Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Study the Domains of Infinite Algorithms of Calculation of Nilpotent Matrix Groups

Amarendra Kumar Pattanayak and Dr. Arihant Jain

Department of Mathematics, Dr. A. P. J. Abdul Kalam University, Indore (M.P.), India
Corresponding Author Email: amarpattanayak1@gmail.com

Article Info
Page Number:9082 - 9090
Publication Issue:
Vol 71 No. 4 (2022)

Article History
ArticleReceived*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Abstract
We design algorithms for nilpotent groups using the methods we describe for computing with matrix groups defined over a variety of infinite domains. In particular, we present an efficient approach for checking the nilpotency of matrix groups over an infinite field. For a given nilpotent matrix group, we also propose techniques that resolve a number of related structural concerns.

Keywords: Nilpotent, Algorthim, Matrix Group, Homomorphism,IsFinite

1. Introduction

In a very new and underdeveloped area of computational group theory, computing with matrix groups over infinite fields presents quite different obstacles than those encountered when computing with groups over finite fields. [1] One reason is that some classes of matrix groups over infinite fields make it impossible to solve even the most fundamental computational tasks, such as membership checking and the conjugacy problem. Matrix entry growth is one example of the kind of serious complexity problem that can occur. For any category of groups, finiteness proofs are a fundamental computational problem. As a matter of course, it's possible that finiteness can't be decided in general. For matrix groups, though, things seem better. Keep in mind that the integral domain R F generated by the entries of the elements of S .S_1 is the definition space for a matrix group given by a finite set S of generators over a field F. For this reason, it is sufficient to build algorithms just for the fields

$$F = P(X_1, \ldots, X_m),$$

where Xi are independent indeterminates, m = 0, and P is either a number field or a finite field.

Both deterministic and random techniques have been devised by different authors to determine whether or not a given matrix group over Q is finite. [3] Finiteness testing over any number field is now possible with the use of these techniques and a standard reduction derived by modelling algebraic numbers as matrices over Q. However, this strategy can only go so far because increasing the matrix degree is a time-consuming and resource-intensive process. For deciding finiteness, groups over functional fields are studied. The importance of computation in matrix algebras is a recurring issue in these articles. Algorithms in polynomial time have been presented in both zero

and positive characteristics, although their usefulness is constrained. Not only are there no public implementations, but there are none available either. A method for determining whether or not a set is finite differs fundamentally from previous approaches by shifting the ground domain using congruence homomorphism.

This method is generic and applicable across all domains, with the same implementation. In, the method was applied to the problem of determining whether or not a given matrix group is nilpotent. [2] The 'Nilmat' GAP package contains an implementation of algorithms from The effectiveness of the Nilmat algorithms in testing the finiteness of nilpotent matrix groups over Q at very large degrees, where other known techniques fail, has been demonstrated experimentally. This research utilises the method to create workable methods for determining the finiteness of matrix groups over functional fields. Actually, we take on a more general task, which is to determine whether or not a given group G is finite, and if it is, then compute |G| (because computing orders is a fundamental computational problem). Our focus is on the special case of zero characteristics, but we also provide brief descriptions of related ideas for positive characteristics. Our core approach is now available in GAP for functional fields over Q. As shown by J.S. Milne (2020), Galois' qualification between groups simples and groups créatifs as the main polarity in the theory of change groups was lauded by Camille Jordan in the preface to his Traité, as shown by J.S. Milne (2020). As well, Jordan began building a database of restricted straightforward groups in the Traite, including the rotating groups of at least 5 degrees and a sizable chunk of the conventional projective direct groups over fields of prime cardinality. Ludwig Sylow eventually disseminated his widely held speculations on classes of prime-force requesting subgroups in. Barring the invention of a fundamentally new way to rank groups, there can be no straightforward reason why an arrangement is doable. At least with current methods for order by centralizers of involutions, one concern is that each basic group must be tested to see if it prompts additional simple groups containing it in the centralizer. For instance, the infant beast had a double coat when it was discovered, suggesting it could have been the centralizer of an involution inside a larger, more straightforward group. However, there appears to be no unquestionable purpose behind why one can't have an endless chain of bigger and bigger irregular groups, each of which has a twofold cover that is a centralizer of an involution in the following one, if one doesn't check each restricted fundamental gathering. Due to this problem (and others), it was unclear until very late in the process whether there would be a finite or infinite number of inconsistent groups. [5]

2. Changing the Ground Domain Via Congruence Homomorphism

Lemma

So, we'll say that is a unique factorization domain, q is irreducible, and is the primary ideal q of Let's pretend that the torsion elements of G(n, Δ, ϱ) aren't all zero.

