

# TENSOR DECOMPOSITION OF THE REE GROUPS

HENRIK BÄÄRNHIELM

ABSTRACT. We give a polynomial time Las Vegas algorithm that, given  $X \subseteq \mathrm{GL}(d, q)$  such that  $d > 7$  and  $\langle X \rangle$  is isomorphic to a small Ree group  $\mathrm{Ree}(q)$ , finds an explicit isomorphism from  $\langle X \rangle$  to  $\mathrm{Ree}(q)$ .

The algorithm consists of several cases depending on the degree of  $\langle X \rangle$  and on the field size.

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

## 1. INTRODUCTION

The problem of *constructive recognition* of  $G \leq \mathrm{GL}(d, q)$  can be defined as follows: given  $X \subseteq \mathrm{GL}(d, q)$  such that  $\langle X \rangle \cong G$ , construct an *explicit isomorphism* from  $G$  to a *standard copy*  $H$  of  $G$ . An explicit isomorphism  $\psi : G \rightarrow H$  is an isomorphism where  $\psi(g)$  and  $\psi^{-1}(h)$  can be computed efficiently for every  $g \in G$  and  $h \in H$ .

This paper will consider constructive recognition for the small Ree groups  $\mathrm{Ree}(q)$ , where  $q = 3^{2m+1}$  for  $m > 0$ , one of the infinite families of finite simple groups. In [1] we considered constructive recognition  $\mathrm{Ree}(q)$  in any of its equivalent representations in dimension 7.

When  $G \cong \mathrm{Ree}(q)$  and  $G \leq \mathrm{GL}(d, q')$  where  $q'$  is not an odd power of 3, then by [14] and [19],  $d \geq q(q-1)$  so  $q \in O(\sqrt{d})$ . Thus  $q$  is polynomial in the size of the input and all interesting problems regarding  $G$  can be solved efficiently using permutation group techniques.

Here we show how to construct explicit isomorphisms from  $G \leq \mathrm{GL}(d, q)$ , where  $G \cong \mathrm{Ree}(q)$ ,  $d > 7$  and  $q = 3^{2m+1}$  for  $m > 0$ , to the standard copy of  $\mathrm{Ree}(q)$ . The standard copy we use is defined in [1]. The motivation for the constructive recognition of  $\mathrm{Ree}(q)$  comes from the *matrix recognition project* (see [15]).

Let  $V$  be the given module of  $G$ . In general we want an algorithm that works when  $V$  is any projective module of  $\mathrm{Ree}(q)$  in characteristic 3, but we can reduce to the case where  $V$  is absolutely irreducible and written over the minimal field modulo scalars, using the MeatAxe (see [12] and [13]) and [10], so henceforth assume that this is the case. Then  $V$  is isomorphic to a tensor product of *twisted versions* (see Section 2) of either the natural module of  $\mathrm{Ree}(q)$  or its module of dimension 27. Hence, to construct an explicit isomorphism from  $G$  to a conjugate  $H$  of  $\mathrm{Ree}(q)$ , it is sufficient to find a tensor decomposition of  $V$  and then possibly decompose the 27-dimensional module. In Section 2 we describe the theoretical background in more detail.

Tensor decomposition amounts to finding a basis of  $V$  that exhibits  $V$  as a tensor product. This is described in Section 4. In Section 3 an algorithm for decomposing the 27-dimensional module is described.

Implementations of the algorithms are available in MAGMA (see [4]).

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

## 2. PRELIMINARIES

We now discuss the theoretical background in more detail. If  $V$  is an  $FG$ -module for some group  $G$  and field  $F$ , with action  $f : V \times FG \rightarrow V$ , and if  $\Phi$  is an automorphism of  $G$ , denote by  $V^\Phi$  the  $FG$ -module which has the same elements as  $V$  and where the action is given by  $(v, g) \mapsto f(v, \Phi(g))$  for  $g \in G$  and  $v \in V^\Phi$ , extended to  $FG$  by linearity. We call  $V^\Phi$  a *twisted version* of  $V$ , or  $V$  *twisted by*  $\Phi$ .

