

# Identifying geometries preserved by matrix groups

Steve Linton and Colva M. Roney-Dougal\*

November 18th, 2005

School of Computer Science, University of St Andrews,  
North Haugh, St Andrews, Fife, KY16 9SX.

and

School of Mathematics and Statistics, University of St Andrews,  
North Haugh, St Andrews, Fife, KY16 9SS.

## Abstract

In this article we show that given a matrix group  $G$  of low dimensions over a finite field, there exists at least one Aschbacher class containing  $G$  for which one can find all of the corresponding geometries that are preserved by  $G$ . For several Aschbacher classes we prove that one can find all ways in which  $G$  is a member of that class, irrespective of whether  $G$  is a member of another class.

## 1 Introduction and motivation

The purpose of this paper is to show that if a finite dimensional matrix group  $G$  over a finite field lies in at least one geometric Aschbacher class, then for one of the classes containing  $G$  we can find all of the corresponding geometries preserved by  $G$ .

This work builds on the Matrix Group Recognition Project [17], which used geometric techniques to develop a suite of algorithms which compute composition trees for finite matrix groups. This project has now been substantially completed, for a detailed survey see [24].

The geometries concerned are all derived from Aschbacher's theorem [1]. In its full generality, this algorithm divides the subgroups of almost all of the finite classical groups into nine classes. We state here a simplified version of the theorem, for the general linear group.

**Theorem 1.1 (Aschbacher's theorem)** *Let  $V$  be the natural module for  $\mathrm{GL}(d, q)$ , and let  $Z := Z(\mathrm{GL}(d, q))$ . Let  $G$  be a subgroup of  $\mathrm{GL}(d, q)$ . Then at least one of the following holds:*

*C1  $G$  acts reducibly:  $G$  stabilises a subspace  $0 < W < V$ .*

*C2  $G$  acts imprimitively:  $G$  preserves a decomposition of  $V$  as a direct sum  $V = V_1 \oplus \cdots \oplus V_r$  of  $r > 1$  subspaces of  $V$ , each of dimension  $s := d/r$ , which are permuted transitively by  $G$ .*

---

\*The second author was partially supported by EPSRC grant number GR/S30580

- C3*  $G$  acts on  $V$  as a group of semilinear automorphisms of a  $(d/e)$ -dimensional space over the extension field  $\text{GF}(q^e)$ , for some  $e > 1$ , and so  $G$  embeds in  $\Gamma\text{L}(d/e, q^e)$ .
- C4*  $G$  preserves a decomposition of  $V$  as a tensor product  $U \otimes W$  of spaces of dimensions  $r, s > 1$  over  $\text{GF}(q)$ , and so is a subgroup of the central product  $\text{GL}(r, q) \circ \text{GL}(s, q)$ .
- C5*  $G$  can be defined, modulo scalars, over a proper subfield  $\text{GF}(q')$  of  $\text{GF}(q)$ : for some  $g \in \text{GL}(d, q)$  we have  $G^g \leq \text{GL}(d, q')$ .
- C6* The dimension  $d = r^m$  for a prime  $r$  such that  $r \mid q - 1$  and  $G$  contains an extraspecial normal subgroup of order  $r^{1+2m}$  (or if  $r = 2$  then maybe  $2^{2+2m}$ ), which acts absolutely irreducibly on  $V$ .
- C7*  $G$  preserves a decomposition of  $V$  as  $V_1 \otimes \cdots \otimes V_m$ , where  $m > 1$ , each  $V_i$  has dimension  $r$ ,  $d = r^m$  and  $\{V_1, \dots, V_m\}$  is permuted transitively by  $G$ .
- C8*  $G$  lies between a quasisimple classical group in its natural representation, and the normaliser of that classical group in  $\text{GL}(d, q)$ .
- C9*  $G$  is almost simple modulo scalars, and is absolutely irreducible.

Note that a group may lie in several classes. To reduce the number of classes containing any given group we require, unless otherwise stated, that all groups not in class *C1* are irreducible, and that groups other than those in *C1* and *C3* are absolutely irreducible. Classes other than *C9* are called *geometric*.

The algorithms developed for the Matrix Group Recognition Project take as input a set of generators for a finite matrix group  $G$ , and start by determining at least one of the Aschbacher classes containing  $G$ . Algorithms now exist for all of the geometric classes, and recognition algorithms exist for many families of *C9* groups. Many of the class identification algorithms are *constructive*, determining exactly the geometric structure stabilised by a geometric group, or an explicit isomorphism to the standard form of the group in class *C9*. In the geometric cases, the kernel of the action on the geometric structure is a normal subgroup  $N$ , and the data returned by constructive Aschbacher class identification algorithms generally allows an appropriate action of  $G/N$  to be constructed, and elements  $g \in G$  to be projected onto this action.

This class recognition is then iterated to produce a composition tree for the group  $G$ . Using this composition tree, Mark Stather, in as yet unpublished work, has developed an algorithm based on one for permutation groups [4] which computes the set of all normal subgroups of a matrix group. One can also use the composition tree to construct a presentation for a matrix group, and Stather has developed algorithms to do this. These algorithms will be essential tools in what follows.

Additional key tools, albeit tools of last resort, because of their computational expense, are “low index subgroup algorithms”, which provide complete lists of all conjugacy classes of subgroups of specified index in a given group.

There are two main kinds of low index subgroup algorithms. One type [6] are developed for finitely-presented groups. Roughly speaking, they operate by searching for possible coset tables of subgroups in which all the relations of the group hold. Here the input is a presentation for the group, and possibly some elements which must be members of the subgroups to be found. Unlike many finitely-presented group methods, the length of the presentation

is not overwhelmingly important for the performance of these algorithms, especially if there are some short relations, but the number of generators is critical, since it drastically affects the growth of the search space. In our application, presentations would be obtained by Mark Stather’s algorithm. The other, more recent, type [3] are based on direct search for homomorphisms from a given concrete (matrix or permutation) group onto a permutation group of low degree, achieved by descending the composition series of the target group. These algorithms work well, except perhaps when the given group is close to simple, when we can often use constructive recognition and algorithms of [12, 28], to construct the set of all maximal subgroups, and then select those which might contain a subgroup of the required index, recursing if necessary to look inside these maximal subgroups.

