Conjugacy of Subgroups of the General Linear Group

Colva M. Roney-Dougal

CONTENTS

In this paper we present a new, practical algorithm for solving the subgroup conjugacy problem in the general linear group.

1. INTRODUCTORY MATERIAL

This paper presents a new algorithm to solve a subcase of the following:

Problem 1.1. Given two groups $G, H \leq K$, determine whether there exists a $k \in K$ such that $G^k = H$. If so, return one such k.

This problem is known as the subgroup conjugacy problem and is computationally difficult to solve. The usual approach is to modify algorithms for computing normalisers of subgroups, since the set of elements of K which conjugate G to H, if nonempty, is a coset of $N_K(G)$. Butler developed a backtrack search algorithm for permutation and matrix groups [Butler 82] and used this to compute normalisers of permutation groups and to solve the subgroup conjugacy problem in permutation groups [Butler 83]. Butler's ideas for computing subgroup normalisers were extended by Holt [Holt 91], but only for permutation groups. More recently, Leon made significant improvements to the backtrack search algorithm [Leon 97], but once again this was for permutation groups.

We consider the case where $K := \mathrm{GL}(n, q)$ and G and H are given as matrix groups. Eick and Höfling [Eick and Höfling 03] developed an algorithm to determine the conjugacy of irreducible soluble subgroups of $\mathrm{GL}(n, q)$. They represent G and H as polycyclic groups and hence compute $\mathrm{Aut}(G)$ and an explicit isomorphism between G and H. These are combined to determine the existence of an element of $\mathrm{GL}(n, q)$ that conjugates G to H. This technique is effective, but it is limited by the time requirements of computing automorphism groups and is only applicable to irreducible groups.

Our algorithm uses Aschbacher's theorem [Aschbacher 84] to reduce the time spent searching for a conjugating element: its primary goal is to prove that G and H are conjugate, although we present some ideas on how to prove that they are not. It is applicable to geometric subgroups of $\mathrm{GL}(n, q)$. The approach is to use the geometries described in Aschbacher's theorem to find $A, B \in \mathrm{GL}(n, q)$ such that G^A and H^B are contained in a given maximal subgroup $C \leq \mathrm{GL}(n, q)$. Standard conjugacy techniques (for permutation groups) are then used to try to find an element of C that conjugates G^A to H^B. Whilst there is not always a guarantee that such an element exists, experiments show that generally one does; for some of the Aschbacher classes, we prove that one can be found whenever G and H are conjugate in the general linear group.

The development of this algorithm was motivated by the observation that determining the conjugacy of subgroups of $\mathrm{GL}(6, 3)$ often required several days of computing time. Although the methods described in this paper will not always succeed either in finding a conjugating element or in proving that G and H are not conjugate, they are useful because they can often solve the conjugacy problem inside general linear groups that were far too large for previous approaches. The timings data in Section 6 demonstrates this.

An implementation of this algorithm will be released with Version 2.11 of Magma [Bosma et al. 97].

At present the algorithm only works to determine conjugacy under the general linear group. There are several directions in which it could be generalised. The most obvious is to make it work inside any classical matrix group. The biggest problem will be the construction of the relevant maximal subgroups, but recent work of Holt and the author [Holt and Roney-Dougal] gives generating matrices for most of these groups in the linear, symplectic, and unitary cases.

The algorithm could perhaps be made faster by making certain sections of it recursive. Aschbacher's theorem is used to find a maximal subgroup $C \leq \mathrm{GL}(n, q)$ and two matrices $A, B \in \mathrm{GL}(n, q)$ such that $G^A, H^B \leq C$. For many of the Aschbacher classes, it should be possible to recursively apply Aschbacher's theorem to part or all of the group C, to construct $A', B' \in C$ and a maximal subgroup $C' \leq C$ such that $G^{AA'}, H^{BB'} \leq C'$, and then to search C' for a conjugating element. We write $H \sim_K G$ to denote that H is conjugate to G under K. The cost of this recursive approach is that it seems intuitively less likely that $G^{AA'} \sim_{C'} H^{BB'}$ than that $G^A \sim_C H^B$; however, the time gains of computing conjugacy inside a smaller group, with a smaller degree permutation representation, would probably outweigh this.

In Section 2 we make some key definitions, state Aschbacher's theorem, and prove a few elementary results. In Section 3 we give an overview of our algorithm for determining the conjugacy of geometric matrix groups, and then in Section 4 we describe how it works in each geometric Aschbacher class. In Section 5 we discuss the accuracy and reliability of the algorithm and conclude in Section 6 with timings data.

2. PRELIMINARY RESULTS

We now recall some basic mathematical definitions, prove a few fundamental lemmas, and state Aschbacher's theorem.

Let $G \leq \mathrm{GL}(n, q)$ be given, and set $V := \mathbb{F}_q^{(n)}$. Then G is *reducible* if it stabilises a proper nontrivial subspace of V, and is *irreducible* otherwise. If the image of G under the natural embedding into $\mathrm{GL}(n, \mathbb{F})$ is irreducible for all field extensions $\mathbb{F}$ of $\mathbb{F}_q$, then G is *absolutely irreducible*. If G is irreducible and preserves a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_t$ with $t > 1$, then G is *imprimitive*.

Theorem 2.1. (Aschbacher's Theorem [Aschbacher 84].**)** *Let $G \leq \mathrm{GL}(n, q)$ be given, let $q = p^e$, let $V := \mathbb{F}_q^n$, and let $Z := Z(\mathrm{GL}(n, q))$. Then one of the following holds:*

1. *G is reducible.*

2. *G is imprimitive.*

3. *G can be embedded in $\Gamma\mathrm{L}(n/s, q^s)$ for some prime s dividing n.*

4. *G preserves a tensor product $V = V_1 \otimes V_2$, where $\dim V_1 \neq \dim V_2$.*

5. *A conjugate of G is a subgroup of $\mathrm{GL}(n, p^f)Z$, where e/f is prime.*

6. *The dimension $n = r^m$, where r is prime. If r is odd or $n = 2$, then r divides $q - 1$, and G normalises an extraspecial r-group. Otherwise, 4 divides $q - 1$, and G normalises a 2-group of symplectic type.*

7. *G preserves a tensor induced decomposition $V = V_1 \otimes \cdots \otimes V_t$ with $t > 1$.*

8. *G lies between a classical group and its normaliser in $\mathrm{GL}(n, q)$, or preserves a classical form up to scalar multiplication.*

9. *For some nonabelian simple group T, the group $G/(G \cap Z)$ is almost simple with socle T. In this*

case the normal subgroup $(G \cap Z).T$ acts absolutely irreducibly, preserves no nondegenerate classical form, is not a subfield group, and does not contain $\mathrm{SL}(n, q)$.

The original theorem describes subgroups of all classical groups: see [Aschbacher 84].

We follow the notation of [Kleidman and Liebeck 90] when naming classical groups. In particular $\mathrm{O}^\epsilon(n, q)$, where ϵ is $+$, $-$, or omitted, denotes the largest subgroup of $\mathrm{GL}(n, q)$ to preserve a quadratic form of type ϵ. The groups $\mathrm{GSp}(n, q)$ and $\mathrm{GO}^\epsilon(n, q)$ are the normalisers in $\mathrm{GL}(n, q)$ of $\mathrm{Sp}(n, q)$ and $\mathrm{O}^\epsilon(n, q)$.

A group $G \leq \mathrm{GL}(n, q)$ *lies in class* $\mathcal{C}_i$ if the ith condition of the theorem holds, and G is *geometric* if $G \in \mathcal{C}_i$ for some $i \leq 8$. The class $\mathcal{C}_i$ is *recognisable* for G if there exist algorithms to recognise that $G \in \mathcal{C}_i$. Let G be any geometric group other than a member of $\mathcal{C}_8$ that does not fix a classical form (up to scalar multiplication), then, G can be recognised as being a member of at least one Aschbacher class: more details will be given later.