If Z is a set, then there exists a prime p such that p .

To put it another way, pb = $\sum_{i=2}^{p} \left(\frac{p}{i}\right) q^{i-1} b^{i}$. For some b ∈Mat(n, Δ); and

each torsional component of G(n, Δ, ϱ) has a p-power order.[4]

Proof:

h ∈$\mathcal{G}\varrho$ have prime order p.

We get h = 1_n + qbfor some b ∈Mat(n, Δ).

Then$1_n = h^p = 1_n + pqb + \cdots .. + \left(\frac{p}{i}\right)\mathcal{G}^i b^i + \cdots . + q^p b^p$

The binomial coefficients are interpreted modulo char.[7]

Hence

$$pb = -\sum_{i=2}^{p} (\frac{p}{i})\, q^{i-1} b^i$$

Thus, either q divides p or q divides each element of b. Hypothetically, let's say q doesn't split p. As a result, α ≥ 1, $q^{\alpha}$for some positive integer 1, q divides each element of b, while $q^{\alpha+1}$does not. However, (1) implies that $q^{2\alpha+1}$divides pb, which is obviously false. That's why q is a divisor of p. $\mathcal{G}\varrho$ has an element of prime order r ≠ p if and only if it contains a non-trivial element of p-order. Therefore, 1 = px + ryfor some x, y ∈ Zis divisible by q since q divides both p and r. Each $\mathcal{G}\varrho$ torsion element must be a p-element since q cannot be a unit.

Proposition.

In the same way Δ, q ,ϱ as in Lemma, we write[8]

$\mathcal{G}$ (n, Δ, ϱ) torsion elements are all t-elements if and only if char Δ = t > 0

(ii) For any prime p Z, let's assume that char = 0 and that neither q nor q 2 divides p. Therefore, G(n, Δ , ϱ) is not twisted.

Proof.

If $\mathcal{G}\varrho$ has non-trivial torsion, for some primes p and r ∈ Δ that are not divisible by q, p = qrholds.[6]

(ii) For some b, c ∈Mat(n, Δ) We have b, c ∈ Mat(n, Δ). As a result, for some α ≥ 1, q^{α}divides each and every entry in b, while q +1 does not. Since q does not divide r, the contradiction in rb = qb^2 c is that $q^{2\alpha+1}$divides each element of b.

3. Methods of Calculation Using Groups of Nonnegative Potential Matrix Elements

Nilpotent linear groups can be divided.

In linear group theory, we frequently apply this technique of reducing to the simplest possible case. Nilpotent linear groups have an easier time with this reduction than arbitrary linear groups do. In this section, we will think about a computational method for accomplishing the reduction.[9]

Lemma

If and only if $[G_u, G_s] = 1$, then G is nilpotent because G_u and G_s are both nilpotent.

$G \leq G^* = G_u \times G_s$ .if and only if G is nilpotent.

Proof.

The homomorphisms $g \mapsto g_u$ and $g \mapsto g_s$ are defined by the assignments $G \to G_u$ and $G \to G_s$respectively, and $G^* = G_u \times G_s$.holds if and only if G is nilpotent. Contrarily, if both G_u and G_s are nilpotent and $[G_u, G_s] = 1$, then both G* and $G \leq G^*$ are nilpotent as well.

Deciding finiteness.

After verifying that $G \leq GL(n, F)$, is nilpotent, we can move on to more elementary computational issues for G, such as checking whether G is finite. [12]Various writers have addressed how to decide whether or not a matrix group over an algebraic number field or a functional field is finite, and Beals has published a practical implementation of this idea in GAP for groups over Q. In this section, we offer a ground-field-independent, generalised method for determining finiteness.

