ARTICLE IN PRESS YJABR:16481

Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Strong involutions in finite special linear groups of odd characteristic ☆

John D. Dixon [a], Cheryl E. Praeger [b,*], Ákos Seress [1]

[a] School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada
[b] School of Physics, Mathematics and Computing, The University of Western Australia, Crawley, WA 6009, Australia

A R T I C L E I N F O

Article history:
Received 14 March 2017
Available online xxxx
Communicated by Eamonn O'Brien

MSC:
20G40
20F69
20D60
20P05
68W20

Keywords:
Finite classical groups
Involution centralisers
Recognition algorithms

A B S T R A C T

Let t be an involution in $\mathrm{GL}(n,q)$ whose fixed point space E_+ has dimension k between $n/3$ and $2n/3$. For each $g \in \mathrm{GL}(n,q)$ such that tt^g has even order, $\langle tt^g \rangle$ contains a unique involution $z(g)$ which commutes with t. We prove that, with probability at least $c/\log n$ (for some $c > 0$), the restriction $z(g)_{|E_+}$ is an involution on E_+ with fixed point space of dimension between $k/3$ and $2k/3$. This result has implications in the analysis of the complexity of recognition algorithms for finite classical groups in odd characteristic. We discuss how similar results for involutions in other finite classical groups would solve a major open problem in our understanding of the complexity of constructing involution centralisers in those groups.

☆ This work was partially supported by ARC Grant DP160102323. The work for this paper was begun by the second and third authors in 2008, and early written drafts of the analysis, by both of these authors, date back to then. The paper was completed by the first and second authors after the death of their colleague Ákos Seress in February 2013.

* Corresponding author.
E-mail addresses: jdixon@math.carleton.ca (J.D. Dixon), cheryl.praeger@uwa.edu.au (C.E. Praeger).
[1] Deceased.

https://doi.org/10.1016/j.jalgebra.2017.11.047
0021-8693/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The 2001 paper of Altseimer and Borovik [1] marked a break-through in computational group theory by using involution centralisers to distinguish between the simple Lie type groups $\mathrm{PSp}(2n, q)$ and $\Omega(2n+1, q)$, with q odd. These are groups which share many properties, such as having the same order, and they had proved difficult to distinguish computationally. The paper [1] inspired the work of Parker and Wilson [11] who demonstrated that involution-centraliser methods could be used for solving several problems previously believed to be computationally difficult, and gave complexity analyses for methods to construct involutions and their centralisers in quasisimple Lie type groups in odd characteristic. These methods were based on Bray's algorithm [2] for constructing involution centralisers in finite groups. Our aim is to improve the analysis given by Parker and Wilson of Bray's algorithm in the case of finite special linear groups in odd characteristic. This is part of a program to improve the complexity analyses of a number of algorithms for computing with Lie type groups. In particular, we focus on its application in the recognition algorithm for special linear groups of Leedham-Green and O'Brien in [7]. In the rest of this section we give a brief overview of these applications to set the scene for our main result Theorem 1.1, and to pose some open problems.

1.1. Algorithmic background

Leedham-Green and O'Brien [7] describe and analyse an algorithm which constructs a 'standard generating set' for a finite classical group $G = \mathrm{SX}(n, q)$ (q odd) in its natural representation. Here (abusing the notation in [7] slightly) SX is one of $\mathrm{SL}, \mathrm{SU}, \mathrm{Sp}, \mathrm{SO}^\varepsilon$, or Ω^ε, where $\varepsilon \in \{+, -, \circ\}$. In [7, Section 3] the authors define a standard generating set for SX (see especially [7, Table 1] for all groups except those of type Ω^ε, and [7, Lemmas 3.2-3.4] for those of type Ω^ε). The algorithm is recursive in the sense that it finds a certain direct decomposition $V_m \oplus V_{n-m}$ of the underlying n-dimensional vector space, where $\dim(V_m) = m$, $\frac{n}{3} \le m \le \frac{2n}{3}$ and the decomposition is orthogonal if $\mathrm{SX} \neq \mathrm{SL}$. It then constructs classical groups acting on each of V_m and V_{n-m} and finds standard generators for them recursively. The algorithm concludes by 'patching together' these standard generating sets for the subgroups to obtain standard generators for G.

The key challenge is to obtain an appropriate direct decomposition $V_m \oplus V_{n-m}$ and construct the classical subgroups acting on each direct summand. This is done in [7] by finding an involution $t \in G$ with ±1-eigenspaces of suitable dimensions $m, n-m$, then constructing (the second derived subgroup of) its centraliser $C_G(t)$, and extracting the central 'factors' of $C_G(t)$ induced on the eigenspaces of t.

The analysis given in [7] is based on the construction of $O(n)$ random elements at several stages in the algorithm (see [7, bottom of page 835]). O'Brien mentioned in private communication to the second and third authors, probably in 2008, that the practical performance of the algorithm was much faster than the analysis in [7] suggested. He

Please cite this article in press as: J.D. Dixon et al., Strong involutions in finite special linear groups of odd characteristic, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2017.11.047