r}(q) \leq G$. There is a subgroup $S \cong SL_2(q^r)$ of the first factor (embedded as in [6, §4.3]) such that $t \in S$. Let D be a dihedral subgroup of S of order $2(q^r+1)$ containing t, and let $x \in D$ be an element of order q^r+1. The eigenvalues of x on $U \otimes \bar{\mathbb{F}}_q$ (where $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$) are all distinct, so $C_{GL_{2r}(q)}(x)$ is a maximal torus of $GL_{2r}(q)$ and hence is equal to $GL_1(q^{2r})$. It follows that

$$N_G(\langle x\rangle) = N_{GL_{2r}(q)}(\langle x\rangle) \times GL_{d-2r}(q) = (GL_1(q^{2r}).2r) \times GL_{d-2r}(q).$$

Let D_0 be the set of elements in $\langle x\rangle$ of order not dividing any q^i+1 with $i<r$. Then $|D_0| > \frac{1}{2}q^r$, and for $y \in D_0$ we have $C_G(y) = C_G(x)$. All involutions in D are conjugate to t, and the number of pairs of involutions in D with product equal to an element of D_0 is at least $\frac{1}{2}q^{2r}$. Hence the number of ordered pairs of G-conjugates of t with product equal to a conjugate of an element in D_0 is at least

$$N := \frac{1}{2}q^{2r} \times |G : N_G(\langle x\rangle)| = \frac{1}{4r} \cdot \frac{q^{2r} \cdot |GL_d(q)|}{(q^{2r}-1) \cdot |GL_{d-2r}(q)|}.$$

Now $|C_G(t)| = q^{r^2+2r(d-2r)}|GL_r(q)|\,|GL_{d-2r}(q)|$ (see [8, 7.1]). Hence the proportion of pairs of conjugates of t with product of odd order (dividing q^r+1) is at least

$$\frac{N}{|t^G|^2} = \frac{1}{4r} \cdot \frac{q^{2r} \cdot q^{2r^2+4r(d-2r)} \cdot |GL_r(q)|^2 |GL_{d-2r}(q)|}{(q^{2r}-1) \cdot |GL_d(q)|}.$$

Since $|GL_r(q)| > \frac{1}{4}q^{r^2}$, it follows that

$$\frac{N}{|t^G|^2} > \frac{c}{r} \geq \frac{2c}{d},$$

where $c = \frac{1}{64}$. This completes the proof of the lemma. ■

Lemma 2.2 *Theorem* 1 *holds when* $G = PSU_d(q)$ *(*q *even).*

Proof. The proof is very similar to that of the previous lemma. We can replace G by $GU_d(q)$. An involution $t \in G$ is determined up to conjugacy by its Jordan form $\mathrm{diag}(J_2^r, J_1^{d-2r})$. Again t lies in a subgroup $S \times 1 = SL_2(q^r) \times 1 \leq GU_{2r}(q) \times GU_{d-2r}(q)$ of G (where if r is odd, $S = SU_2(q^r)$ embedded in $GU_{2r}(q)$ as in [6, §4.3], and if r is even, $S = SL_2(q^r) \leq GL_r(q^2) < GU_{2r}(q)$). Now we argue as in the previous proof using a dihedral subgoup $D \cong D_{2(q^r+1)}$ of S containing t, noting that for $x \in D$ of order q^r+1 we have $N_G(\langle x\rangle) = ((q^r+1) \times (q^r-(-1)^r).2r) \times GU_{d-2r}(q)$, and also that $|C_G(t)| = q^{r^2+2r(d-2r)}|GU_r(q)|\,|GU_{d-2r}(q)|$. ■

Lemma 2.3 *Theorem* 1 *holds when* $G = Sp_d(q)$ *(*q *even).*

Proof. Let $G = Sp_d(q)$, and write $d = 2n$ and $V = V_{2n}(q)$, the natural module for G. The conjugacy classes of involutions and their centralizers in G were determined in [1], and a convenient statement can be found in [8, 7.3]. We summarize the results. Each involution $t \in G$ is unipotent, and $V \downarrow t$ is an orthogonal direct sum of non-degenerate subspaces of the following forms: $V(2)$, a 2-space on which u acts as a Jordan block J_2; $W(2)$, a 4-space on which u acts as J_2^2, a sum of two singular J_2-blocks; and $W(1)$, a 2-space on which u acts trivially. The involution classes in G are represented by elements

$$a_r \ (r \text{ even}, r \le n), \ \ b_r \ (r \text{ odd}, r \le n), \ \ c_r \ (r \text{ even}, r \le n),$$

where

$$\begin{aligned} V \downarrow a_r &= W(2)^{r/2} + W(1)^{n-r}, \\ V \downarrow b_r &= V(2)^r + W(1)^{n-r}, \\ V \downarrow c_r &= V(2)^r + W(1)^{n-r}. \end{aligned}$$