Theorem (Selberg–Wehrfritz)

Each finitely generated linear group G has a normal subgroup N with a finite index and finite order elements that are all unipotent.[10]

In particular, G is (torsion-free) by-finite if and only if the character F equals zero.

For the maximum in R, we refer $\varphi\rho$ to it as a SW-homomorphism if and only if N is a congruence subgroup G_ρ.

The value N as a G_ρ is not produced in the proof of the Selberg-Wehrfritz theorem.

IsFinite(S)

The input will be a finite subset S of GL(n,R) , R is a character vector with the least significant$R = p \geq 0$.

The output will be true if and only if $G = \langle S \rangle$ is finite, and false otherwise.

SW-homomorphism $\varphi_\rho$and compute $\varphi_\rho(G) \leq GL(n, q)$, $|R/\rho| = q$.

N:=NormalGenerators(S, φ_ρ).

When $p = 0$ and $N = \{1_n\}$,

If either $p > 0$ or $\langle N \rangle^G$is unipotent, return true; otherwise, return false.[11]

Setting virtual property standards

An SF linear group has a unipotent-by-abelian (i.e., triangularizable) normal subgroup of finite index. This subgroup is used to figure out the Tits class of G, or to see if G is almost solvable (solvable-by-finite, SF).

The Tits theorem states that if G is not SF, then it must contain a non-abelian free subgroup F. However, our approach does not generate such a subgroup.[14]

Our method is novel in that it is consistent and applicable to any F.

Using Wehrfritz's requirements, if G is SF, then G is unipotent-by-abelian

Theorem

Allow G to be solvable-by-finite in $G \leq GL(n, R)$ and let it be an ideal in R.

If and only if G_ρ is abelian unipotent,

This means that R has a prime characteristic larger than n, or

If R is a Dedekind domain with zero characteristics, then is a maximal ideal of R, then $\text{char}(R/\rho) = p > 2$, and $\rho \notin p^{p-1}$

There is a Zariski connection to G. In.

$G_\rho$is unipotent-by-abelian for SF if and only if it is an ideal of R such that it is.

We say that it isφ_ρ a W-homomorphism if and only if $G \leq GL(n, R)$,

W-homomorphisms, like SW-homomorphisms, can be built for any fundamental type F, just like SW-homomorphisms.

IsSolvableByFinite(S)

Finite $S \subseteq GL(n, R)$. as input

If $G = \langle S \rangle$ is solvable by finiteness, then true is returned; otherwise, false is returned.

Select $\rho \subseteq R$ that is $\varphi\rho$ a W-homomorphism and compute $\varphi\rho(G)$.[13]

N:=NormalGenerators(S, $\varphi\rho$).

Finally, if $\langle N\rangle^G$is unipotent by abelian, then 3 should be returned; otherwise, false should be returned.

Multiple cycles in one presentation.

The (consistent) presentation of a finitely produced nilpotent group is polycyclic since it is polycyclic. Gaining access to the many pre-existing algorithms for abstract polycyclic groups is one advantage of having a polycyclic presentation for a nilpotent subgroup G of GL(n, F).[15]

Let G be a subgroup of GL(n, F) that is created finitely, with F assumed to be perfect for the sake of brevity. Either G_u is not nilpotent or $G \leq \langle G_u, G_s\rangle$after applying Reduction(G). It is true that $[G_u, G_s] = 1$, as G_u is unipotent. The latter case features G_u and Gs presentations with many rings. It is important to remember that the finitely produced nilpotent group $G_u \leq UT(n, F)$ is unquestionably polycyclic if we continue on from Reduction(G).

Presentation Nilpotent(G)

Return false if Reduction (G) is not true; otherwise, proceed to step (2).[18]

Find a polycyclic presentation of G_u that is a subgroup of UT(n, R), where R is a subring of F.

In order to generate a polycyclic representation of $\psi\varrho(G_s)$, one must first compute a generating set for $\psi\varrho\ (G_s)$.. It should return false if the attempt fails.

Find the generating set of $(G_s)\varrho$. If $(G_s)\varrho$ is not a pivotal part of Gs, then false is returned. Or, you may make a polycyclic representation of the finitely generated abelian group $(G_s)\varrho$.

