Journal of Mathematical Problems, Equations and Statistics

E-ISSN: 2709-9407
P-ISSN: 2709-9393
JMPES 2020; 1(1): 52-55
© 2020 JMPES
www.mathematicaljournal.com
Received: 17-11-2019
Accepted: 21-12-2019

Behnam Razzaghmaneshi
Assistant Professor of
Department of Mathematics
Talesh Branch, Islamic Azad
University, Talesh, Iran

Correspondence
Behnam Razzaghmaneshi
Assistant Professor of
Department of Mathematics
Talesh Branch, Islamic Azad
University, Talesh, Iran

Generating permutations of the general linear groups (GPGLG)

Behnam Razzaghmaneshi

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

Keywords: Matrix groups, conjugacy, algorithms

1. Introduction

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 $Gk = H$. 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 $NK(G)$. 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 H¨ofling [Eick and H¨ofling 03] developed an algorithm to determine the conjugacy of irreducible soluble subgroups of GL (n, q). They represent G and H as polycyclic groups and hence compute Aut (G) and an explicit isomorphism between G and H. These are combined to determine the existence of an element of 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 GA and HB 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 GA to HB. 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 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 $C \leq$ GL (n, q) and two matrices $A,B \in$ GL(n, q) such that $GA,HB \leq C$. 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 $GAA\_,HBB\_ \leq C\_$, 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 $GAA\_ \sim C\_\ HBB\_$ than that $GA \sim C\ HB$; 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 $G \leq$ GL (n, q) be given, and set V:= F$(n)q$. 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 GL $(n$, F) is irreducible for all field extensions F of Fq, then G is *absolutely irreducible*. If G is irreducible and preserves a direct sum decomposition $V = V1 \oplus \cdot \cdot \oplus Vt$ with $t > 1$, then G is *imprimitive*.

Theorem 2.1. (Aschbacher's Theorem [Aschbacher 84].)

Let $G \leq$ GL(n, q) be given, let $q = pe$, let V:= Fnq, and let Z:= Z(GL(n, q)). Then one of the following holds:

1. *G is reducible.*
2. *G is imprimitive.*
3. *G can be embedded in ΓL$(n/s, qs)$ for some prime s dividing n.*
4. *G preserves a tensor product $V = V1 \otimes V2$, where* dim $V1$ _= dim $V2$.
5. *A conjugate of G is a subgroup of* GL$(n, pf\ )Z$*, where e/f is prime.*
6. *The dimension $n = rm$, 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 $V = V1 \otimes \cdot \cdot \otimes Vt$ with $t >$* 1.
8. *G lies between a classical group and its normaliser in* 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*

Roney-Dougal: Conjugacy of Subgroups of the General Linear Group 153 *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* 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 O_(n, q), where _ is +, −, or omitted, denotes the largest subgroup of GL(n, q) to preserve a quadratic form of type _.

The groups GSp(n, q) and GO_(n, q) are the normalisers in GL(n, q) of Sp(n, q) and O_(n, q).

A group $G \leq$ GL(n, q) *lies in class Ci* if the ith condition of the theorem holds, and G is *geometric* if $G \in Ci$ for some $i \leq 8$. The class Ci is *recognisable* for G if there exist algorithms to recognise that $G \in Ci$. Let G be any geometric group other than a member of $C8$ 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 Fpe are stored as polynomials of degree $e - 1$ over Fp. Thus, field operations require time O (log q), and elements of GL (n, q) are constructed in $O(n2$ log $q)$. We assume that matrix multiplication is O $(n3$ 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 $z \in$ F$*q$, the groups* GL (n, q), SL(n, q) *and* Sp(n, q) *can be constructed in time* $O(n2$ log $q)$. *The groups* GU (n, q) *and* SU(n, q) *can be constructed in time* $O(n2$ log q + log2 $q)$. *Proof:* Pairs of generating matrices are known for GL(n, q), SL(n, q), Sp(n, q), GU(n, q), and SU(n, q) [Taylor 87]. In the linear and symplectic cases, all coefficients lie in the set S: = $\{0,\pm1,\pm z\pm1\}$. All coefficients in the unitary case lie in T: = $S \cup \{\pm z\pm p,\pm(1+zp-1)-1\}$. The set S can be constructed in O(log q), and T can be constructed in O(log2 q).