The centralizers are as follows:

t	$C_G(t)/O_2(C_G(t))$	$\lvert C_G(t)\rvert \sim$
a_r	$Sp_r(q) \times Sp_{2n-2r}(q)$	$q^{n^2+(n-r)^2+n}$
b_r	$Sp_{r-1}(q) \times Sp_{2n-2r}(q)$	$q^{n^2+(n-r)^2+n-r}$
c_r	$Sp_{r-2}(q) \times Sp_{2n-2r}(q)$	$q^{n^2+(n-r)^2+n-r}$

Here, when we write $|C_G(t)| \sim q^R$ we mean that $|C_G(t)|$ is a polynomial in q with leading term q^R.

Consider $t = b_r$ or c_r. Let S be a subgroup $Sp_2(q^r)$ of $Sp_{2r}(q)$, embedded as in [6, §4.3]. One checks that an involution in S acts on the natural module for $Sp_{2r}(q)$ as $V(2)^r$, so that S contains a conjugate of t. As in previous proofs, let $D \cong D_{2(q^r+1)}$ be a dihedral subgroup of S containing t. For $x \in D$ of order dividing $q^r + 1$ but not $q^i + 1$ for $i < r$, we have $N_G(\langle x\rangle) = (D.r) \times Sp_{2n-2r}(q)$. Hence the number of ordered pairs of G-conjugates of t with product of odd order (dividing $q^r + 1$) is at least

$$N := \frac{1}{2}q^{2r} \times |G : N_G(\langle x\rangle)| = \frac{1}{4r} \cdot \frac{q^{2r} \cdot |Sp_{2n}(q)|}{(q^r + 1) \cdot |Sp_{2n-2r}(q)|}.$$

The proportion of pairs of conjugates of t with product of odd order is therefore at least $N/(|t^G|^2)$, and using the above information on $C_G(t)$, we see that this proportion is at least c/r, where $c = \frac{1}{64}$.

Now consider $t = a_r$. In this case t lies in a subgroup $Sp_4(q^{r/2})$ of $Sp_{2r}(q)$ (acting on the natural 4-dimensional module for $Sp_4(q^{r/2})$ as $W(2)$). Indeed,

$$t \in S := SL_2(q^{r/2}) \otimes 1 < SL_2(q^{r/2}) \otimes SL_2(q^{r/2}) = \Omega_4^+(q^{r/2}) < Sp_4(q^{r/2}).$$

As usual, let $D \cong D_{2(q^{r/2}+1)}$ be a dihedral subgroup of S containing t. For $x \in D$ of order dividing $q^{r/2} + 1$ but not $q^i + 1$ for $i < r/2$, we have

$C_{Sp_{2r}(q)}(x) = (q^{r/2}+1) \otimes SL_2(q^{r/2}) \cong GU_2(q^{r/2})$, and hence $N_G(\langle x\rangle) = ((D.(r/2)) \otimes SL_2(q^{r/2})) \times Sp_{2n-2r}(q)$. Now argue as above to obtain the conclusion. ■

Lemma 2.4 *Theorem* 1 *holds when* $G = \Omega_d^{\pm}(q)$ *(q even).*

Proof. Let $G = \Omega_d^{\epsilon}(q)$, and write $d = 2n$ and $V = V_{2n}(q)$. We can assume that $n \geq 4$. Involution classes and centralizers in G can be found in [8, 7.3] (originally in [1]). The class representatives are the involutions a_r and c_r defined in the previous proof (the involutions b_r lie in $O(V) \setminus \Omega(V)$), noting that if n is even, a_n lies in $\Omega_{2n}^{+}(q)$ but not $\Omega_{2n}^{-}(q)$, and $a_n^{O_{2n}^{+}(q)}$ splits into two classes in $\Omega_{2n}^{+}(q)$. Also,

$$\begin{aligned} C_G(a_r)/O_2(C_G(a_r)) &= Sp_r(q) \times \Omega_{2n-2r}^{\epsilon}(q), \ \ |C_G(a_r)| \sim q^{n^2+(n-r)^2-n+r}, \\ C_G(c_r)/O_2(C_G(c_r)) &= Sp_{r-2}(q) \times Sp_{2n-2r}(q), \ \ |C_G(c_r)| \sim q^{n^2+(n-r)^2-n}. \end{aligned}$$

As in the previous proof, an involution a_r lies in a subgroup $S = SL_2(q^{r/2})$ of $\Omega_4^{+}(q^{r/2})$, and this is contained in a subgroup $\Omega_{2r}^{+}(q)$ of G. Elements $x \in S$ of order dividing $q^{r/2}+1$ but not q^i+1 for $i < r/2$ satisfy $N_G(\langle x\rangle) = ((q^{r/2}+1).r) \otimes SL_2(q^{r/2})) \times \Omega_{2n-2r}^{\epsilon}(q)$, and now we obtain the conclusion in the usual way.