Now assume that  $G \leq \text{GL}(d, q)$  where  $G \cong \text{Ree}(q)$ ,  $d > 7$  and  $q = 3^{2m+1}$  for some  $m > 0$ . Then  $\text{Aut } \mathbb{F}_q = \langle \phi \rangle$ , where  $\phi$  is the Frobenius automorphism. Let  $W$  be the given module of  $G$  and let  $V$  be the natural module of the standard copy of  $\text{Ree}(q)$ , so that  $\dim W = d$  and  $\dim V = 7$ . We will assume that  $W$  is absolutely irreducible and over the minimal field modulo scalars. From [21] we then know that

$$W \cong M^{\phi^{i_0}} \otimes M^{\phi^{i_1}} \otimes \cdots \otimes M^{\phi^{i_{n-1}}} \quad (2.1)$$

for some integers  $0 \leq i_0 < i_1 < \cdots < i_{n-1} \leq 2m$ , and where  $M$  is either  $V$  or the absolutely irreducible 27-dimensional submodule  $S$  of the symmetric square  $\mathcal{S}^2(V)$ . In fact we may assume that  $i_0 = 0$ , and if we can find an explicit isomorphism between  $V$  and  $W$ , we will immediately obtain an explicit isomorphism between  $G$  and a conjugate of  $\text{Ree}(q)$ . Hence the essential problem is to find a tensor decomposition of  $W$ . This amounts to finding a change of basis  $c \in \text{GL}(d, q)$  which exhibits  $W$  as the tensor product of (2.1). When  $W$  is such an explicit tensor product, it is straightforward to find the image of an element of  $W$  in one of the tensor factors.

More specifically, it is sufficient to find an isomorphism  $W \cong U_1 \otimes U_2$  where  $\dim U_1 \in \{7, 27\}$ . Then  $U_1$  is a twisted version of  $V$  or  $S$ . The tensor decomposition algorithm of [16] can be used to find such an isomorphism of  $W$ . By [17] it is sufficient to find a *flat* in a projective geometry corresponding to the decomposition, where a flat is a subspace of  $W$  of the form  $A \otimes U_2$  where  $A$  is a proper subspace of  $U_1$ . This flat contains a *point*, which is a flat with  $\dim A = 1$ . If we can provide a flat to the algorithm of [16], then it will find a tensor decomposition in polynomial time. Thus the essential problem is to find a flat of  $W$ . We consider this problem in Section 4.

If  $\dim U_1 = 27$ , we also have to decompose  $S$  into  $V$  to obtain an isomorphism between  $W$  and  $V$ . We consider this problem in Section 3.

**Proposition 2.1.** *Let  $G \leq \text{GL}(27, q)$  such that  $G \cong \text{Ree}(q)$ , let  $j \in G$  be an involution and let  $H = C_G(j)' \cong \text{PSL}(2, q)$ . Then  $S_H \cong V_6 \oplus V_9 \oplus V_{12}$  as an  $H$ -module, where  $\dim V_i = i$ . Moreover,  $V_9$  is absolutely irreducible and  $V_6$  and  $V_{12}$  are uniserial with submodules  $V_6 \geq V_5 \geq V_1 \geq V_0 = 0$  and  $V_{12} \geq V_8 \geq V_4 \geq V_0 = 0$ . The 4-dimensional composition factors at the top and bottom of  $V_{12}$  are isomorphic, while the middle one is twisted by  $\phi^{m+1}$ .*

*Proof.* Experimental evidence. □

**Corollary 2.2.** *Let  $G \leq \text{GL}(27, q)$  such that  $G \cong \text{Ree}(q)$ , let  $j \in G$  be an involution and let  $H = C_G(j)' \cong \text{PSL}(2, q)$ . Then  $\dim \text{Hom}_H(S_H, S_H) = 5$ .*

*Proof.* □

**2.1. Complexity.** We shall be concerned with the time complexity of the algorithms involved, where the basic operations are the field operations, and not the bit operations. All simple arithmetic with matrices can be done using  $O(d^3)$  field

operations, and raising a matrix to the  $O(q)$  power can be done using  $O(d^3)$  field operations using [7].

We will need to find an element of order  $q - 1$ . The order can be computed using the algorithm of [7]. To obtain the *precise* order, this algorithm requires a factorisation of  $q - 1$ , otherwise it might return a multiple of the correct order. However, it is sufficient for our purposes to learn the *pseudo-order* of the element, which is a multiple of its order, since it is sufficient to find a nontrivial element of order dividing  $q - 1$ . Hence we avoid the requirement to factorise  $q - 1$ . The algorithm of [7] can also be used to obtain the pseudo-order, and for this it has time complexity  $O(d^3 \log(q) \log \log(q^d))$  field operations.

**2.2. Random elements.** Our analysis assumes that we can construct uniformly distributed random elements of a group  $G$  defined by a generating set  $X$ . The polynomial time algorithm of [2] produces nearly uniformly distributed random elements; an alternative polynomial time algorithm is the *product replacement* algorithm of [8]. We will assume that we have a random element oracle, which can produce a uniformly random element using  $O(\xi(d))$  field operations, where  $\xi : \mathbb{N} \rightarrow \mathbb{N}$ .

