

A Non-Constructive Recognition Algorithm for the Special Linear and Other Classical Groups

Frank Celler and C. R. Leedham-Green

ABSTRACT. In the first part of this note we present a Monte Carlo algorithm that decides if a given set of matrices generates a group containing the special linear group. In the second part we give timings and extend the algorithm to the other classical groups.

1. Introduction

Inspired by the Neumann-Praeger algorithm [6] for recognising whether the subgroup of $GL(d, q)$ generated by some finite subset contains $SL(d, q)$, we present our own version.

The two methods are both Monte Carlo algorithms, in that they will either give a positive answer with proof, or a negative answer to a prescribed degree of confidence, subject to the fact that both require a number of random elements of the group, which will in fact be produced by multiplying elements of the given generating set X . Both algorithms use the Aschbacher classification of subgroups of classical groups, see [3], and hence will extend to recognising whether subsets of other classical groups generate the whole group. Our algorithm is easier to generalise to other classical groups, simply because it is by far the more naïve as we only use the orders, the minimal and characteristic polynomials of random elements, while the Neumann-Praeger algorithm tries to find two particular types of elements, which, however, will rule out almost all possible subgroups at once.

We believe, as a result of many experiments, that our algorithm, when given generators for a subgroup G of $GL(d, q)$ will, with probability greater than $1/2$, be able to prove that G contains $SL(d, q)$, if this is indeed the case, by examining at most six random elements of G , for any values of d and q .

We assume throughout that we can construct random elements of G . In practice we use the algorithm described in [2]. After a pre-processing, this algorithm returns pseudo-random elements of G , each requiring a single matrix multiplication.

As the estimate of six elements is purely experimental, a more rigorous approach would be to find generators for the subgroup H of $GL(d, q)$ that contains $SL(d, q)$, and with the same image as G under the determinantal map; that is to say, that if

1991 *Mathematics Subject Classification*. Primary 20G40; Secondary 20-04.

G contains $SL(d, q)$ then it is equal to H . Suppose now that G contains $SL(d, q)$; if we start the algorithm in parallel for G and H and stop as soon as either G or H has been proved to contain $SL(d, q)$ then G and H have an equal chance to win this race because they are equal. If G has been proved to contain $SL(d, q)$ this result is always correct and we can stop. If G is equal to H and the test elements are chosen from G and H in a way that is (in effect) independent of the given set of generators, the probability that H will win in n independent races is 1 in 2^n . Although the above approach guarantees a certain error probability, we have great confidence that our estimate of six tries is very reasonable.

We have successfully run our algorithm in dimensions up to 750. The time for fixed d is approximately proportional to $\log q$. While theoretically the average complexity of our algorithm is slightly worse than $O(d^3 \log q)$ finite field operations, our implementation, in the group-theoretic package `GAP`, takes time that is almost proportional to $d^{2.5}$ for fixed q within this range. When dealing with matrices of larger dimension problems of storage arise which cause discrepancies.

2. Recognising the Special Linear Group

Our main algorithmic tools are a random element generator for G and an implementation of an algorithm that hopes to determine the order of an element of $GL(d, q)$, modulo scalars, in the time that it takes to perform a few multiplications. See [2] and [1] for details.

REMARK. The order algorithm can fail to give a precise answer in case of large orders, because of the problems of factorising large integers, but it always gives enough information to determine whether or not the projective order of the element in question divides a given integer n , and this is all that is required.

The general idea of our algorithm is to construct random elements of $G = \langle X \rangle$, where X is the given generating set, and try to exclude the possibility that the elements constructed to date could lie in any of the subgroups of $GL(d, q)$ of Aschbacher's list not containing $SL(d, q)$. If the given elements do not lie in any of these groups, we have a positive answer, if not, a negative conjecture.

Given random elements of G or using [2] the average complexity of our algorithm is thus $O(d^3 \log q \log \log q^d)$ finite field operations, as this is the complexity of our algorithm for computing the order of an element of $GL(d, q)$, and this is the slowest component of our algorithm. We assume here our unproved conjecture that a fixed number of trials, independent of d and q , will suffice.

The tests we use give necessary (and often sufficient) conditions for an element not to be conjugate in $GL(d, q)$ to an element of the group, or class of groups, that we are trying to exclude. We have not tried to make these tests as tight as possible in cases that are easily excluded.

Suppose then that we have found a set $\{g_i\}$ of elements of G where g_i has order n_i modulo scalars, characteristic polynomial $f_i(x)$, and the degrees of the irreducible factors of $f_i(x)$ form a partition P_i of d . Let S_k denote the symmetric group of degree k , and $\exp(H)$ the exponent of a group H .

