Available online at www.sciencedirect.com
SCIENCE DIRECT

Journal of Algebra 292 (2005) 4–46

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules

Robert Beals [a], Charles R. Leedham-Green [b], Alice C. Niemeyer [c,1], Cheryl E. Praeger [c,*,1], Ákos Seress [d,2]

[a] *IDA Center for Communications Research, Princeton, NJ 08540, USA*
[b] *School of Mathematical Sciences, Queen Mary and Westfield College, London E1 4NS, United Kingdom*
[c] *School of Mathematics and Statistics, University of Western Australia, Crawley, WA 6009, Australia*
[d] *Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA*

Received 1 March 2004

Available online 14 March 2005

Communicated by Eamonn O'Brien

Abstract

We present a Las Vegas algorithm which, for a given matrix group known to be isomorphic modulo scalars to a finite alternating or symmetric group acting on the fully deleted permutation module, produces an explicit isomorphism with the standard permutation representation of the group. This algorithm exploits information available from the matrix representation and thereby is faster than existing 'black-box' recognition algorithms applied to these groups. In particular, it uses the fact that certain types of elements in these groups can be identified and constructed from the structure of their characteristic polynomials. The algorithm forms part of a large-scale program for computing with groups of matrices over finite fields. When combined with existing 'black-box' recognition algorithms, the results of this paper prove that any d-dimensional absolutely irreducible matrix rep-

* Corresponding author.
E-mail addresses: beals@idaccr.org (R. Beals), crlg@maths.qmw.ac.uk (C.R. Leedham-Green), alice@maths.uwa.edu.au (A.C. Niemeyer), praeger@maths.uwa.edu.au (C.E. Praeger), akos@math.ohio-state.edu (Á. Seress).

1 Partially supported by Australian Research Council Discovery Project Grant DP0209760.
2 Partially supported by the National Science Foundation.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.01.035

resentation of a finite alternating or symmetric group, over a finite field, can be recognised with $O(d^{1/2})$ random group elements and $O(d^{1/2})$ matrix multiplications, up to some logarithmic factors.

Keywords: Constructive recognition; Matrix groups; Alternating and symmetric groups; Probabilistic method

1. Introduction

In this paper we present an algorithm designed to recognise finite alternating and symmetric groups acting naturally as matrix groups in their smallest dimensional, faithful, absolutely irreducible representations over a finite field of characteristic p. The reason for focusing on the special case of these representations of A_n and S_n is that they arise in a special way as maximal subgroups (modulo scalars) of finite classical groups. The algorithm given in this paper requires $O(n^\alpha)$ random selections and $O(n^\alpha \log^2 n)$ matrix multiplications, where $\alpha = 1/3$ if $p \neq 3$ and $\alpha = 1/2$ for $p = 3$, and is asymptotically faster than an implementation for these groups of the fastest known 'black-box' algorithm to recognise finite alternating and symmetric groups. Moreover, the algorithm given in this paper, combined with the 'black-box' algorithm in [5], provides a uniform complexity of $O(d^{1/2})$ random selections and $O(d^{1/2})$ matrix multiplications (up to some logarithmic factors) to recognise any d-dimensional absolutely irreducible representation of a finite alternating or symmetric group over a finite field, see Section 2.1 for details.

Aschbacher [1] described eight families of maximal subgroups of the finite classical groups of dimension d over a field $\mathbb{F}$ of order q (where $q = p^a$ for some prime p). He proved that any maximal subgroup G not lying in one of these eight families must be nearly simple, that is $G/(G \cap Z)$ has a simple socle S where Z denotes the subgroup of non-zero scalar matrices. Moreover, for these nearly simple groups, the pre-image of S in G is absolutely irreducible on the underlying vector space V, is not realisable over a proper subfield, and is not a classical group in its natural representation. Every abstract finite simple group can occur in this way as the simple group S. In Section 2 we briefly describe how Aschbacher's result has been used as the underpinning framework for a matrix recognition project for matrix group computation, and how the algorithm of this paper fits into this framework.

Moreover, it was shown by Liebeck [22] that, for sufficiently high dimensions, the largest among the nearly simple maximal subgroups mentioned above are the groups $Z \times S_n$ acting on the fully deleted permutation module over $\mathbb{F}$ corresponding to the natural transitive permutation action of S_n of degree n. This module will be described in detail in Section 3.1. Its dimension is $n - 1$ if the characteristic p does not divide n, and is $n - 2$ if p does divide n.

Our main result is Theorem 1.1. It involves several parameters, namely ω, ρ_F and ξ. The parameter ξ is an upper bound on the cost of producing one random element of G; ρ_F is an upper bound on the cost of performing one operation (addition, multiplication or finding an inverse) in the finite field $\mathbb{F}$ of order q; and ω is a real number for which