A matrix group G is *AS-maximal* if G is a maximal member of an Aschbacher class. Aschbacher proved a theorem that may be informally stated by saying that, with the exception of reducible AS-maximals that are conjugate under the duality automorphism, the geometric AS-maximals of a given type are all conjugate under the general linear group [Aschbacher 84, Theorem BΔ].

An *AS-overgroup* for a geometric group G is an AS-maximal that preserves a structure of the same type as G: constructions for canonical AS-overgroups will be given later. If G has been conjugated into a given AS-overgroup, then G has been *standardised* (with respect to that AS-overgroup).

We finish with some algorithmic preliminaries. We assume that integer operations require constant time. We also assume that primitive polynomials are known for all finite fields that we encounter and that elements of $\mathbb{F}_{p^e}$ are stored as polynomials of degree $e - 1$ over $\mathbb{F}_p$. Thus, field operations require time $O(\log q)$, and elements of $\mathrm{GL}(n, q)$ are constructed in $O(n^2 \log q)$. We assume that matrix multiplication is $O(n^3 \log q)$ and that primitive field elements are known. We will not assume the availability of discrete logs. By *constructing* a group we mean producing a set of generating elements for the group: usually these will be a collection of matrices.

Lemma 2.2. *Given a primitive element* $z \in \mathbb{F}_q^*$, *the groups* $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$ *and* $\mathrm{Sp}(n, q)$ *can be constructed*

in time $O(n^2 \log q)$. *The groups* $\mathrm{GU}(n, q)$ *and* $\mathrm{SU}(n, q)$ *can be constructed in time* $O(n^2 \log q + \log^2 q)$.

Proof: Pairs of generating matrices are known for $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$, $\mathrm{Sp}(n, q)$, $\mathrm{GU}(n, q)$, and $\mathrm{SU}(n, q)$ [Taylor 87]. In the linear and symplectic cases, all coefficients lie in the set $S := \{0, \pm 1, \pm z^{\pm 1}\}$. All coefficients in the unitary case lie in $T := S \cup \{\pm z^{\pm p}, \pm(1 + z^{p-1})^{-1}\}$. The set S can be constructed in $O(\log q)$, and T can be constructed in $O(\log^2 q)$. $\quad\square$

If $D = (d_{ij})_{n \times n}$ is diagonal, we write $D = \mathrm{Diag}[d_{11}, d_{22}, \ldots, d_{nn}]$. If $d_{ij} = 0$ unless $j = n - i + 1$, we write $D = \mathrm{AntiDiag}[d_{1n}, d_{2(n-1)}, \ldots, d_{n1}]$. When generated as in Lemma 2.2, $\mathrm{Sp}(d, q)$ preserves a form $\mathrm{AntiDiag}[1, \ldots, 1, -1, \ldots, -1]$, and $\mathrm{GU}(d, q)$ preserves a form $\mathrm{AntiDiag}[1, \ldots, 1]$. For odd q we assume that $\mathrm{SO}(2m+1, q)$ preserves a form with matrix I_{2m+1}. When q is odd, we assume that $\mathrm{SO}^\pm(2m, q)$ preserves an orthogonal form with matrix $\mathrm{Diag}[z, 1, \ldots, 1]$ or I_{2m}, depending on whether $(q-1)n/4$ is even or odd. For even q we assume that the orthogonal groups of $+$ and $-$ type preserve the form given by Magma.

Lemma 2.3. *There is a Las Vegas* $O(\log^3 q)$ *algorithm that, with probability of success* $1/2$, *finds* $a, b \in \mathbb{F}_q$ *such that* $a^2 + b^2 = z$.

Proof: Search $\mathbb{F}_q^*$ for an element b such that $z - b^2$ is a square. At least half of the field elements are squares, and each test of squareness costs $O(\log^3 q)$ [Lidl and Niederreiter 83]. $\quad\square$

Lemma 2.4. *For* $\epsilon \in \{+, -, \circ\}$, *the groups* $\Omega^\epsilon(n, q)$, $\mathrm{SO}^\epsilon(n, q)$, $\mathrm{O}^\epsilon(n, q)$, *and* $\mathrm{GO}^\epsilon(n, q)$ *may be constructed in time* $O(n^3 \log q + \log^3 q)$.

Proof: Let $S := \{0, 1, z, \nu, \overline{\nu}\}$, where $\langle \nu \rangle = \mathbb{F}_{q^2}^*$. The set S can be constructed in time $O(\log^2 q)$. In [Rylands and Taylor 98] small sets of generating matrices are given for $\Omega^\epsilon(n, q)$, which can be constructed in time $O(n^2 \log q)$, given S.

Let S_ϵ extend $\Omega^\epsilon(n, q)$ to $\mathrm{SO}^\epsilon(n, q)$, if these groups are not equal. Let R_s be a reflection in a vector of square norm and R_n be a reflection in a vector of nonsquare norm: R_s and R_n can be constructed in time $O(n^2 \log q)$. By [Kleidman and Liebeck 90, Sections 2.6–2.8], we may take $S_\epsilon := -I$ if n is even, q is odd, and the discriminant of the form is nonsquare; $S_\epsilon := R_s R_n$ if n is odd or n is even, q is odd, and the discriminant is square; or $S_\epsilon := R_s$

if n and q are both even. Thus, we construct S_ϵ in time $O(n^3 \log q)$.

Let T_ϵ extend $\mathrm{SO}^\epsilon(n, q)$ to $\mathrm{O}^\epsilon(n, q)$, if these groups are not equal. By [Kleidman and Liebeck 90, Sections 2.6–2.8], we may take $T_\epsilon := R_s$ if n is even and q is odd, and $T_\circ := -I$ if q is odd, in time $O(n^2 \log q)$.

Let D_ϵ extend $\mathrm{O}^\epsilon(n, q)$ to $\mathrm{GO}^\epsilon(n, q)$. Assume that the quadratic form has matrix $\mathrm{AntiDiag}[1, \ldots, 1]$ in type $+$ and either the identity or $\mathrm{Diag}[z, 1, \ldots, 1]$ in type $-$: a matrix conjugating our original group to one preserving this form can be constructed in time $O(n^3 \log q)$ [Holt and Roney-Dougal]. Then $D_\epsilon := zI_n$ if n is odd or q is even. If q is odd, then $D_+ := \mathrm{Diag}[z, \ldots, z, 1, \ldots, 1]$ and $D_- := \mathrm{Diag}[P, \ldots, P]$ or $\mathrm{Diag}[\mathrm{AntiDiag}[z, 1], P, \ldots, P]$, depending on whether the discriminant of the form is square or nonsquare, where a and b are as in Lemma 2.3 and

$$P := \begin{pmatrix} a & b \\ b & -a \end{pmatrix}. \qquad \square$$

Lemma 2.5. *Given a set $\mathcal{S}$ of generating matrices for $G \leq \mathrm{GL}(n, q)$ and a set $\mathcal{T}$ of generating permutations for $H \leq \mathrm{Sym}(d)$, a set of generating matrices for $G \wr H \leq \mathrm{GL}(nd, q)$ can be constructed in time $O((|\mathcal{S}| + |\mathcal{T}|)(nd)^2 \log q)$.*

Proof: For each generating matrix $X \in \mathcal{S}$, define a matrix $\mathrm{Diag}[X, I_n, \ldots, I_n]$. For each $Y \in \mathcal{T}$, define an $nd \times nd$ block matrix whose (i, j)th block is I_n, if Y maps $i \mapsto j$, and 0 otherwise. The group $G \wr H$ is generated by these $(|\mathcal{S}| + |\mathcal{T}|)$ matrices. $\square$

Let $G \leq \mathrm{GL}(n, q)$ and $H \leq \mathrm{GL}(m, q)$. By $G \otimes H$ we mean a group isomorphic to $(G \times H)/\langle (x, x^{-1}) : x \in G \cap H \cap Z(\mathrm{GL}(nm, q)) \rangle$. Note that if G and H are absolutely irreducible, then this reduces to the standard central product $G \circ H$. The group $G \otimes H$ has a natural action on $\mathbb{F}_q^{(n)} \otimes \mathbb{F}_q^{(m)}$.