Returning to the analysis of matrix groups, we observe that, in many cases, the geometric structure found by the algorithms of the Matrix Group Recognition Project is far from unique, and it is interesting to ask which of the possible structures will be found by a particular algorithm, and to seek extended algorithms with desirable properties in this respect. We introduce a taxonomy of such algorithms.

- find one: algorithms which guarantee to return a geometric structure of the appropriate type if one exists, but make no claim as to which one is produced if more than one exists;
- find all: algorithms which return all essentially different geometric structures of the appropriate type which are preserved by  $G$ ;
- find random: randomised algorithms which return one of the geometric structures preserved by  $G$  chosen randomly with some known probability distribution, which might be almost uniform, or merely guaranteed to be nonzero;
- find best: algorithms that return all the maximal geometric structures preserved by  $G$ , according to some partial order.

The main focus of this paper will be on solving the “find all” problem: the “find one” problem is essentially done. To be more precise, for any geometric group  $G$  there exists at least one Aschbacher class containing  $G$  for which the “find one” problem has been solved.

Our motivation for solving the “find all” problem is an application to backtrack search, which is used to compute subgroup centralisers, intersections, normalisers and conjugacy, amongst other problems. At present, work of O’Brien and Murray [21] is used to select an appropriate collection of points and subspaces to produce an object that is similar to a base for a permutation group, and this structure is used to construct and then depth-first search a tree. For certain specific backtrack search problems there are refinements to this approach which deal with the group in layers, lifting the answer through successive quotients. We propose to build on the algorithm for subgroup conjugacy in the general linear group given in [25], to avoid parts of the search space by deducing geometric information about the groups concerned. For instance, it is shown in [25] that given two reducible groups  $G, H \leq \text{GL}(d, q)$ , if one can find a submodule  $V'$  of the natural module for  $G$ , and find all  $\dim(V')$ -dimensional submodules for  $H$ , then  $G$  and  $H$  are conjugate in the general linear group if and only if  $G$  and  $H^x$  are conjugate in the stabiliser of  $V'$  in  $\text{GL}(d, q)$ , for an element  $x \in \text{GL}(d, q)$  that lies in an easily constructed short list of matrices. There should be many other results of a similar nature, enabling one to drastically reduce search time if one can obtain all of the ways in which a group can preserve a particular type of geometry.

Backtrack search problems for matrix groups become difficult very quickly — even solving problems in dimension 10 over GF(2) can be time-consuming. We will therefore pay particular attention to finding all geometries for matrix groups in dimension at most 60.

In Section 2 we discuss a preliminary step for many of our algorithms, that of examining the composition factors of a matrix group  $G$  to reduce the number of possible geometries that might be preserved by  $G$ . Then in Sections 3 to 10 we present our algorithms for each class in turn. In each case we either show that any matrix group belongs to that class in an essentially unique way, or how to upgrade the existing class identification algorithms to find all geometries of that type that are preserved by the group, possibly subject to the group not being a member of some other class. Finally we conclude in Section 11 with some open problems.

## 2 Examining composition factors

In several cases, but in particular the imprimitive, tensor and tensor-induced, we start by examining the known nonabelian composition factors of the matrix group  $G$  to check whether they could be composition factors of groups preserving geometric structures with particular parameters. In particular we need to know:

1. whether a composition factor could be a section of  $L_s(q)$ ?
2. whether a composition factor could be a section of  $S_k$ ?

where the values of  $s$  and  $k$  depend on the geometry that we are considering.

Since we are looking for embeddings of a simple group  $S$  as a section of  $L_s(q)$  or  $S_k$ , we can find the minimal degree  $d$  of a projective representation of  $S$  and conclude that  $d \leq s$ , and similarly the minimal degree of a permutation representation must be less than  $k$ . We list here a few rough-and-ready rules which can be used to decide that various composition factors cannot embed in an appropriate linear or symmetric group: these could easily be extended further. We are particularly interested in the minimal degrees of matrix representations for  $s \leq 30$ , as in the imprimitive, tensor and tensor induced cases we have  $s|n$  and  $s < n$ . We also require the minimal degrees of permutation representations for  $k \leq 60$  as in the imprimitive case we have  $k|n$  and in the tensor induced case we have  $k \sim \log n$ .

### 2.1 Alternating groups

The minimal degree of a permutation representation of  $A_n$  is simply  $n$ . For  $n \geq 9$  the minimal value of  $s$  such that  $A_n$  has a faithful representation as a subgroup of  $L_s(q)$  for any  $q$  is  $n - 2$ . For  $n = 5$  we have  $s = 2$ , otherwise  $s \geq n - 4$  [14, Proposition 5.3.7].

### 2.2 Groups of Lie Type

First we consider matrix representations of groups of Lie type in their natural characteristic: in the case of exceptional isomorphisms we consider each possibility in turn and choose the minimal degree. In natural characteristic, the minimal degree representation of classical groups is their natural representation. Turning to the exceptional groups, the minimal degrees of representations in defining characteristic of all of the twisted and untwisted exceptional groups of Lie type are listed in [19].

For cross characteristic representations, lower bounds for the minimal degrees of projective representations of the simple groups of Lie type are given in [27, Table 1]. For matrix representations in degree at most 30 we use [8], which gives the exact degrees of all such representations of degree up to  $s = 250$ : for degree at most 30 only 12 groups of Lie type occur (excluding those which are isomorphic to alternating groups).