Aschbacher's theorem states that any subgroup of $GL(d, q)$ that does not contain $SL(d, q)$ is congruent, modulo scalars, to a group in the following list. For each group, or class of groups, we give the test used to prove that $\langle X \rangle$ does not lie in such a group.

1. *Reducible groups.* G is irreducible if there is no partition P of d into more than one part to which each P_i is subordinate; that is to say, it is impossible to define an equivalence relation on the parts of each P_i in such a way that, for each i , the parts of P are the unions of the parts in the various equivalence classes of P_i .
2. *Imprimitive groups.* G is primitive if it is irreducible, and for every divisor e of d where $e < d$, for some i ,

$$n_i / \gcd(n_i, \exp(\mathrm{PGL}(e, q)))$$

is not the order of some element of $S_{d/e}$.

3. *Tensor products.* The natural module V for G is not a non-trivial tensor product if for every divisor e of d , with $1 < e < d$, some n_i does not divide

$$\mathrm{lcm}(\exp(\mathrm{PGL}(e, q)), \exp(\mathrm{PGL}(d/e, q))).$$

4. *Tensor induced groups.* The natural module V for G is not contained in a non-trivial tensor power, extended by a group that permutes the tensor factors, if whenever $d = e^k$, with $k > 1$, for some i ,

$$n_i / \gcd(n_i, \exp(\mathrm{PGL}(e, q)))$$

is not the order of some element of S_k .

5. *Groups defined, modulo scalars, over smaller fields.* G does not belong to this category if, for some i , and for each $\zeta \in F_q^*$, $f_i(\zeta x)$ has its coefficients in no proper subfield of F_q . To check this possibility, it is not necessary to quantify over the elements of F_q^* . For details, see section 6 of [6].
6. *Groups defined in smaller degree over larger fields.* More precisely, the natural module V is isomorphic to a module of smaller dimension on which an extension field of F_q acts semi-linearly. G does not lie in this category if, for every divisor e of d with $e < d$, some n_i does not divide

$$\exp(\mathrm{PGL}(e, q^{d/e})).$$

7. *Classical groups in their natural representations.* If G is orthogonal or symplectic, then $f_i(x) = \pm x^d f(x^{-1})$. If it is unitary then $f_i(x) = c^{-1} x^d f_i^*(x^{-1})$, where $c = \det(g_i) = f_i(0)$. Since we need to test whether or not our group lies in one of these groups modulo scalars, it is necessary to check that $f_i(\zeta x)$ does not satisfy these conditions for each $\zeta \in F_q^*$. It is trivial to check this condition without quantifying over ζ , see section 3.
8. *Extensions of an r -group.* $d = r^m$ for some prime r and G is an extension of a symplectic r -group by $Sp(m, r)$, modulo scalars. Since a symplectic r -group has exponent dividing r^2 , this case is excluded if some n_i does not divide

$$r^2 \times \exp(\mathrm{Sp}(m, r)).$$

9. *Central extensions of almost simple groups.* The almost simple groups that could arise, and are not amongst those already described, have order less than q^{3d} by [5], and of course their order must divide that of $GL(d, q)$. If they are Chevalley groups defined in a different characteristic from that of q , then the lower bounds of Landazuri/Seitz/Zaleskii, see [4] and [8], for non-trivial representations of Chevalley groups in unnatural characteristics reduce the number of cases to be considered to an easily manageable set.

Having made a list of the possible almost simple groups that might arise, we then try to eliminate them by testing whether or not n_i divides their order. In fact we can do better for classical groups, as their exponents are easily calculated (or at least the ℓ -primary part of the exponent, where ℓ is the prime over which they are defined), and better still in the sporadic and alternating cases, where the possible orders of elements are known.

REMARK. Problems arise in very large cases. We have already mentioned the fact that precise projective orders may no longer be available, and how to deal with this. Another problem with large cases is that it takes a rather long time to determine whether or not the order of the various Chevalley groups divides the order of $GL(d, q)$. Our answer to this is to omit this test in large cases. We expect to eliminate such groups with one test element since most elements of $GL(d, q)$ will have very large order, and it is faster to check that the order n of the Chevalley group is not a multiple of the order of the element than to decide whether n divides the order of the general linear group in question.

3. The Other Classical Groups

Other classical groups are dealt with similarly. We first run the given generators through the above algorithm for the special linear group, retaining the information obtained. If G is some other classical group in its natural representation, we will be given very strong evidence that it does at least preserve a bilinear or sesquilinear form, up to scalars and acts absolutely irreducibly on V .

