

# A reduction algorithm for matrix groups with an extraspecial normal subgroup

*Peter Brooksbank, Alice C. Niemeyer and Ákos Seress* \*

**Abstract.** We describe an algorithm which, for any given group  $G$  containing an absolutely irreducible, extraspecial normal subgroup, constructs a homomorphism, with nontrivial kernel, from  $G$  onto a nontrivial group of permutations or matrices. Thus we reduce the problem of computing with  $G$  to two smaller problems. The algorithm, which uses a blend of geometric and black-box techniques, forms part of the broader project to determine the structure of an arbitrary matrix group.

2000 Mathematics Subject Classification: 20H30, 20P05, 20C40

## 1. Introduction

Computation with matrix groups is currently one of the most active areas of computational group theory. There are two basic kinds of algorithms: *reduction* and *solution of the word problem*. We define these notions in the more general setting of black-box groups. A *black-box group* is a group whose elements are encoded (not necessarily uniquely) as 0-1 strings of uniform length  $N$ , equipped with an oracle (the “black box”) that performs standard group operations. Specifically, given any (strings representing)  $g, h \in G$ , one can compute (strings representing)  $gh$  and  $g^{-1}$ , and one can also decide whether  $g = 1$ . For a set of generators  $X$  of a group  $G$ , and  $g$  an element of  $G$ , a *straight-line program from  $X$  to  $g$*  is a sequence of expressions that encode a construction of  $g$  from the elements of  $X$ . One can think of a straight-line program as a shortcut for a long word in  $X$ .

**Definition 1.1.** We say that an algorithm *solves the word problem for a black-box group*  $G = \langle X \rangle$  if it constructs a new generating set  $Y$  from  $X$  by a sequence of black box operations, and sets up a procedure that, for any given  $g \in G$ , computes a straight-line program from  $Y$  to  $g$ .

We say that an algorithm is a *reduction algorithm for a black-box group*  $G$  if it defines a homomorphism  $\varphi : G \rightarrow H$  for some group  $H$  with nontrivial image, and sets up a procedure that, for any given  $g \in G$ , computes  $\varphi(g)$ .

---

\*This work forms a part of a research project funded by the Australian Research Council Discovery Grant DP0209706. The third author is partially supported by the NSA and the NSF.

There are two basic approaches to reduction algorithms for matrix groups. The *geometric approach*, summarized in [12] (see also [14] in this volume), tries to find a category in Aschbacher’s classification of matrix groups [1] to which the given group  $G = \langle X \rangle \leq \mathrm{GL}(n, q)$  belongs; it then computes a normal subgroup  $N \triangleleft G$  naturally associated with this category, and recursively handles  $G/N$  and  $N$ . By contrast, the *black-box group approach* of Babai and Beals [3] tries to determine the abstract group-theoretic structure of  $G$  and does not use the geometry associated with the matrix group action of  $G$ .

One of Aschbacher’s classes, usually denoted  $C_6$ , consists of matrix groups  $G \leq \mathrm{GL}(d, q)$  with  $d = r^n$  for some prime  $r$  dividing  $q - 1$ , such that  $G$  contains an extraspecial normal subgroup  $R$  of order  $r^{1+2n}$  (or maybe  $2^{2+2n}$  in the case  $r = 2$ ) acting absolutely irreducibly on  $\mathrm{GF}(q)^d$ . For such a group  $G$ , a direct application of the Babai–Beals method produces a permutation representation of  $G$ , of degree at most  $d^2$ , in polynomial time. However, a straightforward implementation does not seem to be practical, since the permutation domain consists of  $d \times d$  matrices. The geometric approach attempts to find (generators for)  $R$ , as well as matrix representation of the conjugation action of  $G$  on  $R/Z(R)$ , as a subgroup of  $\mathrm{GL}(2n, r)$ . So far, the geometric approach has been completed only for the case  $n = 1$  [13].

In this paper we present a reduction algorithm for  $C_6$  groups that blends the geometric and black box approaches. Like many algorithms that have been developed for matrix groups, ours is a randomized algorithm. A randomized algorithm is *Monte Carlo* if it always returns an output, but there is an uncomfortable possibility of error. However, our algorithm is of the *Las Vegas* variety: here any output is guaranteed to be correct, which is more comforting, but “failure” may also be reported. For either variety of algorithm, a lower bound on the probability that a (correct) output is returned – the *reliability* of the algorithm – may be prescribed by the user. The main theoretical result of this paper may be stated as follows.

**Theorem 1.2.** *Let  $R \leq \mathrm{GL}(d, q)$  be an absolutely irreducible, extraspecial group of order  $r^{1+2n}$ , or possibly  $2^{2+2n}$ , where  $d = r^n$  for some  $n \geq 2$ . Let  $G = \langle X \rangle$  be any given group such that  $R \triangleleft G \leq N := N_{\mathrm{GL}(d, q)}(R)$ , with  $G/RZ(G) \cong N/RZ(N)$  if  $n > 2$ . Then there exists a Las Vegas algorithm with  $O^\sim(\xi + |X|d^4\rho_F)$  running time that sets up a data structure for a nontrivial homomorphism  $\varphi: G \rightarrow H$ , where  $H = \mathrm{GL}(2m, r)$  or  $H = S_{r^m}$  for some  $m \in \{1, 2, \dots, n\}$ . The data structure requires  $O^\sim(d^2)$  memory and, given any  $g \in G$ ,  $\varphi(g)$  can be computed by a deterministic algorithm in  $O^\sim(d^3\rho_F)$  time.*

**Notation and complexity parameters:** We use the “soft” version of the  $O$ -notation:  $O^\sim(f(n))$  means  $O(f(n) \log^c f(n))$  for some absolute constant  $c$ . The parameter  $\rho_F$  denotes the time required for field operations in  $F = \mathrm{GF}(q)$ , and  $\xi$  is the time requirement for the construction of independent, (nearly) uniformly distributed random elements in  $G$ .

Although the analysis of our algorithm has only been completed for the special cases stated in the theorem, we do not anticipate any insurmountable problems in the general case. Indeed we have implemented the algorithm in GAP and tested

it on a wide variety of examples, of dimension  $d$  up to 250, and encountered no difficulties whatsoever.

## 2. Outline of the algorithm

Our algorithm consists of two main steps. Given  $G \leq \text{GL}(d, q)$  containing  $R \triangleleft G$  with  $R \cong r^{1+2n}$ , or possibly  $R \cong 2^{2+2n}$  in the case  $r = 2$ , it proceeds as follows:

- (1) Find a non-scalar  $u \in G$  such that  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is an elementary abelian  $r$ -group, and construct generators for  $U \leq \langle u^G \rangle$  such that  $U / (U \cap Z(G)) \cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$ .
- (2) Construct a subgroup  $A \leq U$  such that  $A / (A \cap Z(G)) \cong Z(U) / (Z(U) \cap Z(G))$ . If  $A / (A \cap Z(G))$  is trivial then set up a data structure that enables us to compute the conjugation action of any  $g \in G$  on the vector space  $U / (U \cap Z(G))$ ; if  $A / (A \cap Z(G))$  is nontrivial then construct the homogeneous components of the  $A$ -module  $\text{GF}(q)^d$ , and set up a data structure that enables us to compute the permutation action of any  $g \in G$  on the set of homogeneous components.

