Bull. Aust. Math. Soc. **91** (2015), 175–176
doi:10.1017/S0004972714000756

ESTIMATION AND COMPUTATION WITH MATRICES OVER FINITE FIELDS

BRIAN P. CORR

(Received 28 April 2014; first published online 14 October 2014)

2010 *Mathematics subject classification*: primary 20G40; secondary 20C40, 05E15.

Keywords and phrases: matrix group, constructive recognition, Las Vegas algorithm, complexity.

The matrix group recognition project is a worldwide effort to produce efficient algorithms for working with arbitrary matrix groups over finite fields (see [3, 6]). Such groups are potentially very large in comparison to the input length, and dealing with them using deterministic methods is impractical.

When a generating set for a group is input into a computer, a *constructive recognition* algorithm names the group and finds an efficient mapping between the input generators and a set of 'standard generators'. This allows various important questions to be answered quickly. Constructive recognition is a major natural goal in computational group theory.

To recognise an arbitrary group, there are two tasks to perform. The first is to decompose the group into smaller components if possible, and work recursively. The second is to deal with irreducible cases, which in this case are the finite simple groups.

This paper addresses constructive recognition of matrix groups from 'both ends': on the one hand, we give an improved analysis of the Norton irreducibility test, part of the `MEAT-AXE` algorithm (see [1]), by providing a lower bound of the form $a_1 - a_2q^{-bc}$ for the proportion of primary cyclic matrices in $\mathrm{M}(c, q^b)$, where a_1, a_2 are constants depending only on q, b. To achieve this, we generalise the Kung–Stong cycle index (see [2, 7]) to compute a generating function for the proportion.

On the other hand, we solve a particular family of base cases for the constructive recognition recursion, by extending the work of Magaard *et al.* [4] to provide a Las Vegas algorithm for constructive recognition of classical groups in irreducible representations of moderate degree. When the degree of the representation is large, existing black-box methods are effective. On the other hand, when the degree is equal to the natural degree, there are specific methods to address the problem.

Thesis submitted to The University of Western Australia in May 2013; degree approved 13 January 2014; supervisors: Cheryl Praeger and Ákos Seress.

The algorithms presented in this paper address the middle ground: working algorithms dealing with the case $d < n \leq d^2$, where d is the natural degree, are presented, analysed and implemented in GAP.

We present a Las Vegas algorithm to rewrite elements of a classical group over $\mathbb{F}_q$, represented as an irreducible subgroup of $\mathrm{GL}(n, q)$ (with exceptions in some small cases), as elements of $\mathrm{GL}(d, q)$, as follows.

(i) The procedure `Initialise`, which must be run once to set up a data structure, is a Las Vegas algorithm with complexity

$$O(\xi_H d^2 \log^2 q \log \epsilon^{-1} \\ + \rho_q(d^9 \log d \log\log d \log q + d^8 \log d \log\log d \log^3 q \log \epsilon^{-1})),$$

where ξ_H is the cost of choosing a random element of H, ρ_q is the cost of a field operation in $\mathbb{F}_q$ and ϵ is an acceptable probability of failure supplied by the user.

(ii) The procedure `FindImage`, which computes the image of g in a representation of natural degree d, is a Las Vegas algorithm with complexity

$$O((\xi_H + \rho_q d^8 \log d \log\log d \log q) \log \epsilon^{-1}).$$

Since $n = O(d^2)$, the efficiency of these algorithms in terms of the input length $N = n^2 \log q$ is of the order $O(N^{9/2})$ and $O(N^4)$, respectively. To analyse these algorithms, we use the Quokka theory of Niemeyer and Praeger [5], which we also extend to deal with sets of matrices which may be singular, and apply this new theory to a second count of primary cyclic matrices.

References

[1] D. F. Holt and S. Rees, 'Testing modules for irreducibility', *J. Aust. Math. Soc. (Ser. A)* **57** (1994), 1–16.

[2] J. P. S. Kung, 'The cycle structure of a linear transformation over a finite field', *Linear Algebra Appl.* **36** (1981), 141–155.

[3] C. R. Leedham-Green, 'The computational matrix group project', in: *Groups and Computation III,* Vol. 8 (De Gruyter, Berlin, Boston, 2001), 229–247.

[4] K. Magaard, E. A. O'Brien and Á. Seress, 'Recognition of small dimensional representations of general linear groups', *J. Aust. Math. Soc.* **85** (2008), 229–250.

[5] A. C. Niemeyer and C. E. Praeger, 'Estimating proportions of elements in finite groups of Lie type', *J. Algebra* **324** (2010), 122–145.

[6] E. A. O'Brien, 'Towards effective algorithms for linear groups', in: *Finite Geometries, Groups and Computation, Proc. Conf. Finite Geometries, Groups and Computation*, Pingree Park, Colorado, USA (Walter de Gruyter, 2006), 163–190.

[7] R. Stong, 'Some asymptotic results on finite vector spaces', *Adv. Appl. Math.* **9** (1988), 167–199.

BRIAN P. CORR, School of Mathematics and Statistics,
The University of Western Australia,
Crawley, WA 6009, Australia
e-mail: brian.p.corr@gmail.com

https://doi.org/10.1017/S0004972714000756 Published online by Cambridge University Press