Writing projective representations over subfields

S.P. Glasby, C.R. Leedham-Green and E.A. O'Brien

Abstract

Let $G = \langle X \rangle$ be an absolutely irreducible subgroup of $\mathrm{GL}(d, K)$, and let F be a proper subfield of the finite field K. We present a practical algorithm to decide constructively whether or not G is conjugate to a subgroup of $\mathrm{GL}(d, F).K^{\times}$, where $K^{\times}$ denotes the centre of $\mathrm{GL}(d, K)$. If the derived group of G also acts absolutely irreducibly, then this algorithm is Las Vegas and costs $O(|X|d^3 + d^2 \log |F|)$ arithmetic operations in K. This work forms part of a recognition project based on Aschbacher's classification of maximal subgroups of $\mathrm{GL}(d, K)$.

1 Introduction

Let $F < K$ be finite fields. One of the classes of maximal subgroups of $\mathrm{GL}(d, K)$ in Aschbacher's classification theorem [1] is the set of conjugates of $\mathrm{GL}(d, F).K^{\times}$, where $K^{\times}$ denotes the centre of $\mathrm{GL}(d, K)$.

The *matrix recognition project* [10] seeks to develop a practical algorithmic version of this classification. As one component, we present an algorithm that takes as input a subset X of $\mathrm{GL}(d, K)$ and decides constructively whether or not $G := \langle X \rangle$ is conjugate to a subgroup of $\mathrm{GL}(d, F).K^{\times}$. If so, we obtain a conjugating matrix.

If we assume that G' acts absolutely irreducibly on the given KG-module, then we obtain a provably efficient algorithm which runs in polynomial time. An easy application of Clifford theory shows that if G is primitive, tensor-indecomposable, and not semilinear, then this hypothesis is satisfied.

If G acts absolutely irreducibly but G' does not, then the situation is more complicated. We present a simple practical algorithm to deal with this more general case. We also develop one illustrative component of a provably efficient algorithm based on an analysis of this situation following Clifford's theorem: the case where G' acts absolutely irreducibly on a block in a system of imprimitivity fixed by G'.

Underpinning our work is a new and highly efficient algorithm which solves the following special case of the more general problem: given an absolutely irreducible group

We thank Bill Kantor and Cheryl Praeger for their criticisms of drafts of this paper. This work was supported in part by the Marsden Fund of New Zealand via grant UOA 412. 2000 *Mathematics Subject Classification.* Primary 20C20, 20C40.

$G \leq \mathrm{GL}(d,K)$, decide whether or not G is conjugate to a subgroup of $\mathrm{GL}(d,F)$. This algorithm, which incorporates ideas from the MeatAxe [7], has Las Vegas complexity approximately $O(d^3)$ field operations in K; for a more precise statement see Theorem 2.1.

Glasby & Howlett [6] present an algorithm to answer this special case, which has similar complexity, given an oracle to construct discrete logarithms in F. For a description of discrete logarithm algorithms, see [15, Chapter 4]. Our algorithm avoids the use of the discrete logarithm, and hence its performance is demonstrably better if F is "large".

We summarise our notation. Throughout $\mathrm{GF}(q) = F < K = \mathrm{GF}(q^e)$ are finite fields, and $G \leq \mathrm{GL}(d,K)$ for some fixed $d > 1$. Also, $\mathrm{M}(d,K)$ denotes the K-algebra of $d \times d$ matrices over K, and $F[G]$ denotes the F-subalgebra of $\mathrm{M}(d,K)$ spanned by G. If G is conjugate to a subgroup of $\mathrm{GL}(d,F)$ we say that G can be *written over* F. If G is conjugate to a subgroup of $\mathrm{GL}(d,F).K^\times$, where $K^\times$ denotes the centre of $\mathrm{GL}(d,K)$, we say that G can be *written over F modulo scalars in K*.

We may view $V := K^d$ either as a module over the group algebra KG, or over the enveloping algebra $K[G] \subseteq \mathrm{M}(d,K)$. Note that G can be written over F if and only if the KG-module V has an FG-submodule of F-dimension d.