Step (1) is the part of the algorithm that has not yet been fully analyzed; it uses a mixture of geometric and black-box techniques and is described in Section 5. Step (2) uses geometric techniques and it is described in Section 6.

## 3. Extraspecial groups and their normalizers

Let  $r$  be a prime and  $R$  an  $r$ -group. For odd  $r$ ,  $R$  is called *extraspecial* if

$$Z(R) = \Phi(R) = R' \cong \mathbb{Z}_r. \quad (3.1)$$

If  $r = 2$  then we shall call a 2-group  $R$  extraspecial if it satisfies (3.1), or is a central product of  $\mathbb{Z}_4$  with a group satisfying (3.1). An extraspecial  $r$ -group is the central product of extraspecial  $r$ -groups of order  $r^3$ , and maybe one copy of  $\mathbb{Z}_4$  in the case  $r = 2$ , and thus has order  $r^{1+2n}$  or  $2^{2+2n}$  for some  $n$ . We are interested in extraspecial  $r$ -groups of exponent  $r \cdot \gcd(r, 2)$  and order at least  $r^5$ . If  $r$  is odd then there is only one group,  $R_0$  say, of order  $r^3$  and exponent  $r$ , whereas if  $r = 2$  the groups  $D_8$  and  $Q_8$  are extraspecial of exponent 4. If  $r$  is odd then there is exactly one extraspecial  $r$ -group of order  $r^{1+2n}$  and exponent  $r$  and this group is the central product of  $n$  copies of  $R_0$ . If  $r = 2$  then  $R$  is a central product of  $n - 1$  copies of  $D_8$  with either another  $D_8$  or a  $Q_8$ , and possibly a  $\mathbb{Z}_4$ . If all copies are  $D_8$  then we say that  $R$  has type  $2_+^{1+2n}$ ; if there is a copy of  $Q_8$  then the type is  $2_-^{1+2n}$ ; if there is a copy of  $\mathbb{Z}_4$  and there are  $n$  copies of  $D_8$  or  $Q_8$  (in any combination of these we get the same group  $R$ ) then the type is denoted  $2^{2+2n}$ .

Let  $R$  denote an extraspecial group of order  $r^{1+2n}$  or  $2^{2+2n}$ , with  $n \geq 2$  and exponent  $r \cdot \gcd(2, r)$ . Suppose that  $r \mid q - 1$ , and further  $4 \mid q - 1$  in the case of type  $2^{2+2n}$ . Then  $R$  has a faithful and irreducible representation of dimension  $d = r^n$  over  $GF(q)$ . Thus we may identify  $R$  with a subgroup of  $GL(d, q)$ , which we shall also call  $R$ . The members of the Aschbacher class  $C_6$  are subgroups  $G$  of  $N := N_{GL(d, q)}(R)$  containing  $R$ . The structure of  $N$  in each case is as follows.

$$\begin{aligned} Z(GL(d, q)) \circ r^{1+2n} \cdot \text{Sp}(2n, r) & \quad r \text{ odd,} \\ Z(GL(d, q)) \circ 2^{2+2n} \cdot \text{Sp}(2n, 2) & \quad r = 2, 4 \mid q - 1, \\ Z(GL(d, q)) \circ 2_+^{1+2n} \cdot \text{O}^+(2n, 2) & \quad r = 2, \\ Z(GL(d, q)) \circ 2_-^{1+2n} \cdot \text{O}^-(2n, r) & \quad r = 2. \end{aligned}$$

For an element  $g \in GL(d, q)$ , let  $o_g$  denote the *projective order* of  $g$  (the smallest positive integer  $m$  such that  $g^m$  is a scalar matrix). We say that an element of  $y \in G$  is *good* if it powers up to a noncentral element of  $RZ(G)$ ; that is, if  $r \mid o_y$  and  $y^{o_y/r} \in R \setminus Z(G)$ . Let  $\Pi(G)$  denote the proportion of good elements in  $G$ .

For the remainder of this section we will assume that  $G$  is a  $C_6$  group such that  $G/RZ(G) \cong N/RZ(N)$ . Thus if  $V$  denotes the  $2n$ -space  $R/Z(R)$ , then  $G$  induces  $\text{Sp}(2n, r)$  or  $\text{O}^\pm(2n, 2)$  on  $V$ ; we refer to these possibilities generically as  $\text{Cl}(V)$ .

We now prove two technical lemmas concerning the abundance of certain elements in such groups. These results are needed to establish the correctness and reliability of our main algorithm. The proofs make use of primitive prime divisors: for an integer  $k$ , a *primitive prime divisor* of  $r^k - 1$  is a prime  $s \mid r^k - 1$  such that  $s \nmid r^i - 1$  for  $i < k$ ; we say that a group element has  $\text{ppd}^\#(r; k)$ -*order* if its order is divisible by a primitive prime divisor of  $r^k - 1$ .

**Lemma 3.1.** *If  $G/RZ(G) \cong N/RZ(N)$ , then  $\Pi(G) \geq 1/\{8(n-1)r(r+1)\}$ .*

*Proof.* For  $y \in G$ , let  $\tilde{y}$  denote the automorphism of  $R$  induced by  $y$ , and let  $\tilde{G}$  denote the corresponding group of automorphisms. Then it is well known that  $\tilde{G} \cong V \cdot \text{Cl}(V)$ . (Griess [9] showed that this extension is nonsplit if and only if  $r = 2$  and  $n \geq 3$ .) Each  $\alpha \in \tilde{G}$  may be identified with an ordered pair  $(v_\alpha, T_\alpha)$ , where  $v_\alpha \in V$  and  $T_\alpha \in \text{Cl}(V)$ , with product  $(v_\alpha, T_\alpha)(v_\beta, T_\beta) = (v_\alpha + v_\beta T_\alpha, T_\alpha T_\beta)$  (see [8] for a treatment of the  $r = 2$  case). Evidently  $y \in G$  is good if and only if  $\tilde{y}^{|T_{\tilde{y}}|}$  is a nontrivial automorphism of  $R$ , where  $|T_{\tilde{y}}|$  is the order of the transformation  $T_{\tilde{y}}$ .

*Claim 1:* A coset  $yR$  in  $G/R$  contains a good element if and only if the transformation  $S_{\tilde{y}} := \sum_{i=0}^{|T_{\tilde{y}}|-1} T_{\tilde{y}}^i$  is nontrivial. Furthermore, if  $S_{\tilde{y}}$  is nontrivial, then at least half of the elements of  $yR$  are good.

*Proof of Claim 1:* Let  $v = v_{\tilde{y}}$ ,  $T = T_{\tilde{y}}$  and  $S = S_{\tilde{y}} = \sum_{i=0}^{|T|-1} T^i$ . Then an elementary calculation reveals that, for any positive integer  $k$ ,

$$(v, T)^k = \left( \sum_{i=0}^{k-1} vT^i, T^k \right).$$

Thus  $\tilde{y}^{|T|}$  is nontrivial if and only if  $v$  is not contained in the nullspace of  $S$ . The necessity of the condition in the claim is clear. As to the sufficiency, note that as  $x$  ranges over  $yR$ ,  $T_{\tilde{x}} = T_{\tilde{y}} = T$  is fixed and  $v_{\tilde{x}}$  ranges uniformly over  $V$ . In particular, if  $S$  is nontrivial, at least half of the elements  $x \in yR$  are such that  $v_{\tilde{x}}$  is not in the nullspace of  $S$ .