By $H\mathrm{TensWr}K$, where $H \leq \mathrm{GL}(n, q)$ and $K \leq \mathrm{Sym}(t)$ is transitive, we mean the subgroup of $\mathrm{GL}(n^t, q)$ given by

$$(H \otimes \cdots \otimes H) : K.$$

The group K permutes the factors in the central product.

Lemma 2.6. *Let $G := \langle \mathcal{S} \rangle \leq \mathrm{GL}(n, q)$ and $H := \langle \mathcal{T} \rangle \leq \mathrm{GL}(m, q)$. The group $G \otimes H \leq \mathrm{GL}(mn, q)$ can be constructed in $O((|\mathcal{S}| + |\mathcal{T}|)(mn)^2 \log q)$, and $G\mathrm{TensWr}\,\mathrm{Sym}(t)$ can be constructed in $O(|\mathcal{S}| n^{2t} \log q)$.*

Proof: The group $G \otimes H$ is generated by the Kronecker products of elements of $\mathcal{S}$ with 1_H and of 1_G

with elements of $\mathcal{T}$. Given $X \leq G$ and $Y \leq H$, the Kronecker product $X \otimes Y$ has $X_{ij}Y_{kl}$ in position $((i-1)m + k, (j-1)m + l)$. Each matrix is therefore written down in time $O((mn)^2 \log q)$.

The final claim is from [Holt and Roney-Dougal]. $\square$

3. ALGORITHMIC OVERVIEW

We give a description of the algorithm for geometric groups, which is then specialised for each Aschbacher class.

```
IsGLConjugate(G, H)
```

1. Input: $G, H \leq \mathrm{GL}(n, q)$.

2. If $G = H$, return `true`. If not then compute several group-theoretic invariants of G and H. If these are different, return `false`.

3. Replace G and H by random $\mathrm{GL}(n, q)$-conjugates.

4. For each $\mathcal{C}_i \neq \mathcal{C}_9$ to which G can be recognised as belonging:

   (a) Identify a structure S that G preserves, construct an AS-overgroup C for G, and find $A \in \mathrm{GL}(n, q)$ that standardises G.

   (b) If H can be shown not to preserve a structure isomorphic to S, then return `false`.

   (c) Form a faithful representation ρ of C.

   (d) For at least one structure isomorphic to S that is preserved by H do:

      i. Find $B \in \mathrm{GL}(n, q)$ which standardises H.

      ii. Use an existing conjugacy algorithm for permutation groups to decide whether there exists an $X\rho \in C\rho$ such that $(G^A)\rho^{X\rho} = (H^B)\rho$.

      iii. If so, return `true`, AXB^{-1}. If not, and $i = 6$, then return `false`.

   (e) If $i \in \{1, 8\}$ return `false`.

5. Return `unknown`

In Step 2, various invariants are computed for G and H, including their orders and their orbit lengths on vectors, and 1- and 2-spaces. If they are not soluble, then we compute their soluble radicals and apply the same comparisons to them. If G and H are small and soluble, then we compute their conjugacy classes and check that there is a bijection between them that preserves class sizes and the characteristic polynomials of the class representatives.

In Step 3, we replace G and H by random conjugates. This is to ensure that if `unknown` is returned and the algorithm is run again, then different behaviour will be displayed.

The behaviour of the algorithm at Step 4(d) depends on the Aschbacher class $\mathcal{C}_i$. For instance, in class $\mathcal{C}_1$ we can find *all* appropriate structures, up to the action of H. However, in other classes this is not so: in the imprimitive case, for instance, we can specify the block size that we require, but beyond this there is no control over what structures we find. This will be discussed on a case-by-case basis in Section 4.

If $G \sim_{\mathrm{GL}(n,q)} H$, there are two ways that `unknown` may be returned. *Type 1 failure* occurs when, for each identifiable Aschbacher class for G and H, no matching structures can be found for the loop 4(d). *Type 2 failure* is when, for each identifiable class for G and for each standardising matrix that is tested for H, the standardised copies of G and H are not conjugate in their AS-overgroup in Step 4(d)ii. We will discuss the probability of these failures in Section 5.

If $G \not\sim_{\mathrm{GL}(n,q)} H$, then `unknown` is returned if G and H pass the invariant tests of Step 2 of the main algorithm, lie in the same Aschbacher classes, and cannot be shown to preserve structures of different types: in practice this almost never happens.

4.   DETAILS FOR EACH CLASS

For $1 \leq i \leq 8$, we now describe how to recognise that a group is in $\mathcal{C}_i$, how to construct canonical AS-overgroups, and how to standardise groups in $\mathcal{C}_i$. In classes $\mathcal{C}_1$ and $\mathcal{C}_8$, we show that it is possible to return `false` in Step 4(e), and in $\mathcal{C}_6$ we show that one may return `false` in Step 4(d)iii.

Let $\{e_i \; : \; 1 \leq i \leq n\}$ be the standard basis for $V := \mathbb{F}_q^{(n)}$.

4.1   Reducible Groups

Meataxe-based techniques can recognise that G is reducible [Holt and Rees 94], in time polynomial in n and $\log q$.

Let $G \leq \mathrm{GL}(n,q)$, and let M and N be G-modules over $\mathbb{F}_q$. By $\mathrm{Hom}_{\mathbb{F}[G]}(M, N)$ we denote the subspace of $\mathrm{Hom}_{\mathbb{F}_q}(M, N)$ consisting of all homomorphisms that commute with the action of $\mathbb{F}[G]$, where $\mathbb{F}$ is a splitting field for N. The map $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(M, N)$ is an *isomorphism of G-modules* if ϕ is invertible and for all $v \in M$ and $g \in G$ we have $(vg)\phi = (v\phi)g$. The *constituents* of a G-module M are representatives of G-isomorphism

classes of composition factors of M. The *multiplicity* of a constituent C is the number of composition factors of M_G that are isomorphic, as G-modules, to C.

Proposition 4.1. *Suppose $G, H \leq \mathrm{GL}(n,q)$ have beeen recognised as reducible. Then an AS-overgroup C can be constructed in time $O(n^2 \log q)$. In time polynomial in n and $\log q$, a standardising matrix A for G and a list $\mathcal{M}_H$ of standardising matrices for H may be constructed, where $|\mathcal{M}_H| \leq n$.*

Proof: Let M_G be the natural G-module. We start by identifying a submodule W of M_G, which we will use to determine the type of AS-overgroup to construct and to standardise G. We will denote the dimension of W by d.

We use the algorithms of [Cannon et al., Section 4] to form a set $\mathcal{I}_G$ of constituents of M_G, in time polynomial in n and $\log q$. If some of the constituents in $\mathcal{I}_G$ have multiplicity 1 and a nontrivial image in M_G (so that they correspond to irreducible submodules of M_G), then we select one of these, of dimension as close as possible to $n/2$, and let W be its image in M_G.

Otherwise, if all constituents of multiplicity 1 do not correspond to submodules of M_G, there are two possibilities. If there exists a constituent Δ of dimension e such that $\mathrm{Hom}_{\mathbb{F}[G]}(\Delta, M_G)$ has dimension k and $ke < n$, then we let W be the submodule of M_G generated by the images of a basis of $\mathrm{Hom}_{\mathbb{F}[G]}(\Delta, M_G)$, under the natural inclusion map into M_G. This is a proper submodule of M_G, of dimension $d = ke$.

If no such constituent Δ exists, then we let W be any irreducible submodule of M_G (all irreducible submodules of M_G are G-module isomorphic to W) and let d denote the dimension of W.

We create an AS-overgroup $M(n, d, q)$ that is the stabiliser in $\mathrm{GL}(n,q)$ of $\langle e_{n-d+1}, \ldots, e_n \rangle$, in time $O(n^2 \log q)$ by [Holt and Roney-Dougal].