The organisation of the paper is as follows. In Section 2 we state our main results. In Section 3 we present our new algorithm to decide whether or not G can be written over F. In Section 4 we consider the case where the derived group G' acts absolutely irreducibly and, in this case, we present a provably efficient algorithm to decide whether or not G can be written over F modulo scalars in K. In Sections 5 and 6 we consider the general case where G' does not act absolutely irreducibly. We first outline a simple backtrack algorithm to decide whether or not G can be written over F modulo scalars in K. Next we analyse (following Clifford's theorem) the case where G' acts absolutely irreducibly on a block in a system of imprimitivity fixed by G'. Finally, we report on the performance of an implementation in Magma [2].

2 The main results

Our aim is to describe and analyse algorithms to decide whether or not an absolutely irreducible subgroup G of $\mathrm{GL}(d,K)$ can be written over F modulo scalars in K. Our first result is the following.

Theorem 2.1 *There is a Las Vegas algorithm that takes as input the finite fields $F < K$, and an absolutely irreducible group $G := \langle X \rangle \leq \mathrm{GL}(d,K)$, and decides in $O(|X|d^3)$ field operations in K, plus $O\tilde{}(d \log |F|)$ field operations in F, whether or not G is conjugate to a subgroup of $\mathrm{GL}(d,F)$. If so, then a conjugating matrix is returned; otherwise* false *is returned.*

That the algorithm is Las Vegas reflects the fact that random elements of $F[G]$ are used. Other relevant algorithms – including the critical MeatAxe [7] – rely on the use of such random elements. In Section 3, we prove that the probability that any random element of $F[G]$ will cause the algorithm to terminate is greater than an absolute constant. In practice, "low-quality" random elements of $F[G]$ will suffice and we assume that they can be obtained in $O(d^3)$ field operations in K.

The algorithm takes $O(d^3)$ field operations in K and $O\tilde{~}(d \log q)$ field operations in F to find the required change-of-basis matrix – namely, a basis for an FG-module V_0 that spans V as K-space; and $O(|X|d^3)$ field operations in K to conjugate the given generators by the change-of-basis matrix.

Our second main result is the following.

Theorem 2.2 *There is a Las Vegas algorithm that takes the same input as the algorithm in Theorem* 2.1*, but with the additional assumption that G' acts absolutely irreducibly on the given KG-module V; if G is conjugate to a subgroup of* $\mathrm{GL}(d, F)K^\times$*, it returns a conjugating matrix, or otherwise returns* false*. This algorithm has the same complexity as the algorithm in Theorem* 2.1*.*

As far as the matrix recognition project is concerned, Theorem 2.2 suffices. However, one may wish to write G over F (possibly modulo scalars in K) when G acts absolutely irreducibly, but G' does not. We generalise the algorithm of Theorem 2.2 in two ways. Firstly we observe that it suffices, for the algorithm in Theorem 2.1 to produce a positive answer, that we find for each $g \in X$ a scalar $k_g \in K^\times$ such that if g is replaced by $k_g g$ then the resulting set generates a group that can be conjugated into $\mathrm{GL}(d, F)$. We find such scalars by considering the elements of X in turn, and then carry out a backtrack search through all possible scalars. We can restrict the choice of scalars significantly as we discuss in Section 5. In many cases little or no backtracking is needed.

The second approach is to use Clifford's theorem to analyse the structure of the given KG-module V. This analysis becomes complicated, and raises questions that appear to us to be rather unnatural. For example, it may turn out that G' acts irreducibly but not absolutely irreducibly on V, in which case we could write G' in smaller dimension over a field L properly containing K. Suppose that $|L| = q^{ef}$, where $\gcd(e, f) = 1$. Then $L \cong K \otimes_F L_0$ where $L_0 = GF(q^f)$. We now have to decide whether or not a given LG'-module can be written over L_0 modulo scalars in K. Additional complications arise when G' consists entirely of scalars, so that Clifford's theorem cannot be usefully applied to G'. In Section 6 we illustrate this analysis when G' does not consist of scalars, and acts absolutely irreducibly on the homogeneous components of V, regarded as a KG'-module.