We complete the proof of the lemma by establishing the following claim.

*Claim 2:*  $\Pi(G) \geq 1/\{16(n-1)\}$  if  $r = 2$  and  $\text{Cl}(V)$  is orthogonal, and  $\Pi(G) \geq 1/\{8(n-1)r(r+1)\}$  if  $\text{Cl}(V)$  is symplectic.

*Proof of Claim 2:* By Claim 1 it suffices to compute the proportion of elements  $T \in \text{Cl}(V)$  for which  $\sum_{i=0}^{|T|-1} T^i \neq 0$ . Let  $c = 1$  if  $\text{Cl}(V) = \text{O}^+(2n, 2)$  and  $c = 2$  otherwise, and let  $T \in \text{Cl}(V)$  satisfy the following property:

$$T \text{ centralizes a hyperbolic line } \Lambda \text{ and induces an element} \quad (3.2) \\ \text{of } \text{ppd}^\#(r; c(n-1))\text{-order on the } (2n-2)\text{-space } \Lambda^\perp.$$

Note first that if  $T$  satisfies (3.2) then  $(|T|, r) = 1$  so the multiplicity of  $x-1$  in  $x^{|T|} - 1$  is one; consequently,  $x-1$  is not a factor of the polynomial  $\sum_{i=0}^{|T|-1} x^i = (x^{|T|} - 1)/(x - 1)$ . On the other hand (since  $T$  centralizes  $\Lambda$ )  $x-1$  is a factor of the minimal polynomial of  $T$ , which clearly divides  $x^{|T|} - 1$ . It follows that the minimal polynomial of  $T$  does not divide  $\sum_{i=0}^{|T|-1} x^i$  and so  $\sum_{i=0}^{|T|-1} T^i \neq 0$ . Hence, by Claim 1, we have  $\Pi(G) \geq \Pi'/2$ , where  $\Pi'$  is the proportion of elements of  $\text{Cl}(V)$  satisfying (3.2).

We now establish a lower bound for  $\Pi'$ .

Let  $\sigma$  denote the number of singular points of  $V$ . Then  $\sigma = r^{2n} - 1$ ,  $(r^n + 1)(r^{n-1} - 1)$  or  $(r^n - 1)(r^{n-1} + 1)$  in cases  $\text{Sp}$ ,  $\text{O}^-$  or  $\text{O}^+$ , respectively [17, p. 140]. Also, the number of hyperbolic lines in  $V$  is  $r^{2n-2}\sigma/(r^\delta + 1)$ , where  $\delta$  is 1 or 0 according as  $V$  is symplectic or orthogonal [17, pp. 70 and 141].

For a fixed hyperbolic line  $\Lambda$  of  $V$ , there are at least  $|\text{Cl}(\Lambda^\perp)|/\{4(n-1)\}$  elements of  $\text{Cl}(V)$  inducing an element of  $\text{ppd}^\#(r; c(n-1))$ -order on  $\Lambda^\perp$  and the identity on  $\Lambda$  [10, Lemma 2.5]. Hence, in each case, the total number of suitable elements of  $\text{Cl}(V)$  is at least

$$\gamma := \frac{r^{2n-2}\sigma}{r^\delta + 1} \cdot \frac{|\text{Cl}(\Lambda^\perp)|}{4(n-1)}.$$

It follows that  $\Pi' \geq \gamma/|\text{Cl}(V)|$ . Claim 2 now follows by computing  $\gamma/|\text{Cl}(V)|$  for each case: if  $V$  is symplectic, then  $\gamma/|\text{Cl}(V)| = 1/\{4(n-1)r(r+1)\}$ ; and if  $V$  is orthogonal (in which case  $r = 2$ ), then  $\gamma/|\text{Cl}(V)| = 1/\{8(n-1)\}$ .  $\square$

The next result will be used in an alternative method for producing noncentral elements of  $RZ(G)$  when  $r$  is odd.

**Lemma 3.2.** *Let  $r > 2$  and suppose that  $G/RZ(G) \cong N/RZ(N)$ . Let  $cRZ(G)$  denote the central coset of  $G/RZ(G)$ . Then the proportion of elements  $y \in G$  such that  $2|_{o_y}$  and  $y^{o_y/2} \in cRZ(G)$  is at least  $1/(8n)$ .*

*Proof.* Put  $\overline{G} = G/RZ(G) \cong \text{Sp}(2n, r)$  and, for  $y \in G$ , denote the coset  $yRZ(G) \in \overline{G}$  by  $\overline{y}$ . As in the proof of Lemma 3.1, there are at least  $|\text{Sp}(2n, r)|/4n$  elements of  $\text{Sp}(2n, r)$  of  $\text{ppd}^\#(r; 2n)$ -order. For any such element  $\overline{y}$ , at least one of  $\overline{y}$  and  $\overline{cy}$  has even  $\text{ppd}^\#(r; 2n)$ -order. It follows that the proportion of elements  $y \in G$  with  $\overline{y}$  of even  $\text{ppd}^\#(r; 2n)$ -order is at least  $1/(8n)$ ; for any such element  $y$ , we have  $y^{o_y/2} \in cRZ(G)$ .  $\square$

## 4. Algorithmic preliminaries

In this section we describe the general algorithmic techniques necessary for computing with matrix groups, as well as some technical subroutines needed in our main algorithm.

**Random group elements.** Randomized algorithms rely on finding random elements in groups. We say that an algorithm outputs a *nearly uniformly distributed* random element of a group  $G$  if each  $g \in G$  is output with probability at least  $1/(2|G|)$  and at most  $3/(2|G|)$ . There is a Monte Carlo algorithm [2] which, after some preprocessing, outputs independent, nearly uniformly distributed random elements at a cost of  $O(\log |G|)$  multiplications per random element. In practice, the product replacement algorithm [5],[15] is used for random element generation. After preprocessing, that algorithm outputs random elements at a cost of one or two multiplications per random element. We denote by

RANDOM( $G$ )

the procedure that produces random elements in a given matrix group  $G$  and, by  $\xi$ , an upper bound on the time required for a single call to this procedure.

**Projective orders.** The projective order of any given  $g \in \text{GL}(d, q)$  can be computed in  $O(d^4 \rho_F)$  time, provided that the prime factorizations of the numbers  $q^i - 1$  ( $i \leq d$ ) are known [4]. In our situation, the prime factors of  $o_g$  are bounded from above by a polynomial of  $d$ , and in this case the same time bound is valid even if the factorizations of the numbers  $q^i - 1$  are not known.

**Normal closures.** We use a Monte Carlo algorithm by Cooperman and Finkelstein [6] to compute normal closures. Their method is also described in [16, Lemma 2.3.8, Theorem 2.3.9, and Lemma 2.3.3], and is based on computations with random subproducts. Given a list  $L = (g_1, \dots, g_k)$  of elements of some group, a *random subproduct* of  $L$  is an instance  $g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$ , where the  $\varepsilon_i$  are uniformly distributed, independent,  $\{0, 1\}$ -valued random variables.