**2.3. Las Vegas algorithms.** Most of the algorithms we consider are probabilistic of the type known as *Las Vegas algorithms*. This type of algorithm is discussed in [22, Section 25.8], [20, Section 1.3] and [11, Section 3.2.1]. In short it is a probabilistic algorithm with an input parameter  $\varepsilon$  that either returns **failure**, with probability at most  $\varepsilon$ , or otherwise returns a correct result. The time complexity naturally depends on  $\varepsilon$ .

We present Las Vegas algorithms as probabilistic algorithms that either return a correct result, with probability bounded below by  $1/p(n)$  for some polynomial  $p(n)$  in the size  $n$  of the input, or otherwise return **failure**. By enclosing such an algorithm in a loop that iterates  $\lceil \log \varepsilon / \log(1 - 1/p(n)) \rceil$  times, we obtain an algorithm that returns **failure** with probability at most  $\varepsilon$ , and hence is a Las Vegas algorithm in the above sense. Clearly if the enclosed algorithm is polynomial time, the Las Vegas algorithm is polynomial time.

One can also enclose the algorithm in a loop that iterates until the algorithm returns a correct result, thus obtaining a probabilistic time complexity, and the expected number of iterations is then  $O(p(n))$ .

### 3. THE SYMMETRIC SQUARE

The two basic irreducible modules of  $\text{Ree}(q)$  are the natural module  $V$  of dimension 7, and an irreducible submodule  $S$  of the symmetric square  $\mathcal{S}^2(V)$ . The symmetric square itself is not irreducible, since  $\text{Ree}(q)$  preserves a quadratic form, and  $\mathcal{S}^2(V)$  therefore has a submodule of dimension 1. The complement of this has dimension 27 and is the irreducible module  $S$ .

**Lemma 3.1.** *The exterior square of  $S$  has a composition factor isomorphic to a twisted version of  $V$ .*

*Proof.* Use results of Ryba? □

**Theorem 3.2.** *There exists a Las Vegas algorithm that, given  $X \subseteq \text{GL}(27, q)$  with module  $W$  such that  $W$  is isomorphic to a twisted version of  $S$ , finds an explicit isomorphism from  $\langle X \rangle$  to  $\text{Ree}(q)^g$  for some  $g \in \text{GL}(7, q)$ . The algorithm has time complexity  $O(|X| \log(q))$  field operations.*

*Proof.* Using Lemma 3.1, this is just an application of the MeatAxe. We construct the exterior square  $\wedge^2(W)$  of  $W$ , which has dimension 351, and find a composition series of this module using the MeatAxe. By the Lemma, the natural module of

dimension 7 will be one of the composition factors and the MeatAxe will provide an explicit isomorphism to this factor, in the form of a change of basis  $A \in GL(27, q)$  of  $W$  that exhibits the action on the composition factors.

This induces an isomorphism  $\phi : \langle X \rangle \rightarrow H$ , where  $H$  is conjugate to  $\text{Ree}(q)$ . For  $g \in \langle X \rangle$ ,  $\phi(g)$  is computed by taking a submatrix of  $g^A$  of degree 7. Clearly  $\phi$  can be computed using  $O(1)$  field operations.

Since the MeatAxe is Las Vegas and has time complexity  $O(|X| \log(q))$ , the Theorem follows.  $\square$

#### 4. TENSOR PRODUCTS

Given a module  $W$  of the form (2.1), we now consider the problem of finding a flat. We will use the notation from Section 2.

If  $\phi^{i_0}, \dots, \phi^{i_{n-1}}$  are the elements of  $\text{Gal}(\mathbb{F}_q, \mathbb{F}_s)$  where  $\mathbb{F}_s \leq \mathbb{F}_q$ , then  $G$  is conjugate in  $GL(d, q)$  to a subgroup of  $GL(d, s)$ . Therefore,  $W$  may be given to our algorithms as an  $\mathbb{F}_s G$ -module, but the recognition algorithm of [3] will determine  $q$  such that  $G \cong \text{Ree}(q)$ . In the case where  $W$  is not over  $\mathbb{F}_q$ , we can embed it canonically into an  $\mathbb{F}_q G$ -module, so henceforth assume that  $W$  is an  $\mathbb{F}_q G$ -module.

For  $k = 0, \dots, n-1$ , let  $H_k$  be the image of the representation corresponding to  $M^{\phi^{i_k}}$ , so  $H_k \leq GL(7, q)$  or  $H_k \leq GL(27, q)$ , and let  $\psi_k : G \rightarrow H_k$  be an isomorphism. Our goal is then to find  $\psi_k$  explicitly for some  $k$ .