We check this by looking for a suitable module isomorphism between V and its dual V^* , again up to scalars, using the following trick. If g has minimal polynomial $\sum_{i=0}^r m_i x^i$, and fixes a symplectic or orthogonal form modulo scalars, then there exists an element ζ_g of F_q such that $(\zeta_g^2)^i = m_{r-i}/(m_0 m_i)$ for all i with $m_i \neq 0$, and $g \cdot \zeta_g^{-1}$ fixes the form. We therefore look for elements g such that $\gcd\{i \mid m_i \neq 0\}$ is 1, allowing us to compute ζ_g^2 from $\{m_{r-i}/(m_0 m_i) \mid m_i \neq 0\}$.

Given ζ_g^2 , $g\zeta_g^{-1}$ is determined up to multiplication by $-I$, this sign will be irrelevant. Having obtained a number of elements of the form $g\zeta_g^{-1}$, we construct random elements in the algebra they generate, looking for an element of nullity one. If we can find no such element g , or no element of nullity one in the algebra generated by the $g\zeta_g^{-1}$, we give up, assuming that G is not a classical group modulo scalars. Having found an element with nullity one we use Norton's irreducibility test to decide whether the group generated by the $g\zeta_g^{-1}$ acts indeed absolutely irreducibly, see [7]. If it does, we look for an isomorphism between V and V^* . It is easy to check if such an isomorphism gives a symplectic or orthogonal form fixed by G modulo scalars. The unitary cases can be handled similarly.

If $p = 2$ in the orthogonal case, we need to decide whether G also preserves a quadratic form Q , and if so to find it. Q is determined by the symmetric form and the images $Q(b_i)$ of a basis $\{b_i\}$ of V . The conditions $Q(b_i \cdot g) = \zeta_g^2 Q(b_i)$ for all $g \in X$ and i describe a system of linear equations; a quadratic form is fixed by G modulo scalars if a solution exists.

After we have found a suitable form, using the above algorithm, we have already ruled out cases 1, 6 and proper subgroups satisfying 7. The reason that case 1 is ruled out is that we found a subgroup acting irreducibly. The reason that case 6 is ruled out is that, since we only use elements g with minimal polynomial $\sum_{i=0}^r m_i x^i$, with $\gcd\{i \mid m_i \neq 0\} = 1$, in case 6 such an element would lie in a copy of $GL(e, q^{d/e})$

rather than $\Gamma L(e, q^{d/e})$, and hence we would be looking at elements of a sub-algebra of $F_q G$ that only has elements with nullity a multiple of d/e .

Now Aschbacher's theorem applies not only to subgroups of the special linear group, but also to subgroups of the other classical groups, though with certain natural changes. For example, in the imprimitive case there are either only two blocks or the action of the normaliser of a block must belong (modulo scalars) to the same classical type. It may be that the Aschbacher categories other than the classical group in question have already been ruled out. If not, we expect in general to be able to rule them out by the fact that many of the Aschbacher categories now correspond to smaller groups. If necessary, we can try more random elements of G in an attempt to rule out the remaining possibilities.

If we can prove that G does contain a classical group, it remains to check a number of details to determine G . It is easy to determine the scalars in G but not in the classical group by considering the action of G on the form in question. It is again a triviality to check the determinant of the given generators, and hence determine the image of G under the determinantal map. In the case of an orthogonal group in characteristic two, we need also to determine the image of the generators under the spinor norm. This we do by using the discriminants of the corresponding Wall forms of the generators, see [9] page 163. The type of the orthogonal group (O^+ or O^-) can be checked by choosing a basis consisting of hyperbolic pairs $\{e_i, f_i\}$ for the symmetric form and examining the quadratic form restricted to $\langle e_i, f_i \rangle$. If we get an odd number of types “-”, the whole group is of type “-”. Thus in all cases we can determine G precisely.

4. Small Cases

We assume that $d \geq 2, 3, 4, 7$ in the linear, unitary, symplectic, or orthogonal case, respectively. We don't deal with various isomorphisms of $O_d(q)$ for $d \leq 6$ and cannot rule out the possibility of $O_7(q)$ embedded as irreducible subgroup of $O_8^+(q)$.

There are various small cases, typically when $d = 2$ and $d = 3$, when the above tests are inadequate; for example some soluble classical groups arise, which have to be eliminated by methods other than consideration of minimal polynomials. Also, we may have to use the fact that some simple group is not involved in $GL(d, q)$, because our general criteria are not strong enough to rule this out. These exceptions are very easy to deal with. However, we have to recognise $Sp(4, 2)$ by computing a permutation representation and then using the Schreier-Sims algorithm.