As for permutation representations, we use the fact that the degree of the minimal permutation representation of the classical group has a lower bound that is given in [14, Table 5.2A]. For the exceptional groups, in general we may use the fact that if a group has a primitive permutation representation of degree  $k$  then its representation as permutation matrices in characteristic coprime to the group order has a constituent of degree  $k - 1$ . So the minimal degree of a permutation representations is at least one greater than the minimal degree of a matrix representation.

We have more specific information for small degree actions. All primitive permutation representations of exceptional groups of Lie type on up to 2499 points are described in [26]: there are only six such groups, and none have representations of degree less than 60.

### 2.3 Sporadic Groups

The minimal degrees of permutation and matrix representations of the sporadic groups are well known, and for matrix representations in dimension up to 250 all such degrees are listed in [8]. In dimension at most 30, only 16 of the sporadics arise. The only sporadic groups with permutation representations of degree less than 60 are the Mathieu groups.

Thus for each simple group  $S$  we can eliminate many possible containments of  $S$  in linear or symmetric groups at minimal computational cost.

## 3 Reducible groups

The geometric structure in this case is an invariant subspace, so the problem of finding all structures is simply that of determining the whole lattice of submodules. Likewise the “find best” problem, under the inclusion (resp. reverse inclusion) partial order, simply becomes that of finding all maximal (resp. irreducible) submodules.

An effective method for solving these problems is given in [20], which uses a theorem of Benson and Conway about modular lattices to define a data structure from which the full list of submodules, or subsets such as the minimal submodules, can be read off efficiently.

## 4 Imprimitve groups

Let  $G \leq \text{GL}(d, q)$  be imprimitive, preserving a direct sum decomposition  $V = V_1 \oplus \cdots \oplus V_r$  of  $r > 1$  subspaces of  $V$ , each of dimension  $s := d/r$ , which are permuted transitively by  $G$ . We wish to find all such decompositions. This is equivalent to finding one  $V_i$  in each.

We first attempt to restrict the possible values for  $r$ , which are initially all divisors of  $d$  (other than 1). Since we know  $|G|$ , we can rule out any values of  $r$  for which  $|G|$  does not divide  $|\text{GL}(s, q)|^r \cdot r!$ . We also use the data outlined in Section 2 to check whether the nonabelian composition factors of  $G$  could all be subgroups of  $L_s(q)$  or  $S_r$ , and store in each case whether any of them could *not* be a subgroups of  $S_r$ .

We then repeatedly apply the exponent test given in [10], and follow up with the characteristic polynomial test. Both of these tests are cheap, effective at ruling out possible values of  $r$ , and may produce elements  $g$  which would have to lie in the kernel of any imprimitive action of degree  $r$ . For now, we store such elements. After these two tests are completed, we should be reasonably confident of finding at least one imprimitive decomposition for each remaining value of  $r$ .

If for all remaining values of  $r$  there must be a nontrivial kernel, we now compute the set of all normal subgroups of  $G$ . If  $|G|$  does not divide  $r!$  then there must be a kernel of the action, so in particular  $G$  must have at least one normal subgroup of index dividing  $r!$ . A similar argument applies to the composition factors. We also re-examine any kernel elements  $g$  that were produced by the exponent and characteristic polynomial tests. We firstly check that each such  $g$  lies in at least one normal subgroup whose index divides  $r!$  (if none exists, then we can eliminate  $r$  as a possible number of blocks). Secondly, we can eliminate any normal subgroups that do not contain all such elements  $g$  from our list of possible kernels for an action of degree  $r$ . Thirdly we can eliminate all normal subgroups that do not contain the appropriate composition factors.

We now start analysing each  $r$ , and first consider the case that there is a kernel of the action. That is, there is a subgroup  $N \trianglelefteq G$  such that the natural module splits as a direct sum of  $N$ -submodules  $W_1 \oplus \cdots \oplus W_{rt}$  for some  $t \geq 1$ . In this case SMASH [9] is applicable.

If none of the submodules are pairwise isomorphic, then a straightforward application of SMASH, with generators of the normal subgroup  $N$  as input, will often find a block decomposition. If  $t = 1$  then we apply MINBLOCKS to  $W_1$  to check whether it is a block. If  $t > 1$  then we know that each block is a span of  $t$  of the  $W_i$ s, so we look for a block of dimension  $s$  containing  $W_1$  and  $W_i$  for  $2 \leq i \leq rt$ . For each of these that produces a block system with a multiple of  $r$  blocks, with kernel of block action  $N$ , we attempt to extend the block by adding more of the  $W_i$ s, until we have found all possible block systems with  $r$  blocks whose kernel is  $N$ . If the value of  $t$  is large, then there might be too many possible block systems with kernel  $N$ , so if necessary we can revert to our approach in the faithful case, but store the information that  $N$  must be contained in the point stabiliser.

If the submodules are all pairwise isomorphic then we apply the algorithms of Section 6 to  $N$  to find a tensor decomposition of  $V$  as  $U \otimes W_1$ . If  $G$  is imprimitive on  $V$  with kernel  $N$  then the induced action of  $G$  on  $U$  is also imprimitive [10], so we find the action of  $G$  on  $U$ , test that for primitivity, then pull back the results. This will work provided that  $G$  is not also semilinear with kernel containing  $N$ , in which case we revert to the strategy that we use when  $G$  is faithful on blocks, storing the information that  $N$  is contained in the point stabiliser.

The final case is when the  $N$ -submodules split up into more than one class of pairwise isomorphic irreducible  $N$ -modules, and each class contains more than one module. In that case it is certainly true that  $G$  permutes these classes, but the blocks of the action of  $G$  could be spans of arbitrary linear combinations of isomorphic  $N$ -modules, so we revert to the strategy that we use when  $G$  is faithful on blocks, storing the information that  $N$  is contained in the point stabiliser.