For  $\lambda \in \mathbb{F}_q^\times$  denote  $E_\lambda = \{1, \lambda^{\pm t}, \lambda^{\pm(t-1)}, \lambda^{\pm(2t-1)}\}$  and  $S_\lambda = \{xy \mid x \in E_\lambda, y \in E_\lambda\}$ . We need the following conjectures.

**Conjecture 4.1.** *Let  $\text{Ree}(q) \cong G \leq GL(d, q)$  with module  $W$  of the form (2.1), with  $\dim W = d = 7^n$  for some  $n > 1$ .*

*Let  $g \in G$  have order  $q-1$  and let  $E$  be its multiset of eigenvalues. If  $2m > n$  then there exists  $\lambda \in \mathbb{F}_q^\times$  such that  $E_\lambda \subset E$  and the sum of the eigenspaces of  $g$  corresponding to  $E_\lambda$  has dimension  $\dim V$ .*

**Conjecture 4.2.** *Let  $\text{Ree}(q) \cong G \leq GL(d, q)$  with module  $W$  of the form (2.1) and  $\dim W = d > 7$ . Let  $j \in G$  be an involution.*

*If there are tensor factors both of dimension 7 and 27, then  $W|_{C_G(j)}$  has unique submodules  $W_3$  and  $W_4$  of dimensions 3 and 4 respectively, such that  $W_3 + W_4$  is a point of  $W$  of dimension 7.*

**Conjecture 4.3.** *Let  $\text{Ree}(q) \cong G \leq GL(d, q)$  with module  $W$  of the form (2.1) and  $\dim W = 27^n$  for some  $n > 1$ . Let  $j \in G$  be an involution and let  $H = C_G(j)'$ .*

*If  $2m > n$  then  $\dim \text{Hom}_H(S_H^{q^i}, W_H) = 5$  for some  $0 \leq i \leq 2m$ .*

**Theorem 4.4.** *Assuming Conjecture 4.1 and given a random element oracle for subgroups of  $GL(d, q)$  with time complexity  $O(\xi(d))$  field operations, there exists a Las Vegas algorithm that, given  $\langle X \rangle \leq GL(d, q)$ , where  $q = 3^{2m+1}$ ,  $d = 7^n$ ,  $n > 1$ ,  $2m > n$  and  $\langle X \rangle \cong \text{Ree}(q)$ , with module  $W$  of the form (2.1), finds a point of  $W$ . The algorithm has time complexity*

$$O(\xi(d) + d^3 \log(q) \log \log(q^d))$$

*field operations.*

*Proof.* Let  $G = \langle X \rangle$ . By [1, Lemma 2.7], we can easily find  $g \in G$  such that  $|g| \mid q-1$ . Our approach is to construct a point as a suitable sum of eigenspaces of  $g$ . We know that for  $k = 0, \dots, n-1$ ,  $\psi_k(g)$  has 7 eigenvalues  $\lambda_k^{\pm t}, \lambda_k^{\pm(t-1)}, \lambda_k^{\pm(2t-1)}$  and 1 for some  $\lambda_k \in \mathbb{F}_q^\times$ . Let  $E$  be the multiset of eigenvalues of  $g$ . Each eigenvalue has the form

$$\lambda_0^{j_0} \lambda_1^{j_1} \dots \lambda_{n-1}^{j_{n-1}} \quad (4.1)$$

where each  $\lambda_k \in \mathbb{F}_q^\times$  and each  $j_k \in \{\pm t, \pm(t-1), \pm(2t-1), 1\}$ . We can easily compute  $E$ .

Because each  $\lambda_k^{j_k}$  may be 1, for each  $k = 0, \dots, n-1$  we have  $E_{\lambda_k} \subset E$ . We can determine which  $\lambda \in E$  can be one of the  $\lambda_k$  since if  $\lambda = \lambda_k$  for some  $k$  then  $E_{\lambda^{3t}} \subset E$ .

Thus we can get a list with length between  $n$  and  $d$  of subsets  $E_\lambda$  of  $E$ . Now Conjecture 4.1 asserts that there is some  $\mu \in \mathbb{F}_q^\times$  such that  $E_\mu \subset E$  and such that the sum of the eigenspaces corresponding to  $E_\mu$  has dimension 7, and by its construction it must therefore be a point of  $W$ . Since  $\mu^t \in E$ , the set  $E_\mu$  will be on our list, and we can easily find the point.