Finally, an involution c_r lies in a subgroup $D := O_2^{\epsilon}(q^r) \cong D_{2(q^r-\epsilon)}$ of $\Omega_{2r}^{\epsilon}(q) < G$, and for $x \in D$ of order dividing $q^r - \epsilon$ but not $q^i - \epsilon$ for $i < r$ we have $N_G(\langle x\rangle) \leq (D.r) \times \Omega_{2n-2r}^{\epsilon}(q)$, leading to the result in the usual way. ■

3 Proof of Theorem 2

Let G be a simple group of exceptional Lie type over $\mathbb{F}_q$ with q even. The conjugacy classes of involutions in G can be found in Tables 22.2.1-6 of [8] (originally in [1]). For convenience we postpone the proof for the twisted types ${}^2F_4(q)'$, ${}^3D_4(q)$, ${}^2B_2(q)$ until the end of the section; so assume for now that G is not one of these types.

For each involution class in G, we argue as follows, letting $c_1, c_2, \ldots$ denote positive absolute constants. Let t be an involution in the class. For suitable k (specified in Table 1), we find a torus T_k of order a polynomial in q of degree k, such that every element of T_k is inverted by t. Then all involutions in the coset $T_k t$ are conjugate to t. For sufficiently large q, at least $c_1 q^k$ of the elements $x \in T_k$ satisfy $C_G(x) = C_G(T_k)$. Hence the number of pairs of conjugates of t with product equal to a conjugate of such an element x is at least

$$N := c_2 q^{2k} \times |G : N_G(T_k)|.$$

We have $N \geq c_3 q^{2k+s}$, where s is the degree of the polynomial $|G : C_G(T_k)|$, computed using Table 1 (noting that $|N_G(T_k) : C_G(T_k)|$ is bounded by the order of the Weyl group of G) . Also $|t^G| < c_4 q^l$, where l is also in Table 1. In all cases we calculate that $2k + s = 2l$. Hence the proportion $N/|t^G|^2$ is greater than some positive absolute constant, as required for Theorem 2.

For each involution class, the entries in Table 1 are justified by choosing an involution $w_0(D)$ in the Weyl group $W(G)$ as a representative of the class, where D is a subsystem subgroup given in column 3 of the table and $w_0(D)$ denotes the longest element of $W(D)$. This involution inverts a maximal torus T_k of D, and $C_G(T_k)$ is a Levi subgroup of G which is easily computed using knowledge of $C_G(D)$ (see [8, Chapter 11]).

Table 1:

G	t	rep.	k	type of $C_G(T_k)$	l, where $\lvert t^G\rvert \sim q^l$
$E_8(q)$	A_1	$w_0(A_1)$	1	$T_1E_7(q)$	58
	A_1^2	$w_0(A_1^2)$	2	$T_2D_6(q)$	92
	A_1^3	$w_0(D_4)$	4	$T_4D_4(q)$	112
	A_1^4	$w_0(E_8)$	8	T_8	128
$E_7(q)$	A_1	$w_0(A_1)$	1	$T_1D_6(q)$	34
	A_1^2	$w_0(A_1^2)$	2	$T_2A_1(q)D_4(q)$	52
	$(A_1^3)^{(1)}$	$w_0(A_1^3)$	3	$T_3D_4(q)$	54
	$(A_1^3)^{(2)}$	$w_0(D_4)$	4	$T_4A_1(q)^3$	64
	A_1^4	$w_0(E_7)$	7	T_7	70
$E_6^\epsilon(q)$	A_1	$w_0(A_1)$	1	$T_1A_5^\epsilon(q)$	22
	A_1^2	$w_0(A_1^2)$	2	$T_3A_3^\epsilon(q)$	32
	A_1^3	$w_0(D_4)$	4	T_6	40
$F_4(q)$	A_1	$w_0(A_1)$	1	$T_1C_3(q)$	16
	$\tilde{A}_1$	$w_0(\tilde{A}_1)$	1	$T_1B_3(q)$	16
	$(\tilde{A}_1)_2$	$w_0(B_2)$	2	$T_2B_2(q)$	22
	$A_1\tilde{A}_1$	$w_0(F_4)$	4	T_4	28
$G_2(q)$	A_1	$w_0(A_1)$	1	$T_1A_1(q)$	6
	$\tilde{A}_1$	$w_0(G_2)$	2	T_2	8

It remains to handle the cases where G is ${}^2F_4(q)'$, ${}^3D_4(q)$ or ${}^2B_2(q)$.