We now adapt the general method presented in [6] to our setting. The given group  $G$  is a  $C_6$  group with  $R \leq G \leq N_{\text{GL}(d, q)}(R) \leq \text{GL}(d, q)$ , where  $d = r^n$ . The input will always be a nonscalar matrix  $u \in G$  and there will be two possibilities: either

- (1)  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is abelian, or

(2)  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is non-abelian.

In the abelian case, we require generators for a subgroup  $H \leq \langle u^G \rangle$  such that  $H/(H \cap Z(G)) \cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$ . In the nonabelian case we only need generators for a subgroup  $H \leq \langle u^G \rangle$  such that  $H/(H \cap Z(G))$  is *not* abelian.

The following is a Monte Carlo algorithm to compute normal closures in this setting. The input is an element  $u \in G$  and a reliability parameter  $\delta$ .

**NORMALCLOSURE**( $u, \delta$ )

```

 $L := (u)$ ;
repeat  $\lceil 16n \log r \log(1/\delta) \rceil$  times
     $y :=$  random subproduct of  $L$ ;
     $x :=$  random subproduct of generators of  $G$ ;
    Add  $y^x$  to  $L$ ;
done;
return  $L$ ;

```

**Lemma 4.1.** *NORMALCLOSURE is a Monte Carlo algorithm which, with probability at least  $1 - \delta^{n/2}$ , returns a set  $L$  such that  $\langle L \rangle / (\langle L \rangle \cap Z(G)) \cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$ , or such that  $\langle L \rangle / (\langle L \rangle \cap Z(G))$  is nonabelian. The running time is  $O(d^3(|X| + \log d \log(1/\delta)) \log d \log(1/\delta))$ .*

*Proof.* Note that, if  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is abelian, then it is necessarily elementary abelian of exponent  $r$ , and order at most  $r^{2n}$ . Moreover, no abelian subgroup of  $G/Z(G)$  has order greater than  $r^{2n}$ .

If  $\langle L \rangle / (\langle L \rangle \cap Z(G)) \not\cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  then an execution of the repeat-loop adds  $y^x$  to  $L$  and this increases  $\langle L \rangle / (\langle L \rangle \cap Z(G))$  with probability at least  $1/4$ , by [16, Lemma 2.3.8]. Hence, applying [16, Lemma 2.3.3] with parameters  $\varepsilon = 1/2$ ,  $p = 1/4$ , and  $t = \lceil 16n \log r \log(1/\delta) \rceil$ , the output is correct with probability at least  $1 - \delta^{n/2}$ . The stated timing is for the  $O((|X| + \log d \log(1/\delta)) \log d \log(1/\delta))$  group multiplications used by the procedure.  $\square$

**Commutativity modulo scalars.** We conclude this section by giving a Monte Carlo algorithm which, for any given element  $u \in G$ , decides whether  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is abelian. We remark that our algorithm is *1-sided Monte Carlo*: if it decides that  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is nonabelian, then this answer is guaranteed to be correct. In that case, rather than return the answer “false”, the algorithm instead returns a nonscalar element of  $\langle u^G \rangle'$ , the derived subgroup of  $\langle u^G \rangle$ .

**TESTABELIAN**( $u, \delta$ )

```

 $L :=$  NORMALCLOSURE( $u, \delta/2$ );
repeat  $\lceil (4/3) \log(2/\delta) \rceil$  times
     $y :=$  random subproduct of  $L$ ;
     $x :=$  random subproduct of  $L$ ;
    if  $[x, y]$  is nonscalar then
        return  $[x, y]$ ;

```

**fi;**  
**done;**  
**return** “true” (i.e.,  $\langle u^G \rangle / (Z(G) \cap \langle u^G \rangle)$  is abelian);

**Lemma 4.2.** *TESTABELIAN is a Monte Carlo algorithm to test whether  $\langle u^G \rangle / (Z(G) \cap \langle u^G \rangle)$  is abelian. If this factor group is abelian, then the algorithm will return “true” with probability 1; if it is not, then the algorithm will return a non-scalar element of  $\langle u^G \rangle'$  with probability at least  $1 - \delta$ .*

*The algorithm runs in  $O(d^3(|X| + \log d \log(1/\delta)) \log d \log(1/\delta))$ -time.*

*Proof.* If  $\langle u^G \rangle / (Z(G) \cap \langle u^G \rangle)$  is abelian, then it is clear that the algorithm behaves as stated. If  $\langle u^G \rangle / (Z(G) \cap \langle u^G \rangle)$  is not abelian then the commutator  $[x, y]$ , computed in an execution of the repeat-loop, is nonscalar with probability at least  $1/4$  by [16, Lemmas 2.3.11, 2.3.14]. Thus TESTABELIAN( $u, \delta$ ) returns the correct output with probability at least  $1 - \delta$  (because with probability at least  $1 - \delta/2$ , the normal closure computation returns a set  $L$  such that  $\langle L \rangle / (\langle L \rangle \cap Z(G))$  is non-abelian; and then, with probability at least  $1 - \delta/2$ , a nontrivial commutator is computed). Again the stated timing reflects the number of group operations used in the procedure.  $\square$

## 5. Step (1): Blind descent

Blind descent is one of the lovely ideas of Babai and Beals [3]. Suppose that an element chosen at random from  $G$  is unlikely to lie in a proper normal subgroup of  $G$ . Suppose further that we cannot (or are not willing to) test whether any given element belongs to a proper normal subgroup. Blind descent is a Monte Carlo procedure that, with high probability, constructs a nontrivial element of  $G$  lying in a proper normal subgroup  $K$  of  $G$ . The basic idea is to construct a sequence of random elements  $(g_1, \dots, g_k)$  in  $G$ , as well as all of the commutators  $c_2 = [g_1, g_2]$ ,  $c_i = [c_{i-1}, g_i]$  for  $3 \leq i \leq k$ . If *any* of the  $g_i$  belongs to the proper normal subgroup  $K$ , then  $c_k \in K$ . A complication to be considered is that one of the commutators  $c_i$  is trivial; then either  $c_{i-1} \in Z(G)$ , or a suitable random conjugate  $g_i^x$  of  $g_i$  can be used to define  $c_i = [c_{i-1}, g_i^x] \neq 1$ .

For the remainder of the paper,  $R$  will denote an absolutely irreducible extraspecial  $r$ -subgroup of  $\mathrm{GL}(d, q)$ , and  $N := N_{\mathrm{GL}(d, q)}(R)$  will denote its normalizer. For any given  $G = \langle X \rangle \leq \mathrm{GL}(d, q)$  with  $R \triangleleft G \leq N$ , the goal in this section is to find some  $u \in G \setminus Z(G)$  such that  $\langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is an elementary abelian  $r$ -group. This is achieved using a slight modification of the above black-box blind descent procedure, taking advantage of some geometric properties of  $G$ . Specifically, we can compute projective orders of elements, we can easily test whether any given  $g \in G$  is in  $Z(G)$  (since  $Z(G)$  consists of scalar matrices), and we can also test whether  $\langle u^G \rangle$  has the desired structure.