The algorithm is Las Vegas since we can easily calculate the dimensions of the subspaces. The complexity of finding  $g$  is  $O(\xi(d))$  field operations, and by [7] we can find its order using  $O(d^3 \log(q) \log \log(q^d))$  field operations. We find the characteristic polynomial using  $O(d^3)$  field operations and then find the eigenvalues using  $O(d(\log d)^2 \log \log(d) \log(dq))$  field operations (see [22, Corollary 14.16]). Hence the time complexity is as stated.  $\square$

**Theorem 4.5.** *Assuming Conjecture 4.2 and given a random element oracle for subgroups of  $\text{GL}(d, q)$  with time complexity  $O(\xi(d))$  field operations, there exists a Las Vegas algorithm that, given  $\langle X \rangle \leq \text{GL}(d, q)$ , where  $q = 3^{2m+1}$ ,  $7 \mid d$  and  $\langle X \rangle \cong \text{Ree}(q)$ , with module  $W$  of the form (2.1), finds a point of  $W$ . The algorithm has time complexity*

$$O(\xi(d) + d^3 \log(q)(\log \log(q^d) + |X|))$$

*field operations.*

*Proof.* Let  $G = \langle X \rangle$ . Similarly as in [1, Corollary 6.8], we find an involution  $j \in G$  and probable generators for  $C_G(j)$ . Using the MeatAxe, we find the composition factors of  $W|_{C_G(j)}$ . For each pair of factors of dimensions 3 and 4 we compute module homomorphisms into  $W|_{C_G(j)}$  and then find the sum of their images.

Conjecture 4.2 asserts that this will produce a point of  $W$ . We can easily calculate the dimensions of the submodules and hence verify that we do obtain a point, so the algorithm is Las Vegas.

The time complexity to find  $j$  is  $O(\xi(d))$  field operations, and by [7] we can find its order using  $O(d^3 \log(q) \log \log(q^d))$  field operations. From the proof of [1, Corollary 6.8] we see that we can find  $C_G(j)$  using  $O(d^3)$  field operations. The MeatAxe uses  $O(d^3 \log(q) |X|)$  field operations and the rest of the algorithm is just linear algebra.  $\square$

**Theorem 4.6.** *Assuming Conjecture 4.3 and given a random element oracle for subgroups of  $\text{GL}(d, q)$  with time complexity  $O(\xi(d))$  field operations, there exists a Las Vegas algorithm that, given  $\langle X \rangle \leq \text{GL}(d, q)$ , where  $q = 3^{2m+1}$ ,  $d = 27^n$ ,  $n > 1$ ,  $2m > n$  and  $\langle X \rangle \cong \text{Ree}(q)$ , with module  $W$  of the form (2.1), finds a point of  $W$ . The algorithm has time complexity*

$$O(\xi(d) + d^3 \log(q)(\log \log(q^d) + |X|))$$

*field operations.*

*Proof.* Let  $G = \langle X \rangle$ . Similarly as in [1, Corollary 6.8], we find an involution  $j \in G$  and probable generators for  $H = C_G(j)' \cong \text{PSL}(2, q)$ . Using the MeatAxe, we find the composition factors of  $W_H$ . Let  $S_1$  be the group corresponding to a non-trivial composition factor. Using [9] we constructively recognise  $S_1$  as  $\text{PSL}(2, q)$  and obtain an explicit isomorphism  $\alpha : \text{PSL}(2, q) \rightarrow H$ .

Now let  $R$  be the image of the representation corresponding to  $S$ , so  $R \leq \text{GL}(27, q)$ . Again we find an involution  $j' \in R$  and probable generators for  $K =$

$C_R(j')' \cong \text{PSL}(2, q)$ . As above, we chop the module  $S_K$  with the MeatAxe, constructively recognise one of its factors and obtain an explicit isomorphism  $\beta : \text{PSL}(2, q) \rightarrow K$ .

Now  $\gamma = \alpha \circ \beta^{-1}$  is an explicit isomorphism between  $K$  and  $H$ . For each  $i = 0, \dots, 2m$ , do the following:

- (1) Find  $M = \text{Hom}_{\text{PSL}(2, q)}(S_K^{\phi^i}, W_H)$  using  $\gamma$ .
- (2) Find random  $f \in M$  such that  $\dim \text{Ker } f = 0$ .
- (3) Let  $U = \text{Im } f$  and use [16] to test if  $U$  is a point. If so then return  $U$ .