If  $G$  is faithful on blocks, there will not be a kernel for us to use, and so our strategy is to use one of the available low index subgroups algorithms. This part of the algorithm is more expensive than the others, so we only apply it if we know that  $|G|$  divides  $r!$ , so that there is a good chance that such an action exists, or if we have found a candidate kernel

$N$  under which  $V$  splits into too many submodules. Note that in the former case  $G$  must be a comparatively small subgroup of  $\text{GL}(rs, q)$ , and in the latter case we have additional relations.

We are looking for all subgroups (up to conjugacy) of index  $r$ , as one of these must represent a block stabiliser  $H$  if  $G$  is to be imprimitive. It is shown in [10] that if  $H$  is a block stabiliser for a block  $V_1$ , then  $V_1$  is irreducible as a  $\text{GF}(q)H$ -module. We follow the procedure given in [10, Section 5.1] to test each such  $H$ , and find the corresponding system of imprimitivity.

Thus in each case we can find all ways in which  $G$  is imprimitive.

## 5 Semilinear Groups

Let  $G \leq \text{GL}(d, q)$  be semilinear. Then  $G$  is irreducible and for some divisor  $e$  of  $d$  there exists an embedding  $\phi : G \rightarrow \Gamma\text{L}(d/e, q^e)$ . If  $G$  is not absolutely irreducible, then in fact  $\phi : G \rightarrow \text{GL}(d/e, q^e)$ , otherwise there exists a normal subgroup  $N \trianglelefteq G$  which is maximal subject to  $\phi(N) \leq \text{GL}(d/e, q^e)$ : the group  $N$  is the kernel of the map  $\psi : G \rightarrow \text{Aut}(\text{GF}(q^e))$ . The quotient  $G/N$  is therefore cyclic, of order dividing  $e$ , and  $\phi(G)$  acts as powers of the Frobenius automorphism on  $\phi(N)$ .

We distinguish different semilinear embeddings of  $G$  by the matrices which correspond to the centre of  $\text{GL}(d/e, q^e)$ : the “find all” problem is to find all possible choices for the embedding of the group of scalars of  $\Gamma\text{L}(d/e, q^e)$ , as a subgroup of  $C_{\text{GL}(d, q)}(G)$ .

We subdivide into four cases:

1.  $G$  is not absolutely irreducible.
2.  $G$  is absolutely irreducible, and  $N$  is irreducible.
3.  $G$  is absolutely irreducible,  $V|_N = V_1 \oplus \cdots \oplus V_s$ , where the  $V_i$  are pairwise isomorphic as  $N$ -modules.
4.  $G$  is absolutely irreducible,  $V|_N = V_1 \oplus \cdots \oplus V_s$ , where the  $V_i$  are not all pairwise isomorphic as  $N$ -modules.

In case 1, the existing approach is to use the Holt-Rees modification of the Meataxe [11]. Let  $A$  be the  $\text{GF}(q)$ -algebra generated by  $G$ . Since  $G$  is irreducible but not absolutely irreducible, the centraliser of  $A$  in the matrix algebra  $M(d, q)$  is  $\text{GF}(q^e)$  for some  $e > 1$ . Let  $\rho$  be a primitive element of  $\text{GF}(q^e)$ , represented as a  $d \times d$  matrix over  $\text{GF}(q)$ , so that  $\langle \rho \rangle = C_{M(d, q)}(A)$ . Notice that  $\langle \rho \rangle$  is uniquely determined, so the Holt-Rees algorithm solves the “find all” problem. The algorithm returns a matrix  $C$  that is a power of  $\rho$ , such that  $C$  generates  $\text{GF}(q^e)$  as a field over  $\text{GF}(q)$ .

In case 2, we construct all embeddings as semilinear groups by using Stather’s algorithm to find all normal subgroups  $N$  of  $G$ . We select all that are irreducible, with cyclic quotients, and then apply the algorithm given in part 1 of this section to  $N$ . Following step 9 in SMASH [9] we then use ISSEMI LINEAR to check whether the generators of  $G$  act as field automorphisms on  $C$ .

In the third case,  $G$  is absolutely irreducible but  $V|_N = V_1 \oplus \cdots \oplus V_s$ , where the  $V_i$  are pairwise isomorphic as  $N$ -modules. We show that this cannot happen when  $N = \text{Ker}(\psi)$ .

**Theorem 5.1** *Let  $G$  be an absolutely irreducible semilinear group, and let  $N$  be the kernel of the map  $\psi : G \rightarrow \text{Aut}(\text{GF}(q^e))$ . Then  $V$  does not split into a direct sum of pairwise isomorphic irreducible  $N$ -modules.*

PROOF: Suppose that  $V = V_1 \oplus \cdots \oplus V_s$  is a decomposition of  $V$  into pairwise isomorphic irreducible  $N$ -modules. Then  $G$  acts projectively on  $\{V_1, \dots, V_s\}$ , so there is a homomorphism  $\pi : G \rightarrow \text{PGL}(s, q)$ . Since  $N$  fixes each  $V_i$  as a subspace, and acts in the same way on each of them, the group  $N$  is in the kernel of  $\pi$ , and so  $\pi(G)$  is cyclic, of order dividing  $e$ .

Since  $G$  is absolutely irreducible,  $\pi(G)$  is an absolutely irreducible subgroup of  $\text{PGL}(s, q)$ , contradicting the fact that  $\pi(G)$  is cyclic.