The procedure `BLINDDESCENT` takes as input a group  $G \leq \text{GL}(d, q)$  and  $\delta > 0$ . The output is either a list of generators for a subgroup  $U \leq \langle u^G \rangle$  with  $U/(U \cap Z(G)) \cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  abelian, or “failure”.

```

BLINDDESCENT( $G, \delta$ )
1   $x := \text{RANDOM}(G)$ ;
2  repeat up to  $48n \log(1/\delta)$  times
3     $y := \text{RANDOM}(G)$ ;
4     $o_y :=$  projective order of  $y$ ;
5    if  $r \mid o_y$  then
6      if TESTABELIAN( $y^{o_y/r}, \delta$ ) = “true” then
7        return NORMALCLOSURE( $y^{o_y/r}, \delta$ );
8      fi;
9    fi;
10   for primes  $p$  dividing  $o_y$  and for  $p = o_y$  do
11     if  $[x, y^{o_y/p}] \notin Z(G)$  then  $x := [x, y^{o_y/p}]$ ; fi;
12   od;
13    $o_x :=$  projective order of  $x$ ;
14   if  $r \mid o_x$  then
15     if TESTABELIAN( $x^{o_x/r}, \delta$ ) = “true” then
16       return NORMALCLOSURE( $x^{o_x/r}, \delta$ );
17     else
18        $x := \text{TESTABELIAN}(x^{o_x/r}, \delta)$ ;
19     fi;
20   else
21      $x := \text{TESTABELIAN}(x, \delta)$ ;
22   fi;
23 done;
24 return “failure”;

```

The timing of the procedure is  $O(\xi \log(1/\delta) + d^4 |X| \rho_F \log^3(1/\delta))$ . The main results in this section assert that `BLINDDESCENT`( $G, \delta$ ) succeeds with high probability whenever  $G$  is the full normalizer of the group  $R$  in  $\text{GL}(d, q)$ , or whenever  $d = r^2$ . We begin with a theoretical result that will be useful in both settings.

**Lemma 5.1.** *Let  $H$  be a finite group, and let  $A$  be an elementary abelian, normal  $r$ -subgroup of  $H$ . Then the following hold:*

- (i) *Let  $r > 2$ , and suppose that  $c \in H$  is a fixed element inducing  $-\text{Id}$  on  $A$ . Let  $b$  be any element of the coset  $cA$ . Then, for a uniformly distributed random element  $h \in H$  and any integer  $k$ , the conditional probability*

$$\text{Prob}(h^k = b \mid h^k \in cA) = \frac{1}{|A|}.$$

- (ii) *Let  $b \in H$  be a fixed element acting nontrivially on  $A$ . Then for any fixed coset  $C$  of  $A$  in  $H$ , and for a uniformly distributed random  $h \in C$ , the*

*conditional probability*

$$\text{Prob}([b, h] \neq 1 \mid [b, h] \in A) \geq 1 - \frac{1}{r}.$$

*Proof.* First let  $r > 2$  and let  $c$  be as in part (i). Then, for any  $a \in A$ , we have  $c^a = ca^2$ . Hence the  $H$ -conjugacy class of  $c$  contains  $cA$ , and it is clear that elements of a conjugacy class occur equally frequently as powers.

Next let  $r$  be any prime and let  $b \in H$  be as in part (ii). Suppose that  $[b, h] = 1$  for some  $h \in C$ , and consider  $ha$  for  $a \in A$ . Then  $[b, ha] = (a^{-1})^b [b, h] a = [b, a]$ . Thus  $[b, ha] = 1$  if and only if  $a$  is a fixed point for the action of  $b$  on  $A$ . Since  $b$  acts nontrivially, it has at most  $|A|/r$  fixed points. Hence the proportion of  $a \in A$  for which  $[b, ha] \neq 1$  is at least  $(|A| - |A|/r)/|A| = 1 - 1/r$ .  $\square$

**Lemma 5.2.** *Let  $G = \langle X \rangle \leq \text{GL}(d, q)$  be any given group satisfying  $R \triangleleft G$  and  $G/RZ(G) \cong N/RZ(N)$ . Then  $\text{BLINDDESCENT}(G, \delta)$  succeeds with probability greater than  $1 - 2\delta$ .*

*Proof.* We prove that  $\text{BLINDDESCENT}$  returns a (non-failure) output with probability at least  $1 - \delta$ , and that the probability that the output is correct is at least  $1 - \delta$ . The result then follows by combining these two estimates.

First consider the case  $r = 2$ . By Lemma 3.1, with probability at least  $1 - \delta$ , at least one of our  $48n \log(1/\delta)$  choices  $y \in G$  satisfies  $2|o_y$  and  $y^{o_y/2} \in RZ(G) \setminus Z(G)$ . For such a  $y$ , an output is returned on line 7 of  $\text{BLINDDESCENT}$ .

Next suppose that  $r$  is odd, and put  $H = G/Z(G)$  and  $A = RZ(G)/Z(G)$ . Let  $cA$  denote the central coset of  $H/A \cong \text{Sp}(2n, r)$ . If  $y \in G$  has even projective order, then  $\bar{y} := yZ(G)$  has even order in  $H$ . By Lemma 3.2, the probability that some choice  $y \in G$  has even projective order with  $\bar{y}^{o_y/2} \in cA$  is at least  $1/(8n)$ . For any such  $y$ , Lemma 5.1(i) ensures that  $\bar{y}^{o_y/2}$  is uniformly distributed in  $cA$ . Now if the current value of  $x$  is in  $G \setminus RZ(G)$ , then  $\bar{x} := xZ(G)$  acts nontrivially on  $A$ . It follows from Lemma 5.1(ii) that the commutator  $[\bar{x}, \bar{y}^{o_y/2}]$  is a nontrivial element of  $A$  with probability at least  $1 - 1/r$ .

This shows that for fixed  $y$ , the loop beginning on line 10 in  $\text{BLINDDESCENT}$  (with  $p = 2$ ) computes an element  $x \in RZ(G) \setminus Z(G)$  with probability

$$\frac{1}{8n} \left(1 - \frac{1}{r}\right) > \frac{1}{16n}.$$

Hence at least one of  $16n \log(1/\delta)$  choices  $y \in G$  gives rise to a suitable  $x$  on line 11 with probability at least  $1 - \delta$  (an output is then returned on line 16).

For arbitrary values of  $r$ , and no matter which line of  $\text{BLINDDESCENT}$  returned an output, the output is correct with probability at least  $1 - \delta$  because  $\text{NORMALCLOSURE}(z, \delta)$  succeeds with such probability.  $\square$

We next consider the case  $n = 2$ .

**Lemma 5.3.** *Let  $d = r^2$ , and suppose that some iteration of the main loop in  $\text{BLINDDESCENT}(G, \delta)$  constructs a nonscalar  $x \in K$  for some solvable normal*

subgroup  $K$  of  $G$ . Then, with probability greater than  $1 - 5\delta$ ,  $\text{BLINDDESCENT}(G, \delta)$  succeeds in at most four further iterations.