First, $G = {}^2B_2(q)$ has one class of involutions, and contains a dihedral subgroup of order $2(q-1)$. Hence an involution t inverts a torus T_1 of order $q-1$, and we have $C_G(T_1) = T_1$ and $|t^G| \sim q^3$. In the above calculation we now have $k = 1$, $s = 4$ and $l = 3$, so that $2k + s = 2l$, giving the conclusion of the theorem as before.

When $G = {}^2F_4(q)'$ there are two classes of involutions; representatives are denoted by z and t in [1, (18.2)]. For $q = 2$ we can check the result using [4, p.74], so assume $q > 2$. Now z is a long root involution, so the conclusion for this class follows from [7, 3.9]. The involution t lies in a subgroup $A_1(q)$ of G, so inverts a torus T_1 of order $q + 1$ in this subgroup, and $C_G(T_1) = T_1 A_1(q)$. Since $|t^G| \sim q^{12}$ the result follows in the usual way.

Similarly, $G = {}^3D_4(q)$ has two involution classes. A representative t of the non-root involution class can be taken to lie diagonally in a subgroup $A_1(q) \times A_1(q^3)$, and hence to invert a torus of order $(q + 1)(q^3 - 1)$. Also $|t^G| \sim q^{16}$ (see [1, (18.5)]), and the conclusion follows as usual.

This completes the proof of Theorem 2. ■

Remark By keeping track of the various polynomials in q occurring in the proof (namely $|T_k|$, $|G : N_G(T_k)|$ and $|t^G|$), it is straightforward to see that taking $b = \frac{1}{100}$ suffices in the conclusion of Theorem 2. We justify this briefly for $G = E_8(q)$; the other groups are very similar. For t in the class A_1, the conclusion follows from [7, 3.9] with $b = \frac{1}{4}$. When t is in the class A_1^2, it inverts a torus T_2 of order $q^2 + 1$ in a subgroup $A_1(q^2) \cong \Omega_4^-(q) \leq \Omega_4^-(q) \times \Omega_{12}^-(q) \leq D_8(q)$, and $N_G(T_2) = (T_2 \times \Omega_{12}^-(q)).4$. More than half the elements of T_2 have the same centralizer as T_2 itself, so as in the above proof, the proportion of pairs of conjugates of t with product equal to a conjugate of an element of T_2 is at least

$$\frac{\frac{1}{2}|T_2|^2 \cdot |G : (T_2 \times \Omega_{12}^-(q)).4|}{|t^G|^2},$$

and $|t^G| = |G|/q^{78}|B_6(q)|$ (see [8, Table 22.2.1]). The above ratio is easily seen to be greater than $\frac{1}{100}$. An involution t in the class A_1^3 inverts a torus T_4 of order $q^4 + 1$ in a subgroup $A_1(q^4) \cong \Omega_4^-(q^2) < \Omega_8^-(q) < \Omega_8^-(q) \times \Omega_8^-(q) < D_8(q)$, and $N_G(T_4) = (T_4 \times \Omega_8^-(q))$.[8], while $|t^G| = |G|/q^{81}|A_1(q)|\,|F_4(q)|$, giving the assertion as above. Finally, an involution t in the class A_1^4 inverts a cyclic torus T_8 of order equal to the cyclotomic polynomial $\Phi_{30}(q) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$, and $N_G(T_8) = T_8.30$ (see [3]). We have $|t^G| = |G|/q^{84}|C_4(q)|$, and the assertion follows as before.

References

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

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

[3] R.W. Carter, Conjugacy classes in the Weyl group, in *Seminar on algebraic groups and related finite groups* (eds. A. Borel et al.), Springer Lecture Notes No. 131, Springer-Verlag, Berlin, 1970.

[4] J.H.Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

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

[6] P. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.

[7] M.W. Liebeck and E.A. O'Brien, Finding the characteristic of a group of Lie type, *J. London Math. Soc.* **75** (2007), 741–754.

[8] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, Vol.180, American Math. Soc., Providence, RI, 2012.

[9] C.W. Parker and R.A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers, *J. Algebra* **324** (2010), 885–915.