3 Writing G over F

We now prove Theorem 2.1 by presenting the relevant algorithm. Recall that G acts absolutely irreducibly on $V = K^d$. Underpinning the algorithm is the simple observation that, as with the question of reducibility, this problem can be set in the context of algebras rather than groups. Namely, *if G can be written over the smaller field F, then so can the F-algebra $F[G]$.*

The relevant algorithm is the following.

1. Repeatedly select a random $a \in F[G]$ until either the characteristic polynomial $c_a(t)$ of a does not lie in $F[t]$, or until $c_a(t) \in F[t]$ and a has an eigenvalue $\lambda \in F$ with multiplicity 1. In the former case return *false*, and in the latter proceed to the next step.

2. Find a non-zero λ-eigenvector v for a.

3. Construct sufficient images of v under the action of G to obtain a basis B of V.

4. Write the given generators of G with respect to the basis B, and return *false* if one does not lie in $\mathrm{M}(d, F)$. Otherwise return the conjugating matrix with rows B.

The algorithm relies on the following two theorems.

Theorem 3.1 *Let G be an absolutely irreducible subgroup of* $\mathrm{GL}(d, K)$*, and let F be a subfield of K. There is a subfield L of K containing F such that $F[G]$ is conjugate in* $\mathrm{GL}(d, K)$ *to the full matrix algebra* $\mathrm{M}(d, L)$*. Hence G can be written over L, but not over any proper subfield of L containing F.*

PROOF: Since $F[G]$ is a simple F-algebra, Wedderburn's structure theorem [5, p. 171] implies that $F[G] \cong \mathrm{M}(d', L)$ where L is a division algebra. Since L is finite, L is a field by another theorem of Wedderburn. Moreover, $F \subseteq Z(\mathrm{M}(d', L)) \subseteq C_{\mathrm{M}(d,K)}(F[G]) = K$. Therefore $L = Z(\mathrm{M}(d', L))$ satisfies $F \subseteq L \subseteq K$. Since K^d is an absolutely irreducible $K[G]$-module, $K[G] = \mathrm{M}(d, K)$ and so

$$\mathrm{M}(d', K) \cong \mathrm{M}(d', L) \otimes_F K = F[G] \otimes_F K \cong K[G] = \mathrm{M}(d, K).$$

Thus $d = d'$. By a generalization of the Skolem-Noether theorem [5, Theorem 4.9], the isomorphism $F[G] \cong \mathrm{M}(d, L)$ is induced by an inner automorphism of $\mathrm{M}(d, K)$. Therefore $F[G]$ can be written over L, but not over any proper subfield of L containing F. □

Theorem 3.2 *Let F be a proper subfield of a finite field L, and let a be a uniformly random element of* $\mathrm{M}(d, L)$*. Then the probability, π, that $c_a(t) := \det(tI - a)$ does not lie in $F[t]$ satisfies $\pi > \frac{2}{3}(1 - (|F|/|L|)^d) \geq 1/2$.*

PROOF: Let $f(t) \in L[t]$ be a monic polynomial of degree d, and let n_f denote the number of $a \in \mathrm{M}(d, L)$ such that $c_a(t) = f(t)$. An empirical observation is that $n_f \approx n_g$ if $f(t), g(t) \in L[t]$. Hence π is approximately $1 - (|F|/|L|)^d$. We shall make this argument rigorous.

Recall from [12] that $a \in \mathrm{M}(d, L)$ is *cyclic* if L^d is cyclic as an $L\langle a\rangle$-module. Fix a monic polynomial $f(t) \in L[t] - F[t]$ of degree d. By [12, p. 267]

$$\mathrm{Prob}(a \text{ is cyclic and } c_a(t) = f(t)) \geq \frac{|\mathrm{GL}(d, L)|}{|\mathrm{M}(d, L)|} \frac{1}{|L|^d - 1}.$$

Since $|L| > |F|$, it follows that $|L| \geq 4$. Thus

$$\frac{|\mathrm{GL}(d, L)|}{|\mathrm{M}(d, L)|} = \prod_{i=1}^{d} (1 - |L|^{-i}) > \prod_{i=1}^{\infty} (1 - 4^{-i}) > \frac{2}{3}.$$