Let $X \in \mathrm{GL}(n,q)$ have as rows the basis vectors of a complement of W in $\mathbb{F}_q^n$ followed by a basis for W, and put $A := X^{-1}$. All matrices in G^A have a $(d \times (n-d))$ block of zeros in the bottom left corner, so $G^A \leq M(n, d, q)$.

Next we turn to H: we aim to construct a list $\mathcal{J}_H$ of suitable representatives of the d-dimensional submodules of the natural H-module, M_H. We again use [Cannon et al., Section 4] to compute the set $\mathcal{I}_H$ of constituents of M_H.

If W is the image of a constituent of multiplicity 1 and M_H does not have at least one constituent of multiplicity 1 and dimension d, then $G \not\sim_{\mathrm{GL}(n,q)} H$. For each $U \in \mathcal{I}_H$

of multiplicity 1 and dimension d, we let $\mathcal{B}_U$ be a basis for $\mathrm{Hom}_{\mathbb{F}[H]}(U, M_H)$. For $V \in \mathcal{B}_U$ we append $\mathrm{Im} V$, viewed as a submodule of M_H, to $\mathcal{J}_H$.

If W is the image in $\mathcal{M}_G$ of k composition factors of M_G, then if M_H does not have at least one constituent of dimension e and multiplicity k, then $G \not\sim_{\mathrm{GL}(n,q)} H$. For each such constituent we append a submodule S to $\mathcal{J}_H$, constructed in the same way as W.

Finally, if W is one possible image in $\mathcal{M}_G$ of a constituent C of multiplicity k and dimension $d = n/k$, then if M_H does not also have a single constituent C of multiplicity k and dimension d, then $G \not\sim_{\mathrm{GL}(n,q)} H$. Let $\mathcal{B}$ be a basis of $\mathrm{Hom}_{\mathbb{F}[H]}(C, M_H)$, and let $\mathcal{J}_H$ contain the image of a single $V \in \mathcal{B}$, considered as a submodule of M_H.

Note that $|\mathcal{J}_H| \leq n/d$, since there is at most one element of $\mathcal{J}_H$ for each composition factor of $\mathcal{M}_H$. For each $S \in \mathcal{J}_H$, we define a change of basis matrix Y_S, in the same way as we formed X for G, and let $B_S := Y_S^{-1}$. Let $\mathcal{M}_H := \{B_S \; : \; S \in \mathcal{J}_H\}$, then for each $B_S \in \mathcal{M}_H$, we have $H^{B_S} \leq M(n, d, q)$, so each B_S standardises H.   □

The following theorem shows that we can return `false` in Step 4(e) of the main algorithm, since the loop in Step 4(d) may be made to consider all submodules in $\mathcal{J}_H$.

Theorem 4.2. *We have $G \sim_{\mathrm{GL}(n,q)} H$ if and only if there exists $B \in \mathcal{M}_H$ with $G^A \sim_{M(n,d,q)} H^B$.*

Proof: One direction is clear, we prove the converse.

Suppose without loss of generality that $G \leq M(n, d, q)$, so that $A = 1$. Let $E \in \mathrm{GL}(n, q)$ conjugate G to H. We wish to show that there exists $B \in \mathcal{M}_H$ and $X \in M(n, d, q)$ such that $G^{XB^{-1}} = H$.

Suppose first that W is an irreducible submodule that is isomorphic to a unique composition factor of M_G. Then, for some $T \in \mathcal{J}_H$, we have $TE = W$. Now, $M(n, d, q)$ contains all elements of $\mathrm{GL}(n, q)$ fixing W, and $WB_T = T$. Thus the coset $M(n, d, q)B_T^{-1}$ contains all elements of $\mathrm{GL}(n, q)$ mapping T to W, and so $E \in M(n, d, q)B_T^{-1}$.

Next suppose that W is a ke-dimensional reducible submodule of M_G, generated by k isomorphic irreducible submodules, each of dimension e. Then, $\mathcal{J}_H$ will consist of all ke-dimensional submodules of M_H that are generated by sets of k pairwise isomorphic irreducible e-dimensional submodules. Thus, for some $T \in \mathcal{J}_H$, we must have $TE = W$, and the argument is identical to the previous case.

Finally, suppose that W is an irreducible submodule of M_G and that M_G has a basis consisting of submodules

isomorphic to W. Then, since $G \sim_{\mathrm{GL}(n,q)} H$, the set $\mathcal{J}_H$ consists of a single submodule T, chosen from a basis of isomorphic submodules for M_H. Now, $N_{\mathrm{GL}(n,q)}(G)$ can map any such basis of submodules for M_G to any other, and hence there exists at least one $D \in N_{\mathrm{GL}(n,q)}(G)$ such that $G^{DE} = H$ and $T(DE) = W$. The result then follows as in case 1.   □

One alternative to Proposition 4.1 is to match up the entire composition series of V under G with the composition series of V under H and to then look for a conjugating element inside the maximal subgroup of $\mathrm{GL}(n, q)$ to preserve this composition series. This may often be faster in practice, but multiplies the complexity by $n!$.

4.2 Imprimitive Groups

The AS-maximals in $\mathcal{C}_2$ are isomorphic to $\mathrm{GL}(m, q) \wr \mathrm{Sym}(t)$, where $mt = n$ and $t > 1$. A recognition algorithm for absolutely irreducible imprimitive groups is given in [Holt et al. 96a], which also returns a set $\mathcal{B}_G$ of blocks for G. The algorithm can be made to look for blocks of a specific dimension, so the conjugacy algorithm returns `false` at Step 4(b) if no blocks of the correct dimension exist. No further choices can be specified by the user, so the loop in Step 4(d) is repeated up to 20 times, replacing H by a random conjugate each time.

Lemma 4.3. *Suppose that G has been recognised as $\mathcal{C}_2$. An AS-overgroup can be constructed in time $O(n^2 \log q)$ and G can be standardised in $O(n^3 \log q)$.*

Proof: Let $\mathcal{B}_G := \{V_1, \ldots, V_t\}$. The AS-overgroup $\mathrm{GL}(m, q) \wr \mathrm{Sym}(t)$ is constructed in $O(t + m^2 \log q + n^2 \log q) = O(n^2 \log q)$, by Lemmas 2.2 and 2.5.

To standardise, let A be a matrix whose $((i-1)m+1)$-th to im-th rows are a set of basis vectors of V_i, for $1 \leq i \leq t$. Then the i-th block of imprimitivity preserved by $G^{A^{-1}}$ is $V_i A^{-1} = \langle e_{(i-1)m+1}, \ldots, e_{im} \rangle$, so $G^{A^{-1}} \leq C$.   □

4.3 Superfield Groups

Definition 4.4. *A group $G \leq \mathrm{GL}(n, q)$ is a superfield group of degree s if for some $s | n$ with $s > 1$ the group G may be embedded in $\Gamma \mathrm{L}(n/s, q^s)$.*

The AS-maximals in $\mathcal{C}_3$ are isomorphic to $\Gamma \mathrm{L}(n/s, q^s)$, for each prime divisor s of n. If G is not absolutely irreducible, then this can be recognised by an algorithm of Holt and Rees [Holt and Rees 94]. If $G \in \mathcal{C}_3 \setminus \mathcal{C}_2$

is absolutely irreducible, then this can be recognised by Smash [Holt et al. 96b]. Both algorithms also return s and a *centralising matrix* $Z_G \in \mathrm{GL}(n, q)$. This has order dividing $q^s - 1$ but not $q^i - 1$, for $i < s$, and centralises a normal subgroup of G, which is maximal, subject to being conjugate to a subgroup of $\mathrm{GL}(n/s, q^s)$.

If G is not absolutely irreducible, then the recognition algorithm will correctly identify the degree of the field extension; thus the conjugacy algorithm can return `false` in Step 4(b) if the degrees do not match or if one group is absolutely irreducible and the other is not. However, if both groups are absolutely irreducible, then there may be several different choices of normal subgroup that can be embedded in $\mathrm{GL}(n/s, q^s)$, so the loop in Step 4(d) is run up to 20 times, replacing H by a random conjugate each time.

In the following proposition, let $\phi(n)$ denote Euler's phi function.