In the final case,  $G$  is absolutely irreducible,  $N$  is reducible, and  $V|_N$  splits into  $st$  irreducible (but not absolutely irreducible)  $N$ -submodules  $V_1, \dots, V_{st}$ , which are not all pairwise isomorphic. Instead, for some  $t$  the set  $\{V_1, \dots, V_{st}\}$  can be partitioned into  $s > 1$  sets containing  $t$  pairwise isomorphic  $\text{GF}(q)N$ -modules each, so that  $V = W_1 \oplus W_2 \cdots \oplus W_s$  and  $G$  is transitive on  $\{W_1, \dots, W_s\}$ . In this instance, for  $G$  to be semilinear with kernel  $N$ , the normal subgroup  $N$  must embed as a subgroup of  $\text{GL}(d/(se), q^e)$ , and  $G_{W_1}$  embeds as an irreducible subgroup of  $\Gamma\text{L}(d/se, q^e)$ . We start by applying the imprimitivity testing, with  $N$  being a subgroup of the kernel of the action on blocks, to find a permutation  $\alpha$  which generates the image of  $G/N$  in its action on the homogeneous components  $\{W_1, \dots, W_s\}$ . Note that since  $G/N$  is cyclic and transitive,  $\alpha$  should be an  $s$ -cycle. By reordering  $\{W_1, \dots, W_s\}$  if necessary we can assume that  $\alpha = (12 \dots s)$ . We store a preimage  $g$  of  $\alpha$ .

Armed with this information, we now treat  $W_1$  as an  $N$ -module, and use steps 4 and 5 and the first part of step 7 of SMASH to find a centralising matrix  $C_1$  for the action of  $N$  on  $W_1$ . We check that the element  $g \in G$  conjugates a matrix which acts as  $C_1$  on  $W_1$  and the identity on  $W_2, \dots, W_s$  into a matrix whose restriction to  $W_2$  has the same order as  $|C_1|$ , that acts as the identity on  $W_1, W_3, \dots, W_s$ , and that centralises  $N$ . If not, then  $G$  is not acting semilinearly with kernel  $N$ . If so then we store  $C_2$ , and look in  $\langle C_2 \rangle$  for the possible powers  $C_2^{i_2}$  that could have been mapped under a power of the Frobenius automorphism to  $C_2$ . Eventually we will either have constructed a matrix  $C$  with  $d/s \times d/s$  blocks  $C_1, C_2^{i_2}, \dots, C_s^{i_s}$  on the diagonal that centralises  $N$ , and is mapped by  $g$  to a  $q^j$ th power of itself for some  $j$ , or shown that  $G$  is not semilinear. We finish by using the ISSEMLINEAR test from SMASH to check whether the generators of  $G$  act as field automorphisms on  $C$ .

Thus, given any irreducible matrix group  $G$  we can find all ways in which  $G$  is semilinear, irrespective of the membership of  $G$  in other Aschbacher classes.

## 6 Tensor product groups

A matrix group  $G$  is a *tensor product group* if  $G$  fixes a decomposition of  $V$  as  $U \otimes W$ , where  $\dim(U) = r$ ,  $\dim(W) = s$ , and  $d = rs$ . The group  $G$  is a subgroup of the central product of  $\text{GL}(r, q)$  and  $\text{GL}(s, q)$ , so  $G/(G \cap Z) \leq \text{PGL}(r, q) \times \text{PGL}(s, q)$ .

We will recurse to this case when considering tensor induced groups, so the only restriction that we make on  $G$  is to insist that it acts irreducibly on at least one of the factors in the decomposition. We subdivide into two cases:

1.  $G$  has a (nonscalar) subgroup  $N$  which acts as scalars on one of the tensor factors.

Without loss of generality we suppose this factor to be  $U$ . It follows immediately that  $N \trianglelefteq G$ .

2. The only subgroup of  $G$  which acts as scalars on either factor is  $G \cap Z(\mathrm{GL}(d, q))$ .

Since we are looking for *all* ways in which  $G$  preserves a tensor decomposition, we consider both cases simultaneously.

Stage one of the algorithm attempts to rule out the existence of a tensor decomposition with a factor of dimension  $r$ . For each factorisation  $d = rs$ , we check that the order of  $G$  divides  $|\mathrm{GL}(r, q) \circ \mathrm{GL}(s, q)|$ . We then use the ideas in Section 2 to check that each nonabelian composition factor of  $G$  could be a subgroup of either  $L_r(q)$ , or  $L_s(q)$ , or both, and store this information. We then apply the projective order test, and the polynomial factorisation test, as given in [15, Sections 2 and 3]. If  $G$  has passed each of these tests for some given  $\{r, s\}$  then we can be confident that  $G$  preserves a decomposition of the corresponding type.

We check whether there exists a value of  $r$  such that  $G$  might have a type 2 decomposition, or if for each tensor decomposition  $U \otimes W$  of  $V$  the action on at least one of the tensor factors must be non-faithful, modulo scalars. If  $G$  is almost simple then all decompositions of  $G$  must be of type 2. Conversely, for  $G$  to have a type 2 decomposition, the projective order of  $G$  must divide both  $|\mathrm{PGL}(r, q)|$  and  $|\mathrm{PGL}(s, q)|$ , and all nonabelian composition factors of  $G$  must be potential subgroups of both  $L_r(q)$  and  $L_s(q)$ .

If a single one of the possible values of  $r$  could lead to a type 2 decomposition, we use the tests for type 2. Otherwise, we use the type 1 tests, which are likely to be faster.

## 6.1 Type 1 tests

Finding all decompositions of type 1 is relatively straightforward. We use [15], and upgrade the algorithms to take advantage of the fact that we know  $|G|$ , and can find all normal subgroups of  $G$ . We consider each remaining possible pair  $(r, s)$ , and look for a normal subgroup that acts as scalars on  $U$ . An element that acts as scalars on one of the tensor factors is called a *projectivity*.

The procedure ISPROJECTIVITY of [15, 16] takes as input the generators of  $G$ , and an element  $g \in G$ , and returns one of the following:

1. A nontrivial tensor decomposition of  $V$  on which  $g$  acts as a projectivity.
2. “False” if a proof has been constructed that no such tensor decomposition exists.
3. “Unknown” if it has discovered that  $G$  acts semilinearly on  $V$  over an extension field.