*Proof.* In successive iterations of the loop, line 18 or 21 constructs elements  $x$  in the subgroups of the derived series of  $K$ , or returns that for the current value of  $x$ ,  $\langle x^G \rangle$  is abelian modulo scalars. Thus, in at most three iterations, we construct some  $x$  for which  $\langle x^G \rangle$  is abelian modulo scalars because any solvable subgroup of  $\text{Sp}(4, r)$  has derived length at most 3, and so  $K''' \leq R$ . The probability that these iterations and the final normal closure computation succeed is at least  $1 - 5\delta$ , as stated.  $\square$

**Lemma 5.4.** *Let  $d = r^2$ , and let  $G = \langle X \rangle \leq \text{GL}(d, q)$  be a perfect subgroup of  $N$  containing nonscalar elements of  $R$ . Then  $\text{BLINDDESCENT}(G, \delta)$  succeeds with probability greater than  $1 - 6\delta$ .*

*Proof.* We consider the various possibilities for  $\overline{G} = G/(R \cap G) \leq \text{Sp}(4, r)$ , based on [11]. The solvable residuals of the maximal subgroups of  $\text{Sp}(4, r)$  are  $r^3 \cdot \text{SL}(2, r)$ ,  $r^{1+2} \cdot \text{SL}(2, r)$ ,  $\text{SL}(2, r) \times \text{SL}(2, r)$ ,  $\text{SL}(2, 5)$ ,  $\text{SL}(2, r^2)$ ,  $\text{SL}(2, r)$ ,  $2^{1+4} \cdot A_5$ ,  $2 \cdot A_6$ , as well as  $2 \cdot A_7$  in the case  $r = 7$  and  $A_5$  in the case  $r = 2$ . As perfect subgroups of these, we also have to consider  $r^3 \cdot \text{SL}(2, 5)$ ,  $r^{1+2} \cdot \text{SL}(2, 5)$ ,  $\text{SL}(2, 5) \times \text{SL}(2, r)$ ,  $\text{SL}(2, 5) \times \text{SL}(2, 5)$ , and  $A_5$  for odd  $r$ . (Note that we do not assume that  $G$  contains  $R$ , just that  $R \cap G$  contains nonscalar elements.)

If  $G/(R \cap G) \cong N/Z(N)$  then the result follows from Lemma 5.2.

Next consider the case  $\overline{G} \cong A_5$ . In any loop of  $\text{BLINDDESCENT}$ , if the current value of  $x$  is in  $G \setminus R$ , then for the next choice of the random element  $y$  we have  $\text{Prob}(\overline{y} \in C_{\overline{G}}(\overline{x})) \geq 1/20$ . Then, by Lemma 5.1(ii),  $\text{Prob}([x, y] \in R \setminus Z(R)) \geq 1/40$ . For such a choice  $y$ , line 11 with  $p = o_y$  reassigns  $x$  to a nonscalar element of  $R$ . Hence the procedure successfully finds such an  $x$  with probability at least  $1 - \delta$  after  $40 \log(1/\delta)$  elements  $y$  have been processed.

From now on, we may assume that  $r$  is odd because the perfect subgroups of  $\text{Sp}(4, 2)$  are covered by the previous two cases. In view of Lemma 5.3 we need merely show that  $\text{BLINDDESCENT}(G, \delta)$  constructs a nonscalar element  $x$  of a solvable normal subgroup of  $G$  with sufficiently high probability. (We will show in fact that for a suitable choice of  $y$  on line 3, such an  $x$  is constructed on line 11 with either  $p = 2$  or  $p = o_y$ .)

In the case  $\overline{G} \cong 2^{1+4} \cdot A_5$ , let  $\overline{K} = O_\infty(\overline{G})$  be the solvable radical of  $\overline{G}$ , so that  $\overline{G}/\overline{K} \cong A_5$ . As above, if  $x \in G$  with  $\overline{x} \notin \overline{K}$ , then  $\text{Prob}(\overline{y}\overline{K} \in C_{\overline{G}/\overline{K}}(\overline{x}\overline{K})) \geq 1/20$ . Putting  $H = \overline{G}/Z(\overline{G})$  and  $A = \overline{K}/Z(\overline{G})$ , by Lemma 5.1(ii) we see that  $[x, y]$  is a nonscalar element of a solvable normal subgroup of  $G$  with probability at least  $1/40$ . Hence line 11 (with  $p = o_y$ ) produces a suitable  $x$  with that probability.

All remaining cases fall into one of two categories, both of which are handled by considering involutions of  $G$ :

(1)  $Z(\overline{G})$  is elementary abelian of order 2 or 4 and every involution of  $\overline{G}$  is central; or

(2)  $\overline{G}$  is a (perfect) subgroup of a point stabilizer in  $\mathrm{Sp}(4, r)$  containing an extraspecial normal subgroup of order  $r^3$ .

For groups belonging to type (1), note that at least half of the elements of  $\overline{G}$  have even order. (For if  $\bar{t} \in \overline{G}$  is a fixed involution, and  $\bar{y}$  is any element, then at least one of  $\bar{y}$  and  $\bar{y}\bar{t}$  has even order.) Let  $H = G/Z(R \cap G)$  and let  $A = (R \cap G)/Z(R \cap G)$ . We consider the two possibilities for  $|Z(\overline{G})|$  separately.

If  $|Z(\overline{G})| = 2$  and  $y \in G$  has even order, then  $y^{o_y/2}$  induces  $-\mathrm{Id}$  on  $A$ . Following the now familiar argument, for any such  $y$  we have  $[x, y^{o_y/2}] \in R \setminus Z(G \cap R)$  with probability at least  $1/2$ . Hence line 11 (with  $p = 2$ ) produces a suitable  $x$  with probability at least  $1/4$ .

On the other hand, if  $|Z(\overline{G})| = 4$ , then  $\overline{G} \cong 2.T_1 \times 2.T_2$  for some  $T_1, T_2 \in \{A_5, \mathrm{PSL}(2, r)\}$ . In this case the proportion of elements in  $2.T_i$  of order congruent to 2 mod 4 is at least  $1/4$ . It follows that, with probability at least  $1/16$ , the image  $\bar{y} = (\bar{y}_1, \bar{y}_2)$  in the factor group  $\overline{G} = 2.T_1 \times 2.T_2$  has both  $\bar{y}_1$  and  $\bar{y}_2$  of even order, but not divisible by 4. For any such element  $y$ ,  $y^{o_y/2}$  acts as  $-\mathrm{Id}$  on  $A$ . As in the  $|Z(\overline{G})| = 2$  case, line 11 produces a suitable  $x$  with probability at least  $1/32$ .

We now turn to the groups belonging to type (2). Suppose that  $\overline{G} \leq Y \times \mathrm{SL}(2, r)$ , where  $Y$  is extraspecial of order  $r^3$ . Here we put  $H = \overline{G}/Z(Y)$  and  $A = Y/Z(Y)$ . Then for any nonscalar involution  $t \in G$ ,  $\bar{t}Y$  is central in  $\overline{G}/Y$  and  $\bar{t}$  induces  $-\mathrm{Id}$  on  $A$ . Hence, if  $y$  is any element of even projective order, then  $c := [x, y^{o_y/2}]$  satisfies  $1 \neq \bar{c} \in Y$  with probability at least  $1/2$ . Furthermore, since  $\overline{G}$  has a factor group isomorphic to either  $\mathrm{SL}(2, r)$  or  $\mathrm{SL}(2, 5)$ , the proportion elements of  $G$  of even projective order is at least  $1/2$ . Hence line 11 produces a suitable  $x$  with probability at least  $1/4$ .  $\square$

By Lemmas 5.3 and 5.4, if the input group  $G \leq \mathrm{GL}(d, q)$  containing  $R$  is solvable or perfect then  $\mathrm{BLINDDDESCENT}(G, \delta)$  terminates successfully with probability at least  $1 - 6\delta$ . In order to handle the general case, we take the preparatory step of replacing  $G$  by its fourth derived subgroup  $G^{(4)}$  unless  $G^{(4)}$  consists of scalar matrices. (Note that if  $G^{(4)}$  consists of scalar matrices, then  $G$  is solvable.) If  $G$  is not solvable then  $G^{(4)}$  is perfect. It is possible that  $G^{(4)}$  does not contain all elements of  $R$ , but in this case we have  $G^{(4)} \cong r^{1+2}.T$  for  $T \in \{A_5, \mathrm{PSL}(2, r)\}$ , and Lemma 5.4 still applies.