Proposition 4.5. *Let s be a prime divisor of n, and suppose that G has been recognised as semilinear of degree s. An AS-overgroup for G may be constructed in time $O(n^2 \log q + \log^2 q)$. Ignoring the time required for integer factorisation, G can be standardised in time $O(\phi(q^s - 1)n^4 \log q + n^3 \log q \log\log q^n)$.*

Proof: The first claim follows from [Holt and Roney-Dougal].

Let Z_C and Z_G be centralising matrices for C and G, respectively. We may assume that $|Z_C| = q^s - 1$, as Z_C is known explicitly, see [Holt and Roney-Dougal].

We use [Cellar and Leedham-Green 97] to compute $|Z_G|$ in time $O(n^3 \log q \log\log q^n)$: the order is a divisor of $q^s - 1$. Let $a := (q^s - 1)/|Z_G|$, and set $S := Z_C^a$. We search $\langle Z_G \rangle$ for an element Z_G^i similar to S, in time $O(n^4 \log q)$ for each test. Functions to determine similarity of matrices also return a change of basis matrix, A.

Then $G^{A^{-1}}$ has centralising matrix S, so $G^{A^{-1}} \leq N_{\mathrm{GL}(n,q)}(\langle S \rangle) = C$. $\square$

This has worse complexity than any other Aschbacher class except $\mathcal{C}_6$. If $d \neq s$, there is an alternative approach for standardisation. Since $|Z_G|$ divides $q^s - 1$, the group $\langle Z_G \rangle$ acts reducibly on V, as does $\langle S \rangle$. We know that $\langle Z_G \rangle \sim_{\mathrm{GL}(n,q)} \langle S \rangle$. Therefore, we may use the conjugacy algorithm from Section 3 to standardise G.

If $d = s$ and $\phi(q^s - 1)$ is large, then the algorithm of Proposition 4.5 may take a while to find a standardising element. However, the AS-overgroup in this case is $\Gamma\mathrm{L}(1, q^d)$, so the final conjugacy check is fast.

4.4 Groups Normalising an Extraspecial Group

Definition 4.6. A group $G \leq \mathrm{GL}(n, q)$ is of *extraspecial type* if G is absolutely irreducible and one of the following is true:

- $n = r^m$ for an odd prime r with $q \equiv 1 \bmod r$, and $r^{1+2m} \trianglelefteq G \leq r^{1+2m} . \mathrm{Sp}(2m, r)$.

- $n = 2^m$, $q \equiv 1 \bmod 4$, and $2_\epsilon^{1+2m} \leq G \leq (4 \circ 2^{1+2m}) . \mathrm{Sp}(2m, 2)$, where $\epsilon \in \{+, -\}$.

- $n = 2$, $q \equiv 3 \bmod 4$ and $G = 2_-^{1+2} . O^-(2, 2)$.

We write the AS-maximal as $C := P . N$, where P is the extraspecial normal subgroup.

An algorithm is given in [Holt et al. 96b] to determine whether an absolutely irreducible group G is of extraspecial type. If it succeeds, then it returns an extraspecial or symplectic-type r-group $P_G \trianglelefteq G$, with $|P_G| \geq r^{1+2m}$.

The following lemma will be used to standardise the extraspecial groups.

Lemma 4.7. *Let $E_1, E_2 \leq \mathrm{GL}(n, q)$ be extraspecial or of symplectic type, of order r^{1+2m} or 2^{2+2m}, let C_I be an imprimitive AS-overgroup for E_1 and E_2, and suppose that $E_1^A, E_2^B \leq C_I$. Then $E_1 \sim_{\mathrm{GL}(n,q)} E_2$ if and only if $E_1^A \sim_{C_I} E_2^B$.*

Proof: One direction is clear; we prove the converse. For $i \in \{1, 2\}$, let N_i be such that $E_i . N_i = N_{\mathrm{GL}(n,q)}(E_i)$, and suppose that $X \in \mathrm{GL}(n, q)$ is such that $E_1^X = E_2$. Then, $E_1^Y = E_2$ for all $Y \in (E_1 . N_1)X$.

Since all AS-maximals in $\mathcal{C}_6$ are $\mathrm{GL}(n, q)$-conjugate [Aschbacher 84, Theorem BΔ], the same is true for all extraspecial subgroups of order r^{1+2m} or 2^{2+2m} that are of the same type. In particular, any extraspecial group is GL-conjugate to one consisting of monomial matrices, since there is a well-known monomial construction for such extraspecial groups.

We may therefore suppose, without loss of generality, that $A = B = I_n$, so that E_1 preserves a decomposition $V := \langle e_1 \rangle \oplus \cdots \oplus \langle e_n \rangle$ and let $C_I := \mathrm{GL}(1, q) \wr \mathrm{Sym}(n)$. Let K_1 be the kernel of the action of E_1 on the set $\mathcal{S} := \{\langle e_i \rangle : 1 \leq i \leq n\}$, and let K_1' be the kernel of the action of E_2 on $\mathcal{S}$. Note that $|K_1| = r^{1+m}$ or 2^{2+m}. Now, E_2 has several elementary abelian normal subgroups of order r^{1+m} (or 2^{2+m}), and K_1^X is not necessarily equal to K_1'. Denote the set of elementary abelian normal subgroups of order r^{1+m} (or 2^{2+m}) in E_i by $\mathcal{K}_i$.

The groups in $\mathcal{K}_i$ are all conjugate under the action of N_i, as they correspond to maximal isotropic subspaces

of $P/Z(P)$. The set of images $\{K_1^Q : Q \in (E_1 . N_1)X\} = \{K_1^Q : Q \in N_1\}^X = \mathcal{K}_1^X = \mathcal{K}_2$. Thus, there exists an element $Y \in (E_1 . N_1)X$ such that $K_1^Y = K_1'$. Now, K_1 fixes $\langle e_i \rangle$, for $1 \leq i \leq n$, and so does K_1'. Therefore, $Y \in C_I$ and $E_1^Y = E_1^X = E_2$, as required. $\qquad\square$

Proposition 4.8. *Suppose that G has been recognised as an extraspecial normaliser. An AS-overgroup for G may be constructed in time $O(n^3 \log q)$. The group G may be standardised in the time required to solve the conjugacy problem for imprimitive matrix groups, as described in Section 4.1. Furthermore, this use of the algorithm in Section 4.1 is guaranteed to return* true *and a conjugating element.*

Proof: An AS-overgroup $C = P.N$ may be constructed in time $O(n^3 \log q)$ [Holt and Roney-Dougal].

Since G has been recognised as of extraspecial type, an extraspecial or symplectic-type r-group $P_G \trianglelefteq G$ has been identified. The group $P \leq C$ consists of monomial matrices and hence is a subgroup of $\mathrm{GL}(1,q) \wr \mathrm{Sym}(n)$. If $|P_G| = |P|$, then we set $P_2 := P_G$. Otherwise $|P_G| = |P|/2$, and we set $P_2 := \langle \mu I_n, P_G \rangle$, where μ is a primitive fourth root of unity in $\mathbb{F}_q$. We use the imprimitive case of `IsGLConjugate(P_2,P)` to find an element A such that $P_2^A = P$. Then, $G^A \leq N_{\mathrm{GL}(n,q)}(P_2^A) = C$.

The final statement follows from Lemma 4.7. $\qquad\square$

The following proposition implies that for $\mathcal{C}_6$ we may return false in Step 4(d)iii of `IsGLConjugate`.

Proposition 4.9. *Let G and H be of extraspecial type, and suppose that C is an extraspecial AS-overgroup for G and H and that $G^A, H^B \leq C$. Then $G^A \sim_C H^B$ if and only if $G \sim_{\mathrm{GL}(n,q)} H$.*

Proof: If $|P_G| = |P|$, then $P_G^A = P$ is the unique normal subgroup of both G^A and H^B of order $|P|$. Therefore, if $G^X = H$, then $X \in N_{\mathrm{GL}(n,q)}(P) = C$.