□

Even if Conjectures 4.1 and 4.3 are true, we still need another algorithm in the case  $2m \leq n$  and  $d = 7^n$ . Then  $q \in \mathcal{O}(d)$  so we are content with an algorithm that has time complexity polynomial in  $q$ . The approach is not to use the tensor decomposition algorithm of [16], since in this case we have no efficient method of finding a flat. Instead we find an explicit isomorphism from  $G$  to  $\text{Ree}(q)$  using permutation group techniques, then enumerate all tensor products of the form (2.1) and for each one we determine if it is isomorphic to  $W$ .

**Lemma 4.7.** *Given a random element oracle for subgroups of  $\text{GL}(d, q)$  with time complexity  $\mathcal{O}(\xi(d))$  field operations, there exists a Las Vegas algorithm that, given  $X \subseteq \text{GL}(d, q)$  such that  $q = 3^{2m+1}$  with  $m > 0$  and  $\langle X \rangle \cong \text{Ree}(q)$ , finds an explicit injective homomorphism  $\Pi : \langle X \rangle \rightarrow \text{Sym}(O)$  where  $|O| = q^3 + 1$ . The algorithm has time complexity  $\mathcal{O}(\xi(d) + |X| d^2(d^2 \log(q) + q^3))$  field operations.*

*Proof.* By [1, Proposition 2.2],  $\text{Ree}(q)$  acts doubly transitively on a set of size  $q^3 + 1$ . Hence  $G = \langle X \rangle$  also acts doubly transitively on  $O$ , where  $|O| = q^3 + 1$ , and we can find the permutation representation of  $G$  if we can find a point  $P \in O$ . The set  $O$  is a set of projective points of  $\mathbb{F}_q^d$ , and the algorithm proceeds as follows.

- (1) Choose random  $g \in G$ . Determine if  $|g| \mid q - 1$  and return with failure if not.
- (2) Choose random  $x \in G$  and let  $h = g^x$ . Let  $M$  be the natural module of  $\langle g, h \rangle$ . Determine if  $M$  is reducible and return with failure if not.
- (3) Find a composition series for  $M$  and let  $P \subseteq M$  be the submodule of dimension 1 in the series.
- (4) Find the orbit  $O = P^G$  and compute the permutation group  $S \leq \text{Sym}(O)$  of  $G$  on  $O$ , together with an explicit isomorphism  $\Pi : G \rightarrow S$ .

By [1, Proposition 2.3], elements in  $G$  of order dividing  $q - 1$  fix two points of  $O$ , and hence  $\langle g, h \rangle \leq G_P$  for some  $P \in O$  if and only if  $g$  and  $h$  have a common fixed point. All composition factors of  $M$  have dimension 1, so a composition series of  $M$  must contain a submodule  $P$  of dimension 1. This submodule is a fixed point for  $\langle g, h \rangle$  and its orbit must have size  $q^3 + 1$ , since  $|G| = q^3(q^3 + 1)(q - 1)$  and  $|G_P| = q^3(q - 1)$ . It follows that  $P \in O$  and that  $M$  is reducible if and only if  $g$  and  $h$  have a common fixed point.

To find the orbit  $O = P^G$  we can compute a Schreier tree on the generators in  $X$  with  $P$  as root, using  $\mathcal{O}(|X| |O| d^2)$  field operations. Then  $\Pi(g)$  can be computed for any  $g \in \langle X \rangle$  using  $\mathcal{O}(|O| d^2)$  field operations, by computing the permutation on  $O$  induced by  $g$ . Hence  $\Pi$  is explicit, and  $S$  is found by computing the image of each element of  $X$ . Therefore the algorithm is correct and it is clearly Las Vegas.

Finding  $g$  and  $h$  uses  $\mathcal{O}(\xi(d))$  field operations. Finding a composition series for  $M$  using [12] and [13] uses  $\mathcal{O}(|X| d^4 \log(q))$  field operations. Thus the theorem follows. □

**Theorem 4.8.** *Given a random element oracle for subgroups of  $\text{GL}(d, q)$  with time complexity  $\mathcal{O}(\xi(d))$  field operations, there exists a Las Vegas algorithm that, given*

$\langle X \rangle \leq \text{GL}(d, q)$ , where  $q = 3^{2m+1}$ ,  $n > 1$  and  $d = 7^n$  or  $d = 27^n$  and  $\langle X \rangle \cong \text{Ree}(q)$ , with module  $W$  of the form (2.1), finds a tensor decomposition of  $W$ . The algorithm has time complexity  $O(\xi(d) + |X| d^2((d \binom{2m}{n-1} + d^2) \log(q) + q^3))$  field operations.