If  $g$  is a projectivity, then the characteristic polynomial  $f(x)$  of  $g$  is a  $uth$  power. ISPROJECTIVITY finds an irreducible factor  $h(x)$  of  $f(x)$  such that  $f(x)$  is not a power of  $h(x)$ : the kernel of  $h(g)$  is then a flat. If  $f(x)$  is a power of a single irreducible polynomial, then we search in the algebra generated by  $g$  and its conjugates under  $G$  for an element whose characteristic polynomial is not a power of an irreducible. This will work unless the algebra is a field  $\mathrm{GF}(q^e)$  for  $e > 1$ . We upgrade ISPROJECTIVITY to finding *all* tensor decompositions on which  $g$  acts as a projectivity by considering all irreducible factors of the characteristic polynomial of  $g$ , rather than a single one, as in [16, Section 4.1]. Once a flat has been found, then the algorithms of [16, Section 3] will find the corresponding tensor decomposition.

For each non-scalar normal subgroup  $N$  of  $G$  of order dividing  $|\mathrm{GL}(s, q)|$ , such that  $|G/N|$  divides  $|\mathrm{GL}(r, q)|$ , and the nonabelian composition factors of  $N$  could all be subgroups of

$L_s(q)$ , and the remaining nonabelian composition factors of  $G$  could all be subgroups of  $L_r(q)$ , we test whether  $V|_N$  splits into a direct sum  $V = V_1 \oplus \cdots \oplus V_r$  of pairwise isomorphic irreducible  $N$ -modules. We then apply the upgraded version of ISPROJECTIVITY to a random element of  $N$ . If the algorithm is decisive, we may stop there. Otherwise, we try several random elements in the hope that “unknown” will not be returned for all of them. If it is, then we must apply the more expensive techniques of Case 2.

## 6.2 Type 2 tests

Now let us consider the second case, where  $G$  preserves a decomposition of  $V$  as  $U \otimes W$  but there is not necessarily a normal subgroup of  $G$  that acts as scalars on  $U$  or  $W$ , other than any scalars in  $G$ .

We use unpublished work of Mark Stather to compute the  $p$ -core of  $G$ , where  $p$  is the characteristic of the field. This can then be used by the algorithms in [15] to construct  $U$ : at least one of the subspaces fixed by  $O_p(G)$  must be a flat in the projective geometry which corresponds to  $U \otimes W$  [16]. If  $O_p(G)$  fixes too many subspaces, an alternative approach is to find a prime  $r$  such that  $r$  divides  $|G|$  but  $r^2$  does not, and instead to calculate  $O_r(G)$ . Again, this is guaranteed to fix a flat in the projective geometry which describes  $U \otimes W$  [16]; if it fixes fewer submodules than  $O_p(G)$  then this approach will be faster.

## 7 Subfield groups

A matrix group  $G$  always has a unique smallest field over which it can be written (by change of basis), namely the field containing the corresponding character [13, VII Theorem 1.17]. Furthermore,  $G$  can only be written over any given subfield in one way. More precisely:

**Proposition 7.1** *Let  $G \leq \mathrm{GL}(d, q)$  be a matrix group, let  $\mathrm{GF}(q') \subset \mathrm{GF}(q)$ , and let  $g, g' \in \mathrm{GL}(d, q)$  be such that  $G^g \leq \mathrm{GL}(d, q')$ .  $Z \geq G^{g'}$ . Then there exists  $h \in \mathrm{GL}(d, q')$  such that  $G^{g^h} = G^{g'^h}$ . In other words, if  $G$  embeds in a subfield group in two different ways, they are equivalent over the subfield.*

PROOF: This is a restatement of [5, Theorem (29.7)] in the language of matrix groups.  $\square$

The algorithms of [7] determine the minimal field  $\mathrm{GF}(q')$  over which  $G$  can be written (modulo scalars) and find a matrix  $x$  demonstrating this, so that  $G^x \leq \mathrm{GL}(d, q')$ .  $Z$ . Since  $\mathrm{GL}(d, q').Z \leq \mathrm{GL}(d, q'').Z$  for any  $q''$  such that  $\mathrm{GF}(q') \leq \mathrm{GF}(q'')$  this calculation effectively solves the “find all” problem without modification.

## 8 Extraspecial normaliser groups

Recall that  $G$  is in class  $C6$  when  $G$  contains an absolutely irreducible extraspecial normal subgroup  $N$  of order  $r^{1+2m}$  (or maybe a 2-group  $4 \circ 2^{1+2m}$  in the case  $r = 2$ ),  $d = r^m$ , and  $r|q - 1$ . When  $G/N$  is an irreducible subgroup of  $\mathrm{Sp}(2m, r)$ , then the algorithm of [2] will recognise this situation, and find  $N$  inside  $G$ . Given normal subgroup generators for  $N$ , a second algorithm of [2] gives a constructive homomorphism  $G \rightarrow G/N \leq \mathrm{Sp}(2m, r)$ .

If  $G/N$  is reducible, then the algorithm of [2] will not necessarily find all of  $N$ , but even if it finds only a subgroup, this will still allow a composition tree to be established. Alternatively, this subgroup will serve to demonstrate that  $G$  is tensor decomposable.

Given a group  $G$  for which a composition tree is known, we test whether it is of extraspecial type by examining the normal subgroups. If there is a normal subgroup of the appropriate extraspecial form  $r^{1+2m}$  or  $2^{2+2m}$  acting absolutely irreducibly in dimension  $r^m$  then  $G$  must be of this type, otherwise it is not. It is easy to check whether an absolutely irreducible normal subgroup given by generators is extraspecial, and Aschbacher has shown [1, Theorem B $\Delta$ ], that each relevant type of extraspecial group has just one absolutely irreducible representation of degree  $r^m$  over suitable fields.