So suppose that $|P_G| = |P_H| = 2^{1+2m}$. We may assume without loss of generality that $A = B = I_n$, so that $G, H \leq C$. Suppose that there exists $X \in \mathrm{GL}(n,q)$ such that $G^X = H$, and let $G = P_G . N_G$, $H = P_H . N_H$, and $C = P . N$, with $|P| = 2^{2+2m}$.

All groups of order 2^{1+2m} that are of the same type as P_G are conjugate in C. Therefore, there exists an element $Y \in C$ such that $(P_G^X)^Y = P_G$. But $N_{\mathrm{GL}(d,q)}(P_G) = 2^{2+2m} : \mathrm{O}^\epsilon(2m,2) \leq C$, so $XY \in C$ and therefore $X \in C$. $\qquad\square$

4.5   Classical Groups

Several methods exist for finding a classical form preserved by an absolutely irreducible group G: see [Holt and Rees 94] for instance. Since these methods allow one to specify the type of form that is being sought (symplectic, unitary, or orthogonal), the conjugacy algorithm may return false at Step 4(b). The loop in Step 4(d) is run only once, since the form preserved by an absolutely irreducible group is unique, up to scalar multiplication. Note that the full normaliser of $\mathrm{Sp}(n,q)$ and $\mathrm{SO}^\pm(n,q)$ does not fix a form, even up to multiplication by scalars.

We remark that groups containing $\mathrm{SL}(n,q)$ are normal in $\mathrm{GL}(n,q)$, thus two groups of this type are conjugate if and only if they are equal. This possibility will therefore be dealt with at Step 2 of the algorithm.

In the following proposition, the matrix D_S is diagonal and acts as z on the first $n/2$ basis vectors and as 1 on the remainder.

Proposition 4.10. *Let $Z := Z(\mathrm{GL}(n,q^2))$, then $N_{\mathrm{GL}(n,q^2)}(\mathrm{SU}(n,q)) = \langle Z, \mathrm{GU}(n,q)\rangle$, $\mathrm{GSp}(n,q) = \langle Z(\mathrm{GL}(n,q)), \mathrm{Sp}(n,q), D_S\rangle$, and $N_{\mathrm{GL}(n,q)}(\mathrm{SO}^\epsilon(n,q)) = \mathrm{GO}^\epsilon(n,q)$.*

Proof: This follows from various results in [Kleidman and Liebeck 90, Section 4.8]. $\qquad\square$

Theorem 4.11. *Suppose that a group G has been recognised as $\mathcal{C}_8$. An AS-overgroup C of G can be constructed in time $O(n^3 \log q + \log^3 q)$, and G can be standardised in time $O(n^3 \log q)$. Furthermore, if $H \sim_{\mathrm{GL}(n,q)} G$, and A, B are standardising matrices, then $G^A \sim_C H^B$.*

Proof: By Lemmas 2.2 and 2.4 the classical group can be constructed in time $O(n^3 \log q + \log^3 q)$. In each case the normaliser is generated by the classical group and at most two other matrices, each of which can be written down in time $O(n^2 \log q)$.

The standardisation function is described in [Holt and Roney-Dougal]. It is shown there to have complexity $O(n^3 \log q)$.

For the final claim, we may suppose without loss of generality that $A = B = 1$, so that $G, H \leq C$. Let $X \in \mathrm{GL}(n,q)$ satisfy $G^X = H$. Then H preserves the same form as C^X, but since H is absolutely irreducible, it must preserve a unique form of any given type. Thus, C^X preserves the same form as C, so $X \in N_{\mathrm{GL}(n,q)}(C) = C$, and the result follows. $\qquad\square$

4.6 Tensor Product, Subfield, and Tensor Induced Groups

We consider these families together, as each of their recognition algorithms also returns a standardising matrix.

Definition 4.12. If the group $G \leq \mathrm{GL}(n,q)$ preserves a decomposition $V = V_1 \otimes V_2$, then G is a *tensor product group*.

Suppose that $n = m^s$ for $s > 1$. If $G \leq \mathrm{GL}(n,q)$ preserves a decomposition $V = V_1 \otimes \cdots \otimes V_s$ with $\dim(V_i) = m$ for $1 \leq i \leq s$, then G is *tensor induced*.

A group $G \leq \mathrm{GL}(n,q)$ is *subfield* if there exists a subfield $\mathbb{F}_{q_0} \subset \mathbb{F}_q$ such that a conjugate of G may be embedded in $\mathrm{GL}(n,q_0)Z$.

The AS-maximals in $\mathcal{C}_4$ are $\mathrm{GL}(n_1,q) \circ \mathrm{GL}(n_2,q)$, with $n_1 < \sqrt{n}$. Recognition algorithms for absolutely irreducible tensor product groups are given in [Leedham-Green and O'Brien 97a, Leedham-Green and O'Brien 97b]. In $\mathcal{C}_7$, the AS-maximals are $\mathrm{GL}(m,q)\mathrm{TensWr}\,\mathrm{Sym}(s)$. A recognition algorithm for absolutely irreducible $\mathcal{C}_7$ groups is given in [Leedham-Green and O'Brien 02]. Both of these recognition algorithms allow the user to specify the degrees of the tensor factors, so if factors of the correct degree cannot be found, we return `false` in Step 4(b). However, in each case there may be several different decompositions preserved by the group, so the loop in Step 4(d) is repeated up to 20 times, with H replaced by a random conjugate each time.

Lemma 4.13. *Suppose that G has been recognised as tensor product or tensor induced. An AS-overgroup C of G can be constructed in time $O(n^2 \log q)$, and G can be standardised in time $O(n^3 \log q)$.*

Proof: The construction claims follow from Lemma 2.6, and the standardisation claims are clear. □

The AS-Maximals in $\mathcal{C}_5$ are $\mathrm{GL}(n,q_0)Z$, where $\mathbb{F}_{q_0}$ has prime index in $\mathbb{F}_q$. In [Glasby and Howlett 97] an algorithm is given which determines whether an absolutely irreducible group G is conjugate to a subgroup of $\mathrm{GL}(n,q_0)$; this is extended to a general subfield group in [Glasby et al.]. In both cases, the degree of the subfield representation may be specified by the user, so if matching fields are not found, then the algorithm returns `false` at Step 4(b). The loop in Step 4(d) is run up to 20 times, with H replaced by a random conjugate each time.

Lemma 4.14. *Suppose that $G \leq \mathrm{GL}(n,q)$ has been recognised as subfield. Given a primitive element of $\mathbb{F}_{q_0}$, an AS-overgroup C of G can be created, and G can be standardised, in time $O(n^3 \log q + \log^2 q)$.*

Proof: This is clear. □

5. ACCURACY

The following theorem is a summary of our main results. In it we assume that G and H have already been recognised as members of some geometric Aschbacher class. This is because many of the identification algorithms have not been fully analysed for timing complexity.

Theorem 5.1. *Let $G \sim H \leq \mathrm{GL}(n,q)$, and suppose that G and H have been recognised as lying in a geometric Aschbacher class. Then there exist algorithms to construct a group $C \leq \mathrm{GL}(n,q)$, and $A, B \in \mathrm{GL}(n,q)$, such that $G^A, H^B \leq C$. Let $\mathcal{I} = \{1,2,4,5,7,8\}$, then if $G \in \bigcup_{i \in \mathcal{I}} \mathcal{C}_i$, these algorithms run in time polynomial in n and $\log q$.*

Proof: This follows from Theorem 4.11, Lemmas 4.3, 4.13, and 4.14, and Propositions 4.1, 4.5, and 4.8. □

We now consider whether this approach is an effective method for determining $\mathrm{GL}(n,q)$-conjugacy.

Proposition 5.2. *If `IsGLConjugate(G, H)` returns `true`, then $G \sim_{\mathrm{GL}(n,q)} H$. If `IsGLConjugate(G, H)` returns `false`, then $G \not\sim_{\mathrm{GL}(n,q)} H$.*

Proof: If `IsGLConjugate(G, H)` returns `true`, then it has found a conjugating element. If `IsGLConjugate(G, H)` returns `false`, then there is a group or representation invariant that has different values for G and H. □

The following is a corollary of Theorems 4.2 and 4.11 and Proposition 4.9.