Combine the presentations of $\psi\varrho(G_s)$ and $(G_s)\varrho$ found in Methods 3 and 4 to create a polycyclic presentation of G_s.

Merge the G_u Presentation from Step Two with the G_s Presentation from Step Five to obtain the polycyclic presentation of$G* = G_uG_s$.

4. Adjoint Representation for Testing Nipotent With an Abelian Series

Techniques based on the properties of nilpotent linear groups for determining whether or not a matrix group is nilpotent These methods were first developed for groups over finite fields, but they can be used with groups over any field.[16]

Lemma

Non-trivial torsion for C_l is a property of G if and only if it is not nilpotent in the abelian group.

Proof.

In this scenario, it is assumed that C_1 does not undergo any torsion. Assume you have $a \in Z_2(G) \setminus Z(G)$. Given that there exists a $^m \in Z(G)$ such that $[g, a] \in Z(G)$ has finite non-trivial order, then a m $Z(G)$ for some m (dividing m). Thus, this goes against $[g, a] \in A1 \leq Cl$.

For the sake of argument, let's say G is finite. At that point, we'll be ready to submit an application to G. This is done by first factorising the cyclic quotients of the refined series into primes and then verifying that the factors of various primes commute in order to determine whether or not G is nilpotent. As a result, G's nilpotency can be checked using the algorithm IsNilpotent from. In the more generic context, we refer to this algorithm as being finitely nilpotent. However, the Sylow decomposition of nilpotent G can also be obtained using this approach, which takes just finite $G \leq GL(n, F)$ as input. estimating whether or not something is finite, infinite, or nilpotent.

Nilpotency testing via change of ground domain and abelian series.

Lastly, we show how to combine our methods in the easiest and most useful way to find out if a finitely produced matrix group over a perfect field F is nilpotent or not.[17]

The algorithm.

Using Reduction(G) (if F is perfect) and applying a congruence homomorphism to Gs, where satisfied, IsNilpotentMatGroup checks for nilpotency over an infinite field F. To determine whether or not m to Gs is satisfied, an abelian sequence of GL nilpotent groups is used, and IsNilpotentMatGroup checks for nilpotency over an infinite field F.To determine whether G_s is nilpotent$\psi\varrho$(Gs) an abelian sequence of $\psi\varrho$ (Gs) in GL(n, q)used.This hypothesis can be investigated because $(Gs)\varrho \leq Z(Gs)$, is a testable conjecture if G is nilpotent.

The IsNilpotentMatGroup methodology has various benefits. First, we want to avoid potential problems that arise while calculating over infinite fields by minimising the amount of computation over the original field F (e.g., a blow-up in the size of matrix entries). In addition, there is a problem with tight upper bounds on the nilpotency class. TestSeries techniques that depend on a class bound for the possibly nilpotent group $\psi\varrho(G)$, to end quickly will end faster if G is nilpotent than if G were a randomly chosen subgroup of GL (n, q).[15]

Lemma

If Gs is nilpotent and p > n, then any $(\psi\varrho (G_s))$upreimage in G_s is centred.

Proof.

Put $g \in G_s$ .Then, for some $\psi\varrho (g)_u = \psi\varrho (g^{1})$and for some $\psi\varrho (g^{lp^k}) = 1$ i.e.,

$g^{lp^k} \in (Gs)\varrho \leq Z(Gs)$. $g^{1} \in Z(Gs)$. is a corollary of the previous statement . $\psi\varrho(Gs)$ suggests that, if is selected so that p > n, we can anticipate (G_s) to be totally reducible. Of course, if n is huge, it is better to work with $p \leq n$.[19]

5. Conclusions

In addition to these primary functions, 'Nilmat' also has tools for determining whether or not a group is finite, computing the order of a finite nilpotent group, locating the Sylow system of a nilpotent group over a finite field, and determining whether or not the group is totally reducible. Nilmat also includes a collection of primitive groups that are nilpotent over finite fields. [20]Because of the significance of nilpotency in group theory, checking for it is a fundamental feature of any computational group theory system. Here, we offer the first general and efficient method for working with infinite nilpotent matrix groups in computation. Some of the nilpotency testing methods in GAP and MAGMA fail to decide nilpotency even for tiny finite matrix groups, and they fail for practically all infinite matrix groups.[7] To address this issue, we have implemented our algorithms as part of the GAP package 'Nilmat' across finite fields and Q. Since then, we have achieved significant advancements, especially concerning finite solvable groups.

