Journal of Algebra 421 (2015) 431–437

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

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

ARTICLE INFO

Article history:
Received 9 July 2014
Available online 11 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

Keywords:
Finite groups of Lie type
Involutions
Computational group theory

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.

Dedicated to the memory of Ákos Seress

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; moreover, 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

http://dx.doi.org/10.1016/j.jalgebra.2014.08.037

[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 Remark at the end of the paper). Again, this is undoubtedly far from best possible.

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 $GL(U) \times GL(W) = GL_{2r}(q) \times GL_{d-2r}(q) \le G$. 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

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