The derived subgroup can be computed by collecting the commutators of pairs of generators, and then taking the normal closure of this set. A somewhat faster method is in [16, Theorem 2.3.12]. We note, however, that the proposed preparatory step may be omitted entirely in practice.

## 6. Step (2): Coordinatization

We now assume that the output of Step (1) is as desired, namely we have an element  $u \in G$ , and generators for a subgroup  $U \leq \langle u^G \rangle$  such that  $V := U/(U \cap$

$Z(G) \cong \langle u^G \rangle / (\langle u^G \rangle \cap Z(G))$  is an elementary abelian  $r$ -group. The first objective of this section is to obtain a decomposition of  $U$  as a central product

$$U = \langle e_1, f_1 \rangle \circ \cdots \circ \langle e_m, f_m \rangle \circ A, \quad (6.1)$$

where  $\langle e_i, f_i \rangle$  is an extraspecial group of order  $r^3$ , possibly extended by some scalars, and  $A$  is an abelian group. (It is possible that  $m = 0$ , in which case  $U$  is abelian.)

We will then consider two possibilities:

(1) *A consists entirely of scalar matrices.* In this case we output the homomorphism  $\varphi : G \rightarrow \text{GL}(2m, r)$  corresponding to the conjugation action of  $G$  on  $V$ . (Note that this action is nontrivial since  $m \geq 1$ , and the element  $uZ(G)$  must be moved by the conjugation action of  $G$ .) The construction of  $\varphi$  is described in Section 6.1.

(2) *A contains nonscalar matrices.* In this case, by Clifford's theorem, the homogeneous components of the  $A$ -module  $\text{GF}(q)^d$  are blocks of imprimitivity for  $G$ . We will construct this block system  $\{B_1, \dots, B_{r^\ell}\}$  and output the homomorphism  $\varphi : G \rightarrow S_{r^\ell}$  corresponding to the permutation action of  $G$  on the blocks. The construction of the block system and of  $\varphi$  is described in Section 6.2.

The following subroutine returns the decomposition (6.1). It takes as input a generating set  $Y$  for  $U$ , and returns a list  $L_1$  containing the elements  $e_i, f_i$ , as well as a list  $L_2$  containing generators for  $A$ .

DECOMPOSE( $Y$ )

$L_1 := \emptyset; L_2 := \emptyset;$

$gens := Y;$

**while**  $gens \neq \emptyset$  **do**

$g :=$  first element of  $gens$ ;

**if**  $g$  commutes with all  $x \in gens$  **then**

Add  $g$  to  $L_2$ ;

delete  $g$  from  $gens$ ;

**else**

$h :=$  an element of  $gens$  with  $[g, h] \neq 1$ ;

Add  $g, h$  to  $L_1$ ;

delete  $g, h$  from  $gens$ ;

compute the eigenspaces of  $g, h$ ;

replace each  $y \in gens$  by  $yg^i h^j$ , such that  $yg^i h^j$  fixes

each eigenspace of  $g$  and  $h$ ;

**fi**;

**od**;

**Lemma 6.1.** DECOMPOSE( $Y$ ) is a deterministic algorithm that returns a decomposition of  $\langle Y \rangle$  behaving as in (6.1). The running time is  $O(|Y|^2 \rho_F d^3)$ .

*Proof.* For the correctness of DECOMPOSE( $Y$ ), observe that for any  $x, y \in \langle Y \rangle$ , the eigenspaces of  $x$  are permuted by  $y$  and this permutation is trivial if and only

if  $x$  and  $y$  commute. Moreover, for a fixed  $x \in \langle Y \rangle$ , the permutations induced on the eigenspaces of  $x$  by the elements  $y \in \langle Y \rangle$  are all in the same cyclic group of order  $r$ . In the while loop of the procedure,  $g$  and  $h$  permute each other's eigenspaces cyclicly, so for any  $y \in gens$ , there exist powers  $g^i, h^j$  such that  $yg^i$  fixes the eigenspaces of  $h$  and  $yh^j$  fixes the eigenspaces of  $g$ . Consequently,  $yg^i h^j$  commutes with  $g$  and  $h$ .

We claim that each execution of the while loop runs in  $O(|Y|\rho_F d^3)$  time, and so the total time requirement is  $O(|Y|^2 \rho_F d^3)$ . Indeed, it can be checked in  $O(|Y|\rho_F d^3)$  time whether  $g$  commutes with every element of  $gens$ . If a noncommuting  $h \in gens$  is found then the eigenvalues of  $g$  can be obtained by computing  $g^r$ , which is a scalar matrix  $c \cdot \text{Id}$  for some  $c \in \text{GF}(q)^*$ , and then taking the  $r^{\text{th}}$  roots of  $c$ . This requires  $O(\rho_F d^3)$  time. One eigenspace  $E_1$  of  $g$  can be computed in  $O(\rho_F d^3)$  time, and the other eigenspaces  $E_2, \dots, E_r$  are obtained as the orbit of  $E_1$  under  $\langle h \rangle$ , in  $O(\rho_F d^3)$  time. The eigenspaces of  $h$  are computed by reversing the role of  $g$  and  $h$ . Finally, for  $y \in gens$ , taking some  $v_1 \in E_1$  and determining which  $E_i$  the vector  $y(v_1)$  belongs to, determines which power  $h^j$  must  $y$  be multiplied with. Hence  $yg^i h^j$  is computed in  $O(\rho_F d^3 \log r) = O(\rho_F d^3)$  time.  $\square$

### 6.1. $A$ consists of scalar matrices.

In this case, we output the set  $B = \{e_i, f_i \mid 1 \leq i \leq m\}$ , together with eigenspace bases for each member of  $B$  (these were already computed during the execution of  $\text{DECOMPOSE}(Y)$ ). Then  $B$  projects onto a basis for  $V$ .