If $D = (dij)\ n\times n$ is diagonal, we write D = Diag$[d11, d22,..., dnn]$. If $dij = 0$ unless $j = n - i + 1$, we write D = Anti Diag $[d1n, d2(n-1),..., dn1]$. When generated as in Lemma 2.2, Sp(d, q) preserves a form Anti Diag [1,..., 1,−1,...,−1], and GU(d, q) preserves a form Anti Diag [1,..., 1]. For odd q we assume that SO$(2m+1, q)$ preserves a form with matrix $I2m+1$. When q is odd, we assume that SO±$(2m, q)$ preserves an orthogonal form with matrix Diag$[z$, 1,..., 1] or $I2m$, 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(log3 q) algorithm that, with probability of success 1/2, finds $a, b \in$ Fq such that $a2$

$+ b2 = z$.

Proof: Search F $*q$ for an element b such that $z - b2$ 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].

Lemma 2.4: For _ $\in \{+,-, \circ\}$, the groups Ω_(n, q), SO_(n, q), O_(n, q), and GO_(n, q) may be constructed in time $O(n3 \log q + \log 3\ q)$.

Proof: Let $S := \{0, 1, z, v, v\}$, where v_ = F $*q2$. 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 Ω_(n, q), which can be constructed in time $O(n2 \log q)$, given S. Let S_ extend Ω_(n, q) to SO_(n, q), if these groups are not equal. Let Rs be a reflection in a vector of square norm and Rn be a reflection in a vector of nonsquare norm: Rs and Rn can be constructed in time $O(n2 \log q)$.
By [Kleidman and Liebeck 90, Sections 2.6–2.8], we may take S_:= $-I$ if n is even, q is odd, and the discriminant of the form is nonsquare; S_:= $RsRn$ if n is odd or n is even, q is odd, and the discriminant is square; or S_:= Rs 154 Experimental Mathematics, Vol. 13 (2004), No. 2 if n and q are both even. Thus, we construct S_ in time $O(n3 \log q)$.
Let T_ extend SO_(n, q) to O_(n, q), if these groups are not equal. By [Kleidman and Liebeck 90, Sections 2.6–2.8], we may take T_:= Rs if n is even and q is odd, and $T\circ := -I$ if q is odd, in time $O(n2 \log q)$. Let D_ extend O_(n, q) to GO_(n, q). Assume that the quadratic form has matrix Anti Diag [1,..., 1] in type + and either the identity or Diag[z, 1,..., 1] in type −: a matrix conjugating our original group to one preserving this form can be constructed in time $O(n3 \log q)$ [Holt and Roney-Dougal]. Then D_:= zIn if n is odd or q is even. If q is odd, then $D+$:= Diag[z,..., z, 1,..., 1] and $D-$:= Diag[P,..., P] or Diag [Anti Diag [z, 1], P,..., 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:= _a b b $-a$_.

Main Theorem. *Given a set S of generating matrices for G* $\leq$ GL(n, q) *and a set T of generating permutations for H* $\leq$ Sym(d), *a set of generating matrices for G* $\otimes$ *H* $\leq$ GL(nd, q) *can be constructed in time* $O((|S| + |T|)(nd)2 \log q)$.

Proof*:* For each generating matrix $X \in S$, define a matrix Diag[X, In,..., In]. For each $Y \in T$, define an $nd \times nd$ block matrix whose (i, j)th block is In, if Y maps $i \rightarrow j$, and 0 otherwise. The group G _ H is generated by these ($|S| + |T|$) matrices.
Let $G \leq$ GL(n, q) and $H \leq$ GL(m, q). By $G \otimes H$ we mean a group isomorphic to ($G \times H$)/(x, $x-1$): $x \in G \cap H \cap Z$(GL(nm, q))_. 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 F(n)q $\otimes$F(m)q. By HTensWrK, where $H \leq$ GL(n, q) and $K \leq$ Sym(t) is transitive, we mean the subgroup of GL(nt, q) given by ($H \otimes \cdot \cdot \otimes H$): K.

The group *K* permutes the factors in the central product.
Lemma 2.6: *Let G*: = S_ $\leq$ GL(n, q) *and H*:= T _ $\leq$ GL(m, q). *The group G* $\otimes$ *H* $\leq$ GL(mn, q) *can be constructed in* $O((|S| + |T|)(mn)2 \log q)$, *and G*TensWr Sym($t$) *can be constructed in* $O(|S|n2t \log q)$.

Proof: The group $G \otimes H$ is generated by the Kronecker products of elements of S with 1H and of 1G with elements of T. Given $X \leq G$ and $Y \leq H$, the Kronecker product $X \otimes Y$ has $XijYkl$ 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].