Theorem 5.3. *If G is recognisable as a member of $\mathcal{C}_1 \cup \mathcal{C}_8$, then `IsGLConjugate(G, H)` returns `true` or `false` for all H. If G and H have been recognised as members of $\mathcal{C}_6$, then `IsGLConjugate` always returns `true` or `false`.*

As a consequence of the preceding theorem, in Step 4 of `IsGLConjugate`, we consider the case $G \in \mathcal{C}_8$ as soon as possible: namely, as soon as we have checked that $G \notin \mathcal{C}_1 \cup \mathcal{C}_3$ (for we require absolute irreducibility).

From now on, we assume that G and H are geometric and consider the likelihood of `IsGLConjugate` returning `unknown`.

Proposition 5.4. *Let $G \sim_{\mathrm{GL}(n,q)} H$. Suppose that G can be recognised as lying in an Aschbacher class such that G preserves a unique structure in that class, and let C be the corresponding AS-overgroup. If $G^A \leq C$ and $H^B \leq C$, then $G^A \sim_C H^B$.*

Proof: We may assume that $A = B = I_n$, so that $G, H \leq C$. Let $X \in \mathrm{GL}(n,q)$ be such that $G^X = H$. Then $H = G^X \leq C^X \neq C$, and so $H \in C \cap C^X$. Therefore, $G \in C^{X^{-1}} \cap C$, and so $X \in C$. Thus, G and H are conjugate inside an AS-overgroup from an identifiable Aschbacher class. $\square$

We finish with a couple of more speculative lemmas, which show what work needs to be done to make the algorithm deterministic.

Proposition 5.5. *Let $G, H \leq \mathrm{GL}(n,q)$ be geometric. If $G \in \mathcal{C}_i$ for some i, and all Aschbacher structures of type $\mathcal{C}_i$ that are preserved by G can be identified, then `IsGLConjugate` can be modified so that `unknown` is never returned.*

Proof: Suppose that all structures S_G of type $\mathcal{C}_i$ that are preserved by G can be identified, and let $\mathcal{S}_H$ be the set of identified structures of type $\mathcal{C}_i$ that are preserved by H. If $G \sim_{\mathrm{GL}(n,q)} H$, then $\mathcal{S}_H$ contains all structures of type $\mathcal{C}_i$ preserved by H. For one choice of S_G, let S_C be the corresponding structure for the AS-overgroup.

We loop through $S_H \in \mathcal{S}_H$, testing whether, for $X, Y \in \mathrm{GL}(n,q)$ such that $S_G X^{-1} = S_C$ and $S_H Y^{-1} = S_C$, we have $G^X \sim_C H^Y$. If none exists, then an argument similar to Proposition 4.1 shows that $G \nsim_{\mathrm{GL}(n,q)} H$. $\square$

Thus, one way to eliminate failures of types 1 and 2 is to improve the Aschbacher identification algorithms.

Lemma 5.6. *Let $G \sim_{\mathrm{GL}} H$, and suppose that G and H are irreducible and geometric. Suppose that an AS-overgroup C of G and H has been constructed and that G and H have been standardised. If there are m conjugacy classes in C of subgroups that are conjugate to G under $\mathrm{GL}(n,q)$, then the probability of type 2 failure is $(m-1)/m$, for each run of the loop in Step 4(d).*

Proof: Each run of Step 4(d) will put H into a random C-class. $\square$

It appears that m is generally small: in the trials described in the next section, for only four pairs of conjugate groups was `unknown` returned in more than two consecutive trials.

6.   TIMINGS

We performed a variety of timing experiments. The main focus of this article is to develop an algorithm for proving that groups *are* conjugate, so we have not included timings in the case where they are not. The algorithms tested in these trials constitute Steps 3 to 5 of the main algorithm. We used `IsGLConjugate`, implemented only for semilinear and imprimitive groups, when computing the irreducible subgroups of $\mathrm{GL}(4,5)$ and $\mathrm{GL}(6,3)$ in [Roney-Dougal and Unger 03], and found that this reduced the time required from an estimated six months to around 20 minutes in the case of $\mathrm{GL}(6,3)$, and from approximately two weeks to around 30 minutes for $\mathrm{GL}(4,5)$.

For each $i \leq 8$, we computed a set $\mathcal{S}$ of subgroups of $\mathrm{GL}(n,q)$ that lay in $\mathcal{C}_i$. For each group we created three random GL-conjugates and found the average time to identify a conjugating element. Where possible, this was compared with existing conjugacy algorithms in Magma Version 2.10.

We created sets $\mathcal{S}$ for $\mathcal{C}_6$ by constructing all groups that could be identified as lying in $\mathcal{C}_6$, up to conjugacy in a given AS-maximal. For $\mathcal{C}_2$ and $\mathcal{C}_7$ we generated sets $\mathcal{S}$ by successively computing maximal subgroups of the AS-maximal and choosing a random one that could be identified as lying in class $\mathcal{C}_i$. This produces a chain of subgroups, all of which lie in $\mathcal{C}_i$: we made five for each AS-maximal.

For the remaining classes, each set $\mathcal{S}$ consisted of 100 random two-generated subgroups of the AS-maximal C, of index at least 3 in C. This made our timing comparisons with existing conjugacy algorithms slightly worse than they should be, as `IsGLConjugate` often shows the most dramatic improvement over existing algorithms with small groups.

In the tables, times are in seconds and are averages over all trials for that class. Times in brackets are for the standard `IsConjugate` algorithm, as implemented in Magma Version 2.10. The symbol F denotes that the trial took an average of over 2,000 seconds per pair of groups.

For very small general linear groups (roughly $n = 2$ and $q < 20$, $n = 3$, and $q < 7$), the new algorithm may

	$n = 3$	4	5		7	
q	$d = 1$	2	4	3	5	3
3	0.03(0.03)	0.08(0.12)	0.56(0.85)	0.52(0.81)	18.1(24.8)	15.1(25.1)
4				1.97(3.38)	190(263)	167
5	0.07(0.08)	0.46(0.88)	7.10(11.6)	5.45(9.25)		
7	0.16(0.20)	1.53(2.85)	48.2(88.9)	33.7(89.8)		
8	0.30(0.31)	3.21(5.45)		78.8(486)		

TABLE 1. Reducible groups: groups stabilising a d-space.

	$d = 2$			$d = 3$	$d = 4$	$d = 5$
q	$s = 2$	3	5	2	2	2
2					0.47(5.86)	1.76(72.9)
3				0.46(2.01)	1.08(F)	
5	0.28(0.79)	0.70(F)	96.3	1.25(F)		
9	0.45(F)	2.38(F)		26.9		
19	5.16(F)					

TABLE 2. Imprimitive groups: $\mathrm{GL}(d, q)\mathrm{wr}\,\mathrm{Sym}(s) \leq \mathrm{GL}(ds, q)$.

(n, s)	$q_0 = 2$	3	4	5	7	8
(3, 3)		0.05(0.03)	0.08(0.04)	0.11(0.06)		
(4, 2)		0.10(0.12)		0.44(279)	2.33	13.2
(6, 2)	0.13(0.40)	0.95(78.0)	5.82(F)			
(8, 2)	0.84(13.5)	40.1				

TABLE 3. Superfield groups: $\Gamma\mathrm{L}(n/s, q_0^s) \leq \mathrm{GL}(n, q_0)$.