It remains to describe how, for any given  $g \in G$ , the homomorphic image  $\varphi(g) \in \text{GL}(V)$  is computed. For each basis vector  $b \in B$ , we compute  $b^g \in U$  and find the coefficients of  $b^g$  in  $B$ . The latter task is accomplished by mimicking the construction of  $B$ : the permutation of the eigenspaces of  $e_i$  induced by  $b^g$  determines the coefficient of  $f_i$ ; similarly the coefficient of  $e_i$  is determined by the permutation of the eigenspaces of  $f_i$  induced by  $b^g$ . In this way, integers  $0 \leq \varepsilon_i, \psi_i < r$  ( $1 \leq i \leq m$ ) may be computed such that  $c := b^g \prod e_i^{-\varepsilon_i} f_i^{-\psi_i}$  fixes all eigenspaces of all  $e_i, f_i$ : then  $c$  is a scalar matrix. Hence the vector  $(\varepsilon_1, \psi_1, \dots, \varepsilon_m, \psi_m) \in \text{GF}(r)^{2m}$  is the  $b^{\text{th}}$  row of the matrix  $\varphi(g)$ .

The total cost of finding all coefficients of  $b^g$  is  $O(d^3 \rho_F)$ , and so computing the entire matrix  $\varphi(g)$  can also be done in  $O(d^3 \rho_F)$  time, since  $m = O(\log d)$ .

### 6.2. $A$ contains nonscalar matrices.

In this case, we discard the  $e_i, f_i$  and compute the homogeneous components of the  $A$ -module  $\text{GF}(q)^d$ . This is done the following way. Recall that  $A = \langle L_2 \rangle$ .

Let  $\alpha$  denote an  $r^{\text{th}}$  root in  $\text{GF}(q)^*$ . Since  $A$  is abelian, its elements are simultaneously diagonalizable (over  $\text{GF}(q)$  if  $r$  is odd, and over  $\text{GF}(q)$  or  $\text{GF}(q^2)$  if  $r = 2$ ). First we compute a basis change matrix  $M$  such that in the new basis  $B = \{v_1, \dots, v_d\}$  each element of  $A$  is diagonal. In the new basis  $B$ , any  $a \in L_2$  has a matrix of the form  $a = \text{diag}(a_1, \dots, a_d) = a_1 \text{diag}(1, a_2/a_1, \dots, a_d/a_1)$ , with

$a_1 \in \text{GF}(q^2)$  and  $a_i/a_1 \in \{\alpha^0, \alpha, \dots, \alpha^{r-1}\}$ . Then we compute equivalence classes of the basis vectors in  $B$  with  $v_i \sim v_j$  if and only if  $a_i/a_1 = a_j/a_1$  for all  $a \in L_2$ . These equivalence classes of basis vectors generate the homogeneous components  $B_1, \dots, B_{r^\ell}$ .

We claim that the procedure described in the previous paragraph requires  $O((rd^3|L_2| + |L_2|^2d^3)\rho_F) = O(d^{7/2}|Y|^2\rho_F)$  time. As described in the analysis of the subroutine `Decompose(Y)`, the eigenvalues of any  $y \in \langle Y \rangle$  can be computed in  $O(d^3\rho_F)$  time. The diagonalization of  $L_2$  can then be obtained in  $O(rd^3|L_2|\rho_F)$  time, in the following way: decompose  $\text{GF}(q)^d$  as the direct sum of eigenspaces of the first element of  $L_2$ ; then decompose each summand as the direct sum of eigenspaces of the second element of  $L_2$ , restricted on the summand, and so forth. Eventually  $\text{GF}(q)^d$  is written as the direct sum of common eigenspaces of all elements of  $L_2$ , and choosing the new basis vectors for  $\text{GF}(q)^d$  from the summands ensures that each element of  $A$  is diagonal in the new basis  $B$ . The transformation matrix  $M$  is just the concatenation of the elements of  $B$ . Writing the elements of  $L_2$  in  $B$  requires  $O(d^3|L_2|\rho_F)$  time. Finally, the computation of the equivalence classes of the basis vectors  $v_i$  is just a sorting algorithm on a set of sequences of length  $|L_2|$ , performed in  $O(d|L_2|\rho_F)$  time.

For any  $g \in G$ , the permutation  $\varphi(g)$  of the homogeneous components can be computed in  $O(d^3\rho_F)$  time as follows: write  $g$  relative to the new basis  $B$ ; for each  $1 \leq i \leq r^\ell$ , choose any basis vector  $v_i \in B_i$ ; and now use the matrix of  $g$  to read off the homogeneous component  $B_j$  that contains  $v_i^g$ .

**Acknowledgment:** We are indebted to Bill Kantor for a suggestion simplifying the coordinatization process in Section 6 and to Derek Holt for improving the presentation of Lemma 5.4. Derek Holt, Steve Linton, and Eamonn O'Brien helped with the construction of examples to test the implementation.

## References

- [1] Michael Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* 76 (3), pages 469–514, 1984.
- [2] László Babai, Local expansion of vertex-transitive graphs and random generation in finite groups, *Proc. 23rd ACM STOC*, pages 164–174, 1991.
- [3] László Babai and Robert Beals, A polynomial-time theory of black box groups, I, In *Groups St. Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lecture Note Ser.*, pages 30–64, Cambridge Univ. Press, Cambridge, 1999.
- [4] Frank Celler and C. R. Leedham-Green, Calculating the order of an invertible matrix, In *Groups and Computation, II (New Brunswick, NJ, 1995)*, volume 28 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 55–60, Amer. Math. Soc., Providence, RI, 1997.
- [5] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and E. A. O'Brien, Generating random elements of a finite group, *Comm. Algebra*

- 23 (13), pages 4931–4948, 1995.
- [6] Gene Cooperman and Larry Finkelstein, Combinatorial tools for computational group theory, In *Groups and Computation (New Brunswick, NJ, 1991)*, volume 11 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 53–86, Amer. Math. Soc., Providence, RI, 1993.
  - [7] The GAP Group, Aachen–St Andrews, GAP – Groups, Algorithms, and Programming, Version 4.4, <http://www.gap-system.org>, 2004.
  - [8] Steven P. Glasby, On the faithful representations, of degree  $2^n$ , of certain extensions of 2-groups by orthogonal and symplectic groups, *J. Austral. Math. Soc. Ser. A* 58 (2), pages 232–247, 1995.
  - [9] Robert L. Griess, Jr., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, *Pacific J. Math.* 48, pages 403–422, 1973.
  - [10] William M. Kantor and Ákos Seress, Black box classical groups Memoirs of the AMS, volume 149, Number 708, 2001.
  - [11] Peter Kleidman, The subgroup structure of some finite simple groups, PhD Thesis, Cambridge, 1987.
  - [12] Charles R. Leedham-Green, The computational matrix group project, In *Groups and Computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 229–247, de Gruyter, Berlin, 2001.
  - [13] Alice C. Niemeyer, A constructive recognition algorithm for normalisers of small extra-special groups as matrix groups, to appear in *Intern. J. Algebra Comp.*
  - [14] Eamonn A. O’Brien, Towards effective algorithms for linear groups, In this volume.
  - [15] Igor Pak, What do we know about the product replacement algorithm? In *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 301–347, de Gruyter, Berlin, 2001.
  - [16] Ákos Seress, *Permutation Group Algorithms*, volume 152 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 2003.
  - [17] Donald E. Taylor, *The Geometry of the Classical Groups*, volume 9 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1992.

Peter Brooksbank, Department of Mathematics, Bucknell University, Lewisburg, PA 17837, USA

Email: pbrooksb@bucknell.edu

Alice C. Niemeyer, School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia

Email: alice@maths.uwa.edu.au

Ákos Seress, Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA

Email: akos@math.ohio-state.edu