Journal of Algebra 421 (2015) 460–492

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Effective black-box constructive recognition of classical groups ☆

Heiko Dietrich [a], C.R. Leedham-Green [b], E.A. O'Brien [c,*]

[a] *School of Mathematical Sciences, Monash University, Melbourne, VIC 3800, Australia*
[b] *School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, United Kingdom*
[c] *Department of Mathematics, Private Bag 92019, Auckland, University of Auckland, New Zealand*

ARTICLE INFO

Article history:
Received 30 April 2014
Available online 13 September 2014
Communicated by William M. Kantor

Keywords:
Classical groups
Constructive recognition
Black-box algorithms

ABSTRACT

We describe a black-box Las Vegas algorithm to construct standard generators for classical groups defined over finite fields. We assume that the field has size at least 4 and that oracles to solve certain problems are available. Subject to these assumptions, the algorithm runs in polynomial time. A practical implementation of our algorithm is distributed with the computer algebra system Magma.

Dedicated to the memory of Ákos Seress

☆ This work was supported in part by the Marsden Fund of New Zealand via grant UOA 105. Dietrich was supported by an ARC-DECRA Fellowship, project DE140100088. The last two authors were supported by GNSAGA-INdAM while this work was completed; we thank our hosts, Patrizia Longobardi and Mercede Maj of the University of Salerno, for their generous hospitality. We thank Damien Burns for early work on the odd characteristic case; we thank Jianbei An, Gerhard Hiss, and Martin Liebeck for helpful discussions; we thank the referee and editor for their comments.

* Corresponding author.
E-mail addresses: heiko.dietrich@monash.edu (H. Dietrich), c.r.leedham-green@qmul.ac.uk (C.R. Leedham-Green), obrien@math.auckland.ac.nz (E.A. O'Brien).

http://dx.doi.org/10.1016/j.jalgebra.2014.08.039
0021-8693/

1. Introduction

In [19,26] we developed constructive recognition algorithms for the classical groups in their natural representation. These are well-analysed and efficient, both theoretically and in practice; our implementations are distributed with the computer algebra system Magma [9]. A core idea is to construct centralisers of involutions, and use these to construct, as subgroups of the input group, classical groups of smaller rank, so facilitating recursion. We now develop these ideas to obtain such algorithms for classical groups given as black-box groups.

Let $\tilde{G} \leq \mathrm{GL}_d(q)$ be a classical group in its natural representation, and let $G = \langle X \rangle$ be isomorphic to a central quotient of $\tilde{G}$, where X is a given generating set. A *constructive recognition* algorithm for G constructs a surjective homomorphism from $\tilde{G}$ to G, and for any given $g \in G$ constructs an element of its inverse image in $\tilde{G}$. We realise such an algorithm in two stages. For each classical group $\tilde{G}$, we define a specific ordered set of *standard generators* $\tilde{\mathcal{S}}$. The first task is to construct, as words in X, an ordered subset $\mathcal{S}$ of G that is the image of $\tilde{\mathcal{S}}$ under a surjective homomorphism from $\tilde{G}$ to G. The second task is to solve the *constructive membership problem* for G with respect to $\mathcal{S}$: namely, express $g \in G$ as a word in $\mathcal{S}$, and so as a word in X; we also solve the constructive membership for $\tilde{G}$ with respect to $\tilde{\mathcal{S}}$. Now the surjective homomorphism $\varphi\colon \tilde{G} \to G$ that maps $\tilde{\mathcal{S}}$ to $\mathcal{S}$ is *constructive*: $\tilde{g} \in \tilde{G}$ is written as a word $w(\tilde{\mathcal{S}})$ in $\tilde{\mathcal{S}}$, and its image $\varphi(\tilde{g})$ is $w(\mathcal{S})$. Similarly, we compute a preimage in $\tilde{G}$ of $g \in G$ under φ. In summary, we provide an algorithm to solve the first of these tasks; we discuss the second in Section 1.3.

Babai and Szemerédi [6] introduced the concept of a *black-box group*: group elements are represented by bit strings of uniform length, where more than one bit string may represent the same element. Three *oracles* are provided to supply the group-theoretic functions of multiplication, inversion, and checking for equality with the identity element. A *black-box* algorithm is one that uses only these oracles. A common assumption is that other oracles are available to perform certain tasks.

For an overview of the *Matrix Group Recognition Project*, to which this work contributes, see [37]. Much of the background and preliminaries needed for this paper are summarised in [19,26,37].

1.1. The groups and their standard copies

Throughout, $\mathrm{GL}_d(q)$ is the group of invertible $d \times d$ matrices over the field $\mathrm{GF}(q)$. The groups under discussion are $\mathrm{SL}_d(q)$, $\mathrm{Sp}_d(q)$, $\mathrm{SU}_d(q)$, $\Omega_d^{\pm}(q)$, and $\Omega_d(q)$. We assume that $q \geq 4$, and $d \geq 3$ for the orthogonal groups. All of the groups are perfect, and with the exception of $\Omega_4^+(q)$, all are quasisimple.

The definition of these groups, except for the first, depends on the choice of a bilinear or quadratic form. Groups defined by two forms of the same type are conjugate in the corresponding general linear group; the *standard copy* of a classical group is its unique conjugate which preserves a chosen *standard form*. Our standard forms and copies are