(n_1, n_2)	$q = 3$	4	5	7	8	9
(2, 3)	0.61(3.85)	0.49(176)	0.91	4.29	4.19	10.1
(2, 4)	0.71(F)	2.14				
(3, 3)	0.67(F)	1.75				
(3, 4)	2.56					

TABLE 4. Tensor product groups: $\mathrm{GL}(n_1, q) \otimes \mathrm{GL}(n_2, q) \leq \mathrm{GL}(n_1 n_2, q)$.

p^s	$n = 2$	3	4	5	6
2^2			0.07(0.32)	0.17(2.88)	0.60(52.9)
2^3			0.09(154)	0.22(1634)	0.72
3^2		0.06(0.50)			
3^3		0.10(F)	0.42		
5^2	0.04(0.12)	0.25(37.6)			
5^3	0.14(33.0)	0.73			

TABLE 5. Subfield groups: $\mathrm{GL}(n, p)Z \leq \mathrm{GL}(n, p^s)$.

q	$n = 2$	3	4
7		0.64(0.16)	
9			3.35(111)
13		1.01(19.5)	9.77
16		0.98(12.9)	
19		1.25 (224)	
49	0.01(0.50)		

TABLE 6. Extraspecial normalisers.

q	$d^s = 2^2$	2^3	2^4	3^2	3^3	4^2
3	1.32(0.11)	4.12(969)	30.0	2.48(729)	27.7	10.6
4	1.42(0.34)	3.45	58.8	8.53		
5	1.45(0.75)	7.21		7.19		
7	1.78(2.86)	8.00		41.8		
13	3.04(F)					

TABLE 7. Tensor induced groups: $\mathrm{GL}(d,q)\mathrm{TensWr}\,\mathrm{Sym}(s) \leq \mathrm{GL}(d^s, q)$.

n	Case	$q = 2$	3	4	5	7	11
3	U	0.05(0.04)	0.10(0.31)	0.54(1.68)	1.22(7.74)	14.3(133)	
	O				0.03(0.06)	0.03(0.13)	0.05(0.38)
4	U	0.31(0.32)	0.92(8.69)	7.11(95.9)	65.6		
	S	0.04(0.03)	0.07(0.12)	0.18(0.33)	0.39(0.75)	1.90(3.70)	33.3
	O^+			0.14(0.30)	0.09(0.68)	0.19(4.38)	0.64(169)
	O^-			0.20(0.29)	0.08(0.63)	0.15(1.80)	0.46(9.96)
5	U	0.43(2.90)	13.0(F)				
	O		0.10(0.65)		0.29(6.95)	0.94(86.8)	5.77
6	U	2.44(18.7)					
	S	0.13(0.38)	0.83(3.99)	4.82(472)			
	O^+		0.27(3.85)	0.87(135)	2.33(F)	13.1	
	O^-		0.24(4.97)	0.90(88.8)	1.74(275)		
7	U	9.22					
	O		0.71(17.9)		12.68		
8	S	0.80(7.45)					
	O^+		4.45(F)				
	O^-		2.40(1524)				

TABLE 8. Classical groups: Case $U : \mathrm{GU}(n,q) \leq \mathrm{GL}(n, q^2)$. Case $S : \mathrm{Sp}(n,q) \leq \mathrm{GL}(n,q)$. Case $O^\epsilon : \mathrm{GO}^\epsilon(n,q) \leq \mathrm{GL}(n,q)$.

be slower than the old one. This is as expected, as the overhead of standardising the group is more expensive than gain from computing conjugacy in an AS-overgroup rather than the general linear group. For larger values of n and q, the time gained is roughly proportional to the index of the AS-overgroup in the general linear group.

ACKNOWLEDGMENTS

REFERENCES

[Aschbacher 84] M. Aschbacher. "On the Maximal Subgroups of the Finite Classical Groups." *Invent. Math.* 76 (1984), 469–514.

[Bosma et al. 97] W. Bosma, J. Cannon, and C. Playoust. "The Magma Algebra System I: The User Language." *J. Symbolic Comput.* 24:3 (1997), 235–265.

[Butler and Canon 82] G. Butler and J. J. Canon. "Computing in Permutation and Matrix Groups I: Normal Closure, Commutator Subgroups, Series." *Math. Comp.* 39 (1982), 663–670.

[Butler 82] G. Butler. "Computing in Permutation and Matrix Groups II: Backtrack Algorithm." *Math. Comp* 39 (1982), 671–680.

[Butler 83] G. Butler. "Computing Normalisers in Permutation Groups." *J. Algorithms* 4 (1983), 163–175.

[Cannon et al.] J. J. Cannon, D. F. Holt, M. Slattery, and A. K. Steel. "Computing Subgroups of Low Index in a Finite Group." Submitted to *J. Symbolic Comput.*

[Cellar and Leedham-Green 97] F. Cellar and C. R. Leedham-Green. "Calculating the Order of an Invertible Matrix." In *Groups and Computation II (New Brunswick, NJ, 1995)*, edited by L. Finkelstein and W. M. Kantor, pp. 55–60. Providence, RI: Amer. Math. Soc., 1997.

[Eick and Höfling 03] B. Eick and B. Höfling. "The Solvable Primitive Permutation Groups of Degree at most 6560." *LMS J. Comput. Math.* 6 (2003), 29–39.

[GAP Group] The GAP Group. *GAP–Groups, Algorithms and Programming, Version 4.3*. Available from World Wide Web (http://www.gap-system.org), 2002.

[Glasby and Howlett 97] S. P. Glasby and R. B. Howlett. "Writing Representations over Minimal Fields." *Comm. Algebra* 25 (1997), 1703–1711.

[Glasby et al.] S. P. Glasby, C. R. Leedham-Green, and E. A. O'Brien. "Writing a Representation over a Smaller Field Modulo Scalars." In preparation.

[Holt 91] D. F. Holt. "The Computation of Normalisers in Permutation Groups." *J. Symbolic Comput.* 12 (1991), 499–516.

[Holt et al. 96a] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees. "Testing Matrix Groups for Primitivity." *J. Algebra* 184 (1996), 795–817.

[Holt et al. 96b] 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 (1996), 818–838.

[Holt and Rees 94] D. F. Holt and S. Rees. "Testing Modules for Irreducibility." *J. Austral. Math. Soc. Ser A* 57 (1994), 1–16.

[Holt and Roney-Dougal] D. F. Holt, and C. M. Roney-Dougal. "Constructing Maximal Subgroups of Black Box Classical Groups." Submitted.

[Kleidman and Liebeck 90] P. Kleidman and M. Liebeck. *The Subgroup Structure of the Finite Classical Groups.* Cambridge, UK: Cambridge University Press, 1990.

[Leedham-Green and O'Brien 97a] C. R. Leedham-Green and E. A. O'Brien. "Tensor Products Are Projective Geometries." *J. Algebra* 189 (1997), 514–528.

[Leedham-Green and O'Brien 97b] C. R. Leedham-Green and E. A. O'Brien. "Recognising Tensor Products of Matrix Groups." *Internat. J. Algebra Comput.* 7 (1997), 541–559.

[Leedham-Green and O'Brien 02] C. R. Leedham-Green and E. A. O'Brien. "Recognising Tensor-Induced Matrix Groups." *J. Algebra* 253 (2002), 14–30.

[Leon 97] J. S. Leon. "Partitions, Refinements, and Permutation Group Computation." In *Groups and Computation II (New Brunswick, NJ, 1995)*, edited by L. Finkelstein and W. M. Kantor, pp. 123–158. Providence, RI: Amer. Math. Soc., 1997.

[Lidl and Niederreiter 83] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia of Mathematics and Its Applications, 20. Reading, MA: Addison-Wesley, 1983.

[Roney-Dougal and Unger 03] C. M. Roney-Dougal amd W. R. Unger. "The Primitive Affine Groups of Degree Less than 1000." *J. Symbolic Comput.* 35 (2003), 421–439.

[Rylands and Taylor 98] L. J. Rylands, and D. E. Taylor. "Matrix Generators for the Orthogonal Groups." *J. Symbolic Comput.* 25 (1998), 351–360.

[Taylor 87] D. E. Taylor. "Pairs of Generators for Matrix Groups, I." *The Cayley Bulletin* 3 (1987), 76–85.

Colva M. Roney-Dougal, School of Computer Science, North Haugh, The University of St. Andrews, St. Andrews, Fife KY16 9SS, United Kingdom (colva@dcs.st-and.ac.uk)