*Proof.* Let  $G = \langle X \rangle$ . The algorithm proceeds as follows:

- (1) Find permutation representations  $\alpha : G \rightarrow S_1$  and  $\beta : \text{Ree}(q) \rightarrow S_2$  using Lemma 4.7, where  $S_1, S_2 \leq \text{Sym}(q^3 + 1)$ .
- (2) Find an isomorphism  $\theta : S_1 \rightarrow S_2$  using [6].
- (3) Let  $\gamma = \beta^{-1} \circ \theta \circ \alpha$ ,  $H = \gamma(G)$  and let  $V$  be the module of  $H$ . If  $3 \mid d$  then replace  $V$  with the 27-dimensional composition factor of  $\mathcal{S}^2(V)$ .
- (4) Construct each module of dimension  $d$  of the form (2.1) using  $V$  as base. For each one test if it is isomorphic to  $W$ , using [12] and [13].
- (5) Return the change of basis from the successful isomorphism test.

The returned change of basis exhibits  $W$  as a tensor product, so by Lemma 4.7 the algorithm is Las Vegas.

The number of modules of dimension  $d$  of the form (2.1) using  $V$  as base is  $\binom{2m}{n-1}$ . Module isomorphism testing uses  $O(|X| d^3 \log(q))$  field operations. Hence by [6] and Lemma 4.7 the time complexity of the algorithm is  $O(\xi(d) + |X| d^2(d^2 \log(q) + q^3) + |X| d^3 \log(q) \binom{2m}{n-1})$  field operations, and the result follows.  $\square$

We are now ready to state the main constructive recognition algorithm.

**Corollary 4.9.** *Assuming Conjectures 4.1, 4.2 and 4.3, and given a random element oracle for subgroups of  $\text{GL}(d, q)$  with time complexity  $O(\xi(d))$  field operations and an oracle for the discrete logarithm problem in  $\mathbb{F}_q$ , there exists a Las Vegas algorithm that, given  $X \subseteq \text{GL}(d, q)$ , where  $q = 3^{2m+1}$ ,  $m > 0$ ,  $d > 7$  and  $\langle X \rangle \cong \text{Ree}(q)$ , finds an explicit isomorphism  $\Psi : \langle X \rangle \rightarrow \text{Ree}(q)$ . The algorithm has time complexity  $O(\xi(d) + d^3 \log(q)(\log \log(q^d) + |X|) + |X| d^5)$  field operations.*

*Proof.* Let  $W$  be the given module of  $G = \langle X \rangle$ . The algorithm proceeds as follows:

- (1) If  $3 \nmid d$  then  $d = 7^n$  for some  $n > 1$ . If  $2m > n$  then use Theorem 4.4 to find a flat  $L \leq M$ . If  $3 \mid d$  but  $d$  is not a power of 27 then use Theorem 4.5 to find such an  $L$ . Otherwise  $d = 27^n$  for some  $n > 1$ . If  $2m > n$  then use Theorem 4.6 to find a flat  $L \leq M$ .
- (2) Use [16] with  $L$  to get  $x \in \text{GL}(d, q)$  such the change of basis determined by  $x$  exhibits  $W$  as a tensor product  $A \otimes B$  with  $\dim A = 7$  or  $\dim A = 27$ . If  $d = 7^n$  or  $d = 27^n$  and  $2m \leq n$  then use Theorem 4.8 to find  $x$ . Let  $G_A$  and  $G_B$  be the images of the corresponding representations.
- (3) Define  $\rho_A : G_A \otimes G_B \rightarrow G_A$  as  $g_a \otimes g_b \mapsto g_a$  and let  $Y = \{\rho_A(g^x) \mid g \in X\}$ . If  $\dim A = 27$  then let  $\theta$  be the explicit isomorphism from Theorem 3.2, otherwise let  $\theta$  be the identity map.
- (4) Let  $Z = \{\theta(x) \mid x \in Y\}$ . Then  $\langle Z \rangle$  is conjugate to  $\text{Ree}(q)$ . Use [1, Theorem 7.4] to obtain  $y \in \text{GL}(7, q)$  such that  $\langle Z \rangle^y = \text{Ree}(q)$ .
- (5) An explicit isomorphism  $\Psi : G \rightarrow \text{Ree}(q)$  is given by  $g \mapsto \theta(\rho_A(g^x))^y$ .

The map  $\rho_A$  is straightforward to compute, since given  $g \in \text{GL}(d, q)$  it only involves dividing  $g$  into submatrices of degree  $d/7$  or  $d/27$ , checking that they are scalar multiples of each other and returning the 7 by 7 or 27 by 27 matrix consisting of these scalars. Hence by Theorem 4.4, Theorem 4.5, Theorem 4.6, [16], Theorem 3.2 and [1, Theorem 7.4], the algorithm is Las Vegas, and  $\Psi$  can be computed using  $O(d^3)$  field operations.

