Journal of Algebra 416 (2014) 139–166

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

# Recognising the small Ree groups in their natural representations

Henrik Bäärnhielm

*Department of Mathematics, University of Auckland, New Zealand*

ARTICLE INFO

*Article history:*
Received 5 June 2012
Available online 10 July 2014
Communicated by William M. Kantor

*Keywords:*
Matrix group recognition
Exceptional groups
Constructive recognition

ABSTRACT

We present Las Vegas algorithms for constructive recognition and constructive membership testing of the Ree groups ${}^2\mathrm{G}_2(q) = \mathrm{Ree}(q)$, where $q = 3^{2m+1}$ for some $m > 0$, in their natural representations of degree 7. The input is a generating set $X \subset \mathrm{GL}(7, q)$.

The constructive recognition algorithm is polynomial time given a discrete logarithm oracle. The constructive membership testing consists of a pre-processing step, that only needs to be executed once for a given $X$, and a main step. The latter is polynomial time, and the former is polynomial time given a discrete logarithm oracle.

Implementations of the algorithms are available for the computer algebra system Magma.



## 1. Introduction

This paper will consider algorithmic problems for a class of finite simple groups, as matrix groups over finite fields, given by sets of generators. The most important problems under consideration are the following:

*E-mail address:* henrik@math.auckland.ac.nz.
*URL:* http://www.math.auckland.ac.nz/~henrik/.

http://dx.doi.org/10.1016/j.jalgebra.2014.06.017
0021-8693/

(1) The *constructive membership* problem. Given $G = \langle X \rangle \leqslant \mathrm{GL}(d, q)$ and $g \in \mathrm{GL}(d, q)$, decide whether or not $g \in G$, and if so express $g$ as a straight line program in $X$.
(2) The *constructive recognition* problem. Given $G = \langle X \rangle \leqslant \mathrm{GL}(d, q)$, construct an *effective isomorphism* from $G$ to a *standard copy* $H$ of $G$, together with an effective inverse isomorphism. An isomorphism $\psi : G \to H$ is effective if $\psi(g)$ can be computed efficiently for every $g \in G$.

In [1] we considered these problems for the Suzuki groups. Here we consider the Ree groups ${}^2\mathrm{G}_2(q) = \mathrm{Ree}(q)$, $q = 3^{2m+1}$ for any $m > 0$. We only consider the *natural representations*, which have dimension 7. Our standard copy is $\mathrm{Ree}(q)$, defined in Section 3.

The primary motivation for considering these problems comes from the *matrix group recognition project* [3,21,27].

The ideas used here for the constructive recognition and membership testing of $\mathrm{Ree}(q)$ are similar to those used in [1] and [11] for $\mathrm{Sz}(q)$ and $\mathrm{SL}(2, q)$, respectively. The results are also similar in the sense that we reduce these problems to the discrete logarithm problem.

In Section 7 we solve the constructive membership problem for $\mathrm{Ree}(q)$. In Section 8 we solve the constructive recognition problem for $\mathrm{Ree}(q)$ in the natural representations.

The main objective of this paper is to prove the following:

**Theorem 1.1.** *Let $q = 3^{2m+1}$ for some $m > 0$. Assume an oracle for the discrete logarithm problem in $\mathbb{F}_q$, with time complexity $\mathrm{O}(\chi_D)$ field operations, and a random element oracle for subgroups of $\mathrm{GL}(7, q)$, with time complexity $\mathrm{O}(\xi)$ field operations.*

(1) *There exists a Las Vegas algorithm that for each $\langle X \rangle \leqslant \mathrm{GL}(7, q)$, such that $\langle X \rangle \cong \mathrm{Ree}(q)$, constructs an effective isomorphism $\Psi : \langle X \rangle \to \mathrm{Ree}(q)$, such that $\Psi^{-1}$ is also effective. The algorithm has expected time complexity $\mathrm{O}(\xi \log\log(q) + \log(q)^2 + \chi_D)$ field operations.*
(2) *There exists a Las Vegas algorithm that for each $\langle X \rangle \leqslant \mathrm{GL}(7, q)$, such that $\langle X \rangle \cong \mathrm{Ree}(q)$, solves the constructive membership problem for $\langle X \rangle$. The algorithm has expected time complexity $\mathrm{O}(\xi + \log(q)^3)$ field operations and also has a preprocessing step, which only needs to be executed once for a given $X$, with expected time complexity $\mathrm{O}((\xi \log\log(q) + \log(q)^3 + \chi_D) \log\log(q)^2)$ field operations. The length of the returned* `SLP` *is $\mathrm{O}((\log(q) \log\log(q))^2)$.*

Implementations of the algorithms have been done in Magma [6].

A version of the material in this paper appeared in [2], relying on a few conjectures. Advice by Bill Kantor and Gunter Malle has led to proofs of the conjectures, for which we are very grateful. In particular, the central idea behind the algorithm in Section 8 is due to Bill Kantor.

We also thank John Bray, Peter Brooksbank, Alexander Hulpke, Charles Leedham-Green, Eamonn O'Brien, Maud de Visscher, Robert Wilson and the anonymous referee for their helpful comments.