It is possible for  $G$  to be an extraspecial normaliser group in more than one way. An example is given by the Sylow 5-subgroup of  $5^{1+2} \cdot \text{Sp}(5, 2)$  which embeds in, for instance,  $\text{GL}(5, 16)$ . This group, of order 625, has a number of extraspecial normal subgroups of order 125, all of them conjugate in  $\text{GL}(5, 16)$ . However, this can only happen which  $G/N$  acts reducibly as a subgroup of  $\text{Sp}(2m, r)$ , as we show in the following proposition:

**Proposition 8.1** *Let  $N$  be an extraspecial matrix group of order  $r^{1+2m}$ , contained in  $\Delta = \text{GL}(r^m, q)$  for some suitable  $q$ . Let  $G$  be a subgroup of  $N_\Delta(N) \cong r^{1+2m} \cdot \text{Sp}(2m, r)$ , such that  $G/N$  maps under the quotient homomorphism to an irreducible subgroup of  $\text{Sp}(2m, r)$ . Then  $G$  does not contain another normal subgroup that is conjugate in  $\Delta$  to  $N$ .*

PROOF: Suppose the contrary and let  $N_1$  be such a subgroup. Then  $N \cap N_1$  is a normal subgroup of  $G$  properly contained in  $N$ . This subgroup corresponds to a  $G/N$ -invariant subspace of the natural module for  $\text{Sp}(2m, r)$ , which, since  $G/N$  acts irreducibly, must be the whole module or the zero module. If it is the whole module then  $N \cap N_1 = N$ , implying that  $N \leq N_1$ . Since  $N$  and  $N_1$  are  $\Delta$ -conjugate, we see that  $N = N_1$ , a contradiction. So this submodule must be zero, implying that  $N \cap N_1 \leq Z(N)$ , so that  $N$  and  $N_1$  commute. But, since  $\text{Sp}(2m, r)$  acts faithfully on its natural module, we can see that  $C_\Delta(N) = N$ , so that  $N_1 \leq N$ , a contradiction.  $\square$

**Remark:** The same argument applies also in the characteristic 2 case where some of the groups have slightly different structure.

## 9 Tensor induced groups

Let  $G$  be tensor induced. Then  $G$  preserves a tensor decomposition  $V = V_1 \otimes \cdots \otimes V_m$ , where each  $V_i$  has dimension  $r > 1$ ,  $d = r^m$ , and the  $V_i$  are permuted transitively by  $G$ .

If  $G$  is primitive and is not semilinear, then a comparatively minor adjustment of the algorithms in [18] will find all ways in which  $G$  is tensor induced with primitive action on  $\{1, \dots, m\}$ , by which we mean finding all possible stabilisers  $G_1$ , up to conjugacy in  $G$ . The algorithm requires the following hypothesis:

**Hypothesis 9.1** *Let  $G$  be an irreducible tensor-induced group, whose induced action on  $\{1, \dots, m\}$  is primitive. If  $G_S$  is the subgroup of an irreducible tensor-induced group  $G$  that fixes each element of a subset  $S$  of  $\{1, \dots, m\}$  in the induced permutation representation of  $G$ , then  $G_S$  acts irreducibly in its induced action on  $\bigotimes_{i \in S} V_i$ .*

If  $G$  is irreducible, primitive and not semilinear, with primitive action on  $\{1, \dots, m\}$ , then it is shown in [18] that the kernel in  $G$  of the action on  $\{1, \dots, m\}$  acts irreducibly on  $V_1 \otimes \cdots \otimes V_m$ , so Hypothesis 9.1 always holds.

1. If  $G$  is not already known to be tensor induced with respect to a subgroup of index  $m$ , first check that  $|G|$  divides  $(q-1) \cdot |\mathrm{PGL}(r, q) \wr S_m|$ . Then apply the element order test given in [18] to a small number of elements of  $G$ , and finally check that each nonabelian composition factor of  $G$  could be a composition factor of  $L_r(q)$  or  $S_m$ . If  $G$  fails any of these tests, return the empty list.
2. If  $G$  is not already known to be tensor induced with respect to a subgroup of index  $m$ , construct a set  $Y$  of elements of the verbal subgroup of  $G$  corresponding to certain laws of  $S_m$ , as in [18]. Then apply all of the “cheap” tests of the tensor product algorithm (see section 6) to  $\langle Y \rangle^G$ . If it can be shown that this group does not preserve a decomposition for  $V$  as  $V_1 \otimes W$  for  $\dim(V_1) = r$ , return the empty list.
3. Use a low index subgroups algorithm to construct all irreducible maximal subgroups of  $G$  of index  $m$ , up to conjugacy in  $G$ , that contain  $\langle Y \rangle^G$ . Call these  $K_1, \dots, K_k$ . Note that since by hypothesis the kernel in  $G$  of the action on  $\{1, \dots, m\}$  is irreducible on  $V_1 \otimes \dots \otimes V_m$ , the same must be true for each  $K_i$  that corresponds to a point stabiliser in a tensor induced action of  $G$ .
4. For each such  $K_i$ , use Section 6 to determine all ways in which  $K_i$  preserves a decomposition of  $V$  as  $V_1 \otimes W$ , where  $V_1$  has dimension  $u$ .
5. For each such decomposition, determine whether this gives rise to a tensor induced decomposition of  $V$  that is preserved by  $G$ .

As a result of this we conclude that if  $G$  is a tensor induced matrix group satisfying Hypothesis 9.1 then we can find all decompositions  $V = V_1 \otimes \dots \otimes V_m$  that are preserved by  $G$ . In particular this will hold whenever  $G$  is irreducible, primitive and not semilinear, and the induced action on  $\{1, \dots, m\}$  is primitive.

## 10 Classical groups

A group in class  $C8$  has a normal subgroup which is a classical group in its natural representation. Effective algorithms exist for finding bilinear and/or quadratic forms stabilised by a given matrix group (or by its derived subgroup in certain cases), and determining when the group contains the whole of the relevant classical group [22, 23]. We note that apart from some very small values of the parameters, the only possible containments of classical groups over the same field are  $O^\pm(2m, 2^e)$  in  $\mathrm{Sp}(2m, 2^e)$ , and various classical groups inside  $\mathrm{SL}(d, q)$ ; however these are not normal subgroups, so the “find all” problem here is the same as the “find one” problem.