In the case where we use Theorem 4.8 we have  $2m \leq n$  and hence  $q < 3d$ . We see that the  $\binom{2m}{n-1} \leq n$  and the time complexity of the algorithm to find  $x$  in Theorem 4.8 simplifies to  $O(\xi(d) + |X| d^5)$ .

In the other cases, by Theorem 4.5 finding  $L$  uses  $O(\xi(d) + d^3 \log(q)(\log \log(q^d) + |X|))$  field operations. From [16], finding  $x$  uses  $O(d^3 \log(q))$  field operations when a flat  $L$  is given.

From Theorem 3.2 finding  $\theta$  uses  $O(|Y| \log(q))$  field operations, and from [1, Theorem 7.4], finding  $y$  uses  $O(\log(q)(\log \log(q) + |Z|))$  field operations.  $\square$

#### APPENDIX A. IMPLEMENTATION AND PERFORMANCE

Implementations of the algorithms are available in MAGMA. The implementations uses the existing MAGMA implementations of the algorithms described in [3], [5], [7], [8], [9], [10], [12], [16] and [22, Corollary 14.16].

All benchmarks were carried out using MAGMA V2.12-20, on a PC with an Intel Xeon CPU running at 2.8 GHz and with 1 GB of RAM.

We used the software package R (see [18]), to produce the figures.

## REFERENCES

1. Henrik Bäärnhielm, *Recognising the Ree groups in their natural representations*, (2006), preprint.
2. L. Babai, *Local expansion of vertex-transitive graphs and random generation in groups*, Proc. 23rd ACM Symp. Theory of Computing (Los Angeles), Association for Computing Machinery, 1991, pp. 164–174.
3. L. Babai, W. M. Kantor, P. P. Pálffy, and Á. Seress, *Black-box recognition of finite simple groups of Lie type by statistics of element orders*, J. Group Theory **5** (2002), 383–401.
4. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
5. J. N. Bray, *An improved method for generating the centraliser of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.
6. J. J. Cannon and D. F. Holt, *Automorphism group computation and isomorphism testing in finite groups*, J. Symbolic Comput. **35** (2003), no. 3, 241–267.
7. F. Celler and C. R. Leedham-Green, *Calculating the order of an invertible matrix*, Groups and Computation II (Larry Finkelstein and William M. Kantor, eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 28, American Mathematical Society, 1997, pp. 55–60.
8. F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O’Brien, *Generating random elements of a finite group*, Comm. Algebra (1995), no. 23, 4931–4948.
9. M. D. E. Conder, C. R. Leedham-Green, and E. A. O’Brien, *Constructive recognition of  $PSL(2, q)$* , Trans. Amer. Math. Soc. **358** (2006), 1203–1221.
10. S. P. Glasby, C. R. Leedham-Green, and E. A. O’Brien, *Writing projective representations over subfields*, J. Algebra **295** (2006), 51–61.
11. D. F. Holt, B. Eick, and E. A. O’Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC, January 2005.
12. D. F. Holt and S. Rees, *Testing modules for irreducibility*, J. Austral. Math. Soc. Series A **57** (1994), 1–16.
13. G. Ivanyos and K. Lux, *Treating the exceptional cases of the MeatAxe*, Experiment. Math. **9** (2000), 373–381.
14. V. Landazuri and G. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.
15. C. R. Leedham-Green, *The computational matrix group project*, Groups and Computation III, Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, 2001, pp. 113–121.
16. C. R. Leedham-Green and E. A. O’Brien, *Recognising tensor products of matrix groups*, Internat. J. Algebra Comput. **7** (1997), 541–559.
17. ———, *Tensor products are projective geometries*, J. Algebra **189** (1997), 514–528.
18. R Development Core Team, *R: A language and environment for statistical computing*, R Foundation for Statistical Computing, Vienna, Austria, 2005, 3-900051-07-0.
19. G. M. Seitz and A. E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley groups, ii*, J. Algebra **158** (1993), 233–243.
20. Á. Seress, *Permutation group algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, 2003.
21. R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56.
22. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 2nd ed., Cambridge University Press, Cambridge, 2003.

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY, UNIVERSITY OF LONDON, MILE END ROAD, LONDON E1 4NS, UNITED KINGDOM

URL: <http://www.maths.qmul.ac.uk/~hb/>

E-mail address: [h.baarnhielm@qmul.ac.uk](mailto:h.baarnhielm@qmul.ac.uk)