5. Timings

We have implemented the algorithm in GAP, and have tested it thoroughly. In fact, the efficacy of the algorithm is assured by experiment rather than theory. The run time does indeed prove to be proportional to $\log q$, as expected, and the dependence on d is in practice better than expected within the range of applicability, as mentioned above.

The following timings were obtained running the program on an Intel Pentium P5, 90 Mhz, running FreeBSD 2.0.5.

The first table gives times to recognise the general linear group in the given dimensions. The timings are the average of ten runs. In this table the first row gives the dimension, the second row gives the run time in seconds, the third row

gives the maximal number of test elements required in one run, and the fourth row gives the average number of test elements required to prove that the given groups are indeed $GL(d, q)$. In all cases in these tables, $q = 7$.

RECOGNISING $GL(d, q)$

	$GL(14, 7)$	$GL(21, 7)$	$GL(50, 7)$	$GL(154, 7)$
d	14	21	50	154
sec	0.7	0.9	7.2	156
max	8	7	15	13
avg	5	3.4	5.3	5

In the second table we consider groups not containing $SL(d, q)$ acting irreducibly on V . We race the given groups five times against the corresponding groups between $SL(d, q)$ and $GL(d, q)$ giving an error probability of 3% as described in section 1. The columns are indexed by the groups. The first row gives the dimensions of the representations, the second row the total run time for the 5 races in seconds.

RACE AGAINST SL

	$L(2, 13)$	M_{22}	$He.2$	M_{22}
d	14	21	50	154
sec	8.6	10.6	66	1136

If the given set does not generate $SL(d, q)$ it is necessary to continue testing some ten or twenty times as many elements, depending on the confidence required; however, this extra time is offset to some degree by having to deal in general with smaller group element orders in which case the order algorithm runs faster. Therefore the run times of the second table are slightly better than ten times the run times of the first table. In a “typical” run for M_{22} in dimension 154, about 70% of the time is spent calculating and factorising the minimal polynomials $m(x)$ and characteristic polynomials, and less than 1% is used computing the orders of x modulo $m(x)$. On the other hand, in a “typical” run for $GL(154, 7)$ about 15% of the time is used computing the minimal polynomials and about 80% is spent computing the orders.

Finding a form and recognising $SU(50, 7) < GL(50, 49)$, $SP(50, 7) < GL(50, 7)$, and $O^+(50, 7) < GL(50, 7)$ took 28, 17, and 18 seconds, respectively. Again this an average of ten runs. As a larger example, we applied the algorithm to $GL(750, 2)$, and the answer was returned after 20 minutes. Of course the time may vary quite considerably from one try to another because of the random nature of the algorithm.

We are grateful to P. Cameron, S. Donkin, R. Parker and L. H. Soicher for helpful conversations.

References

- [1] Frank Celler and C. R. Leedham-Green, *Calculating the Order of an Invertible Matrix*, To appear in the DIMACS proceedings.

- [2] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and E. A. O'Brien, *Generating random elements of a finite group*, *Comm. Algebra* **23** (1995), 4931–4948.
- [3] Peter Kleidman and Martin Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series **129** (1990), Cambridge University Press.
- [4] V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, *J. Algebra* **32** (1984), 418–443.
- [5] M. W. Liebeck, *On the orders of maximal subgroups of the finite classical groups*, *Proc. London Math. Soc.* (3) **50** (1985), 426–446.
- [6] Peter M. Neumann and Cheryl E. Praeger, *A Recognition Algorithm for Special Linear Groups*, *Proc. London Math. Soc.* (3) **65** (1992), 555–603.
- [7] R. A. Parker, *The Computer Calculation of Modular Characters (The Meat-Axe)*, *Computational Group Theory* (Michael D. Atkinson, ed.), Academic Press, London, 1984, pp. 267–274.
- [8] Gary M. Seitz and Alexander E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley groups. II.*, *J. Algebra* **158** (1993), 233–243.
- [9] Donald E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

LEHRSTUHL D FÜR MATHEMATIK, RWTH-AACHEN, 52062 AACHEN, GERMANY
E-mail address: Frank.Celler@Math.RWTH-Aachen.DE

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY AND WESTFIELD COLLEGE, UNIVERSITY OF LONDON, MILE END ROAD, LONDON E1 4NS, GREAT BRITAIN