Since there are $|L|^d - |F|^d$ choices for $f(t)$, we conclude that

$$\pi := \mathrm{Prob}(c_a(t) \notin F[t]) > \left(\frac{2}{3}\right) \frac{|L|^d - |F|^d}{|L|^d - 1} > \frac{2}{3} [1 - (|F|/|L|)^d]. \qquad \square$$

We now consider the correctness and complexity of our algorithm. By Theorem 3.1, $F[G]$ is isomorphic to the full matrix algebra $\mathrm{M}(d, L)$ where L is a field satisfying $F \subseteq L \subseteq K$. Suppose that, for some $\lambda \in F$, $a \in F[G]$ has a λ-eigenspace $\langle v\rangle$ that is of dimension 1 over K. The module $vF[G]$ is a direct sum, say $V_1 \dotplus V_2 \dotplus \cdots \dotplus V_r$, of irreducible submodules each isomorphic to L^d. Suppose that $v = v_1 + v_2 + \cdots + v_r$ where $v_i \in V_i$. Since $v \neq 0$, one of the v_i, without loss of generality v_1, is nonzero. Now $va = \lambda v$ implies that $v_i a = \lambda v_i$ for each i. Since the λ-eigenspace of a is 1-dimensional, there exist scalars $\xi_i \in K$ such that $v_i = \xi_i v_1$. Therefore $v = (1 + \xi_2 + \cdots + \xi_r)v_1$ and it follows that $vF[G]$ equals μV_1 where $\mu = 1 + \xi_2 + \cdots + \xi_r$. This shows that $r = 1$ and $vF[G]$ is an irreducible $\mathrm{M}(d, L)$-module.

Consider Step (1) of our algorithm. If $L \neq F$, then G cannot be written over F, and this can be detected with high probability by Theorem 3.2. It follows from [7, Section 2.3] that the probability that a random element of $\mathrm{M}(d, F)$ has an eigenvalue in F with multiplicity 1 is at least 2/7. Therefore the probability that Step (1) is performed n times is less than c^n for some constant $0 < c < 1$ independent of $d, |F|$ and $|K|$. We remark that the constants involved in our analysis can be reduced by choosing our random matrix a to be cyclic. For a discussion and analysis of the MEATAXE and cyclic matrices, see [12, 13].

If we progress to Step (2), we expect that $F[G] \cong \mathrm{M}(d, F)$. If so, then the module $vF[G]$ is isomorphic to the natural module F^d and this will be confirmed in Step (4). If it is not so, then $F[G] \cong \mathrm{M}(d, L)$ where $L > F$, and this will be detected as some conjugated generating matrix will not lie in $\mathrm{GL}(d, F)$. Thus the algorithm returns the correct information, and the probability that Step (1) fails to find a suitable matrix a can be made arbitrarily small.

Consider now the complexity of the algorithm. Assume that we can find a random $a \in F[G]$ of sufficient randomness in $O(d^3)$ field operations, and that Step (1) is executed a constant number of times. Computing $c_a(t)$ takes $O(d^3)$ operations in K, see [15] or [13] for a sharper bound. Finding the linear factors of $c_a(t)$ takes $O(d \log^2 d \log\log d \log(dq))$ operations in F [16, Corollary 14.16], since the polynomial has its coefficients in F. Step (3) of the algorithm is essentially the "Spin" process as employed by the MEATAXE [7]: it differs from the standard in that the unechelonised images are maintained. Both Step (2) and Step (3) take $O(d^3)$ field operations, see [7] and [13, p. 295]. The conjugation in Step (4) costs $O(|X|d^3)$, and checking whether or not the conjugated generators lie in $\mathrm{GL}(d, F)$ has the same cost. This completes the proof of Theorem 2.1.

4 Modulo scalars: G' acts absolutely irreducibly

We now consider the task of writing G over F modulo scalars in K, when G' acts absolutely irreducibly. In particular, we prove Theorem 2.2 by presenting the relevant algorithm, in essence an application of the algorithm of Section 3 to G'.

The algorithm is based on the following lemma.