References

1. Aschbacher, Aschbacher M. On the Maximal Subgroups of the Finite Classical Groups. Invent. Math 1984;76:469-514.
2. Bosma *et al.* Bosma W, Cannon J, Playoust C. The Magma Algebra System I: The User Language. J Symbolic Comput 1997;24(3):235-265.
3. Butler and Canon 82 Butler G, Canon JJ. Computing in Permutation and Matrix Groups I: Normal Closure, Commutator Subgroups, Series. Math. Comp 1982;39:663-670.
4. Butler 82 Butler G. Computing in Permutation and Matrix Groups II: Backtrack Algorithm. Math. Comp 1982;39:671-680.
5. Butler 83 Butler G. Computing Normalisers in Permutation Groups. J Algorithms 1983;4:163-175.
6. Cannon *et al.* Cannon JJ, Holt DF, Slattery M, Steel AK. Computing Subgroups of Low Index in a Finite Group. Submitted to J Symbolic Comput.
7. Cellar and Leedham-Green 97 Cellar F, Leedham-Green CR. Calculating the Order of an Invertible Matrix. In Groups and Computation II New Brunswick, NJ, edited by L. Finkelstein and WM. Kantor 1995, 55-60. Providence, RI: Amer. Math. Soc., 1997.
8. Eick and H¨ofling 03 Eick B, H¨ofling B. The Solvable Primitive Permutation Groups of Degree at most 6560. LMS J Comput. Math 2003;6:29-39.
9. GAP Group. The GAP Group. GAP–Groups, Algorithms and Programming, Version 4.3. Available from World Wide Web (http://www.gap-system.org) 2002.
10. Roney-Dougal. Conjugacy of Subgroups of the General Linear Group 163 [Glasby and Howlett 97] Glasby SP, Howlett RB. Writing Representations over Minimal Fields. Comm. Algebra 1997;25:1703-1711.
11. Glasby *et al.* Glasby SP, Leedham-Green CR, O'Brien EA. Writing a Representation over a Smaller Field Modulo Scalars. In preparation.
12. Holt 91 Holt DF. The Computation of Normalisers in Permutation Groups. J Symbolic Comput 1991;12:499-516.
13. Holt *et al.* 96a Holt DF, Leedham-Green CR, O'Brien EA, Rees S. Testing Matrix Groups for Primitivity. J Algebra 1996;184:795-817.
14. Holt *et al.* 96b Holt DF, Leedham-Green CR, O'Brien E, Rees S. Computing Matrix Group Decompositions with Respect to a Normal Subgroup. J Algebra 1996;184:818-838.
15. Holt and Rees 94 Holt DF, Rees S. Testing Modules for Irreducibility. J Austral. Math. Soc. Ser A 1994;57:1-16.
16. Holt and Roney-Dougal Holt DF, Roney- Dougal CM. Constructing Maximal Subgroups of Black Box Classical Groups. Submitted.
17. Kleidman and Liebeck 90 Kleidman P, Liebeck M. The Subgroup Structure of the Finite Classical Groups.

Cambridge, UK: Cambridge University Press 1990.

18. Leedham-Green, O'Brien 97a Leedham-Green CR, O'Brien EA. Tensor Products Are Projective Geometries. J Algebra 1997;189:514-528.
19. Leedham-Green, O'Brien 97b Leedham-Green CR, O'Brien EA. Recognising Tensor Products of Matrix Groups. Internat. J Algebra Comput 1997;7:541-559.
20. Leedham-Green, O'Brien 02] Leedham-Green CR, O'Brien EA. Recognising Tensor-Induced Matrix Groups. J Algebra 2002;253:14-30.
21. Leon 97 Leon JS. Partitions, Refinements, and Permutation Group Computation. In Groups and Computation II New Brunswick NJ, edited by L. Finkelstein and WM. Kantor 1995, 123-158. Providence, RI: Amer. Math. Soc., 1997.
22. Lidl, Niederreiter 83 Lidl R, Niederreiter H. Finite Fields, Encyclopedia of Mathematics and Its Applications, 20. Reading, MA: Addison-Wesley 1983.
23. Roney-Dougal, Unger 03 Roney-Dougal CM, Unger WR. The Primitive Affine Groups of Degree Less than 1000. J Symbolic Comput 2003;35:421-439.
24. Rylands, Taylor 98 Rylands LJ, Taylor DE. Matrix Generators for the Orthogonal Groups. J Symbolic Comput 1998;25:351-360.
25. Taylor 87 Taylor DE. Pairs of Generators for Matrix Groups I. The Cayley Bulletin 1987;3:76-85.
26. 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) Received, 2003; accepted February 23, 2004.