References

1. S. Detinko, “On deciding finiteness for matrix groups over fields of positive characteristic”, LMS J. Comput. Math. Vol 4 , issue (1), page 64–72,2001
2. D. Laksov, “Diagonalization of matrices over rings,” Journal of Algebra, vol. 376, issue (1), page 123–138, 2013
3. H.-J. Bartels and D. A. Malinin, “Finite Galois stable subgroups of GLn,” in Noncommutative Algebra and Geometry”, Pure and Applied Mathematics, vol. 243 issue (1), page 1–22, 2006.
4. H.-J. Bartels and D. A. Malinin, “On finite Galois stable subgroups of GLn in some relative extensions of number fields,” Journal of Algebra and its Applications, vol. 8, issue (4), Page 493–503, 2009.
5. J.S. Milne “Group theory”,Journal of Algebra and its Applications,,2020
6. D. A. Malinin, “Galois stability for integral representations of finite groups,” Journal of Algebra and its Applications vol. 12,Issue (3), Page 106–145, 2000
7. P. H. Tiep and A. E. Zalesskii, “Some aspects of finite linear groups: a survey,” Journal of Mathematical Sciences, vol. 100, issue (1), page 1893–1914, 2000.
8. Beals, R., ‘Towards polynomial time algorithms for matrix groups’, DIMACS II, Series in Discrete Mathematics and Theoretical Computer Science ,Vol 12, issue (1), page 31–54,1997.
9. Beals, R., “Algorithms for matrix groups and the Tits alternative”, J. Comput. System Set Vol58 ,issue (1), page (1999) 260–279.
10. Detinko, A. S. and Flannery, D. L., “Classification of nilpotent primitive linear groups over finite fields”, Glasgow Math. J. Vol 46, issue (1), Page 585–594,2004
11. Detinko, A. S. and Flannery, D. L., “Nilpotent primitive linear groups over finite fields”, Comm. Algebra Vol 33 ,issue (1), Page 1–9,2005.
12. D. L. Flannery, “Computing with matrix groups over infinite field”s, London Math. Soc. Lecture Note Ser. Vol 387 ,issue (1), Page 256–270,2011.
13. E. H. Lo and G. Ostheimer, “A practical algorithm for finding matrix representations for polycyclic groups”, J. Symbolic Comput. Vol 28 , Issue(3), Page 339–360,1999.
14. B. Souvignier. “Decomposing homogeneous modules of finite groups in characteristic zero”. J. Algebra, Vol 322, issue (3), Page 948–956, 2009.

15. D. A. Suprunenko. “Matrix groups. American Mathematical Society, Translated from the Russian, Translation edited by K. A. Hirsch, Translations of Mathematical Monographs”, Vol. 45.issue (1), 1976
16. B. Assmann and B. Eick. “Computing polycyclic presentations for polycyclic rational matrix groups”. J. Symbolic Comput., Vol 40, issue (6), Page 1269–1284, 2005.
17. A. S. Detinko and D. L. Flannery. “On deciding finiteness of matrix groups”. J. Symbolic Comput., Vol 44, issue (8), Page 1037–1043, 2009.
18. W. Eberly. “Decomposition of algebras over finite fields and number fields”. Comput. Complexity, Vol 1, Issue (2), Page 183–210, 1991.
19. S. P. Glasby. “The Meat-Axe and f-cyclic matrices”. J. Algebra, Vol 300, Issue (1), Page 77–90, 2006.
20. B. Assmann, “Polycyclic presentations for matrix groups, Diplomarbeit, TechnischeUniversiy at Braunschweig”, 2003.
21. G. Ostheimer, “A practical algorithm for finding matrix representations for polycyclic groups”, J. Symbolic Comput. Vol 28, issue (3), Page 339–36,1999