Lemma 4.1 *If G can be written over F modulo scalars in K, then G' can be written over F, and the F-space spanned by such a basis for G' is unique up to multiplication by a scalar in $K^\times$.*

PROOF: The first observation follows since multiplying each of $g, h \in G$ by a fixed scalar does not change the value of $[g, h]$. The uniqueness follows by applying Schur's Lemma to V as an absolutely irreducible KG'-module. □

We now apply the algorithm of Section 3 where G' replaces G in Steps (1) and (3). If a basis B is found for G', Step (4) decides whether or not the given generating set for G is written over F modulo scalars in K when referred to this basis.

Deciding whether or not G' acts absolutely irreducibly on V can be determined in $O(d^3)$ field operations: the MEATAXE and the associated absolute irreducibility test have this complexity when the group in question (here G') acts irreducibly [7].

Seress [14, Chapter 2] presents a black-box Monte-Carlo algorithm to construct G' in time $O(d^3)$. Leedham-Green & O'Brien [11] present an algorithm to construct random elements of a normal subgroup described by a normal generating set in $O(d^3)$ field operations. Hence we can obtain random elements of G' in $O(d^3)$ field operations.

Hence the complexity of this algorithm is that stated in Theorem 2.1.

5 Modulo scalars: determine scalars

We turn now to the general question: determine constructively whether or not G is conjugate to a subgroup of $\mathrm{GL}(d, F).K^\times$.

If G acts absolutely irreducibly on the given KG-module V but G' does not, we are still able to reduce to the situation of Theorem 2.1.

In summary, for each g in a suitable subset of G, we try to find scalars k_g in $K^\times$ with the property that if each g is multiplied by k_g the resulting subset generates a group that can be written over F. Clearly the map $g \mapsto k_g$ will then define a homomorphism of G/G' into $K^\times/F^\times$.

Our algorithm is based on the following well-known facts.

Theorem 5.1 *Let $G \leq \mathrm{GL}(d, K)$ act irreducibly and let $F < K$. The following conditions are equivalent:*

1. *G can be written over F.*
2. *The characteristic polynomial of every element of $F[G]$ has all its coefficients in F.*
3. *The characteristic polynomial of every element of G has all its coefficients in F.*
4. *The trace of every element of $F[G]$ lies in F.*
5. *The trace of every element of G lies in F.*

PROOF: Obviously (1) implies (2) implies (3) implies (5), and (4) and (5) are clearly equivalent. That (5) implies (1) follows from [9, Theorem 1.17]. □

We now consider how one determines what possible scalars can be used to multiply $g \in G$ when writing G over F modulo scalars in K.

If $g \in G'$, then g can be multiplied only by scalars in $F^\times$; and if G is perfect modulo scalars this observation effectively resolves the problem.

If this is not the case, we consider elements $g \in G$ intrinsically, without regard to their relation to other elements of the group. Let $f(t)$ be the characteristic polynomial of g. A necessary condition for k_g to be a suitable scalar with which to multiply g is that the characteristic polynomial $k_g^d f(tk_g^{-1})$ of $k_g g$ should have its coefficients in F.

Does this condition determine k_g uniquely modulo $F^\times$? No, since the characteristic polynomial $f(t)$ of g may have zero coefficients.

If $f(t)$ is a polynomial in t^s for some $s > 1$ then one obtains a number of expressions for k_g^s modulo $F^\times$ (assuming that s has been chosen to be maximal): one expression for each non-zero non-leading coefficient of $f(t)$. For an affirmative answer these expressions must agree; one may then obtain up to s distinct possibilities for $k_g \bmod F^\times$.

More precisely, let $f(t) = t^d + a_1 t^{d-1} + \cdots + a_d$ and $s := \gcd\{i : a_i \neq 0\}$. The condition that $k_g^d f(tk_g^{-1})$ should have all its coefficients in F reduces to a set of expressions for $k_g^u \bmod F^\times$, where $u = \gcd(s, |K| - 1)$. To solve $k_g^u = \theta \bmod F^\times$, we simply find one solution, say λ; the general solution is now $k_g = \lambda x$ where x runs through the $\gcd(u, |K^\times/F^\times|)$ coset representatives of the u-th roots of 1 in $K^\times/F^\times$.