## 11 Conclusions and Further Work

In this paper, we have introduced and motivated a number of alternatives to the question answered by the Aschbacher class identification algorithms: to demonstrate constructively at least one Aschbacher class containing a given matrix group. Of particular note are the simplifications that become possible once the full list of normal subgroups of  $G$  is available.

We have shown that, for a matrix group  $G$  of low degree over a finite field, there exists at least one Aschbacher class containing  $G$  for which one can, in fact, find **all** of the corresponding geometries that are preserved by  $G$ , allowing for the possibility of using these structures in a range of backtrack search algorithms for matrix groups. Many questions remain open:

- there is neither a complexity analysis nor an implementation of these techniques at this time;
- for some groups and Aschbacher classes the number of structures returned by “find all” may be excessive – can “find random” or “find best” be implemented in these cases?
- for some groups the number of normal subgroups may be excessive – can the generation of the full list of normal subgroups be avoided in these cases?
- some groups that preserve geometries of more than one type cannot be effectively studied in of all the classes that they lie in, for instance groups which are both of extraspecial type and tensor decomposable;
- the use of these techniques to support backtrack search in matrix groups, inspired by [25], is virtually unexplored.

## References

- [1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.
- [2] P. Brooksbank, A.C. Niemeyer, and Á. Seress. A reduction algorithm for matrix groups with an extraspecial normal subgroup. In *Proceedings of Finite Groups, Geometries and Computation*. To appear.
- [3] J.J. Cannon, D.F. Holt, M Slattery, and A.K. Steel. Computing subgroups of low index in a finite group. *J. Symbolic Comput.*, 40(2):1013–1022, 2005.
- [4] J.J. Cannon and B Souvignier. On the computation of normal subgroups in permutation groups. *Internat. J. Algebra Comput.* To appear.
- [5] C.W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. Reprint of the 1962 original, A Wiley-Interscience Publication.
- [6] A. Dietze and M. Schaps. Determining subgroups of a given finite index in a finitely presented group. *Canad. J. Math.*, 26:769–782, 1974.
- [7] S.P. Glasby, C.R. Leedham-Green, and E.A. O’Brien. Writing projective representations over subfields. *J. Algebra*. To appear.
- [8] G. Hiss and G. Malle. Corrigenda: “Low-dimensional representations of quasi-simple groups”. *LMS J. Comput. Math.*, 5:95–126, 2002.
- [9] D.F. Holt, C.R. Leedham-Green, E.A. O’Brien, and S. Rees. Computing matrix group decompositions with respect to a normal subgroup. *J. Algebra*, 184(3):818–838, 1996.

- [10] D.F. Holt, C.R. Leedham-Green, E.A. O'Brien, and S. Rees. Testing matrix groups for primitivity. *J. Algebra*, 184(3):795–817, 1996.
- [11] D.F. Holt and S. Rees. Testing modules for irreducibility. *J. Austral. Math. Soc. Ser. A*, 57(1):1–16, 1994.
- [12] D.F. Holt and C.M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.*, 8:46–79, 2005.
- [13] B. Huppert and N. Blackburn. *Finite groups. II*, volume 242 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. AMD, 44.
- [14] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. Cambridge University Press, Cambridge, 1990.
- [15] C. R. Leedham-Green and E. A. O'Brien. Recognising tensor products of matrix groups. *Internat. J. Algebra Comput.*, 7(5):541–559, 1997.
- [16] C. R. Leedham-Green and E. A. O'Brien. Tensor products are projective geometries. *J. Algebra*, 189(2):514–528, 1997.
- [17] C.R. Leedham-Green. The computational matrix group project. In *Groups and computation, III (Columbus, OH, 1999)*, pages 229–247. de Gruyter, Berlin, 2001.
- [18] C.R. Leedham-Green and E.A. O'Brien. Recognising tensor-induced matrix groups. *J. Algebra*, 253(1):14–30, 2002.
- [19] F. Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.*, 4:135–169, 2001.
- [20] K. Lux, J. Müller, and M. Ringe. Peakword condensation and submodule lattices: an application of the MEAT-AXE. *J. Symbolic Comput.*, 17(6):529–544, 1994.
- [21] S.H. Murray and E.A. O'Brien. Selecting base points for the Schreier–Sims algorithm for matrix groups. *J. Symbolic Comput.*, 19(6):577–584, 1995.
- [22] A.C. Niemeyer and C.E. Praeger. A recognition algorithm for classical groups over finite fields. *Proc. London Math. Soc. (3)*, 77(1):117–169, 1998.
- [23] A.C. Niemeyer and C.E. Praeger. A recognition algorithm for non-generic classical groups over finite fields. *J. Austral. Math. Soc. Ser. A*, 67(2):223–253, 1999.
- [24] E.A. O'Brien. Towards effective algorithm for linear groups. In *Finite Geometries, Groups and Computation, (Colorado), September 2004*. To appear.
- [25] C.M. Roney-Dougal. Conjugacy of subgroups of the general linear group. *Experiment. Math.*, 13(2):151–163, 2004.
- [26] C.M. Roney-Dougal. The primitive groups of degree less than 2500. *J. Algebra*, 292:154–183, 2005.

- [27] G.M. Seitz and A.E. Zalesskii. On the minimal degrees of projective representations of the finite Chevalley groups. II. *J. Algebra*, 158(1):233–243, 1993.
- [28] R.A. Wilson, P. Walsh, J. Tripp, I. Suleiman, S. Rogers, R. Parker, S. Norton, S. Nickerson, S. Linton, and J. Bray. <<http://web.mat.bham.ac.uk/atlas/v2.0/>>, 2005.