If we consider imprimitive groups, such as $\mathrm{GL}(d, q) \wr C_2$ for some odd q written naturally as a subgroup of $\mathrm{GL}(2d, q^2)$, these demonstrate that it is not generally true that $u = 1$ for most choices for g, which would of course lead to an immediate solution to the problem.

The resulting algorithm is the following.

1. Find a random sequence $S = (g_0, g_1, \ldots, g_{t-1})$ of elements of G that together with G' acts absolutely irreducibly.

   Clearly the given generators can be arranged in such a sequence, but there are advantages in having a random sequence, especially if this has fewer elements than the given generating set. We terminate the sequence as soon as we have an absolutely irreducible generating set.

2. For each $j \in [0, \ldots, t-1]$ find the set C_j of cosets $F^\times k$ for $k \in K^\times$ for which kg_j has its characteristic polynomial over F. If $C_j = \emptyset$ for any j then return *false*. Reorder S in order of increasing size of C_j.

3. Now set up a backtrack search. This will take place in a rooted tree of depth t. Every vertex of depth j is joined to $|C_j|$ vertices of depth $j+1$, the corresponding edges being labelled by the elements of C_j. Thus when the backtrack reaches a vertex of depth j, elements k_i have been selected for all $i \in \{0, \ldots, j-1\}$. At this point the algorithm proposes to multiply g_i by k_i for all $i < j$, and is looking for a suitable k_j by which it can multiply g_j. The choice of k_j should be compatible with the previous choices. We explain below how this is tested. Each element of C_j is tried in turn, until either a satisfactory element of C_j is found, and the backtrack advances along the corresponding edge, or it is found that no edge is satisfactory, and the algorithm backtracks. If the algorithm gets to depth t, it has found an element of C_j for all j. In this case we decide whether or not $\langle G', g_0k_0, \ldots, g_{t-1}k_{t-1}\rangle$ can be written over F, and if so whether the original generators of G, when written with respect to the corresponding basis, are now written over F modulo scalars in K. If so, the problem is solved; if not, we backtrack. Thus the algorithm either produces a positive solution, or returns *false* when all $|C_1| \cdots |C_j|$ paths have been considered.

How do we test whether or not a given element k_j of C_j is suitable? A number of random elements of $F[\langle G', g_0k_0, \ldots, g_jk_j\rangle]$ are constructed, where the k_i for $i < j$ are read off from the labels as described above. If the characteristic polynomial of any of these random elements has coefficients which are not in F, then this value of k_j is rejected; otherwise it is accepted.

Observe that this is a powerful theoretical test to determine whether or not a given choice of k_j is suitable. Critical to its strength is that we compute characteristic polynomials of random elements of $F[\langle G', g_0k_0, \ldots, g_jk_j\rangle]$ rather than of $H = \langle G', g_0k_0, \ldots, g_jk_j\rangle$. Theorems 3.1 and 5.1 imply that if H cannot be written over F then $F[H]$ is isomorphic to $\mathrm{M}(d, L)$ for some field L, where $F < L \leq K$. The proportion of elements of $\mathrm{M}(d, L)$ with trace in F is exactly $|F/L|$, and so we can deduce with high probability when H cannot be written over F.

Thus we expect only to backtrack if the rejected choice of $(k_0, \ldots, k_{j-1})$ does give rise to a subgroup of G that can be written over F but this cannot be extended. This can arise even when a positive outcome is eventually reached: passing from one suitable set of scalars to another changes the scalars in a way that is defined by a homomorphism from G/G' to $K^\times/F^\times$, and in some cases not every homomorphism of a subgroup of G/G' to $K^\times/F^\times$ will lift to a homomorphism defined on the whole of G/G'.

6 Modulo scalars: a Clifford based approach

If G' does not act absolutely irreducibly over V, we can adopt a more conclusive approach suggested by Clifford's theorem and its algorithmic realisation in [8].

Suppose that G' acts reducibly on V, and absolutely irreducibly on the homogeneous components of V as G'-module. In this case Clifford's theorem states that these components form the blocks in a system of imprimitivity for G. There is no guarantee that the restriction of G' to any one of these blocks can be written over F modulo scalars in K, even if the action of G on V can be so written. We consider two situations. The first of these is considered in detail in [4].

In each case the input group G acts absolutely irreducibly on V.

1. Let $N \geq G'$ be the subgroup of G that centralises the set of blocks. The number of blocks is t where $t|e$. Let ϕ be the Frobenius automorphism of K over $\mathrm{GF}(q^{e/t})$. Suppose that the set of blocks can be arranged in order as $V_1, V_2, \ldots, V_t$ where $V_i \simeq V_1^{\phi^{i-1}}$.

   Take a K-basis B_1 for V_1, and let B_i be the image of B_1 under an isomorphism from $V_1^{\phi^{i-1}}$ to V_i. Let g be any element of G that permutes the blocks V_i cyclically. Then g^t normalises each block, and (for an affirmative answer) a scalar $k \in K^\times$ can be found such that the matrix of $(kg)^t$, with respect to the ordered basis B obtained from concatenating the bases B_i, is a block diagonal matrix with blocks of the form $(A, A^\phi, \ldots, A^{\phi^{t-1}})$. Then the bases $B_2, B_3, \ldots, B_t$ can be multiplied by unique scalars (one for each block) so that, with respect to the concatenation of these bases, the matrix of g is a block permutation matrix permuting the V_i cyclically, and where the non-zero blocks in successive rows are of the form $A, A^\phi, \ldots, A^{\phi^{t-1}}$. These bases specify compatible FG-isomorphisms between the V_i. Now let C be a basis for K over F, and let C_i be the F-basis $B_iC^{\phi^i}$ of V_i. Then, with respect to the concatenation of the bases C_i, the elements of G appear as block permutation matrices, where every non-zero block is identical. Thus the set of vectors $\{b_1c + b_2c^\phi + \cdots + b_tc^{\phi^{t-1}}\}$, where $b_1 \in B_1$, and $c \in C$, and $b_i \in B_i$ is the image of b_1 under the above isomorphism, is an F-basis for an FG-module, as required.

2. For some subgroup N of G, where $G > N \geq G'$, the given module V is the direct sum $U_1 \oplus \cdots \oplus U_s$ of absolutely irreducible KN-modules that are permuted as a system of imprimitivity by G/N acting regularly, and the restriction of N to U_1 (and hence to any U_i) can be written over F modulo scalars in K.

   Suppose that the restriction of N to U_1 has been written over F modulo scalars in K by finding a suitable basis B_1 for U_1. As N acts absolutely irreducibly, the

F-space generated by B_1 is uniquely determined by U_1 up to a scalar multiple in $K^\times$. Now G/N is an abelian group that acts regularly on the set of blocks. Thus we can obtain the structure of G/N as a direct product of cyclic groups. Each of these cyclic groups is generated by the image of some element of G. Let g be such an element, and let the corresponding cyclic group be of order n. Then $g^n \in N$, and so, for an affirmative answer, g can be multiplied by a scalar so that g^n, restricted to U_1, when referred to B_1, has its coefficients in F. When the generator of each cyclic subgroup in the direct decomposition of G/N is the image of an element of G that has been adjusted in this way, the basis B_1 can be spun to a basis for V under the action of these elements. If G can be written over F modulo scalars in K, this basis will exhibit the fact.

Clearly every case in which G' acts absolutely irreducibly on the homogeneous components of the action of G' on V is covered by first applying Case 1 to a suitable set of blocks, and then applying Case 2.

7 Implementation and performance

We use the product replacement algorithm [3] to construct random elements of G. Once an initialisation phase is complete, we can generate random elements of G with two multiplications. We use a simple generalisation to construct elements of $F[G]$.

An implementation of the complete algorithm is publicly available in Magma. The computations reported in Table 1 were carried out using Magma V2.11-8 on a Pentium IV 1.1 GHz processor. In all cases, we report times averaged over three independent runs.

The input for the first six examples reported in Table 1 are absolutely irreducible subgroups of $\mathrm{GL}(d, K)$ which can be written over F modulo scalars in K. In the column entitled "Time", we list the CPU time in seconds needed to construct the conjugation matrix using the algorithm of Section 4.

The remaining examples are absolutely irreducible subgroups of $\mathrm{GL}(d, K)$ which can be written over F. These are used to contrast the performance of our new algorithm for this task with that of Glasby & Howlett [6]. In the column entitled "Time", we list the CPU time in seconds needed to construct the conjugation matrix using the algorithm of Section 3; in the column labelled "G & H" we record the CPU time taken by our implementation of the Glasby & Howlett algorithm to construct this matrix. We have also compared the performance of both algorithms for degrees in the hundreds and small fields. In summary, the new algorithm is faster when the discrete logarithm calculations in the smaller field are expensive; for larger dimensions and small fields, the original remains very competitive.

Table 1: Performance of algorithms for a sample of groups

d	q	e	Time	G & H
4	5^4	5	0.01	–
12	5^5	4	0.12	–
20	2^4	10	0.46	–
20	5^4	10	2.22	–
30	11^8	5	6.18	–
50	11^8	5	34.93	–
4	5^4	5	0.01	0.03
12	5^{10}	5	1.67	1.73
20	2^{20}	4	1.23	1.85
20	11^{20}	2	1.75	7.48
30	11^{10}	4	6.15	14.14
30	19^{10}	3	22.41	185.67

References

[1] M. Aschbacher, “On the maximal subgroups of the finite classical groups”, *Invent. Math.* **76** (1984), 469–514.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, “The MAGMA algebra system I: The user language”, *J. Symbolic Comput.*, **24**, 1997, 235–265.

[3] Frank Celler, C.R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and E.A. O’Brien, “Generating random elements of a finite group”, *Comm. Algebra* **23**, 1995, 4931–4948.

[4] S.P. Glasby, “Modules induced from a normal subgroup of prime index”, in *Rings, modules, algebras, and abelian groups*, Eds. A. Facchini, E. Houston and L. Salce, *Lecture Notes in Pure and Applied Mathematics* **236** (2004), 257–269.

[5] Nathan Jacobson, *Basic Algebra. II*, Second edition. W. H. Freeman and Co., New York, 1989.

[6] S.P. Glasby and R.B. Howlett, “Writing representations over minimal fields”, *Comm. Algebra* **25** (1997), no. 6, 1703–1712.

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

[8] Derek F. Holt, C.R. Leedham-Green, E.A. O'Brien and Sarah Rees, "Computing matrix group decompositions with respect to a normal subgroup", *J. Algebra* **183**, 1996, 818-838.

[9] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, Berlin, 1982.

[10] Charles R. Leedham-Green, "The computational matrix group project", in *Groups and Computation*, III (Columbus, OH, 1999), 229–247, Ohio State Univ. Math. Res. Inst. Publ., **8**, de Gruyter, Berlin, 2001.

[11] C. R. Leedham-Green and E. A. O'Brien, "Recognising tensor products of matrix groups", *Internat. J. Algebra Comput.* **7** (1997), no. 5, 541–559.

[12] Peter M. Neumann and Cheryl Praeger, "Cyclic matrices over finite fields", *J. London Math. Soc.* **52** (1995), no. 2, 263–284.

[13] Peter M. Neumann and Cheryl Praeger, "Cyclic matrices and the MEATAXE", Groups and Computation III, Ohio State Univ. Math. Res. Inst. Publ. 8 (2001), 291-299.

[14] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2003.

[15] Igor E. Shparlinski, *Finite fields: theory and computation. The meeting point of number theory, computer science, coding theory and cryptography.* Mathematics and its Applications, **477**. Kluwer Academic Publishers, Dordrecht, 1999.

[16] Joachim von zur Gathen and Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, 2002.

Department of Mathematics
Central Washington University
WA 98926-7424, USA
glasbys@cwu.edu

School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS, United Kingdom
C.R.Leedham-Green@qmul.ac.uk

Department of Mathematics
University of Auckland
Private Bag 92019, Auckland
New Zealand
obrien@math.auckland.ac.nz

Last revised July 2005